Hasse-Weil Zeta Functions for Linear Algebraic Groups

by

S M Turner

A thesis submitted to
the Faculty of Science
at the University of Glasgow
for the degree of
Doctor of Philosophy

October 1996

Summary

The aim of the project was to study two questions [unpublished] of R.W.K. Odoni, to discuss which we introduce the following terminology and notation.

Let G be a linear algebraic group defined over an algebraic number field K. We will say that G *has property (Z)* if there exists a finite Galois extension l of K such that the Hasse-Weil zeta function $\zeta(G, K, s)$ of G is an alternating product of Artin L-functions for characters of $Gal(l/K)$.

Odoni's questions can then be formulated as follows.

(Q1) *Which G have property (Z) (and for which Galois extensions l of K)?*

(Q2) *For which G does $\zeta(G, K, s)$ have a functional equation?*

While neither question was settled completely, the following progress was made.

Main Result

(A) If G is connected and solvable, it has property (Z) [6.2.2.1].

(B) For each K-group G, there is a finite extension M of K such that the M-group G has property (Z) with $Gal(l/M)$ trivial, and $\zeta(G, M, s)$ has a functional equation [6.3].

(C) If every connected almost K-simple K-group had property (Z), then all connected K-groups would too [6.2.2.1]. Among the former, those for which the Dynkin diagram has at most two components all have property (Z) [7.1.0.1].

(D) In particular, every almost simple K-group J has property (Z). Further, $\zeta(J, f, s)$ has a functional equation for an extension f of K of degree at most 2 [6.4].

In all cases, *explicit* expressions are given or can be easily reconstructed. Part (A) has almost certainly been known for a long time, though no statement of it was found.

That there should seem to be so little in the literature about zeta functions for algebraic groups is quite surprising. The case in which G is a torus is dealt with in [Se59]; the connected solvable case (A) follows readily from this.

In chapter (1) the necessary absolute algebraic geometry is introduced, until a definition of the notion of complete variety can be given [1.12]. In chapter (2), an account of the relative theory appears. While all of this material has been known for a long time, there is a paucity of convenient reference. The points of view of topology and algebra (especially Galois theory) are considered. The Weil restriction functor [2.8] is a key concept.

Chapter (3) is an exposition of the standard theory of (linear) algebraic groups as far as that of connected groups [3.4]. In chapter (4) is expounded the theory of root systems [4.1] and that of connected reductive groups. Rationality questions are then treated, especially for connected semisimple groups.

In chapter (5) will be found a resumé of the algebraic number theory [5.1] and notions of zeta function [5.2] required. The heart of the chapter [5.3] is the notion of reduction (of a variety) modulo a prime ideal. In [5.4] will be found some results relating to preservation of properties under reduction modulo a prime. In the cases of some of these properties, an assertion of the result (though not a proof) was found in the literature. In other cases the result may be new.

In chapters (6) and (7) the results announced above are obtained. In (6) will be found the proofs of parts (A), (B) and (D). The proof of (C) is deferred to (7) to avoid a very long chapter (6) which there seems no natural place to break.

I would like to thank my supervisor, Professor R.W.K. Odoni, for his suggestion of and interest in the topic, the Department of Mathematics at the University of Glasgow for its help and the use of its facilities, and the University of Glasgow itself for financial support.

Contents

Chapter 1

Background from Algebraic Geometry

We start with enough algebraic geometry to enable definition of affine and complete varieties. The treatment here follows [Bor91] and [Hu75] quite closely.

All rings are associative and commutative; their modules and mutual morphisms thereof are also assumed unital. A ring will be called *entire* if it is also an integral domain - this seems to be a coinage of Serge Lang.

We begin with a review of the absolute case. Let $\mathbb{E}$ be an algebraically closed field: it will be tacitly assumed throughout to be 'sufficiently big'. (In Weil [We46], one would posit $\mathbb{E}$ a 'universal domain' or 'universal field', assumed to have infinite transcendence degree over any proper subfield of interest.) We suppose that all fields subsequently considered in this thesis are contained in $\mathbb{E}$, and make no assumptions about the characteristic until [2].

1.1 Affine varieties

Denote by $\mathbb{A}^n$ the product $\mathbb{E} \times \cdots \times \mathbb{E}$ (n copies). By an *affine variety*, we mean the set of common zeros (in $\mathbb{A}^n$) of a subset S of $\mathbb{E}[T_1, \ldots, T_n]$: clearly we need only consider subsets which are actually ideals. We will have a more intrinsic definition later. The latter ideals

are all finitely generated by the Hilbert Basis Theorem. Define a pair of maps as follows: let $\mathcal{I}$: {subsets of $\mathbb{A}^n$} $\longrightarrow$ {ideals in $\mathbb{E}[T_1, \ldots, T_n]$} take a set X to the ideal $\mathcal{I}(X)$ in $\mathbb{E}[T_1, \ldots, T_n]$ of functions vanishing thereon, and let $\mathcal{V}$ be the map in the reverse direction taking an ideal I to the subset $\mathcal{V}(I)$ of $\mathbb{A}^n$ on which all its elements vanish. Then we clearly have $X \subseteq \mathcal{V}(\mathcal{I}(X))$ and $I \subseteq \mathcal{I}(\mathcal{V}(I))$. Indeed it is easy to see that in the latter inclusion we can actually write $\mathrm{nil}(I) \subseteq \mathcal{I}(\mathcal{V}(I))$, where $\mathrm{nil}(I)$ is the *radical* of the ideal I, namely

$$\mathrm{nil}(I) := \{f \in \mathbb{E}[T_1, \ldots, T_n] : f^r \in I \text{ for some } r \geq 0\}.$$

In fact, we now have equality [Bor91, 3.8].

Theorem 1.1.0.1 (Hilbert's Nullstellensatz)
Let I be an ideal in $\mathbb{E}[T_1, \ldots, T_n]$. Then $\mathrm{nil}(I) = \mathcal{I}(\mathcal{V}(I))$.

Recall that a topological space is said to be *irreducible* if it cannot be written as a union of two proper closed subsets (equivalently, every nonempty open set is dense). An irreducible space is connected. One can readily verify that the affine varieties as defined above can be regarded as the closed sets of a topology on $\mathbb{A}^n$, the *Zariski topology*, in which points are closed. Moreover, it follows that $\mathbb{A}^n$ is quasicompact (*viz.* compact but not Hausdorff), as the Hilbert Basis Theorem shows that the space has the ascending chain condition on open sets: that is, it is a *Noetherian space*. Clearly this is true of affine varieties too, with the induced topology. It is not hard to show that a Noetherian space is a union of finitely many maximal irreducible subspaces, its irreducible components, which are closed. A couple of convenient notations: $A \subseteq_o B$ and $A \subseteq_c B$ will respectively mean that 'A is open (closed) in B'.

It turns out that the closed subsets in $\mathbb{A}^n$ which are irreducible are precisely those whose associated ideals are prime. Further, we can verify that, for an affine variety X, the irreducible components thereof are the affine varieties associated to the minimal prime ideals containing $\mathcal{I}(X)$ (there being finitely many minimal primes in any Noetherian ring).

We need the notion of the product of two affine varieties. Specifically, if we have the affine varieties $X \subseteq_c \mathbb{A}^m$ and $Y \subseteq_c \mathbb{A}^n$, with associated (radical) ideals $\mathcal{I}(X) \lhd$

$\mathbb{E}[T_1, \ldots, T_m]$ and $\mathcal{I}(Y) \lhd \mathbb{E}[U_1, \ldots, U_n]$, then the Cartesian product $X \times Y$ is also an affine variety with corresponding ideal in $\mathbb{E}[T_1, \ldots, T_m, U_1, \ldots, U_n]$ given by

$$\mathcal{I}(X \times Y) = \mathcal{I}(X) \otimes \mathbb{E}[U_1, \ldots, U_n] + \mathbb{E}[T_1, \ldots, T_m] \otimes \mathcal{I}(Y),$$

which is also radical (the tensoring being over $\mathbb{E}$ of course).

The most important remark to make about this situation is that the topology on $X \times Y$ is weakly finer than the product topology thereon - here all topologies are those induced by the ambient affine spaces. For example, the complements of curves in $\mathbb{A}^2$ are Zariski-open, but not usually product-open.

To define (regular) morphisms of affine varieties, we return to polynomial maps (that is, the restrictions to affine varieties of polynomial maps of affine spaces): it is easy to see that these are continuous in the Zariski topology, for if $\phi : X \longrightarrow Y$ is such a map, with C a closed subset of Y, then $\phi^{-1}(C)$ is the vanishing set of $\{f \circ \phi\}$, where the f are the elements of the ideal of functions vanishing on C.

Consider now, for an affine variety $X \subseteq \mathbb{A}^m$, the possible polynomial functions $X \longrightarrow \mathbb{E}$. It is easy to see that these correspond bijectively to elements of $\mathbb{E}[T_1, \ldots, T_m]/\mathcal{I}(X)$. The latter $\mathbb{E}$-algebra is called the *affine algebra* of X, and we will denote it by $\mathbb{E}[X]$: it is *reduced* (has no nonzero nilpotents) and finitely generated. In fact, it is not hard to see that every $\mathbb{E}$-algebra with these properties is the affine algebra of some affine variety. Clearly a polynomial mapping $\phi : X \longrightarrow Y$ induces an $\mathbb{E}$-algebra homomorphism ϕ^* in the opposite direction by sending an element g of $\mathbb{E}[Y]$ to the element $g \circ \phi$ of $\mathbb{E}[X]$. Indeed it turns out that every $\mathbb{E}$-algebra homomorphism between them corresponds to a polynomial mapping from $X \to Y$ - to see this just take generating sets for the algebras. When X is also irreducible, $\mathbb{E}[X]$ is a domain, and its field of fractions is called the *function field* $\mathbb{E}(X)$ of X. This notion of morphism gives an antiequivalence between the categories of affine varieties and (regular) morphisms thereof, and the category of affine $\mathbb{E}$-algebras and $\mathbb{E}$-algebra homomorphisms. Either of the maps ϕ or ϕ^* may be called the *comorphism* of the other.

1.2 Affine subvarieties

If V, W are two affine varieties, with $V \subseteq W$, then, as $\mathcal{I}(W) \subseteq \mathcal{I}(V)$, the quotient of these will be the ideal in $\mathbb{E}[W]$ of functions vanishing on V. If this latter ideal is principal, we say that V is a *hypersurface* in W, and its complement is called a *principal open set* of W. For any affine variety, the principal open sets form a basis for the topology.

It may be worth remarking that the image of a morphism may fail to be closed: for example, take the embedding of the multiplicative group $\mathbb{E}^*$ of $\mathbb{E}$ into $\mathbb{E}$ itself. One easily shows that $\mathbb{E}^*$ can be identified with a closed subvariety of $\mathbb{A}^2$, but that its complement $\{0\}$ in $\mathbb{E}$ is not open therein. A morphism $\phi : X \longrightarrow Y$ is called a *closed embedding* if it is injective, with $\phi(X)$ closed in Y.

Proposition 1.2.0.1 *Let $\phi : X \longrightarrow Y$ be as above.*
(i) ϕ^* is injective iff $\phi(X)$ is dense in Y.
(ii) If ϕ^* is surjective, then ϕ is a closed embedding.

1.3 Projective varieties and the exterior algebra

We define $\mathbb{P}^n$ as usual, to be the set $(\mathbb{E}^{n+1} \setminus \{0\})/R$, where R is the relation that identifies two points if one is a nonzero scalar multiple of the other. We can identify $\mathbb{P}^n$ with the set of lines through the origin of $\mathbb{E}^{n+1}$. Points in $\mathbb{P}^n$ may be described by homogeneous coordinates $X_0, \ldots, X_n$, also defined only up to nonzero scalar multiplication. To define an analogue of the affine variety in this situation, we will therefore have to consider homogeneous polynomials only (those for which all monomials have the same total degree) in $X_0, \ldots, X_n$. A set of such polynomials generates a *homogeneous ideal* (one closed under the operation of taking homogeneous pieces). We topologize $\mathbb{P}^n$ by decreeing that the closed subsets will be those which are the sets of common zeros of some homogeneous ideal. Just as in the affine case, one finds that there is an inclusion-reversing bijection between these closed subsets (the *projective varieties*), and the homogeneous radical ideals of $\mathbb{E}[X_0, \ldots, X_n]$ other than $(X_0, \ldots, X_n)$ - the latter would correspond to the (excluded) origin of $\mathbb{E}^{n+1}$. It turns out that the principal open sets are again a basis for the Zariski

topology on $\mathbb{P}^n$. Particularly useful are the principal open sets of the form $\{X_i \neq 0\}$ - the so-called *affine pieces* of $\mathbb{P}^n$. These can not only be readily identified with the affine space $\mathbb{E}^n$, but are homeomorphic thereto also. This means that a subset of $\mathbb{P}^n$ is closed therein iff its intersection with each of the specified principal open sets is closed in the latter. This is an 'affine criterion' for closure.

The Cartesian product of two projective varieties can also be shown to have a structure of projective variety, *via* the *Segre embedding* $\mathbb{P}^m \times \mathbb{P}^n \longrightarrow \mathbb{P}^{(m+1)(n+1)-1}$ given by sending $(X_0, \ldots, X_m, Y_0, \ldots, Y_n)$ to

$$(X_0Y_0, X_0Y_1, \ldots, X_0Y_n, X_1Y_0, X_1Y_1, \ldots, X_1Y_n, \ldots, X_mY_n).$$

Let V be a vector space over $\mathbb{E}$ of dimension n. We define the *exterior algebra* on V thus: we begin with the tensor algebra on V, namely the direct sum $\oplus_{n\geq 0} V^r$, where the powers of V are tensor powers (use the usual canonical identification of $V^r \otimes_{\mathbb{E}} V^s$ with V^{r+s}). This is graded (by $\mathbb{N}$), with V^0 identified to $\mathbb{E}$, and we have a product defined by convolution. To get the exterior algebra ΛV on V, form the quotient by the (homogeneous) ideal generated by $\{x^2 : x \in V\}$, so that ΛV is also graded - we define the graded part to be zero on negative integers to get grading by $\mathbb{Z}$. One can show that ΛV is anticommutative, and indeed more generally that if $x, y \in \Lambda V$ are such that their homogeneous decompositions are $x = \Sigma_i x_i$ and $y = \Sigma_j y_j$, then $x_i y_j = (-1)^{ij} y_j x_i$, as a consequence of the definition of ΛV, and in fact the k^{th} homogeneous part $(xy)_k$ of xy is given by $(xy)_k = \Sigma_j x_j y_{k-j}$. The graded part $\Lambda^d V$ of degree d has dimension (as $\mathbb{E}$-module) $\binom{n}{d}$. The construction passes in a natural way to subspaces. Now, let S_d be the set of all d-dimensional subspaces of V. Define a map ϕ therefrom to the space $\mathbb{P}(\Lambda^d V)$ by sending each subspace D to the point in $\mathbb{P}(\Lambda^d V)$ corresponding to $\Lambda^d D$. It is readily verified that ϕ is injective, and one shows that its image is closed in $\mathbb{P}(\Lambda^d V)$. The S_d are called the *Grassmann varieties* of V.

1.4 Sheaves

Let A be an irreducible affine variety now. For $x \in A$, the ideal

$$m_x := \{f \in \mathbb{E}[A] : f(x) = 0\}$$

is of course maximal in $\mathbb{E}[A]$, and the localization of $\mathbb{E}[A]$ thereat is called the *local ring* $\mathcal{O}_x$ of x. Clearly $\mathbb{E}[A] \subseteq \mathcal{O}_x \subseteq \mathbb{E}(A)$ for all $x \in A$. Note that $\mathcal{O}_x$ is unchanged by passing to any principal open set of A which contains x. One can show that $\mathbb{E}[A] = \cap_{x \in A} \mathcal{O}_x$. Now let U be an open subset of A. Define an $\mathbb{E}$-algebra $\mathcal{O}_A(U) = \cap_{x \in U} \mathcal{O}_x$ (or just $\mathbb{E}(A)$ if $U = \phi$). In fact, the assignment $U \mapsto \mathcal{O}_A(U)$ makes the collection $\{\mathcal{O}_A(U) : U \text{ open in } A\}$ into a *sheaf* of $\mathbb{E}$-algebras on A. This means that the following two axioms are satisfied:

(i) whenever $V \subseteq U$, both of these being open in A, and $f \in \mathcal{O}_A(U)$, then the restriction of f to V is in $\mathcal{O}_A(V)$;

(ii) whenever we have $U = \cup_{i \in I} U_i$, all of these open in A, and a choice of an $f_i \in \mathcal{O}_A(U_i)$ for each $i \in I$ such that $f_i = f_j$ on $U_i \cap U_j$ for every i, j, then there is an $f \in \mathcal{O}_A(U)$ with $f = f_i$ on U_i for each i.

For irreducible A (not necessarily affine), with $x \in A$, we define the *local ring* at x to be

$$\mathcal{O}_{A,x} = \varinjlim_{U \subseteq_o A : x \in U} \mathcal{O}_A(U)$$

- we will often omit the name of the variety. The corresponding maximal ideal will be denoted $\mathfrak{M}_x$.

Next for a general A (not necessarily irreducible or affine), with irreducible components A_i, we define a sheaf of $\mathbb{E}$-algebras on A thus: for U open in A, put $U_i = A_i \cap U$, and then take $\mathcal{O}_A(U)$ to be

$$\{f : U \longrightarrow \mathbb{E} : f|_{U_i} \in \mathcal{O}_{A_i}(U_i) \ \forall i\}.$$

This formula clearly generalizes that just given for the irreducible case.

Note that a morphism $f : X \longrightarrow Y$ of affine varieties induces a morphism of sheaves $f' : \mathcal{O}_Y \longrightarrow \mathcal{O}_X$ as follows: the comorphism f^* of f induces an obvious map $\mathcal{O}_{Y,f(x)} \longrightarrow$

$\mathcal{O}_{X,x}$ for each $x \in X$. Now if $V \subseteq_o Y$ and $U \subseteq_o X$, with $f(U) \subseteq V$, we get a mapping $\mathcal{O}_Y(V) \longrightarrow \mathcal{O}_X(U)$ by composing with f. This mapping is compatible with the restriction maps - in other language, one can regard a sheaf as a certain kind of contravariant functor, and then the mapping we have just defined will be a natural transformation of two such.

1.5 Prevarieties and varieties

An *irreducible prevariety* X will be an irreducible Noetherian topological space X, together with a sheaf of $\mathbb{E}$-valued functions thereon, such that X is a finite union of open sets U_i, each isomorphic to an affine variety when equipped with the induced sheaf $\mathcal{O}_X|_{U_i}$. Then we will call a Noetherian space X a *prevariety* if its irreducible components $\{X_i\}$ are irreducible prevarieties in this sense, together with a condition that $\mathcal{O}_{X_i}$ and $\mathcal{O}_{X_j}$ induce the same sheaf of functions on $X_i \cap X_j$. Just as in the affine case, one finds that there is a unique sheaf extending the $\mathcal{O}_{X_i}$. For $U \subseteq_o X$, the elements of $\mathcal{O}_X(U)$ will be called the *regular functions* on U, and any $Y \subseteq_o X$ which is (with its sheaf) isomorphic to an affine variety will be called an *affine open subset* of X - for example, the U_i as above. Finally, the elements of $\mathcal{O}_X(U)$, for $U \subseteq_o X$, will be called *regular functions on* U.

A locally closed subset of a prevariety will be called a *subprevariety* of X (recall that *locally closed* means 'open in its closure' - for example, open or closed sets are locally closed). Finally, a subprevariety of a projective variety is called *quasi-projective*. Just as in the affine case, the function field of an irreducible prevariety is that of any of its affine open subsets.

Let $g : X \longrightarrow Y$ be a mapping of prevarieties. We will say that it is a *morphism* if it is continuous and satisfies the condition that, whenever $V \subseteq_o Y$ and $f \in \mathcal{O}_Y(V)$, then $f \circ g \in \mathcal{O}_X(g^{-1}(V))$. This is equivalent to the earlier definition in the affine case. We have the following 'affine criterion' for a mapping to be a morphism.

Proposition 1.5.0.1 *[Hu75, 2.3] Let $g : X \longrightarrow Y$ be a mapping of two prevarieties, and suppose that there is a covering of Y by affine open sets V_i, for $i \in$ (finite) I, and a covering of X by open sets U_i such that*

(a) $g(U_i) \subseteq V_i$ *for each* $i \in I$*; and*

(b) $f \circ g \in \mathcal{O}_X(U_i)$ *whenever* $f \in \mathcal{O}_Y(V_i)$.

Then g *is a morphism of prevarieties.*

If $g : X \longrightarrow Y$ is a morphism of irreducible prevarieties, and so induces a morphism of function fields $g_1 : \mathbb{E}(Y) \longrightarrow \mathbb{E}(X)$, we say that it is a *birational equivalence* if g_1 is an isomorphism. This is a strictly weaker notion than that of being an isomorphism.

It can be shown that, if X and Y are two prevarieties, the Cartesian product $X \times Y$ can be made into a categorical product.

A prevariety X will be called a *variety* if the diagonal $\{(x, x) : x \in X\}$ is closed in $X \times X$. Some examples: affine varieties, subprevarieties of varieties, products of varieties, and projective varieties. (This extra condition would be the Hausdorff axiom if we were considering the product topology.)

1.6 Dimension, degree and dominance

By the *dimension* of a variety we mean the maximum of the dimensions of its irreducible components. For an irreducible variety X, with function field $\mathbb{E}(X)$, the dimension will be defined to be the transcendence degree of this latter field over $\mathbb{E}$. We note that dimension cannot increase if we pass to a closed subset, and that it is preserved (in the irreducible case) by passage to a nonempty affine open subset.

Theorem 1.6.0.1 *[Hu75, 3.4] Let* Y *be a closed irreducible subset of an irreducible variety* X*, of codimension* r *therein. Then there exist closed irreducible subsets* Y_i *in* X*, of codimension* i *therein, such that* $Y_1 \supseteq Y_2 \supseteq \cdots \supseteq Y_r = Y$.

Let $g : X \longrightarrow Y$ be a morphism of varieties. If g maps each component of X onto a dense subset of a component of Y, and $g(X)$ is dense in Y, we say that g is *dominant*. For W closed and irreducible in Y, a component of $g^{-1}(W)$ for which the restriction thereto of g (as map to W) is dominant is said *to dominate* W.

For irreducible X, to say that g is dominant means exactly that $g(X)$ is dense in Y. In this situation, we clearly have that $\dim X \geq \dim Y$. If, further, these dimensions agree, the extension $\mathbb{E}(X)/g^*\mathbb{E}(Y)$ of function fields is finite, and the degree of this extension is called the *degree* of g. Naturally, the separable (inseparable) degrees of the extension are called the *separable degree* and the *inseparable degree* of the morphism.

Theorem 1.6.0.2 *[Hu75, 4.1] Let $g : X \longrightarrow Y$ be a dominant morphism of irreducible varieties, with $r = \dim X - \dim Y$, and let W be a closed irreducible subset of Y. Suppose that Z is an irreducible component of $g^{-1}(W)$ which dominates W; then $\dim Z \geq \dim W + r$. In particular, for $y \in g(X)$, each component of $g^{-1}(\{y\})$ has dimension at least r.*

1.7 Finite morphisms

A morphism $g : X \longrightarrow Y$ of *affine* varieties is said to be *finite* if $\mathbb{E}[X]$ is integral over $g^*(\mathbb{E}[Y])$.

Proposition 1.7.0.1 *[Hu75, 4.3] Let $g : X \longrightarrow Y$ be a finite dominant morphism of affine varieties.*
(a) If $Z \subseteq_c X$, then $g(Z) \subseteq_c Y$, and the restriction of g to Z is finite; further g is surjective.
(b) If W is a closed irreducible subset of Y, and C is any component of $g^{-1}(W)$, then $g(C) = W$.

Proof: Putting $R = \mathbb{E}[X]$ and $S = \mathbb{E}[Y]$, we can view S as a subring of R as g^* is injective. For an ideal $I \lhd R$, R/I is an integral extension of $S/(I \cap S)$.
We prove (a): take I to be the ideal of Z (noting that Z is an affine variety). Now $I' = I \cap S$ is radical in S, and so I' is the ideal of a closed subvariety Z', into which g maps Z. The corresponding affine algebras are S/I' and R/I, so $g : Z \longrightarrow Z'$ is again dominant and finite. (a) will follow once we have shown that any finite dominant morphism is surjective. Pick $y \in Y$: then there exists an $x \in g^{-1}(\{y\})$ iff $g^*(\mathfrak{M}_y) \subseteq \mathfrak{M}_x$ - where the notation refers as usual to the maximal ideal in S (respectively R) vanishing at y (respectively x). Thus

we need only show that $\mathfrak{M}_y$ is contained in a maximal ideal of R: but as R is integral over S, this follows from the well-known 'Going-Up' theorem [AM69, 5.11]. This proves (a).

(b) We have just shown that the restriction of g to C is again finite, and so $g(C)$ is closed and irreducible. Now we need only show that $\dim C = \dim W$. For I and J the ideals corresponding to C (respectively W), then $I \cap S = J$, and both are prime. Just as before, R/I is integral over S/J, so the corresponding field extension is algebraic, and the dimensions coincide. □

We use the following version of the Noether normalization lemma.

Theorem 1.7.0.2 (Noether normalization lemma) *[Hu75, 4.3] Let $S \subseteq R$ be integral domains, with R finitely generated as S-algebra, and both finitely generated as $\mathbb{E}$-algebras. Then there exists $f \neq 0$ in S, and $y_1, \ldots, y_m$ in R, such that the $\{y_i\}$ are algebraically independent over S, and R_f is integral over $S[y_1, \ldots, y_m]_f$, the subscript denoting localization at f.*

This is used to prove the following.

Theorem 1.7.0.3 *[Hu75, 4.3] Let $g : X \longrightarrow Y$ be a dominant morphism of irreducible varieties, and $r = \dim X - \dim Y$. Then there exists $\phi \neq U \subseteq_o Y$ such that*

(a) $U \subseteq g(X)$, and

(b) whenever $W \subseteq_c Y$ with $W \cap U$ nonempty and W irreducible, and Z is a component of $g^{-1}(W)$ with $Z \cap g^{-1}(U)$ nonempty, then $\dim Z = \dim W + r$.

Proof: We can suppose that Y is affine, for if U is an affine open subset of Y which meets W, then $U \cap W$ is dense in W, and we can consider the restriction of g to $g^{-1}(U)$ instead. Moreover, we can assume that X is affine, for having found suitable open sets U_i for the restrictions of g to each of a (finite) cover by affine open sets of X, then we can take $U = \cap_i U_i$. Next identify $\mathbb{E}[Y] =: S \subseteq R := \mathbb{E}[X]$ *via* g^*, and use the normalization lemma above to find an $f \in S$ and $y_1, \ldots, y_m$ in R with the properties asserted therein. Clearly, this m is the same as r. Then S_f and R_f are the affine algebras of principal open

sets Y_f and X_f of Y, X. Further, we can regard $S_f[y_1, \ldots, y_r]$ as the affine algebra of $Y_f \times \mathbb{A}^r$, and can factor the restriction of g to X_f as

$$X_f \xrightarrow{h} Y_f \times \mathbb{A}^r \xrightarrow{pr_1} Y_f$$

with both of these maps being surjective using [1.7.0.1]. Putting $U = Y_f$, we note that $X_f = g^{-1}(U)$, and that $U \subseteq g(X)$, verifying (a).

To verify that this choice of U satisfies (b), we may as well suppose that $U = Y = Y_f$ and $X = X_f$: keeping the same factorization $g = pr_1 \circ h$, with h finite, suppose that $W \subseteq_c Y$ with W irreducible, and Z a component of $g^{-1}(W)$, so Z is a component of $h^{-1}(W \times \mathbb{A}^r)$ - as h is surjective, $h(Z) = W \times \mathbb{A}^r$, and $r + \dim W = \dim h(Z) = \dim Z$ as h is finite. □

1.8 Constructibility

If one takes the Boolean algebra generated by the open (or the closed) subsets of a topological space X - (using finite unions (or intersections) and complementation), the subsets of X of this form are called *constructible*. Equivalently, the subset S of X is constructible if it is a finite union of locally closed subsets.

Theorem 1.8.0.1 (Chevalley) *[Hu75, 4.4] Let $g : X \longrightarrow Y$ be a morphism of varieties: then g maps constructible sets to constructible sets.*

Proof: A locally closed subset of X is a subvariety, and thus a constructible set is also. Hence it suffices to show that $g(X)$ is constructible. Semblably, we can suppose that X and Y are irreducible, and proceed by induction on $\dim Y$, taking the case of dimension zero as read. By induction, we can suppose g dominant, and by [1.7.0.3], we can choose a nonempty set $U \subseteq g(X)$, with $U \subseteq_o Y$. Then the irreducible components $W_1, \ldots, W_t$ of $Y \setminus U$ have lower dimension than Y. By induction, the restrictions of g to the various components Z_{ij} of $g^{-1}(W_i)$ have images constructible in W_i, and so in Y. But $g(X) = U \cup_{i,j} g(Z_{ij})$ and we are done. □

Proposition 1.8.0.2 (Upper Semicontinuity of Dimension) *[Hu75, 4.4]*

If $g : X \longrightarrow Y$ is a dominant morphism of irreducible varieties and $x \in X$, let $e(x)$ be the maximum dimension of a component of $g^{-1}(g(x))$ which passes through x. Then for each $n \in \mathbb{N}$, the set $X_n := \{x \in X : e(x) \geq n\}$ is closed in X.

Proof: By induction on $\dim Y$. □

One situation in which one draw a stronger conclusion is the following, which is important in the construction of the so-called 'geometric quotient' of a variety by an algebraic group [3.2.1].

Theorem 1.8.0.3 *[Hu75, 4.5] Let $g : X \longrightarrow Y$ be a dominant morphism of irreducible varieties, with $r = \dim X - \dim Y$, and suppose that for each irreducible $W \subseteq_c Y$, each irreducible component of $g^{-1}(W)$ has dimension $r + \dim W$. Then g is an open map.*

Proof: By hypothesis, g is surjective, and the irreducible components of $g^{-1}(W)$ all dominate W.

If $x \in X$, and $x \in U \subseteq_o X$, we have to show that $y = g(x)$ is an interior point of $V = g(U)$; if not, then y is in the closure of $Y \setminus V$: now V, and hence $Y \setminus V$ are constructible, and thus y lies in the closure C of some locally closed $O \cap C$ - where $O \subseteq_o Y$, and we can suppose C irreducible, so $O \cap C$ is dense in C. The irreducible components of $C' := g^{-1}(C)$ all have the same dimension, and dominate C. Next, $O' := g^{-1}(O)$ meets each such component, so $C' \cap O'$ is dense in C'. But $C' \cap O' = g^{-1}(C \cap O)$ is contained in the closed set $X \setminus U$, so $C' \subseteq X \setminus U$. But $x \in C'$: contradiction. □

1.9 Tangency

For an affine variety $X \subseteq_c \mathbb{A}^n$, with $x \in X$, $x = (x_1, \ldots, x_n)$ and $f \in \mathbb{E}[T_1, \ldots, T_n]$, define $d_x f := \sum_{j=1}^{n} \partial f / \partial T_j(x)(T_j - x_j)$ where the notation means that the derivative is evaluated at x; then if $\mathcal{I}(X) = (f_1, \ldots, f_t)$ is the ideal corresponding to X, define the *geometric tangent space to* X at x to be $Tan(X)_x$, the (linear) variety given by the

vanishing of the ideal $(d_x f_1, \ldots, d_x f_t)$. For a general variety X, we could pick an affine open subset of X, and proceed as above, but would like a more intrinsic description.

To get this, again suppose firstly that we have $x \in X \subseteq_c \mathbb{A}^n$, with $R := \mathbb{E}[X]$, and let $M := \mathcal{I}(\{x\})$ be the maximal ideal of R which vanishes at x. Now M/M^2 is a finite-dimensional $\mathbb{E}$-module, performing the identification $\mathbb{E} = R/M$. Then any $f \in \mathbb{E}[T_1, \ldots, T_n]$ defines a linear function $d_x f$ on $\mathbb{A}^n$, and so on $Tan(X)_x$. Since $d_x f$ is determined by $f \bmod \mathcal{I}(X)$ we can suppose $f \in R$. Then $d_x f : R \longrightarrow (Tan(X)_x)^*$ is a surjective linear map: moreover, since $R = \mathbb{E} \oplus M$, and $d_x f|_{\mathbb{E}} = 0$, we can take $d_x f : M \longrightarrow (Tan(X)_x)^*$, and it is readily shown that the kernel of this map is M^2. This enables identification of $(M/M^2)^*$ with $Tan(X)_x$. Now if we localize R at M, and use exactness of localization, we can identify the R/M-module M/M^2 with the $\mathcal{O}_x/\mathfrak{M}_x$-module $\mathfrak{M}_x/\mathfrak{M}_x^2$, and finally define the *tangent space* $\mathcal{T}(X)_x$ *to* X *at* x to be $(\mathfrak{M}_x/\mathfrak{M}_x^2)^*$. Moreover, this now works for any irreducible variety X, and in general provided that we define $\mathcal{O}_x$ correctly.

An equivalent way of looking at the tangent space is the following: with the same notation, let $\mathcal{D}_x$ be the $\mathbb{E}$-module of $\mathbb{E}$-linear mappings $\delta : \mathcal{O}_x \longrightarrow \mathbb{E}$ satisfying $\delta(fg) = \delta(f)g(x) + f(x)\delta(g)$ - the so-called *point derivations of* $\mathcal{O}_x$. One can verify that $\mathcal{D}_x$ and $\mathcal{T}(X)_x$ are naturally isomorphic as $\mathbb{E}$-modules.

To pass to the general case now is easy: if $x \in X$, and lies on a unique irreducible component Y, then define $\mathcal{T}(X)_x = \mathcal{T}(Y)_x$: otherwise, with an appropriate definition of $\mathcal{O}_x$, we can use $(\mathfrak{M}_x/\mathfrak{M}_x^2)^*$ as before. It is also now easy to see that if $x \in X$ and $y \in Y$, then $\mathcal{T}_{(x,y)}(X \times Y) = \mathcal{T}_x(X) \oplus \mathcal{T}_y(Y)$.

A point $x \in X$ for which $\dim \mathcal{T}(X)_x = \dim X$ is said to be *simple* (on X) - X is said to be *smooth* if all its points are simple. In fact the following holds.

Recall that a field extension A/B is *separably generated* if A is a separable algebraic extension of a purely transcendental extension of B: for finitely generated extensions, the notion is equivalent to that of being separable.

Theorem 1.9.0.1 *Let X be an irreducible variety. Then $\dim \mathcal{T}(X)_x \geq \dim X \ \forall x \in X$, with equality holding for all x in some dense open subset of X.*

Proof: The equality condition for the case in which X is an irreducible hypersurface in $\mathbb{A}^n$ is easy. As $\mathbb{E}(X)/\mathbb{E}$ is separably generated ($\mathbb{E}$ being perfect), we have $\mathbb{E}(X)/L$ finite and separable, where $L = \mathbb{E}(T_1, \ldots, T_d)$ with $d = \dim X$, and the T_i being algebraically independent over $\mathbb{E}$. We can find $y \in \mathbb{E}(X)$ such that $\mathbb{E}(X) = L(y)$, with $f(T) \in L[T]$ (say) its minimal monic polynomial over L. Then we have $f(T, T_1, \ldots, T_d) \in \mathbb{E}[T, T_1, \ldots, T_d]$ defined on some affine open subset of $\mathbb{A}^{d+1}$, whose set of zeros is a hypersurface Y therein with $\mathbb{E}(Y)$ isomorphic to $\mathbb{E}(X)$:- Y is irreducible as f is. Thus X and Y are birationally isomorphic, so one can find nonempty open sets in each which are isomorphic. By the hypersurface result, the desired conclusion holds for Y, and therefore for X: thus we have equality in a dense open subset.

For an arbitrary $x \in X$, to determine the dimension of $\mathcal{T}(X)_x$, we can replace X by an affine open neighbourhood of x. Thus let $X \subseteq_c \mathbb{A}^n$ for some n, and regard the tangent spaces as linear varieties. Consider pairs $(x, y) \in X \times \mathbb{A}^n$ with $y \in Tan(X)_x$. These form a closed subset A of the product: projection onto the first factor defines a morphism $h : A \longrightarrow X$, with $h^{-1}(x)$ having the dimension of $\mathcal{T}(X)_x$. We have seen that

$$X_d := \{x \in X : \dim \mathcal{T}(X)_x \geq d\}$$

is dense in X, and so it only remains to show that $X_d \subseteq_c X$, which follows from 'upper semicontinuity of dimension' [1.8.0.2] applied to h. □

The next result is a version of Zariski's Main Theorem.

Theorem 1.9.0.2 *[Bor91, AG 18.2] Let $g : V \longrightarrow W$ be a dominant morphism of smooth irreducible varieties, such that, for each $w \in W$, $g^{-1}(\{w\})$ has (finite) constant cardinality n. Then n is the separable degree of (the extension of function fields associated to) g.*

Corollary 1.9.0.3 *If g is birational, it is an isomorphism; if g is bijective, the extension is purely inseparable.*

1.10 Local rings

We need now a few facts about the following situation: let R be a Noetherian local ring, with maximal ideal M. The *Krull dimension* of R is the greatest $k \in \mathbb{N}$ such that there is a chain of prime ideals P_i in R of the form $0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_k = M$. For the local ring $\mathcal{O}_x$ ($x \in X$, with X irreducible), the Krull dimension is just $\dim X$ (as one sees by taking X affine). One can consider also the minimal number of generators of the R-module M: a standard result [Bor91, AG3.9] shows that this is the same as the dimension of the R/M-module M/M^2. An R which has the property that this latter dimension equals its Krull dimension is said to be *regular*. A regular (Noetherian) local ring is an integral domain, and integrally closed [AM69, Ch.11] - in fact, it is even a UFD [Bor91, AG3.9], but we do not need this fact. Thus, the last theorem shows that $\dim X$ is the same as the Krull dimension of $\mathcal{O}_x$ for all simple points $x \in X$, and so that $\mathcal{O}_x$ has all of the properties just discussed for simple x.

1.11 Differentials

For the morphism $g : X \longrightarrow Y$ of irreducible varieties, with $x \in X$ and $y = g(x)$, the comorphism g^* of g is a *local ring morphism* meaning not only that $g^* : \mathcal{O}_y \longrightarrow \mathcal{O}_x$ but also that $g^*(\mathfrak{M}_y) = \mathfrak{M}_x$. Thus composition with g^* induces a mapping $\mathfrak{M}_y/\mathfrak{M}_y^2 \longrightarrow \mathfrak{M}_x/\mathfrak{M}_x^2$, which one verifies to be $\mathbb{E}$-linear. Making the usual identification of these modules with the duals of the tangent spaces gives us a linear map $\partial g : \mathcal{T}(X)_x \longrightarrow \mathcal{T}(Y)_y$, and this behaves functorially. In fact, in the affine case, we can give an explicit description of it, so: suppose $X \subseteq_c \mathbb{A}^m$ and $Y \subseteq_c \mathbb{A}^n$, so $g = (g_1, \ldots, g_n)$, each g_i a coordinate function. Identify the tangent spaces at $x \in X$ and $y = g(x) \in Y$ with subspaces of $\mathbb{E}^m$ and $\mathbb{E}^n$ respectively; this identifies $a = (a_1, \ldots, a_m) \in \mathbb{E}^m$ with the point derivation $\mathcal{O}_x \longrightarrow \mathbb{E}$ given by $\Sigma_i a_i \partial/\partial T_i$ (followed by evaluation at x). Then $\partial g_x(a) = (b_1, \ldots, b_n)$, where $b_j = \sum_i a_i \partial g_j/\partial T_i(x)$.

Example: *det* : $GL_n \longrightarrow GL_1$, the map taking each (invertible) matrix to its determinant. We take x to be the identity matrix I. The tangent space to GL_n can be identified with $\mathbb{E}^{(n^2)}$ - which we take as M_n, the $n \times n$ matrices. The above formula gives,

for $a = (a_{ij}) \in GL_n$, $\partial(det)_I(a) = \sum_i a_{ii}$, which is the trace of the matrix a. $\square$

We will need the following theorem later, which is a composite of those cited in its heading. Note how information about g is deduced from the existence of an x and $g(x)$ with the asserted properties.

Theorem 1.11.0.1 *[Hu75, 5.5][Bor91, AG 17.3] Let $g : X \longrightarrow Y$ be a morphism of irreducible varieties, with $x \in X$ and $y = g(x) \in Y$ both being simple points. Then $\partial g_x : \mathcal{T}(X)_x \longrightarrow \mathcal{T}(Y)_y$ is surjective iff g is dominant and separable.*

1.12 Completeness

A variety X is *complete* if the projection map $p_2 : X \times Y \longrightarrow Y$ is closed for all varieties Y - this would be a compactness criterion (if we had the product topology) in a suitable category of topological spaces. It is easy to show that X is complete iff this is true of each of its irreducible components, and that we need only consider affine irreducible Y.

It turns out that complete varieties and their geometry are central to the understanding of algebraic groups (even though these are affine).

Proposition 1.12.0.1 *Let X and Y be varieties.*

(a) If $Y \subseteq_c X$ and X is complete then Y is complete.

(b) If X and Y are both complete, so is their product.

(c) If $g : X \longrightarrow Y$ and X is complete, then $g(X)$ is closed and complete.

(d) If Y is a complete subvariety of X, then it is closed.

(e) If X is complete and affine, then $\dim X = 0$.

(f) If X is complete and quasiprojective, it is projective.

Proof: (a) and (b) are trivial. To verify (c), note that the graph $\Gamma_g \subseteq_c X \times Y$, where $\Gamma_g := \{(x, g(x)) \in X \times Y : x \in X\}$ - because Γ_g is the inverse image of the diagonal of Y under the morphism $X \times Y \longrightarrow Y \times Y$ which sends (x, y) to $(g(x), y)$ (recall that Y is a variety). The projection $X \times Y \longrightarrow Y$ takes Γ_g to $g(X)$, which is therefore closed in Y by the completeness of X. Now we can assume that $g(X) = Y$. Let $W \subseteq_c Y \times Z$ for any

variety Z, and $q_2 : Y \times Z \longrightarrow Z$ the canonical projection map; write p_2 for the projection map $X \times Z \longrightarrow Z$. Then $q_2(W) = p_2 \circ (g \times 1_Z)^{-1}(W)$ as $g(X) = Y$, and $q_2(W)$ is closed in Z by the completeness of X. (d) follows from (c).

To prove (e), suppose that X is also irreducible to begin with. Note that any morphism $g : X \longrightarrow \mathbb{A}^1$ has a closed complete image by (c): but $\mathbb{A}^1$ is not complete, as (for example) the closed subset $\{(x, y) \in \mathbb{A}^2 : xy = 1\}$ of $\mathbb{A}^2$ projects onto the nonclosed subset $\mathbb{E}^*$ of $\mathbb{A}^1$. Thus g is constant and hence $\mathbb{E}[X] = \mathbb{E}$ (as g must factor *via* the inclusion map into $\mathbb{A}^1$ of a one-point variety). If X is not irreducible, its irreducible components are complete and affine, and this verifies (e). Finally (f) follows from (d). □

The most important examples of complete varieties are given by the next result.

Theorem 1.12.0.2 *Projective varieties are complete.*

Chapter 2

Relative Algebraic Geometry

We now turn to the more delicate question of 'relative' algebraic geometry, and retain the previous notation. Suppose now that k is a subfield of $\mathbb{E}$: we will use standard notations like k^s, k^i and k^a for the *separable (algebraic)*, *inseparable* or *perfect*, and *algebraic* closures of k. These are of course also subfields of $\mathbb{E}$. k^i is the field often denoted by $k^{p^{-\infty}}$: recall that k is called *perfect* if $k = k^i$.

We write p for the *characteristic exponent of* $\mathbb{E}$ - namely $\max(\operatorname{char}\mathbb{E}, 1)$. This turns out to be a more convenient notion than that of the characteristic.

2.1 Notation and notions

Note that any subfield k of $\mathbb{E}$ induces a topology on $\mathbb{A}^n$ (the latter still being defined to be $\mathbb{E} \times \cdots \times \mathbb{E}$). Specifically, we define a subset $S \subseteq \mathbb{A}^n$ to be *k-closed* if it is

(i) closed in the previous sense, and

(ii) there is an ideal $I \lhd \mathbb{E}[T_1, \ldots, T_n]$ such that S is the subset of affine space on which I vanishes, and that I is generated by its intersection I_k with $k[T_1, \ldots, T_n]$, where the polynomial ring over k is of course identified with a subring of that over $\mathbb{E}$. Thus $\mathcal{I}(S) = \operatorname{nil}(I)$. Topological terms unqualified by a field name will be assumed to refer to the $\mathbb{E}$-topology. We will write $A \subseteq_{o,k} B$ (respectively, $A \subseteq_{c,k} B$) to mean *A is k-open (k-closed) in B*.

Note we did not specify that I be radical. This leads to the notion of a subset defined over k: $S \subseteq \mathbb{A}^n$ is said to be *defined over* k, or to be an *affine* k*-variety*, if it is k-closed, and in condition (ii) above, we can take $I = \mathcal{I}(S)$. This is a stronger condition, but turns out to be a more valuable property. We will verify shortly that:

Proposition 2.1.0.1 *If X is k-closed, it is defined over (a finite subextension of) k^i.*

Example: The following $S \subseteq \mathbb{A}^1$ is k-closed but not defined over k. Take $p > 1$, and let $x^p \in k \not\ni x$ (so we are supposing that k is not perfect). Take $I = (Y^p - x^p) \lhd \mathbb{E}[Y]$. Then $I_k = (Y^p - x^p) \lhd k[Y]$; clearly $S = \{x\}$; however $\mathrm{nil}(I) = (Y - x)$, and this is not generated by $\mathrm{nil}(I)_k = I_k$. $\square$

It is clear that the $\mathbb{E}$-topology is T_1, but those induced by proper subfields are not, in general. Clearly, if $F_1 \subseteq F_2$ are two subfields of $\mathbb{E}$, then the F_1-topology is (weakly) coarser than the F_2-topology. More precisely

Proposition 2.1.0.2 *Let F_1, F_2 be any two subfields of $\mathbb{E}$. Then the F_1-topology coincides with the F_2-topology iff $F_1^i = F_2^i$.*

Proof: As any $f \in \mathbb{E}[T_1, \ldots, T_n]$ has the same zeros as f^p, it follows that for any subfield H of $\mathbb{E}$, the H-topology and H^i-topology coincide. Hence we can suppose that F_1 and F_2 are perfect, and moreover this verifies the 'if' part.

Conversely, let $t \in F_1 \setminus F_2$, and write $f(T)$ for the minimal (monic) polynomial for t over F_2 (we take $f = 0$ if t is transcendental over F_2). Put $S = (t, 0, \ldots, 0)$, which is a closed set with $I = (T_1 - t, T_2, \ldots, T_n)$ as ideal. Clearly S is F_1-closed. The result will follow once it is verified that S is not F_2-closed, for which it suffices to show that I_{F_2} vanishes at at least one other point.

Put $J = (f(T_1), T_2, \ldots, T_n)$; clearly $J \subseteq I_{F_2}$, and in fact $J = I_{F_2}$ since if

$$g(T_1, T_2, \ldots, T_n) \in I_{F_2},$$

then we can write $g(T_1, T_2, \ldots, T_n) = h(T_1) + l(T_1, \ldots, T_n)$ where h and l are polynomials with coefficients in F_2, and all monomials which occur in l contain at least one of $T_2, \ldots, T_n$.

Evaluating at the point in S gives $0 = h(t) + 0$, so $f(T_1)$ divides $h(T_1)$ (in $F_2[T_1]$), and thus $g \in (f(T_1), T_2, \ldots, T_n)$. This gives an expression for I_{F_2}. Further, all elements of I_{F_2} will vanish at every point $(s, 0, \ldots, 0)$ such that $f(s) = 0$. If $f = 0$, we can choose s arbitrarily; otherwise f has distinct roots as F_2 is perfect (and its degree is more than one as $t \notin F_2$).

In either case, we have found a point outside S at which all generators of I_{F_2} vanish, so S is not F_2-closed. □

2.2 Algebraic criteria, I

We now examine this idea using more algebra. Let V be an $\mathbb{E}$-module. A *k-structure on* V is a k-submodule $V_k \subseteq V$ such that the canonical map $V_k \otimes_k \mathbb{E} \longrightarrow V$ is an isomorphism of $\mathbb{E}$-modules. Elements of V_k are said to be *rational over k*.

Suppose now that V has a k-structure V_k, and U is an $\mathbb{E}$-submodule thereof. We say that U is *defined over k* if $U_k = U \cap V_k$ is a k-structure on U. (This condition is readily seen to be equivalent to the condition 'U_k spans U as $\mathbb{E}$-module'.) Put $W = V/U$ and write W_k for the projection of V_k onto W; then W_k is a k-structure on W iff U is defined over k.

Next, let $f : V \longrightarrow W$ be a linear map, where V, W are $\mathbb{E}$-modules with k-structures. f is said to be *defined over k*, or to be a *k-morphism*, if $f(V_k) \subseteq W_k$. The collection of all k-morphisms from V to W is a k-submodule $\mathrm{Hom}_{\mathbb{E}}(V, W)_k \subseteq \mathrm{Hom}_{\mathbb{E}}(V, W)$: if W is finite-dimensional (in particular if $W = \mathbb{E}$) then this is a k-structure on $\mathrm{Hom}_{\mathbb{E}}(V, W)$.

One readily verifies that, with the same V, W that $V_k \otimes_k W_k$ is a k-structure on $V \otimes_{\mathbb{E}} W$, and we get k-structures induced on the tensor, exterior and symmetric algebras of V.

Now let A be an $\mathbb{E}$-algebra (recall our conventions). A *k-structure on A* is then a k-structure A_k (as above) which is also a k-subalgebra.

A few properties: given such a structure, with $J \lhd A$, one verifies that J is defined over k iff $J_k = A_k \cap J$ generates J (as ideal). If S is a multiplicative set in A_k, then the localization $S^{-1}(A_k)$ is a k-structure on $S^{-1}(A)$. Finally, if A, B are two such there is

a natural bijection from $\mathrm{Hom}_{k-alg}(A_k, B_k)$ to $\mathrm{Hom}_{\mathbb{E}-alg}(A, B)_k$, where the latter denotes the set of $\mathbb{E}$-linear maps which are defined over k (in the previous sense), also required to be $\mathbb{E}$-algebra homomorphisms.

From above, one sees that if $\mathbb{E}[X]$ is the affine algebra of an affine variety X, then $\mathbb{E}[X]$ has a k-structure in the last sense iff X is defined over k. There is an analogous condition for X to be k-closed. One can easily verify that a product of two k-closed affine varieties (respectively affine k-varieties) has the same property.

2.3 Topological criteria

In fact, we will say that the $\mathbb{E}$-variety X *has a k-structure* if the following axioms are satisfied.

(a) It has a k-topology weakly coarser than the $\mathbb{E}$-topology, containing an affine open cover of X.

(b) For each k-open U, $\mathcal{O}_X(U)$ has a k-structure, and the restriction maps (between pairs of k-open subsets) are defined over k.

(c) Whenever U is affine and k-open in X, a k-structure on U is induced by a k-structure on $\mathcal{O}_X(U)$ thus: a subset Y of U is k-open iff it is complementary to the set on which an ideal of $\mathbb{E}[U]$ which is defined over k vanishes.

Condition (c) tells us that every k-open subset of an affine k-variety X is a finite union of principal k-open sets. The requirement in (a) that an affine open cover be included, though not in [Bor91, AG11.3], appears to be necessary to exclude such cases as that of the indiscrete topology on $\mathbb{P}^n$.

Example: If V is a vector space with k-structure V_k, the image of $V_k \setminus \{0\}$ under the usual projection gives a k-structure on $\mathbb{P}(V)$. □

A *morphism* $g : V \longrightarrow W$ of k-varieties is just a morphism of the underlying $\mathbb{E}$-varieties. It will be a *k-morphism* (or *defined over k*) if it is k-continuous, and such that whenever $A \subseteq_{o,k} V$ and $B \subseteq_{o,k} W$ with $g(A) \subseteq B$, then $g^* : \mathcal{O}_W(B) \longrightarrow \mathcal{O}_V(A)$ is defined over k. The latter condition is that the restriction to the k-topology of g induces a morphism of

'sheaves of $\mathbb{E}$-algebras with k-structures'. Clearly the condition that g be a k-morphism necessitates k-structures on V and W.

2.4 Algebraic criteria, II

Now we look at a subvariety Z of the affine k-variety V. Suppose Z is given by the vanishing of an ideal $J \lhd \mathbb{E}[V]$. Then the exact sequence of $\mathbb{E}$-modules

$$0 \to J \to \mathbb{E}[V] \to \mathbb{E}[Z] \to 0$$

becomes, after pulling back along the ring homomorphism $k \longrightarrow \mathbb{E}$, an exact sequence of k-modules (say)

$$0 \to J_k \to k[V] \to k[Z] \to 0$$

(as this is an exact construction). Note that no assertion has been made about whether or not Z is k-closed. While $k[V]$ is a k-structure on $\mathbb{E}[V]$, $k[Z]$ simply denotes the restriction of $k[V]$ to Z, which is reduced, and J_k is just $J \cap k[V]$. We can tensor the last short exact sequence through by $\mathbb{E}$ (which is a flat k-module) to get the result that

$$\mathbb{E} \otimes_k k[Z] = \mathbb{E}[V]/J_k \cdot \mathbb{E}[V]$$

Hence the kernel of the obvious (surjective) map

$$\mathbb{E} \otimes_k k[Z] \twoheadrightarrow \mathbb{E}[Z]$$

is exactly $J/J_k \cdot \mathbb{E}[V]$. Thus Z is k-closed iff $J = \mathrm{nil}(J_k \cdot \mathbb{E}[V])$, and if this does hold, the kernel mentioned is the nilradical of $k[V] \otimes_k \mathbb{E}$. Then clearly, Z is defined over k iff $J = J_k \cdot \mathbb{E}[V]$ as expected. We summarize all this in the next theorem.

Theorem 2.4.0.1 *The following are equivalent (for Z and V as first mooted):*

(a) Z is defined over k;

(b) $\mathbb{E}$ and $k[Z]$ are linearly disjoint over k in $\mathbb{E}[Z]$;

(c) $k[Z] \otimes_k \mathbb{E}$ *is reduced; and*

(d) $k(Z) \otimes_k \mathbb{E}$ *is reduced (where* $k(Z)$ *means the full ring of fractions of* $k[Z]$*).*

(The equivalence of the last pair follows from the fact that a ring is reduced iff any of its localizations at a set of non-zero divisors thereof is reduced.)

What if we now allow V to be a general k-variety (not necessarily affine) and Z to be a k-closed subvariety? Let U be k-open in V, and put $k[Z \cap U]$ for the restriction to U of $k[Z]$. Then we get the ring of *rational functions on* Z *defined over* k by forming

$$k(Z) := \varinjlim_{\{U : Z \cap U \text{ dense in } Z\}} k[Z \cap U]$$

and it can be shown from this, that just as in the affine case, Z is defined over k iff $\mathbb{E} \otimes_k k(Z)$ is reduced. It is not hard to see that $k(Z)$ is a finite direct sum of finitely generated field extensions of k; by standard arguments from field theory [Bor91, AG2.2], we get the following, which proves the assertion [2.1.0.1].

Theorem 2.4.0.2 *The following are equivalent.*

(a) Z *is defined over* k*.*

(b) $\mathbb{E} \otimes_k k(Z)$ *is reduced.*

(c) $k^i \otimes_k k(Z)$ *is reduced; and*

(d) Each direct summand of $k(Z)$ *is separable over* k*.*

2.5 Components and separable points

For a ring A (recall the conventions in force), we write D_A for the set of zero divisors of A (including zero), and nil A for the nilradical of A (namely the radical of the ideal (0) as at [1.1]). We recall a couple of standard facts, as the argument in [Bor91, AG12.3] is slightly incomplete.

Lemma 2.5.0.1

(i) D_A *is a union of prime ideals and contains* nil A*.*

(ii) nil A *is the intersection of all prime ideals of* A*, and consists of the nilpotent elements of* A.

(iii) If $D_A = \text{nil}\, A$*, then* D_A *is the unique minimal prime ideal of* A.

Proposition 2.5.0.2 *[Ja64, IV,§11,Theorem 24]*

Let A*,* B *and* F *be subfields of* $\mathbb{E}$*, with* $B \subseteq A \cap F$*, and* B *separably closed in* A *(*viz. $B^s \cap A = B$*). Write* $S = A \otimes_B F$*. Then* $D_S = \text{nil}\, S$.

Corollary 2.5.0.3 *Let* C *be a* B*-subalgebra of* $\mathbb{E}$ *whose field of fractions is* F*. Write* $R = A \otimes_B C$*. Then* D_R *is the unique minimal prime ideal of* R.

Proof: Clearly $B \subseteq C$. Since we have an embedding of C into F, and A is a flat B-module, there is an embedding $f : R \longrightarrow S$, and so $f(D_R) \subseteq D_S$. The result follows by the theorem. □

We now verify that

Proposition 2.5.0.4 *The irreducible components of a* k*-variety* V *are defined over* k^s.

Proof: To prove our result, we can assume that $k = k^s$, and that V is affine (as it is enough to verify that it works on each member of a cover of V by k-open affine subvarieties). Otherwise expressed, we need to show that if $P_1, \ldots, P_r$ are the minimal primes of $k[V]$, then $P_i \cdot \mathbb{E}[V]$ is prime in $\mathbb{E}[V]$. By [2.5.0.3], $A_i := \mathbb{E}[V]/P_i \cdot \mathbb{E}[V]$ (which is exactly $\mathbb{E} \otimes_k (k[V]/P_i)$) has a unique minimal prime, so it only remains to verify that A_i is reduced. As $k[V]$ is reduced, we have $k[V] \subseteq \oplus_i (k[V]/P_i)$: both have the same full ring of fractions $k(V)$. But as $\mathbb{E}(V) = k(V) \otimes_k \mathbb{E}$ is reduced, it follows that A_i is reduced, and therefore a domain, as required. □

Now let V be an affine k-variety: the Nullstellensatz [1.1.0.1] shows that we have bijections

$$V \leftrightarrow \text{Hom}_{\mathbb{E}-alg}(\mathbb{E}[V], \mathbb{E}) \leftrightarrow \text{Hom}_{k-alg}(k[V], \mathbb{E})$$

Note that the first of these bijections matches points of V with evaluations thereat:- $x \leftrightarrow (f \mapsto f(x))$. The second holds because the well-known 'tensor product-Hom' adjunction verifiably preserves algebra structures and not just module structures. For any k-algebra B, write $V(B) = \mathrm{Hom}_{k-alg}(k[V], B)$; if B has a k-structure B_k, then $V(B_k)$ is just the subset of $V(B)$ corresponding to the k-algebra morphisms which are defined over k. Points of $V(B)$ are called *B-rational*, if $k \subseteq B \subseteq \mathbb{E}$. In particular $V(k) \subseteq V(k^s) \subseteq V(k^a) \subseteq V$. Elements of $V(k^s)$ are called *separable*. Thus V can be regarded as a representable functor from $\mathbb{E}$-algebras with k-structure to the category **Set**. Indeed, the construction is functorial in V also in a sense one can make precise. We will usually only be concerned with k-algebras which are contained in $\mathbb{E}$; there are however circumstances (such as when studying isogenies of algebraic groups [3.1.0.2]) in which one needs the more general concept.

The above can be generalized *mutatis mutandis* to general k-varieties.

Theorem 2.5.0.5 *[Bor91, AG13.2-13.3] Let $g : V \longrightarrow W$ be a dominant separable k-morphism. Then there is an open dense W_0 in W, $W_0 \subseteq g(V)$, such that for each $x \in W_0(k^s)$, the fibre $g^{-1}(x)$ has a dense set of separable points. Hence $V(k^s)$ is dense in V (take W to be a single point).*

2.6 Galois-theoretic criteria for rationality

Let V be a k-variety and write Γ for the *absolute Galois group* $Gal(k^s/k)$ of k. An action of Γ on V is given thus: we will suppose that V is affine, as $U(k^s)$ will be stabilised for each k-open affine U in V, and so can identify $V(k^s)$ with $\mathrm{Hom}_{k^s-alg}(k^s[V], k^s)$ by the usual evaluation $x \leftrightarrow (e_x : f \mapsto f(x))$. Moreover, Γ clearly acts on $k^s[V] = k^s \otimes_k k[V]$ through the first factor, and we will denote this action by $f \mapsto \sigma_f$ for $\sigma \in \Gamma$. For $x \in V(k^s)$ and $\sigma \in \Gamma$, $\sigma(x)$ is defined by $e_{\sigma(x)} = \sigma \circ e_x \circ \sigma^{-1}$. In terms of the action on $k^s[V]$, one can rewrite this as $\sigma_f(x) = \sigma(f(\sigma^{-1}(x)))$. Writing $V(f)$ for the subvariety of V given by the condition $\{x \in V | f(x) = 0\}$, we see that each σ induces a bijection between the separable points of $V(f)$ and $V({}^\sigma f)$, and similarly, for any ideal $J \lhd k^s[V]$, enabling definition of

the notion of the *conjugate variety* W^σ of any (closed) k^s-subvariety of V. It can be shown that each such $\sigma \in \Gamma$ can be extended to a k^s-isomorphism of varieties $\phi_\sigma : W \longrightarrow W^\sigma$.

More generally, given a k^s-variety V and an automorphism σ of k^s, σ can be extended to an isomorphism $\phi_\sigma : V \longrightarrow V^\sigma$, where V^σ is obtained by 'patching together' k^s-open affine subsets. In the affine case, this amounts to applying σ to the coefficients of the polynomials defining V over k^s.

Next, let $\alpha : V \longrightarrow W$ be a k^s-morphism of k-varieties. Then for each $\sigma \in \Gamma$, one defines a k^s-morphism ${}^\sigma\alpha(x) = \sigma(\alpha(\sigma^{-1}(x)))$ for each $x \in V(k^s)$. While there obviously cannot be more than one ${}^\sigma\alpha$ with this property, its existence must be settled explicitly. To do this, it suffices to exhibit a comorphism $({}^\sigma\alpha)^* : k^s[W'] \longrightarrow k^s[V']$ for each pair $V' \subseteq_{o,k} V$ and $W' \subseteq_{o,k} W$ such that $\alpha(V') \subseteq W'$. But we already have $\alpha^* : k^s[W'] \longrightarrow k^s[V']$, so need only form $\sigma^{-1} \circ \alpha^* \circ \sigma$. This gives an action of Γ on $\mathrm{Hom}_{\mathbb{E}-var}(V, W)_{k^s}$.

Theorem 2.6.0.1 *For the k^s-morphism $\alpha : V \longrightarrow W$ of k-varieties V, W, the following conditions are equivalent.*

(1) α is defined over k;

(2) $\alpha : V(k^s) \longrightarrow W(k^s)$ is Γ-equivariant; and

(3) $\alpha \in \mathrm{Hom}_{\mathbb{E}-var}(V, W)^\Gamma_{k^s}$.

Theorem 2.6.0.2 *Let Z be a closed subvariety of V. The following are equivalent.*

(1) Z is defined over k.

(2) Z is defined over k^s and $Z(k^s)$ is Γ-stable.

(3) There exists a subset $E \subseteq Z \cap V(k^s)$ such that E is Γ-stable and dense in Z.

Proposition 2.6.0.3 *If $\alpha : V \longrightarrow W$ is a k-morphism, then $\alpha(V)$ is defined over k (we are not asserting that it is closed, of course).*

Proof: Since $V(k^s)$ is dense in V, $\alpha(V(k^s))$ is dense in the closure of $\alpha(V)$, and so one can apply criterion (3) of the last result. □

2.7 Unirationality

An irreducible k-variety V is said to be *k-unirational* if there is an injective field map $k(V) \longrightarrow L$ for some field L, where L/k is a finitely generated purely transcendental extension.

Proposition 2.7.0.1 *[Bor91, AG13.7] If V is k-unirational and k is infinite, then $V(k)$ is dense in V.*

2.8 Weil restriction

Suppose we have fields $k^s \supseteq l \supseteq k$ with $[l : k] = d$. Then there is a mapping $R_{l/k}$ called 'Weil restriction' which takes l-varieties to k-varieties; indeed $R_{l/k}$ is a functor right adjoint to the obvious 'base extension functor' in appropriate categories [DG70, I,1,6.6]. We will only be concerned with affine varieties here. Let Γ be as before, and put $\Gamma_l = Gal(k^s/l)$; take $\sigma_1, \ldots, \sigma_d$ as a set of (left) coset representatives of Γ_l in Γ.

Now we define $R_{l/k}(W)$ (for an affine l-variety W) to be a pair (V, p), where V is a k-variety, p is a surjective (regular) l-morphism $V \longrightarrow W$, and the map $f := p^{\sigma_1} \times \cdots \times p^{\sigma_d} : V \longrightarrow W^{\sigma_1} \times \cdots \times W^{\sigma_d}$ is a k^s-isomorphism of varieties. Clearly $R_{l/k}$ multiplies dimensions by d. It is instructive to see how one verifies the existence of $R_{l/k}$, as some rationality information is obtained as a by-product of the working. An example of the whole construction will follow at the end.

Proposition 2.8.0.1 *[Sa71, I §3.3] For every affine l-variety W, there exists $R_{l/k}(W)$, defined as above, which is unique up to k-isomorphism.*

Proof: This is achieved in three stages: the affine line, products of pairs for which the result is already known, and subvarieties of those for which it is already known. Suppose firstly that $W = \mathbb{A}^1$, and $u_1, \ldots, u_d$ is a k-module basis for l, take $V = \mathbb{A}^d$, and $p : \mathbb{A}^d \longrightarrow \mathbb{A}^1$ given by $p(w_1, \ldots, w_d) = \sum_{i=1}^{i=d} w_i u_i$; then obviously p is defined over l, and $p^{\sigma_j}(w_1, \ldots, w_d) = \sum_{i=1}^{i=d} w_i u_i^{\sigma_j}$. Then f (as above) is a polynomial map from $\mathbb{A}^d$ to itself with matrix $(u_i^{\sigma_j})$; this matrix is invertible, as l/k is separable, and this case is done.

Secondly, we consider the product of two affine l-varieties W_1, W_2 for which $R_{l/k}(W_1)$ and $R_{l/k}(W_2)$ are known to exist; but that $R_{l/k}(W_1 \times W_2)$ exists and is k-isomorphic to $R_{l/k}(W_1) \times R_{l/k}(W_2)$ is obvious from the adduced adjunction.

Thirdly, given that $R_{l/k}(W)$ exists, and that Y is an l-subvariety of W, one verifies that $R_{l/k}(Y)$ exists thus: as $B = Y^{\sigma_1} \times \cdots \times Y^{\sigma_d}$ is a subvariety of $W^{\sigma_1} \times \cdots \times W^{\sigma_d}$, it follows that $C := f^{-1}(B)$ is a subvariety of $R_{l/k}(W)$. To show that $R_{l/k}(Y) = (C, p|_C)$, it remains only to show that C is defined over k. As B is clearly defined over the Galois hull (normal closure) of l/k, and f is defined over k^s, we have that C is defined over k^s. Now we can use Galois theory: recall the notion of conjugate variety, and that any automorphism σ of k^s induces a k^s-isomorphism ϕ_σ from an affine k^s-variety V to the affine k^s-variety V^σ. We observe too that $(f^{-1})^\sigma = f^{-1} \circ \phi_\sigma^{-1}$. For $\sigma \in \Gamma$, $C^\sigma = (f^{-1})^\sigma(B^\sigma)$, and $(f^{-1})^\sigma = f^{-1} \circ \phi_\sigma^{-1}$; applying this to B^σ gives $f^{-1}(B)$, by definition of ϕ_σ, and so $C^\sigma = C$. This concludes the proof of the existence of $R_{l/k}(W)$ for any affine l-variety W. The uniqueness follows from an obvious universal property [Sa71, I §3.2]. □

Proposition 2.8.0.2

(1) For $(V, p) = R_{l/k}(W)$, p induces a bijection from $V(k)$ to $W(l)$.

(2) If W is irreducible, so is V.

(3) If W is an algebraic group over l, then V is an algebraic group over k. (For the theory of algebraic groups, see [3.1]).

Proof: We prove (1). Clearly $p(V(k)) \subseteq W(l)$ since p is defined over l. For $y \in W(l)$, $x := R_{l/k}(\{y\}) \in V(k)$ and $p(x) = y$ so there is a surjection onto $W(l)$. On the other hand, x is determined by the conditions $x \in V(k)$ and $p(x) = y$, so $p|_{V(k)}$ is also injective. □

We wish to generalize the bijection in (1) of the last proposition to get information about the m-rational points of V, for a finite separable extension m of k. To this end, note firstly that the set $\Sigma := \{k\text{-embeddings of } l \text{ in } k^s\}$ has cardinality d, and there is an action on Σ by the absolute Galois group $\Gamma_m = Gal(k^s/m)$, by $\sigma.x \mapsto \sigma x$. If Σ_m denotes the set of orbits of this mapping, then one can show that V is m-isomorphic to

$\prod_{\alpha\in\Sigma_m} R_{l^\alpha m/m}(W^\alpha)$, where the notation ought to be clear. We record some special cases of this.

In particular if l/k is Galois, then $l^\alpha = l$ and $W^\alpha = W$ for each α - then V is m-isomorphic to $R_{lm/m}(W^{\#\Sigma_m})$ using the adjunction again, and consequently one has a bijection $V(m) \leftrightarrow W^{\#\Sigma_m}(lm)$, and indeed, $\#\Sigma_m$ must be the same as $[l:k]/[lm:m]$.

Proposition 2.8.0.3 *Suppose (with the above notation), we have* $k = \mathbb{F}_q$, $l = \mathbb{F}_{q^a}$, $m = \mathbb{F}_{q^b}$. *Then*

$$\#V(\mathbb{F}_{q^b}) = \#W^{(a,b)}(\mathbb{F}_{q^{lcm(a,b)}}).$$

Proof: It is a standard fact about finite fields that the compositum $\mathbb{F}_{q^a}\mathbb{F}_{q^b}$ is $\mathbb{F}_{q^{lcm(a,b)}}$ - and hence in this case $\#\Sigma_m = (a,b)$, the greatest common divisor of a and b. □

Example: Take l to be a quadratic extension of $k = \mathbb{Q}$, say $l = \mathbb{Q}(\alpha)$ so that $\{1, \alpha\}$ is a $\mathbb{Q}$-basis for l. The variety SL_2 can be regarded as defined over l (and indeed over $\mathbb{Q}$, though we will ignore this), as the vanishing of the (prime) ideal $I = (WZ - YX - 1) \lhd \mathbb{C}[W, X, Y, Z]$; the corresponding algebra clearly has an l-structure. We will show how to construct the underlying $\mathbb{Q}$-variety of $R_{l/\mathbb{Q}}(SL_2)$, though will ignore the algebraic group structure.

With the decomposition $\Gamma = Gal(\mathbb{Q}^s/\mathbb{Q}) = \coprod_i \Gamma_l \beta_i$ where $\Gamma_l = Gal(\mathbb{Q}^s/l)$, β_1 the identity of Γ, and $\beta_2(\alpha) = -\alpha$, we proceed by analogy with the proof of the existence of $R_{l/k}$ in the general situation [2.8.0.1].

We begin with the ambient spaces, and use the notations above. Define $p : \mathbb{A}^8 \longrightarrow \mathbb{A}^4$ by $(x_1, \ldots, x_8) \mapsto (x_1, \ldots, x_4) + \alpha(x_5, \ldots, x_8)$; if we are to have $(\mathbb{A}^8, p)$ as $R_{l/\mathbb{Q}}(\mathbb{A}^4)$, then we must have that the map $f : \mathbb{A}^8 \longrightarrow \mathbb{A}^4 \times (\mathbb{A}^4)^{\beta_2}$ given by

$$f(x_1, \ldots, x_8) \mapsto ((x_1, \ldots, x_4) + \alpha(x_5, \ldots, x_8), (x_1, \ldots, x_4) - \alpha(x_5, \ldots, x_8))$$

must be a $\mathbb{Q}^s$-isomorphism of varieties: but this is so, as f is a $\mathbb{Q}^s$-linear map with invertible matrix. This parallels the first stage of [2.8.0.1] - the rest of this example parallels the third stage.

Now we look at the variety SL_2 itself. Note that if SL_2 is defined by the vanishing of $(WZ - YX - 1)$, then $(SL_2)^{\beta_2}$ is the vanishing of $(W'Z' - Y'X' - 1)$ (say) where these are names we give to the second quadruple of coordinates. Putting $B = \{(W, X, Y, Z, W', X', Y', Z') : WZ - YX = 1 = W'Z' - Y'X'\}$ we see that B is obviously defined over l. Then we must have $R_{l/\mathbb{Q}}(SL_2) = f^{-1}(B)$, referring to the third stage of [2.8.0.1]. Explicitly, after some manipulations, we get that (up to a unique $\mathbb{Q}$-isomorphism) $R_{l/\mathbb{Q}}(SL_2) = (V, p|_V)$, where p is as before and

$$V = \{(x_1, \ldots, x_8) : x_1x_4 - x_2x_3 + \alpha^2(x_5x_8 - x_6x_7) = 1\}.$$

Chapter 3

Linear Algebraic Groups

3.1 General remarks

Let G be a *linear algebraic group defined over* k (or a *k-group*), k being a subfield of $\mathbb{E}$, and $\Gamma = Gal(k^s/k)$. This means that we have a quadruple (G, μ, i, ϵ) where G is an affine k-variety, and μ, i, ϵ are regular k-morphisms of k-varieties as follows:

(i) $\mu : G \times G \longrightarrow G$ - a 'product' map

(ii) $i : G \longrightarrow G$ - an 'inverse' map and

(iii) $\epsilon : * \longrightarrow G$ - a 'choice of identity', where $*$ is a one-point k-variety.

These are to satisfy the usual group axioms (for example, the right inverse axiom is expressible as $\mu \circ (1_G, i) = \epsilon \circ (* \longleftarrow G)$). The morphisms and conditions above can be equivalently recast as defining a Hopf algebra structure on $\mathbb{E}[G]$ (with appropriate k-structures), and this is the way to realise algebraic groups as representable functors (*viz.* as 'affine group schemes').

By a *subgroup* of a k-group we will always mean an $\mathbb{E}$-closed subgroup, though not necessarily one which is k-closed. [Any more general subgroup will be so described explicitly.] We say that the mapping $f : G \longrightarrow H$ is a *morphism* only if G and H are $\mathbb{E}$-groups, and that f is simultaneously a group homomorphism and a regular morphism of varieties: to say that f is *defined over* k (or is a *k-morphism*) has the obvious meaning and obliges G and H to be defined over k.

Proposition 3.1.0.1 *[Bor91, 1.4]*

For any k-morphism $f : G \longrightarrow H$, $\ker f$ is a k-closed subgroup of G and $f(G)$ a k-subgroup of H. Further, $\dim G = \dim \ker f + \dim f(G)$.

We will call a short exact sequence $1 \to A \xrightarrow{f} B \xrightarrow{g} C \to 1$ of k-groups a *k-sequence* if the groups and morphisms involved are all defined over k. Given this, we say that B is a *semidirect product* of A by C, written $B = A \rtimes C$ if there is also a morphism of algebraic groups σ with $g \circ \sigma = 1_C$ - however σ may fail to be defined over k even if everything else is. More generally, if $H_1, \ldots, H_r$ are connected subgroups of a connected group H, we say that H is *directly spanned* by the H_i if, for some ordering $i_1, \ldots, i_r$ of the H_i, the obvious product map $H_{i_1} \times \cdots \times H_{i_r} \longrightarrow H$ is an isomorphism of varieties.

An algebraic group over $\mathbb{E}$ is not usually a topological group (inverse images of open sets by μ, though Zariski open, need not be open in the product topology) :- indeed, it is a standard result [Hi74, II,§5,Prop.3] that a T_1 topological group is T_2, and G is clearly T_1 with respect to the $\mathbb{E}$-topology, but not T_2 unless of dimension 0. [Recall that T_2 means 'Hausdorff' and T_1 means 'all points are closed'] The k-group G fails to be a topological group with respect to the k-topology too, at least if it is irreducible (the inverse image of the identity under μ is k-closed but not product-closed).

The morphism $f : G \longrightarrow H$ will be called an *isogeny* if G is connected, f is surjective and $\ker f$ is finite (and therefore central in G). f is called *central* if one also has, for each k-algebra A, that the induced group homomorphism

$$f_A : \hom_{k-alg}(k[G], A) \longrightarrow \hom_{k-alg}(k[H], A)$$

has a central kernel. (*Sat sapienti:* Note the appearance of scheme-theoretic ideas here.) Then we say that two connected groups G_1 and G_2 are *strictly isogenous* or *strictly F-isogenous* (which we write as $G_1 \sim_F G_2$) if there exist a connected group H and central isogenies $f_i : H \longrightarrow G_i$ for $i = 1, 2$ where F is any common field of definition for the f_i. This is an equivalence relation (to verify transitivity form the obvious pullback square). Note that several notions of isogeny appear in the literature.

Proposition 3.1.0.2 *[Bor91, 22.11,22.3,AG18.2]*

Let $f : G \longrightarrow H$ be an isogeny.

(1) f is central iff there is a morphism of varieties $\kappa : f(G) \times f(G) \longrightarrow G$ *such that $\kappa \circ (f \times f) : G \times G \longrightarrow G$ coincides with the commutator map $(x, y) \mapsto xyx^{-1}y^{-1}$.*

(2) If f is separable, it is central.

(3) The separable degree of the (finite) field extension $\mathbb{E}(H)/\mathbb{E}(G)$ is exactly $\#\ker f$.

It turns out that the irreducible and connected components of G coincide, and are the cosets of a certain normal subgroup G^0, called the *identity component of G*. We write $\#G$ for the number of components: this of course coincides with the cardinality when this latter is finite. Though we will also use notation such as $\#G(k)$ (*cf.* the discussion preceding [2.5.0.5]) for the number of k-rational points of a k-group G, there ought to be no confusion as all references are to finite quantities. G^0 is itself a k-group, although the other components need not be k-varieties. It is true, however, that

Proposition 3.1.0.3 *There is a finite separable extension L of k such that the components of G are defined over L and pairwise L-isomorphic as varieties.*

Proof: Choose an L such that each component has an L-rational point. Clearly, each point of G is rational over some finitely generated extension of k: but by density of separable points [2.5.0.5], one can choose a k^s-rational one in each component. Then the L-isomorphisms mentioned are composites of left translations by such points and their (group) inverses. □

By an *action of G on a (non-empty) k-variety V*, we mean of course that V is a G-set in the usual sense, and that the 'action map' $\alpha : G \times V \longrightarrow V$ is a regular morphism of varieties: to say that it is *k-morphic* has the obvious meaning. For a closed subset M of V, we define the *normalizer of M in G* to be

$$\mathcal{N}_G(M) := \{g \in G | gM \subseteq M\}$$

and the corresponding *centralizer*

$$\mathcal{Z}_G(M) := \cap_{x \in M} \mathcal{N}_G(\{x\}).$$

Both of these are closed submonoids of G and the latter is even a subgroup: the notions have the expected meaning when $V = G$ and α is 'action by conjugation' thereon. In the latter case, we write $Z(G)$ for the centre $\mathcal{Z}_G(G)$ of G. If G acts (in the above sense) on both V and W, a morphism $\phi : V \longrightarrow W$ is said to be *G-equivariant* if one has $\phi(g.x) = g.\phi(x)$ $\forall x \in V$, $\forall g \in G$. An important technical result is the following 'closed orbit lemma' [Bor91, 1.8].

Proposition 3.1.0.4 *For the action $\alpha : G \times V \longrightarrow V$, with ($G$ and) V defined over k, the orbits are locally closed (in V) smooth subvarieties of V, whose boundaries are orbits of strictly lower dimension.*

In particular, orbits of least dimension are closed, and G is itself a smooth variety.

A principal result is, for each G, the existence of a k-isomorphism to some k-subgroup of $GL_n(\mathbb{E})$ for some n (this being one reason to suppose $\mathbb{E}$ sufficiently large). More exactly, we can express this by supposing that there is a separable k-morphism which is a bijection from $G(k^s)$ to the separable points of the image. This 'concrete' realization of G is sometimes useful.

We say that G is *solvable (nilpotent)* if this is true of the abstract group G: it turns out [Bor91, 2.3] that the commutator subgroups appearing in the derived series (descending central series) for G are closed, and indeed are defined over k. After a couple of sections outlining some needed constructions, we discuss the classification of algebraic groups.

3.2 Some constructions

3.2.1 Quotients

A k-morphism $\pi : V \longrightarrow W$ (of varieties) is called a *quotient* (or *g-quotient* with 'g-' for geometric) morphism (over k) if

(1) π is surjective and open; and

(2) For any $U \subseteq_o V$, the comorphism π^* induces an isomorphism from $\mathbb{E}[\pi(U)]$ onto the set $\{f \in \mathbb{E}[U] : f \text{ constant on fibres of } \pi|_U\}$.

Next, suppose that a k-group G acts morphically on a k-variety V: an *orbit map* is then a surjective morphism $\pi : V \longrightarrow W$ of varieties whose fibres are the orbits of G in V. Then a *g-quotient of V by G over k* is such an orbit map which is also a g-quotient morphism in the previous sense. The condition is stronger than that of (categorical) quotient. In particular, a necessary condition for the existence of a g-quotient of V by G over k is that all orbits must have the same dimension (and so are closed in G [3.1.0.4]). Clearly also, a g-quotient is unique up to a unique k-isomorphism, so we are justified in using notation like V/G or $G\backslash V$. As we will not be concerned with quotients in any other sense than that just described, we drop the qualifying 'g-'.

Proposition 3.2.1.1 *[Bor91, 6.8] Let H be a k-subgroup of the k-group G. Then the quotient $\pi : G \longrightarrow G/H$ exists over k, and G/H is a smooth quasi-projective variety. If, further, H is normal in G, then G/H is a k-group and π a k-group k-morphism.*

It is not usually true that the existence of a quotient over k implies that the obvious map of k-rational points is surjective.

3.2.2 Lie algebras and the adjoint representation

For each $x \in G$, one has the $k(x)$-automorphisms of the (variety) G given by $y \mapsto x.y$ and $y \mapsto y.x^{-1}$, called *left translation* and *right translation* respectively. We will denote their comorphisms respectively by λ_x and ρ_x.

We define the *Lie algebra of G*, denoted $\mathfrak{g}$ or $\mathcal{L}(G)$, to be the $\mathbb{E}$-vector space $\mathfrak{g}$ of left-invariant $\mathbb{E}$-derivations of $\mathbb{E}[G]$, with bracket operation $[D_1, D_2] := D_1D_2 - D_2D_1$. Thus one has

$$\mathfrak{g} = \{\beta \in Der_{\mathbb{E}}(\mathbb{E}[G], \mathbb{E}[G]) \mid \beta \circ \lambda_x = \lambda_x \circ \beta \ \forall x \in G\}$$

This is a 'restricted Lie algebra' in the sense of Jacobson [Bor91, 3.1] with 'p^{th}-power' as p-operation, and it can be shown that $\mathfrak{g}$ has a natural k-structure induced by that of G. Further $\dim \mathfrak{g} = \dim G$, and each L-morphism $f : G_1 \longrightarrow G_2$ of k-groups induces a corresponding L-Lie algebra homomorphism $\mathfrak{f} : \mathfrak{g}_1 \longrightarrow \mathfrak{g}_2$ of the (k-structures on the) Lie algebras.

For each $x \in G$, we have the inner automorphism $Int(x)$ of G, given by conjugation by x; the differential of this is called $Ad(x)$, and we get a map $Ad : G \longrightarrow GL(\mathfrak{g})$, the *adjoint representation* of G; clearly the image of Ad consists of Lie algebra automorphisms, and in fact Ad is a k-morphism of k-groups [Bor91, 3.13]. Note that this also gives us, for every k-subgroup H of G, a k-action (in the sense above) of H on $\mathfrak{g}$.

3.2.3 Jordan decomposition

It is well known that each $x \in GL_n(\mathbb{E})$ is uniquely expressible in the form $x = x_s x_u = x_u x_s$ where x_s is 'semisimple' (*viz.* is conjugate to a diagonal matrix in $GL_n(\mathbb{E})$) and x_u is 'unipotent' (*viz.* has all of its eigenvalues equal to 1). Further, one shows that any (closed) subgroup H of $GL_n(\mathbb{E})$ containing x also contains x_s and x_u. We can extend the definition to a general $\mathbb{E}$-vector space V, at least for those endomorphisms f of V which are 'locally finite' (meaning that V is expressible as a union of finite-dimensional f-stable subspaces). If W is such a subspace, we write $f|_W = (f|_W)_s(f|_W)_u$ and this gives a well-defined decomposition of f. Moreover if a subspace U of V (not necessarily finite-dimensional) is f-stable, then it is f_s-stable and f_u-stable too.

One wishes to do this as it transpires that the $\mathbb{E}$-vector space $\mathbb{E}[G]$ has the property of being a union of finite-dimensional subspaces which are not only defined over k, but are ρ_x-stable for every $x \in G$ (*viz.* the same subspace decomposition works for every x.) Hence we have $\rho_x = (\rho_x)_s(\rho_x)_u$ for each $x \in G$: as each of these factors is a (vector space) automorphism of $\mathbb{E}[G]$, provided we know that they also preserve multiplication (which follows from the commutation of Jordan decomposition with tensor product [Bor91, 4.3]) the assignment $f \mapsto (\rho_x)_s f(1)$ defines an $\mathbb{E}$-algebra homomorphism $\mathbb{E}[G] \to \mathbb{E}$, and so an $x_s \in G$ by [1.1.0.1]; similarly we get an $x_u \in G$.

One verifies that these commute, and that $(\rho_x)_s = \rho_{(x_s)}$, and similarly for x_u. Further, this decomposition is preserved by morphisms, so it really is intrinsic, and coincides in matrix groups with that described before. The obvious rationality question is answered [Bor91, 4.2] by a statement that if $x \in G(L)$ for some field L, then both x_s and x_u are in $G(L^i)$. There are intrinsically defined subsets G_s and G_u in G, namely the subsets $\{x \in G | x = x_s\}$ and $\{x \in G | x = x_u\}$ respectively, though they are not usually subgroups and G_s need not be closed.

3.3 Some standard groups

3.3.1 Connected one-dimensional groups

The following turn out to be the only connected groups of dimension 1, up to k^a-isomorphism [Bor91, 10.9]: the *additive group* $\mathbb{G}_a$ of $\mathbb{E}$, and the *multiplicative group* $\mathbb{G}_m$, or $\mathbb{E}^*$. Clearly these are realised over the prime field and abelian. One also has $\mathbb{G}_m \cong \mathrm{Aut}_{Alg.Gp.}(\mathbb{G}_a)$, acting by multiplication.

A *character* of a k-group G is a morphism from G to $\mathbb{G}_m$.

Proposition 3.3.1.1 *[Ros57, Prop.3] Let $f : G \longrightarrow \mathbb{G}_m$ be a regular morphism of varieties, where G is a connected k-group and $f(e_G) = 1$. Then f is a character of G.*

3.3.2 Unipotent groups

G is called *unipotent* if $G = G_u$ (G_u as above). Unipotent groups are nilpotent [Bor91, 4.8], and have no non-zero characters. For $p = 1$ they are connected, and for $p > 1$ all elements are p-torsion. Good examples are the group U_n of $n \times n$ upper triangular matrices in $GL_n(\mathbb{E})$ having ones on the diagonal, or closed subgroups thereof. The Lie-Kolchin theorem [Bor91, 10.5] shows that every connected example is of this form.

3.3.3 Tori

The k-group S is a *torus* if it is isomorphic to $\mathbb{G}_m^r$ for some r (equivalently, $G = G_s$ and is connected). The set of characters of S (*viz.* the *character module of* S), will be denoted

$X(S)$ or just X. Connected subgroups of tori are also tori, and indeed are direct factors [Bor91, 8.5].

We now describe the ring of (algebraic group) endomorphisms of a standard torus.

Proposition 3.3.3.1

There is a ring isomorphism $M_n(\mathbb{Z}) \cong \mathrm{Hom}_{Alg.Gp.}(\mathbb{G}_m^n, \mathbb{G}_m^n)$ *where* $M_n(\mathbb{Z})$ *denotes the* $n \times n$ *integer matrices. The isomorphism is given by sending the matrix* $M = (m_{ij})$ *to the mapping* $M : \mathbb{G}_m^n \longrightarrow \mathbb{G}_m^n$ *which takes* $(x_1, x_2, \ldots, x_n)$ *to* $(\prod_i x_i^{m_{1i}}, \prod_i x_i^{m_{2i}}, \ldots, \prod_i x_i^{m_{ni}})$.

Of course, this gives the underlying abelian group of $\mathbb{G}_m^n$ a structure of $M_n(\mathbb{Z})$-module. This will be useful later, though we will write the action additively - thus $\mathbf{0}$ will mean the element $(1, 1, \ldots, 1)$ of $\mathbb{G}_m^n$.

Actions of tori on $\mathbb{E}$-vector spaces (*viz.* finite-dimensional representations of tori) are *diagonable*, in the sense that if we have $\theta : S \longrightarrow GL(V)$ (this of course to be a morphism), then $\theta(S)$ can be conjugated into a diagonal subgroup of $GL(V)$ (with respect to some basis for V), and we therefore have

$$V = \oplus_{\alpha \in X} \mathfrak{g}_\alpha \text{ where } \mathfrak{g}_\alpha = \{x \in V : \alpha(t)x = \theta(t).x \ \forall t \in S\};$$

the $\alpha \in X$ for which $\mathfrak{g}_\alpha \neq 0$ are called the *weights of* S *in* V. The nonzero weights are called the *roots of* S *in* V. Note in particular the case where S acts on a group G (usually $S \leq G$ and by conjugation) and so on $\mathfrak{g}$ *via* the adjoint representation. The resulting weights (roots) are called the *weights (roots) of* S *in* G. This set of roots will be denoted $\Phi(S, G)$: these will play a critical role in what follows, as in the whole theory. The space $\mathfrak{g}_0$ will be denoted $\mathfrak{g}^S$ and called the *infinitesimal centralizer of* S *in* $\mathfrak{g}$. $\mathfrak{g}^S$ is a Lie subalgebra of $\mathfrak{g}$: the root spaces $\mathfrak{g}_\alpha$ need not be subalgebras, though they often will be. A result we need is the correspondence of global and infinitesimal centralizers of tori.

Proposition 3.3.3.2 *[Bor91, 9.2]*

Let G *be a* k*-group, and* S *a* k*-torus acting thereon. Then* $\mathfrak{g}^S = \mathcal{L}(\mathcal{Z}_G(S))$.

A *cocharacter* (or multiplicative one-parameter subgroup) is of course a morphism in the opposite direction. The set of these (the *cocharacter module*) will be denoted $X^*(S)$ or just X^*.

We define the following operations: for $\chi_1, \chi_2 \in X$ and $\alpha_1, \alpha_2 \in X^*$,

$$(\chi_1 + \chi_2)(x) := \chi_1(x)\chi_2(x) \text{ for } x \in T \text{ and } (\alpha_1 + \alpha_2)(y) := \alpha_1(y)\alpha_2(y) \text{ for } y \in \mathbb{G}_m.$$

X and X^* are free abelian groups of rank equal to the dimension of S [Bor91, 8.6], and indeed are shown to be in duality by the following construction: if $\chi \in X$ and $\alpha \in X^*$ then $\chi \circ \alpha \in \hom_{Alg.Gp.}(\mathbb{G}_m, \mathbb{G}_m)$ so $\chi \circ \alpha : \mathbb{G}_m \longrightarrow \mathbb{G}_m$ is the map $x \mapsto x^n$ for some $n \in \mathbb{Z}$ [3.3.1]. This gives a surjective homomorphism of abelian groups $X \times X^* \longrightarrow \mathbb{Z}$,which we will write as $(\alpha, \lambda) \mapsto <\alpha, \lambda>$.

Consider now subtori of the group G. An important property of these is their 'rigidity' [Bor91, 8.10], *viz.* that if S is a subtorus of G, then $\mathcal{N}_G(S)^0 = \mathcal{Z}_G(S)^0$: in other words, S has 'few' non-trivial automorphisms. The finite group $\mathcal{N}_G(S)/\mathcal{Z}_G(S)$ is the *Weyl group of G with respect to S*. For S maximal, we just call it the *Weyl group W of G*. Weyl groups are Coxeter groups (are generated by finitely many involutions). All maximal tori of G are conjugate, and this shows that W is independent (up to algebraic group isomorphism) of the choice of maximal torus. One gets a different geometric interpretation of the Weyl group by introducing the notion of a root system [4.1].

For the next result, recall that p is the characteristic exponent of k.

Proposition 3.3.3.3 *[Bor91, 8.12,8.5]*
There is an antiequivalence of categories between k-tori (and k-morphisms thereof) and finitely generated free abelian groups which are p-torsion-free Γ-modules (where Γ acts continuously via *the Krull and discrete topologies).*

The last result will be refined in [4.3.0.2].

3.3.4 Connected solvable groups and the Borel fixed point theorem

Let H be connected, solvable and defined over k.

Proposition 3.3.4.1 *[Bor91, 10.6]*
(i) H_u is a k-closed connected normal subgroup of H which contains $H' = (H, H)$.

(ii) H/H_u is a k-closed torus, and indeed $H \cong_{k^a} H_u \rtimes T$ for any maximal torus T.
(iii) All maximal tori of H are conjugate, and the Weyl group of H is trivial.

We now come to the principal theorem in the theory of algebraic groups.

Theorem 3.3.4.2 (Borel fixed point theorem) *[Bor91, 10.4] Suppose the connected solvable k-group H acts k-morphically on a complete k-variety V, with V nonempty. Then the action has a fixed point.*

We will not make use of the theorem explicitly, but a general algebraic k-group H is studied *via* its maximal connected solvable subgroups (its *Borel subgroups*), such being necessarily closed.

3.4 Connected groups

We pass now to a general connected k-group G.

3.4.1 General remarks and the density theorem

We begin with some results collected from [Bor91, 11.1-4].

Proposition 3.4.1.1

(i) All Borel subgroups of G are conjugate, and G/B is a projective variety.
(ii) The maximal connected unipotent subgroups of G are the unipotent parts of Borel subgroups (and are therefore mutually conjugate).
(iii) The maximal tori of G are maximal tori of Borel subgroups (and are therefore mutually conjugate).
(iv) If an automorphism of G fixes a Borel subgroup, it fixes G.
(v) G has a maximal torus defined over k [Bor91, 18.2].

It is important to note that G may have no Borel subgroup defined over k [Ti66, Table II].

Proposition 3.4.1.2 (Density Theorem) *[Bor91, 11.10] Suppose B and T are respectively a Borel subgroup and a maximal torus of G, and write C for $\mathcal{Z}_G(T)^0$. Then C is*

nilpotent, and the union of the conjugates of B (respectively B_u, T, C) is G (respectively G_u, G_s, contains a dense open subset of G).

Corollary 3.4.1.3

(i) $\mathcal{Z}_B(B) = Z(G)$, and $Z(G)_s$ is the intersection of all of the maximal tori of G [Bor91, 11.11].

(ii) For any torus S in G, $\mathcal{Z}_G(S)$ is connected [Bor91, 11.12].

The centralizer of a maximal torus is called a *Cartan subgroup*. Its dimension is called the *rank of G*.

3.4.2 Parabolic subgroups

A *parabolic subgroup* of G is one such that G/P is complete. By [Bor91, 11.2], G/P is complete iff it is projective.

Theorem 3.4.2.1 *[Bor91, 11.16,11.17] Let P be a parabolic subgroup of G.*

(1) [Chevalley] P coincides with $\mathcal{N}_G(P)$ and is connected;

(2) For any Borel group B, there is a unique parabolic subgroup Q which is conjugate to P and contains B.

3.4.3 Effect of morphisms on Borel subgroups

Proposition 3.4.3.1 *[Bor91, 11.4] (For any connected group G.)*

(1) If $f : G \longrightarrow H$ is a surjective morphism, with $B = B_u \rtimes T$ Borel in G, then $f(B) = f(B)_u \rtimes f(T)$ is Borel in H, and every Borel subgroup of H is so obtained. Further, for any torus S of G, $f(\mathcal{Z}_G(S)) = \mathcal{Z}_H(f(S))$.

(2) If A is a connected subgroup of G, and B_0 is a Borel subgroup of A, then $B_0 = (A \cap B)^0$ for some B Borel in G; if, further A is normal in G, every Borel subgroup of A is so obtained. The analogous results for maximal tori, and for maximal connected unipotent subgroups also hold, mutatis mutandis.

Proposition 3.4.3.2 *[Bor91, 11.15] If G acts transitively on a variety D so that the isotropy groups of points of D are Borel in G, and S is a torus in G, then $\mathcal{Z}_G(S)$ stabilizes*

and acts transitively on each irreducible component of that subvariety of D consisting of the fixed points of S.

Further, if B is Borel in G,and $S \subseteq \mathcal{N}_G(B)$, then $\mathcal{Z}_B(S)$ is Borel in $\mathcal{Z}_G(S)$, and every Borel subgroup of $\mathcal{Z}_G(S)$ is so obtained.

The collection $\mathcal{B}$ of Borel subgroups of G can itself be given a structure of projective variety *via* the map ϕ described below. Fix any $C \in \mathcal{B}$, and let $\pi : G \longrightarrow G/C$ be the obvious quotient map. For each $g \in G$, put $x = \pi(g)$. Then the map $\phi : G/C \longrightarrow \mathcal{B}$ given by $\phi(x) = gCg^{-1}$ is a bijection by [3.4.2.1]. For any connected subgroup H of G, put $\mathcal{B}^H = \{C \in \mathcal{B} : C \supseteq H\}$: then this is the set of fixed points of H in $\mathcal{B}$ (or, of course in G/C) - $\mathcal{B}^H$ is nonempty iff H is solvable. We write $I(H) := (\cap_{B \in \mathcal{B}^H} B)^0$. Thus for a maximal torus T, $I(T) = I(T)_u \rtimes T$.

Recall the Weyl group $W = \mathcal{N}_G(T)/\mathcal{Z}_G(T)$ of G.

Proposition 3.4.3.3 *[Bor91, 11.19] Let B be Borel in, and T a maximal torus in, G.*
(1) W acts simply transitively on $\mathcal{B}^T$ (and so the latter is finite).
(2) $B \supseteq T$ iff $B \supseteq \mathcal{Z}_G(T)$.

Proposition 3.4.3.4 *[Bor91, 11.20] Let G and G' be two connected k-groups.*

If $\alpha : G' \longrightarrow G$ is a surjective morphism, with T' a maximal torus in G', and $\alpha(T') = T$, then T is maximal in G and surjective maps are induced $\mathcal{B}'^{T'} \longrightarrow \mathcal{B}^T$ and $W' \longrightarrow W$ where the notations W' and $\mathcal{B}'$ refer to corresponding quantities in G'. The second map is a morphism of abstract groups.

Further, if $\ker \alpha \subseteq B'$ $\forall B' \in \mathcal{B}'$, the latter two mappings are bijective.

3.4.4 The radical and unipotent radical

We define the *unipotent radical* $u(G)$ to be the maximal connected normal unipotent subgroup of G, and the *radical* $r(G)$ of G to be the maximal connected normal solvable subgroup of G. These notions are well-defined, and both are k-closed. We have

$$r(G) \cong_{k^a} u(G) \rtimes C$$

where C (which is also k-closed) is a maximal normal torus of G which rigidity shows central. One can alternatively characterise $r(G)$ as the identity component of the intersection of all Borel subgroups.

3.4.5 Reductive and semisimple groups

We saw above that for connected solvable H, $u(H) = H_u$. If G has positive dimension, it is called *reductive* if $u(G)$ is trivial and *semisimple* if $r(G)$ is trivial. The obvious quotients $G/u(G)$ and $G/r(G)$ are called the *reductification* and *semisimplification* of G and are k-closed. The rank of the latter quotient is the *semisimple rank* of G. Clearly if G is reductive, $r(G)$ coincides with $Z(G)^0$. If G has no infinite proper connected normal subgroup, it is called *almost simple*. We will say that G is *almost k-simple* if it has no infinite proper connected normal subgroup defined over k. We summarize this information.

Proposition 3.4.5.1

We have the following chain of implications among connected k-groups.

'Almost simple' *implies* 'almost k^i-simple' *implies* 'semisimple' *implies* 'reductive'.

3.4.6 Regular, semiregular and singular tori

Let S now be a subtorus of G, and T a maximal torus of G containing S. For any $s \in S$, we have $\dim \mathcal{Z}_G(\{s\}) \geq \operatorname{rank} G$: S is said to be *regular* if we can choose s such that we get equality here (in which case s is said to be a *regular element* of G). A general element $g \in G$ is called *regular* if g_s is. S is said to be *semiregular (singular)* if $\mathcal{B}^S$ is finite (infinite). We collect together a few salient properties. Recall the notations $I(T)$ for $(\cap_{B \in \mathcal{B}^T})^0 B$ and $\Phi(T, G)$ for the set of roots of T in G (*via* the adjoint representation [3.3.3]). For $\alpha \in \Phi(T, G)$, write $T_\alpha = (\ker \alpha)^0$, each of these having codimension one in T.

Proposition 3.4.6.1 *[Bor91, 12.2,13.1,13.2] Let S, T and G be as just introduced.*

(1) T is regular: indeed the regular elements of T form a dense open subset of T.

(2) Regular tori are semiregular.

(3) The following are equivalent.

(a) S is regular. (b) $\mathcal{Z}_G(S)$ is nilpotent.

(4) The following are equivalent.

(a) S is semiregular. (b) $\mathcal{Z}_G(S)$ is contained in $I(T)$. (c) $\mathcal{Z}_G(S)$ is solvable.

(5) The following are equivalent.

(a) S is singular. (b) $S \subseteq T_\alpha$ for some $\alpha \in \Phi(T,G)$. (c) $\mathcal{Z}_G(S) \not\subseteq I(T)$.

(6) For $\beta \in X(T)$, $\beta \in \Phi(T,G) \Leftrightarrow \mathcal{Z}_G((\ker\beta)^0)$ is not solvable.

3.4.7 Subtori of connected groups

The next results make a hypothesis of reductivity for a connected group tractable.

Theorem 3.4.7.1 *[Bor91, 13.16] If T is a maximal torus in G, then $I(T)_u = u(G)$.*

Corollary 3.4.7.2 *[Bor91, 13.17] Let S be a subtorus of T.*

(a) $u(\mathcal{Z}_G(S)) = \mathcal{Z}_{u(G)}(S)$.

(b) If S is semiregular then $\mathcal{Z}_G(S)_u$ coincides with the groups in (a).

(c) $\mathcal{Z}_G(T) = \mathcal{Z}_{u(G)}(T) \rtimes T$.

Corollary 3.4.7.3 *[Bor91, 13.17]*

Suppose further that G is reductive and that S is a subtorus of T.

(a) $\mathcal{Z}_G(S)$ is reductive.

(b) If S is semiregular, then $\mathcal{Z}_G(S) = T$, and in particular, S is regular.

(c) The Cartan subgroups of G are the maximal tori.

(d) The intersection of all the maximal tori of G is $Z(G)^0$.

Chapter 4

Roots, Reductivity and Rationality

In this chapter, we draw together the standard theory regarding the root system of a connected reductive group, and treat of rationality questions, including the classification theory for semisimple groups.

4.1 Root systems

We refer here to [Bor91, 14.7]. Let V be a finite-dimensional vector space over a subfield R of $\mathbb{R}$, with dual V^*. A *reflection with respect to a (nonzero)* $\alpha \in V$ is an $r \in GL(V)$ with $r(\alpha) = -\alpha$ which fixes pointwise a hyperplane. (Hence $r(x) = x - <x, \lambda> \alpha$, where $\lambda \in V^*$ with $<\alpha, \lambda> = 2$ and $\ker \lambda$ is the given hyperplane.) A *root system in* V is a finite spanning set Φ of nonzero elements of V such that for each $\alpha \in \Phi$ $\exists r_\alpha$, a reflection with respect to α which stabilizes Φ (this being so uniquely determined), and further, that for each $\alpha, \beta \in \Phi$ we have $r_\alpha(\beta) = \beta - n_{\beta,\alpha}\alpha$ with the $n_{\beta,\alpha} \in \mathbb{Z}$. The elements of Φ are then called *roots*.

Suppose now that Φ is a root system in V. A $\lambda \in V^*$ will be called *regular* if $<\alpha, \lambda> \neq 0$ for all $\alpha \in \Phi$. For such a λ, we write

$$\Phi^+(\lambda) := \{\alpha \in \Phi | <\alpha, \lambda> > 0\}$$

and

$$\Delta(\lambda) := \{\alpha \in \Phi^+(\lambda) | \alpha \text{ is not a sum of two elements of } \Phi^+(\lambda)\}.$$

A *basis for* Φ is a subset Δ thereof which is a basis for V such that each $\beta \in \Phi$ is writable as a linear combination $\beta = \pm \sum_{\alpha \in \Delta} m_\alpha \alpha$ with the $m_\alpha \in \mathbb{N}\, \forall \alpha$. Then the *positive roots* (with respect to Δ) are those for which we take the '+' sign in the last sum, and we denote this set by Φ^+. The *Weyl chamber of* Δ (or equivalently of Φ^+), to be denoted $WC(\Delta)$, is defined to be

$$\{\lambda \in V^* | < \alpha, \lambda > > 0 \ \forall \alpha \in \Delta\},$$

and this clearly consists of regular elements.

Φ is called *reduced* if $\alpha \in \Phi$ and $r\alpha \in \Phi$ for some $r \in \mathbb{R} \implies r \in \{\pm 1\}$. The root system Φ in V is called *irreducible* if there do not exist nonzero subspaces V_1 and V_2 with $V = V_1 \oplus V_2$ and Φ_i (*viz.* $\Phi \cap V_i$) being a root system in V_i for each i. A subset A of a root system Φ is called *closed* if the conditions $\alpha, \beta \in A$ and $\alpha + \beta \in \Phi$ imply $\alpha + \beta \in A$. Note what this means if Φ is not reduced.

We also have a notion of *Weyl group* $W = W(\Phi)$ for Φ :- W is the group of automorphisms of Φ generated by the reflections r_α. Any W-invariant scalar product on V or on V^* will be called *admissible*. Clearly W is a finite Coxeter group - it is generated by finitely many involutions r_α, and is contained in the group of permutations of Φ.

For $\alpha, \beta \in \Phi$ write

$$(\alpha, \beta) := \{\gamma \in \Phi : \gamma = r\alpha + s\beta \text{ for some } r, s \in \mathbb{Z}^+\}.$$

Clearly (α, β) may be empty. Similarly, if Ψ, Ψ' are subsets of Φ, we write (Ψ, Ψ') for $\cup_{\alpha \in \Psi, \beta \in \Psi'}(\alpha, \beta)$. We call Ψ *special* if $(\Psi, \Psi) \subseteq \Psi$, and there exists $\lambda \in X^*$ such that $< \alpha, \lambda >$ is greater than zero $\forall \alpha \in \Psi$.

Theorem 4.1.0.1 *Let Φ be a root system in V.*
(1) For any regular $\lambda \in V^*$, $\Delta(\lambda)$ is a basis of Φ, and is the unique basis contained in $\Phi^+(\lambda)$.

(2) A subset $\Psi \subseteq \Phi$ is special iff Ψ is closed and is contained in Φ^+ for some ordering on Φ.

Let Φ be reduced, and Δ any basis thereof.

(3) $W(\Phi)$ acts simply transitively on the set of bases of Φ (or equivalently on the set of Weyl chambers).

(4) $\Phi = \cup_{w \in W(\Phi)} w\Delta$.

(5) The r_α for $\alpha \in \Delta$ generate $W(\Phi)$, and there is a well-defined length function $l : W \longrightarrow \mathbb{N}$ given by

$$\begin{aligned} l(w) &= \min\{t \in \mathbb{N} : \text{ there is an expression } w = r_{\alpha_1} r_{\alpha_2} \ldots r_{\alpha_t} \text{ with each } \alpha_j \in \Delta\} \\ &= \#\{\beta \in \Phi^+ : w.\beta \in \Phi^-\}. \end{aligned}$$

Further, there is a unique element w_0 of maximal length $\#\Phi^+$.

The possible root systems are classified (up to isomorphism) by the Dynkin diagrams, defined thus. For the root system Φ with basis Δ, the *Dynkin diagram* $\mathcal{D} = Dyn(\Phi, \Delta)$ is a graph with (say) $l = \#\Delta$ nodes. Fix any ordering $\{\alpha_1, \ldots, \alpha_l\}$ on Δ, and write n_{ij} for the integer n_{α_i, α_j} defined before (these are the *Cartan integers* of Φ).

Join α_i and α_j by $n_{ij}n_{ji}$ edges (in fact, one always has $0 \leq n_{ij}n_{ji} \leq 3$), and finally, if we have bonds from α_i to α_j, with $n_{ij} \neq -1$, we assign this direction thereto. As is well known, there is in each (connected) component, at most one arrow, and at most one multiple bond. The *short roots* are those towards which any arrow points, and the *long roots* those away from which any arrow points. (By convention, they are all long if there is no arrow.)

Further, these components correspond exactly to the irreducible root subsystems of Φ. The irreducible reduced root systems are to be found in the usual list A_l for $l \geq 1$, B_l for $l \geq 2$, C_l for $l \geq 3$, D_l for $l \geq 4$, E_6, E_7, E_8, F_4 and G_2. The only irreducible nonreduced system is that of type BC_n ($n \geq 1$). This last is (as root system) the union of a B_n with a C_n (identifying long roots in one with short roots in the other).

For further discussion of this see [Bou68, VI,§4.14]. Non-reduced root systems can arise in the relative theory of algebraic groups [Bor91, §21].

There is a convention for numbering the nodes, for details of which we refer to [4.5.5] where it will be more topical.

4.2 Connected reductive groups

In this section G is a connected reductive k-group, and T is a maximal torus in G. For any T-stable subgroup H of G, we write $\Phi(H)$ for $\Phi(T,H)$. If $\alpha \in \Phi(T,G)$ then T_α is defined to be $(\ker\alpha)^0$, $G_\alpha := \mathcal{Z}_G(T_\alpha)$. Finally, we write Ψ for the *set of roots of G outside $I(T)$*, namely

$$\Psi = \{\alpha \in \Phi(T,G) : \mathfrak{g}_\alpha \not\subseteq \mathcal{L}(I(T))\}.$$

4.2.1 The root system of G

Theorem 4.2.1.1 *[Bor91, 13.18,13.20,13.21]*

(1) $\Psi = \Phi$, $\mathcal{L}(T) = \mathfrak{g}^T$ *and* $\mathfrak{g} = \mathfrak{g}^T \oplus_{\alpha\in\Phi} \mathfrak{g}_\alpha$.

(2) The T_α are the singular subtori of T of codimension 1 in T, and

$$(\cap_{\alpha\in\Phi} T_\alpha)^0 = Z(G)^0 = r(G).$$

(3) Φ generates (over $\mathbb{Z}$) a subgroup of finite index in $X(T/Z(G)^0) \subseteq X(T)$. Further, if $\alpha,\beta \in \Phi$ are linearly dependent (over $\mathbb{Z}$), then $\alpha = \pm\beta$.

(4) For each $\alpha \in \Phi$, G_α is reductive of semisimple rank 1, $-\alpha \in \Phi$, $\mathcal{L}(G_\alpha) = \mathfrak{g}^T \oplus \mathfrak{g}_\alpha \oplus \mathfrak{g}_{-\alpha}$, and $\mathfrak{g}_\alpha$ has dimension 1 (so is in particular a Lie subalgebra of $\mathfrak{g}$). Furthermore, there is a unique connected unipotent subgroup U_α in G with $\mathcal{L}(U_\alpha) = \mathfrak{g}_\alpha$.

(5) For each $B \in \mathcal{B}^T$, $\Phi(T, G_\alpha \cap B) = \Phi(B) \cap \{\pm\alpha\}$ is a singleton, so $\Phi(B) \coprod (-\Phi(B)) = \Phi$. Further $\mathcal{L}(B) = \mathfrak{g}^T \oplus \prod_{\alpha\in\Phi(B)} \mathfrak{g}_\alpha$, and there is a total ordering on $X(T)$ such that $\Phi(B)$ is exactly the set of positive elements in Φ.

(6) Let H, H' be any two connected T-stable subgroups of G.

(a) $\mathcal{L}(H) = \mathcal{L}(T \cap H) \oplus \coprod_{\alpha\in\Phi(T,H)} \mathfrak{g}_\alpha$.

(b) $H = <(T \cap H)^0, U_\alpha | \alpha \in \Phi(T,H)>$.

(c) $\mathcal{L}(H \cap H') = \mathcal{L}(H) \cap \mathcal{L}(H')$.

The groups U_α as in (4) are called the *root subgroups* of G with respect to T.

Proposition 4.2.1.2

(1) For $\alpha, \beta \in \Phi$ with $\alpha \neq \pm\beta$, the following set is special.

$$[\alpha, \beta) := \{\gamma \in \Phi : \gamma = r\alpha + s\beta \text{ for } r, s \in \mathbb{Z} \text{ with } s > 0\}$$

Let $\Upsilon \subseteq \Phi$ be special.

(2) The set $\{U_\alpha | \alpha \in \Upsilon\}$ directly spans (in any order) a T-stable subgroup U_Υ of G.

(3) For any $\alpha \in \Phi$ such that $(\alpha, \Upsilon) \subseteq \Upsilon$, U_α normalizes U_Υ.

Proposition 4.2.1.3 *[Bor91, 18.7] G is k-unirational, and so (for infinite k) $G(k)$ is dense in G.*

Theorem 4.2.1.4 *[Bor91, 14.8] Put $V = X(T/r(G)) \otimes_{\mathbb{Z}} \mathbb{Q}$, identified canonically with a subspace of $X(T) \otimes_{\mathbb{Z}} \mathbb{Q}$. Then $\Phi(T, G)$ is a reduced root system in V, with Weyl group $W(\Phi) = W$, where W is $\mathcal{N}_G(T)/\mathcal{Z}_G(T)$, and W acts simply transitively on $\mathcal{B}^T$.*

Further $r(G) = Z(G)^0$ is the (identity component of the) intersection of all root kernels.

Note the appearance of $r(G)$: this signifies that this is essentially a theorem about *semisimple* groups. However G and its semisimplification $G/r(G)$ have the same root system and Weyl group, by [3.4.3.4], or as verified in the proof of [5.4.5.1].

Corollary 4.2.1.5 *For any $B \in \mathcal{B}^T$, put Δ for the set of $\alpha \in \Phi(B)$ which are not sums of two elements of $\Phi(B)$. Then Δ is a basis of Φ (the set of simple roots determined by B and T), and, further, G is generated by $\{G_\alpha | \alpha \in \Delta\}$.*

4.2.2 Bruhat decomposition

We need the following result, whose hypotheses are seen to be satisfied in our situation with T a maximal torus in G, $U = B_u$ for some Borel subgroup B containing T, and action by conjugation.

Lemma 4.2.2.1 *[Bor91, 14.4]*

Let a torus T act on a connected unipotent group U, with $\Phi(H)$ denoting $\Phi(T,H)$ for any T-stable subgroup of U. For each $\alpha \in \Phi(H)$ define $U_\alpha = \{x \in U : (\ker\alpha)^0.x = x\}$, and suppose that:

(i) $\mathcal{L}(U) = \coprod_{\alpha\in\Phi(U)} u_\alpha$ with $\dim u_\alpha = 1$ for each α; and

(ii) whenever α and β are distinct elements of $\Phi(U)$ then $(\ker\alpha)^0 \neq (\ker\beta)^0$.

Then the following hold.

(a) U_α is the unique T-stable subgroup of U such that $\mathcal{L}(U_\alpha) = u_\alpha$.

(b) Any T-stable subgroup H of U is connected, and directly spanned by $\{U_\alpha|\alpha \in \Phi(H)\}$ in any order.

(c) If H and xHx^{-1} are both T-stable subgroups of U they coincide.

Fix $B \in \mathcal{B}^T$, put $U = B_u$, $\Phi^+ = \Phi(B)$ and Δ for the basis of Φ in Φ^+. Similarly, put B^- for the *opposite Borel subgroup* to B (*viz.* that associated to $-\Phi^+$), and U^- for *its* unipotent radical. It is convenient to write $\alpha > 0$ for $\alpha \in \Phi^+$, or $\alpha < 0$ for $-\alpha \in \Phi^+$.

For $y \in G$, and a subgroup H of G, we denote by ${}^yH$ the conjugate yHy^{-1}. In particular, for any $w \in W$, we have ${}^wU$ and ${}^wU^-$, respectively the images of U and U^- under w - recall that w is regardable as a (any) representative of $T = \mathcal{Z}_G(T)$ in $\mathcal{N}_G(T)$, acting on G by conjugation. Then if we write $U_w := U \cap {}^wU$ and $U'_w := U \cap {}^w(U^-)$, these are T-stable subgroups of U (so are connected and directly spanned by the U_γ for $\gamma > 0$ which they contain - in any order [4.2.2.1]). Put Φ^+_w for the set of γ with $U_\gamma \subseteq U_w$.

Proposition 4.2.2.2 *Suppose $\Phi^+_w = \Phi^+_y$ for $w, y \in W$. Then $w = y$.*

Proof: If n is a representative of w in $\mathcal{N}_G(T)$, then the obvious actions of w on X and X^* are given by composition with conjugation by n. Thus if $\alpha \in X$ and $\lambda \in X^*$, we have $\alpha^w \circ \lambda = \alpha \circ {}^w\lambda$ in a notation which reflects the order of that composition. Since G is reductive, every regular $\lambda \in X^*$ lies in a Weyl chamber, and this latter chamber is determined by the signs of the $<\alpha,\lambda>$ for $\alpha \in \Phi^+$. We saw a moment ago that $<\alpha^w,\lambda> = <\alpha,{}^w\lambda>$, so that if we suppose λ in the Weyl chamber determined by B (*viz.* defined by the condition $<\alpha,\lambda> \in \mathbb{Z}^+ \ \forall\alpha \in \Phi^+$), for such positive α, $<\alpha,{}^w\lambda> > 0$ precisely when $\alpha \in \Phi^+_w$. Then the hypothesis implies that ${}^w\lambda$ and ${}^y\lambda$ lie in the same Weyl

chamber: but W acts simply transitively on these chambers, so $w = y$. $\square$

It also follows from [4.2.1.2, 4.2.2.1] that $U = U_w.U'_w = U'_w.U_w$ as the two sets of positive roots involved are closed and partition Φ^+.

Theorem 4.2.2.3 (Bruhat and cellular decompositions)
(1) [Bruhat decomposition of G] $G = \coprod_{w\in W} BwB = \coprod_{w\in W} UwB$, *and, for each* $w \in W$, *there is an isomorphism of varieties*

$$f_w : U'_w \times B \longrightarrow BwB \text{ given by mapping } (x, y) \mapsto xwy.$$

(2) [Cellular decomposition of G/B] G/B *is the disjoint union of the U-orbits Uwx_0 (for $w \in W$) where x_0 is the fixed point of B in G/B. Similarly, the map $U'_w \longrightarrow Uwx_o$ given by $u \mapsto uwx_0$ is an isomorphism of varieties.*

Proof: We include a proof, as this decomposition is central for what follows. Since $BwB = UwB$ and $Bwx_0 = Uwx_0$, the statements (1) and (2) are equivalent. Thus it is enough to show the following.
(a) $w, y \in W$ and $Uwx_0 = Uyx_0$ imply $w = y$.
(b) $G = BWB$.
(c) The map f_w of (1) is an isomorphism of varieties.

By the last proposition, to prove (a), we need only show that $\Phi^+_w = \Phi^+_y$. Suppose we have $yx_0 = uwx_0$ with $u \in U$. Then U_y (*viz.* $U \cap {}^yB$), the stability group in U of yx_0, is the same as that of uwx_0, namely $U_{uw} = {}^uU_w$. Then U_w and U_y are both T-stable subgroups of (unipotent) U, which are moreover conjugate in U. But two such groups must coincide by [4.2.2.1], and we get that $\Phi^+_w = \Phi^+_y$, proving (a).

We prove (b) in stages. *(i) Suppose that G has semisimple rank 1 (so that $\#W = 2$).* Then, by (a), BWx_0 consists of two U-orbits, so it suffices to show that G/B consists of at most two U-orbits. Consider the morphism (of varieties) $U \longrightarrow G/B$ given by $u \mapsto uy$ (where y is not a fixed point of U). Noting that U is isomorphic as variety to $\mathbb{G}_a$, so regardable as $\mathbb{P}^1$ minus a point, and that any morphism $V \longrightarrow C$ from an irreducible smooth curve V to a complete variety C can be extended to a morphism $V_c \longrightarrow C$ where

V_c is the (unique) complete smooth curve in which V is open [Bor91, AG 18.5], we get a morphism $t : \mathbb{P}^1 \longrightarrow G/B$. The image is one-dimensional as y is not a fixed point of U, and is closed by [1.12.0.1]. Thus t is surjective; but the image consists of (some) fixed points of U and a one-dimensional orbit (as U has dimension 1). Fixed points correspond to Borel subgroups of G normalized by U. The Normalizer Theorem [3.4.2.1] guarantees that if C is a Borel subgroup, $C \subseteq \mathcal{N}_G(U)$ iff $U \subseteq \mathcal{N}_G(C) = C$. Hence fixed points correspond bijectively to the Borel subgroups of $M = \mathcal{N}_G(U)^0$. But this last group is actually equal to B, verifying *(i)*.

(ii) For $\alpha \in \Phi$ and $x \in (G/B)^T$, $G_\alpha x = (U_\alpha x) \cup (U_\alpha r_\alpha x)$.

Recall that r_α denotes the simple reflection corresponding to α. To verify the claim, consider $(G_\alpha)_x = G_\alpha \cap B_x$. Recall that this is Borel in G_α by [3.4.3.2], and we get a bijective and G_α-equivariant morphism $G_\alpha/(G_\alpha)_x \longrightarrow G_\alpha x$. As G_α has semisimple rank 1, and Weyl group $< r_\alpha | r_\alpha^2 >$ with respect to T the result follows from *(i)*.

(iii) If now $\alpha \in \Delta$ and $\Psi = \Phi^+ \setminus \{\alpha\}$, Ψ is special, so the U_β for $\beta \in \Psi$ directly span a group U_Ψ, which is normalized by G_α, and $U = U_\alpha U_\Psi = U_\Psi U_\alpha$.

That Ψ is special, and that $(\alpha, \Psi) \subseteq \Psi$ is easy. Moreover, $(-\alpha, \Psi) \subseteq \Psi$, since if $\gamma = r(-\alpha) + s\beta$ with $r, s \in \mathbb{Z}^+$ and $\beta \in \Psi$, then $\beta = \sum_{\delta \in \Delta} m_\delta \delta$ with $m_{\delta_0} > 0$ for some $\delta_0 \neq \alpha$ as Φ is reduced. Then the δ_0-coordinate of γ is $s\delta_0 > 0$ so $\gamma \in \Phi^+$, and is distinct from α. Then the claim about direct spanning follows from [4.2.1.2]; that U_Ψ is normalized by U_α and $U_{-\alpha}$, and hence by G_α is clear. Hence the asserted equalities hold.

(iv) For $\alpha \in \Delta$ and $x \in (G/B)^T$, $G_\alpha B x = (Ux) \cup (Ur_\alpha x)$.

Now $B = UT = U_\alpha U_\Psi T$ by *(iii)*, so

$$G_\alpha B x = G_\alpha U_\alpha U_\Psi T x = G_\alpha U_\Psi x = U_\Psi G_\alpha x$$

by *(iii)*, which is

$$U_\Psi((U_\alpha x) \cup (U_\alpha r_\alpha x)) \text{ by } (ii).$$

But this is just $(Ux) \cup (Ur_\alpha x)$ as required.

(v) Finally, if $\alpha \in \Delta$, $G_\alpha BwB \subseteq BwB \cup Br_\alpha wB$ for any $w \in W$. This holds as

$$G_\alpha BwB = (UwB) \cup (Ur_\alpha wB) \subseteq (BwB) \cup (Br_\alpha wB).$$

Since G is generated by the G_α for $\alpha \in \Delta$ by [4.2.1.5], so $G(BWB) \subseteq BWB$, proving (b).

(c) Finally, as $U_w = U \cap {}^wB = U \cap wBw^{-1} = U \cap wUw^{-1}$, it follows that $U_w w \subseteq U$, and similarly, $U'_w w \subseteq wU^-$. Thus $B = UT = U'_w U_w T$ so $BwB = U'_w U_w wB = U'_w wB$ and hence the given map f_w is surjective. Then $U'_w w \subseteq wU^-$ and $U^- \cap B = \{e\}$ implies that it is injective also. Clearly f_w is a morphism of varieties, so it is now enough to show that it is separable by [1.9.0.2]. But $\mathcal{L}(U^-)$ intersects $\mathcal{L}(B) = \mathfrak{g}^T \oplus \sum_{\alpha>0} \mathfrak{g}_\alpha$ trivially, so df_w is surjective, and hence f_w is separable. □

4.3 Quasisplit and split groups

G is a connected k-group in this section. G is *k-quasisplit* if it has a Borel subgroup defined over k.

A connected solvable k-group B is k-split if it has a composition series $B = B_0 \triangleright B_1 \triangleright \cdots \triangleright B_r = \{e\}$ consisting of connected k-groups such that B_j/B_{j+1} is k-isomorphic to $\mathbb{G}_a$ or $\mathbb{G}_m$ for each $j \in \{0, \ldots, r-1\}$. G is *k-split* if it is k-quasisplit, and it has a Borel subgroup B which is defined over k and k-split.

Any extension m of k such that G is m-split is called a splitting field for G (or *the splitting field* if it is the least such).

Theorem 4.3.0.1 (Splitting for connected k-groups)

(1) G is k^a-split.

(2) If G is reductive, then it is k-split iff it has a maximal torus T which is k-split. When this holds, every component of $\mathcal{N}_G(T)$ has a k-rational point [Bor91, 18.7, 21.2].

(3) If G is unipotent, it is k^i-split.

(4) If H_1 and H_2 are connected reductive k-groups which are k-split and isomorphic, then they are k-isomorphic [BT65, 2.13].

(5) If k is finite, G is k-quasisplit [4.4.0.2].

A connected reductive k-group is said to be *k-anisotropic* if it has no k-split subtorus of positive dimension. For the following results we refer to [Bor91, §8].

Proposition 4.3.0.2 (Splitting for k-tori)

Let T be a k-torus of dimension n and l an algebraic Galois extension of k.

(1) T is k-quasisplit and k^s-split.

(2) The following are equivalent.

(i) T is k-split.

(ii) T is k-isomorphic (as k-group) to $\mathbb{G}_m^n$.

(iii) The group $X(T)_k$ of characters defined over k spans the $\mathbb{E}$-module $\mathbb{E}[T]$.

(3) Every (closed) subgroup of a k-split torus is k-split.

(4) There exist unique k-subtori T_d, T_a of T such that T_d is k-split, T_a is k-anisotropic, $T_d \cap T_a$ is finite, and $T = T_d T_a$.

(5) The antiequivalence [3.3.3.3] induces a bijection between the k-isomorphism classes of l-split k-tori of dimension n and the $\mathbb{Z}$-inequivalent representations of $Gal(l/k)$ in $GL(n, \mathbb{Z})$.

We will formally define $\mathbb{Z}$-inequivalent representations in [5.2.2].

Theorem 4.3.0.3 *[Bor91, 15.13] If H is connected, solvable and k-split, acting k-morphically and transitively on an affine variety V, then V is k-isomorphic (as variety) to $\mathbb{G}_a^b \times \mathbb{G}_m^e$. The numbers b and e are the numbers of factors of the corresponding type in the composition series for H, less those for any isotropy subgroup.*

Corollary 4.3.0.4

(1) If A is a k-group such that $A^0 = H$, then a component of A is defined over k iff it has a k-rational point.

(2) If G is a connected unipotent k-group, then G is k^i-isomorphic (as variety) to affine space of the same dimension.

4.4 Groups over finite fields

There are several special features about these facilitating work therewith, resting on the theorem of Lang below, to describe which we first discuss Frobenius maps. That for the finite field $\mathbb{F}_q$ of q elements can be defined thus. Take an $n \times n$ matrix $A = (a_{ij})$ with entries in $\mathbb{E} \supseteq \mathbb{F}_q$. Then the image of A under the Frobenius map F_q is the matrix $A^{(q)} := (a_{ij}^q)$

- as distinct from A^q. Now if A lies in an algebraic group which is defined over $\mathbb{F}_q$, the same will be true of $A^{(q)}$. To make this intrinsic, we say that, for an $\mathbb{F}_q$-group G, a map $i : G \longrightarrow G$ is a *Frobenius map on* G (for $\mathbb{F}_q$) if there is an $\mathbb{F}_q$-embedding $j : G \longrightarrow GL_n(\mathbb{E})$ for some n such that $(F_q)^s \circ j = j \circ i$ for some $s \in \mathbb{Z}^+$. Clearly any j determines at most one i, and any Frobenius map i is bijective. Of course, the property of Frobeniusness is also independent of the $\mathbb{F}_q$-embedding chosen. Note that the differential dj of j is also injective, so di is zero.

Theorem 4.4.0.1 (Lang)

Let H be a connected $\mathbb{F}_q$-group, and let $i : H \longrightarrow H$ be a Frobenius map (for $\mathbb{F}_q$) on H. Then the map $\phi_H : H \longrightarrow H$ given by $x \mapsto x^{-1} \cdot i(x)$ is a separable surjection.

Proof: This uses a few simple facts about differentials which can be found in [Bor91, 3.2]. ϕ_H fixes the identity e of G. Note that $(d\phi_H)_e(X) = -X + (di)_e X$, so $(d\phi_H)_e$ is surjective. H being irreducible, it follows that ϕ_H is dominant and separable by [1.9.0.2]. Next, pick $y \in H$, and consider the map $t : H \longrightarrow H$,

$$t : z \mapsto z^{-1} \cdot y \cdot i(z).$$

Then $(dt)_e$ maps the tangent space at e into that at y and is also surjective (as it has the same differential as $z \mapsto z^{-1} \cdot y$), and so t is also dominant. We have shown that each of $\phi_H(H)$ and $t(H)$ contains a nonempty open subset of H. The images therefore intersect, and so there exist $g_1, g_2 \in H$ such that $g_1^{-1} \cdot i(g_1) = g_2^{-1} \cdot y \cdot i(g_2)$. Thus $y = g^{-1} \cdot i(g)$ where $g = g_1 \cdot g_2^{-1}$. $\square$

Corollary 4.4.0.2

(1) If $f : H \longrightarrow A$ is an $\mathbb{F}_q$-isogeny then H and A have the same number of $\mathbb{F}_q$-rational points, and the same zeta function over $\mathbb{F}_q$.

(2) [Serre] H is quasi-split over $\mathbb{F}_q$.

(3) If V is an $\mathbb{F}_q$-variety on which H acts $\mathbb{F}_q$-morphically and transitively, then V has an $\mathbb{F}_q$-rational point.

(4) If $1 \to A \to B \to C \to 1$ is a short exact sequence of connected groups over $\mathbb{F}_q$, then

$\forall r \geq 1$, *the induced sequence* $1 \to A_r \to B_r \to C_r \to 1$ *of* $\mathbb{F}_{q^r}$*-rational points is a short exact sequence of abstract groups.*

Proof: All of these facts are standard. We just remark that the proof of (1) consists in observing that $f \circ \phi_H = \phi_A \circ f$, and equating the degrees [1.6] of these maps. □

4.5 Connected semisimple groups

4.5.1 Structure

Let G be a connected semisimple k-group. We write A for the group of algebraic group automorphisms of G, and $Inn(G)$ for the group of inner automorphisms of G (namely $G/Z(G)$). Further, let $A_{B,T}$ be the subgroup of A stabilizing both B and T, where we fix a maximal k-torus T and a Borel subgroup B therecontaining. We also write $\mathcal{D}$ for the Dynkin diagram of G - recall the correspondence between bases for Φ and Borel subgroups of G containing T: the present basis of Φ will be denoted Δ.

Proposition 4.5.1.1

(1) There is a homomorphism $A_{B,T} \longrightarrow \mathrm{Aut}(\mathcal{D})$ *whose kernel is* $A_{B,T} \cap Inn(G)$*;*

(2) $A = Inn(G).A_{B,T}$*;*

(3) $A/Inn(G)$ *injects into* $\mathrm{Aut}(\mathcal{D})$ *and so is finite.*

Proof: *(1)* For $\theta \in A_{B,T}$, as θ stabilizes T, it induces an automorphism of Φ - as θ stabilizes B, it stabilizes Δ, and so induces an automorphism θ' (say) of $\mathcal{D}$. Now if $\theta \in A_{B,T} \cap Inn(G)$, say θ is conjugation by $y \in G$, then $y \in \mathcal{N}_G(B) \cap \mathcal{N}_G(T) = T$, so θ induces the identity map on Φ.

Conversely, if $\theta \in A_{B,T}$ with θ' (defined as before) being the identity map of Φ, then note that θ stabilizes U_α for each $\alpha \in \Delta$, where the U_α are the usual root subgroups. As there is an isomorphism $f_\alpha : \mathbb{G}_a \longrightarrow U_\alpha$ for each α, there is a $c_\alpha \in \mathbb{E}^*$such that $\theta \circ f_\alpha(x) = f_\alpha(c_\alpha x)$ for all $x \in \mathbb{G}_a$ [Bor91, 10.10]. Hence there exists $t \in T$ such that $\alpha(t) = c_\alpha$ for each $\alpha \in \Delta$, because the α are linearly independent over $\mathbb{Z}$. Since, for such a t, conjugation by t has the same effect as θ on each U_α ($\alpha \in \Delta$), we can, replacing θ

by $\theta_1 = Inn(t)^{-1} \circ \theta$, assume that each $c_\alpha = 1$, so that θ_1 fixes all these U_α. For $x \in T$, $\alpha(x) = \alpha \circ \theta_1(x)$ for each $\alpha \in \Delta$: but Δ spans a subgroup of $X(T)$ of finite index therein, so θ_1 actually fixes T too. Hence θ_1 fixes the Borel subgroup $T.U_\alpha$ of $G_\alpha = \mathcal{Z}_G((\ker \alpha)^0)$, and so by [3.4.1.1], fixes G_α. But by [4.2.1.5], the G_α generate G, so θ_1 is the identity. Hence θ must have been inner.

(2) Recall that the maximal tori of B are mutually conjugate, and that so are the Borel subgroups of G. For $a \in A$, there is $g \in G$ such that $cB = B$ where $c = Inn(g) \circ a$. Also, $dT = T$, where $d = Inn(b) \circ c$ for some $b \in B$. Then $d = Inn(b) \circ Inn(g) \circ a$ as required.

(3) This follows from the earlier parts. □

We come now to the major structure theorem (G as above).

Theorem 4.5.1.2

(1) If $\pi : G \longrightarrow G_1$ is a surjective morphism, G_1 is semisimple.

(2) Let H be a connected normal subgroup of G, and write $H' = \mathcal{Z}_G(H)^0$.

(i) H is semisimple.

(ii) $G = H.H'$ and $H \cap H' \subseteq Z(G)$.

(iii) H is defined over k^s.

(3) Let $\{G_i | i \in I\}$ be the minimal connected normal subgroups of G of positive dimension.

(i) The G_i are almost simple, and distinct G_i centralize each other.

(ii) I is finite (say $I = \{1, \ldots, n\}$), and the product map $G_1 \times \cdots \times G_n \longrightarrow G$ is a central isogeny.

(iii) H is generated by $\{G_i | G_i \subseteq H\}$.

(4) G is almost simple iff Φ is irreducible.

Proof: Only the proof of *(2)(iii)*, and the centrality in *(3)(ii)* are not given in [Bor91, 14.10]. To verify *(2)(iii)*, we can assume $k = k^s$. Then G and some maximal k-torus T are both k-split, and the latter normalizes H. For each $\alpha \in \Phi(T, H)$, the group T_α is defined over k (as T is k-split), and hence so is its centralizer H_α in H. But H is reductive by *(2)(i)* and so generated by the H_α by [4.2.1.5]. For *(3)(ii)*, we quote [Bor91, 22.9]. □

Corollary 4.5.1.3

(1) G is strictly k^s-isogenous to a product $G_1 \times \cdots \times G_n$ of connected almost simple k^s-groups.

(2) The G_i are permuted by Γ, and for each orbit $J \subseteq I$, the product G_J, in any order, of $\{G_i : i \in J\}$ is a connected semisimple almost k-simple k-group. Further, in each orbit, the G_i which occur all have the same Dynkin diagram.

4.5.2 The $*$-action and k-index

Let T be a maximal k-torus of G, and S a maximal k-split torus of G. The dimension of S is the *(relative) k-rank of G*. We can suppose $S \subseteq T$ with compatible orderings chosen in $X(S)$ and $X(T)$ [Bor91, 21.8]. Having chosen a basis Δ for $\Phi(T, G)$ which has this property, we put Δ_0 for the subset of Δ which vanishes on S, and Δ_k for the corresponding simple roots in $\Phi(S, G)$. Of course, the elements of $\Delta \setminus \Delta_0$ need not be $\mathbb{Z}$-independent when restricted to S.

Each $\sigma \in \Gamma$ induces an automorphism of $X(T)$, as T is k^s-split, and so of T. Further, $\sigma(\Delta)$ is also the set of simple roots in $\Phi(T, G)$ for some ordering, so there is a unique $w \in W$ such that $w \circ \sigma(\Delta) = \Delta$. We say then that σ induces the permutation $\sigma^* := w \circ \sigma$ of Δ, so Γ acts on the nodes of $\mathcal{D}$. But in fact, the Cartan integers are preserved too, so Γ acts by (directed) graph automorphisms. This is the $*$-action. G is said to be *of inner type* if the $*$-action is trivial, and otherwise *of outer type* - of course, all this is with respect to k.

Recall that a group action is said to be *effective* if distinct group elements induce distinct permutations. Clearly, there is a normal subgroup Γ_l of finite index in Γ such that the quotient acts effectively on $\mathcal{D}$ - the intersection of all isotropy groups: we will call the (finite Galois) extension of k corresponding to Γ_l the *inner field l* of G. Any extension of l will be called *an inner field* for G. For example, splitting fields are inner.

The triple $\{\Delta, \Delta_0, *\text{-action}\}$ is called the *k-index* of G. It is independent (up to isomorphism of Γ-graph) of the choices of S and T. Note that Δ_0 is a union of $*$-orbits: the *distinguished orbits* are those in $\Delta \setminus \Delta_0$.

4.5.3 Classification theorems

The derived group $\mathcal{Z}_G(S)'$ of $\mathcal{Z}_G(S)$ is the *anisotropic kernel* $An(G)$ of G (with respect to k). $An(G)$ is a connected, semisimple k-group and k-anisotropic, and again independent up to k-isomorphism of the choices of S and T. The terminology reflects an analogy with Witt's classification of non-degenerate quadratic forms in characteristic $\neq 2$ [Ja74, 6.5].

Proposition 4.5.3.1

(1) G is k-split iff it is k-quasisplit and of inner type.

(2) G is k-quasisplit iff $An(G)$ is trivial, in which case Δ_0 is empty.

The following theorem appears in [Ti66, 2.7.1] - at least it appears in a more precise formulation which does not concern us.

Theorem 4.5.3.2 *Let G be a connected semisimple k-group.*

(1) G is determined up to k-isomorphism by the following data: the k^s-isomorphism class, the k-index, and the k-isomorphism class of $An(G)$.

(2) G is determined up to strict k-isogeny by the following data: the strict k^s-isogeny class, the k-index, and the strict k-isogeny class of $An(G)$.

Corollary 4.5.3.3 *A connected semisimple k^s-group is determined up to strict k^s-isogeny by its Dynkin diagram. In particular, the strict k^s-isogeny classes of almost simple k^s-groups correspond bijectively to the connected Dynkin diagrams.*

Further, there exist, in a given strict k^s-isogeny class, only finitely many k^s-isomorphism classes (described below).

In the strict k^s-isogeny class containing G, the k^s-isomorphism classes can be described thus [Ti66, 1.5.4]: we put $\mathbb{Z}\Phi$ for the $\mathbb{Z}$-span of Φ (in $X(T)$), and Ω for the lattice of weights of G with respect to T, namely the dual of the lattice of coroots. Then we have inclusions $\mathbb{Z}\Phi \subseteq X \subseteq \Omega$ of free abelian groups, all of the same finite rank. If $X = \mathbb{Z}\Phi$, we say G is *adjoint*, and if $X = \Omega$, we say G is *simply connected*. The k^s-isomorphism class of G is determined by the location of X between the root lattice and the weight lattice (although distinct X will not necessarily yield distinct k^s-isomorphism classes).

In principle, [4.5.3.2] affords a classification up to k-isomorphism: however the determination of the possible $An(G)$ which can occur is in general difficult. For general k, it does not seem to be known if a given strict k-isogeny class can correspond to infinitely many k-isomorphism classes. In [Ti66, Table II] are enumerated the possible indices for almost simple k-groups, with more specific information in the cases of number fields and finite fields (among others).

4.5.4 Almost simple groups

Let G now be an almost simple k-group, and put $g = [l : k]$, where l is the inner field of G. Then G is connected, and has a connected Dynkin diagram ${}^gX_{n,r}$ (say), where n is the rank, and r is the k-rank. We will omit the symbol g when its value is 1: clearly $g \in \{1, 2, 3, 6\}$.

The possible such G have been classified, at least up to strict $\mathbb{F}_p$-isogeny, for the finite field $\mathbb{F}_p$ [Ti66, Table II]. In this situation, by [4.4.0.2], G has the property that $\#G(\mathbb{F}_p)$ is determined by the strict $\mathbb{F}_p$-isogeny class of G.

The data in the following table is based on [Ti66, Table II] (and the polynomials $P(X)$ given can be found in [Ca85, p75]).

Theorem 4.5.4.1 *Let G be an almost simple $\mathbb{F}_p$-group.*

Then G is strictly $\mathbb{F}_p$-isogenous to one of the following types, and $\#G(\mathbb{F}_p) = P(\#\mathbb{F}_p)$ where $P(X) \in \mathbb{Z}[X]$ is as given.

The degree *of P is the dimension of G, and the multiplicity of 0 as a root of P is $\frac{\dim G - n}{2}$ (the number of positive roots in the root system for G).*

Type	$P(X)$	*Conditions on* n
$A_{n,n}$	$X^{n(n+1)/2}\prod_{i=1}^{n}(X^{(i+1)}-1)$	for $n \geq 1$
$B_{n,n}$	$X^{n^2}\prod_{i=1}^{n}(X^{2i}-1)$	for $n \geq 2$
$C_{n,n}$	$X^{n^2}\prod_{i=1}^{n}(X^{2i}-1)$	for $n \geq 3$
$D_{n,n}$	$X^{n(n-1)}(X^n-1)\prod_{i=1}^{n-1}(X^{2i}-1)$	for $n \geq 4$
$E_{6,6}$	$\left\{ X^{36}(X^{12}-1)(X^9-1)(X^8-1)\cdot (X^6-1)(X^5-1)(X^2-1) \right\}$	
$E_{7,7}$	$\left\{ X^{63}(X^{18}-1)(X^{14}-1)(X^{12}-1)\cdot (X^{10}-1)(X^8-1)(X^6-1)(X^2-1) \right\}$	
$E_{8,8}$	$\left\{ X^{120}(X^{30}-1)(X^{24}-1)(X^{20}-1)(X^{18}-1)\cdot (X^{14}-1)(X^{12}-1)(X^8-1)(X^2-1) \right\}$	
$F_{4,4}$	$X^{24}(X^{12}-1)(X^8-1)(X^6-1)(X^2-1)$	
$G_{2,2}$	$X^6(X^6-1)(X^2-1)$	
${}^2A_{n,\lfloor\frac{n+1}{2}\rfloor}$	$X^{n(n+1)/2}\prod_{i=1}^{n}(X^{i+1}-(-1)^{i+1})$	for $n \geq 2$
${}^2D_{n,n-1}$	$X^{n(n-1)}(X^n+1)\prod_{i=1}^{n-1}(X^{2i}-1)$	for $n \geq 4$
${}^3D_{4,2}$	$X^{12}(X^8+X^4+1)(X^6-1)(X^2-1)$	
${}^2E_{6,4}$	$\left\{ X^{36}(X^{12}-1)(X^9+1)(X^8-1)\cdot (X^6-1)(X^5+1)(X^2-1) \right\}$	

We will call a formula like $P(X)$ a *rationality formula* for the corresponding group. One must bear in mind that the rationality formulas for outer types only apply to the field of definition: groups split over extensions in general. Thus $P(\#\mathbb{F}_{\mathfrak{p}^t}) = \#G(\mathbb{F}_{\mathfrak{p}^t})$ may have coefficients which depend on t.

Over $\mathbb{F}_{\mathfrak{p}}$, a notable fact is that r is completely determined once X_n and g are known. Over number fields, there may be several corresponding values of r; one can find the possible indices in [Ti66, Table II], and there is one additional possibility, *viz.* ${}^6D_{4,r}$, which cannot be realised over $\mathbb{F}_{\mathfrak{p}}$ as S_3 cannot be a Galois group thereover.

4.5.5 Almost k-simple connected semisimple k-groups

We recall the notations $S, T, X, \Phi, \Delta, \Delta_0, \Delta_k, \mathcal{D}, An(G), *$-action. Let G be a group as in the heading: we assume it to be of adjoint type.

Let m be the least Galois splitting field for G, and l the inner field [4.5.2] for G. All fields introduced subsequently in this subsection lie between k and m. If f is such a field we write Γ_f for $Gal(k^s/f)$, and H_f for the left coset space Γ/Γ_f. If f/k is normal, we take H_f as $Gal(f/k)$. Note that we have $\Gamma_m \subseteq \Gamma_l \subseteq \Gamma = \Gamma_k$, both normal in Γ, and Γ_l/Γ_m is isomorphic to the kernel of the obvious map $H_m \twoheadrightarrow H_l$. One more useful notation: for $c \in \mathbb{Z}^+$, we write I_c for $\{1, \ldots, c\}$.

Since T is m-split, H_m acts on X, and so on Δ *via* the $*$-action. Further, H_l acts effectively on Δ *via* the same action, so acts on $\mathbb{Z}\Phi$ by linearity, and hence on X, as G is of adjoint type.

Recall that the connected components of $\mathcal{D}$ are (directed-)graph isomorphic, of type X_n, say, where X_n is one of the usual symbols. We will suppose that there are a such Dynkin components.

We use, on each component of $\mathcal{D}$, the standard numbering of the nodes, which we now describe.

For *unbranched* diagrams A_n, B_n, C_n, F_4 or G_2, the nodes are numbered 1 to n along the chain, with the n^{th} node being drawn at the right-hand end (so is *short* for B_n and *long* for C_n, F_4 and G_2).

For *branched* diagrams, we number the nodes 1 to $n-1$ from left to right, and the n^{th} node is then attached to the $(n-2)^{th}$ for D_n, or to the $(n-3)^{th}$ for the E_n.

Thus we have $\mathcal{D} = \coprod_{r=1}^{a} X_n$; we will write (r,s) for the s^{th} node of the r^{th} component, and $\mathcal{D}_r$ for the r^{th} component itself.

The following can be found in [Ti66, 3.1.2]. Recall the Weil restriction functor $R_{f/k}$ for finite separable f/k [2.8].

Theorem 4.5.5.1 *(For connected semisimple almost k-simple adjoint k-group G.) There exist a field f, separable over k with $[f:k] = a$, and a connected almost simple f-group H, such that G is strictly k-isogenous to $R_{f/k}(H)$. Further, $An(G)$ is strictly k-isogenous to $R_{f/k}(An(H))$, and the k-index of G can be deduced from the f-index for H by the procedure described in detail below. By taking the adjoint form of H we can suppose that both these isogenies are actually k-isomorphisms.*

The theorem implies that we have a known action of Γ_f on $\mathcal{D}_1$. We will extend this to an action of Γ on $\mathcal{D}$: then Δ_0 (respectively, the distinguished orbits) for G with respect to k will be the transforms under Γ of Δ_0 (respectively, of the distinguished orbits) for H with respect to f.

The systematization which follows ought to render possible explicit calculations of Hasse-Weil zeta functions for all connected semisimple groups over number fields, though the general case remains out of reach at the time of writing.

We choose a set $\alpha_1, \ldots, \alpha_a$ in Γ such that $\Gamma = \coprod_r \alpha_r \Gamma_f$, with $\alpha_1 = 1$. In fact we will choose the α_r in a particular way. First, suppose that

$$\mathcal{N}_\Gamma(\Gamma_f) = \coprod_{i \in I_b} \rho_i \Gamma_f, \text{ with } \rho_1 = e.$$

Next, we write

$$\Gamma = \coprod_{j \in I_d} \sigma_j \mathcal{N}_\Gamma(\Gamma_f) \text{ with } \sigma_1 = e.$$

Thus $bd = a$, and d is the number of distinct fields which are k-conjugate to f (equivalently, distinct subgroups of Γ containing Γ_m and conjugate to Γ_f). Finally, we define α_r, for $r \in I_a$, by $\alpha_r = \sigma_j \rho_i$, where $j \in I_d$, $i \in I_b$ and $r = id + j - d$. One verifies that this

assignment defines a bijection $I_a \longleftrightarrow I_b \times I_d$, and that the resulting left cosets are distinct, as required. For $t \in I_a$, we write Γ_t for the subgroup $\alpha_t \Gamma_f \alpha_t^{-1}$ of Γ (so Γ_f is the same as Γ_1, but there should be no confusion). We make the further observation that the set $\{\alpha_j \alpha_t \alpha_j^{-1} : t \in I_a\}$ gives an exactly analogous set of left coset representatives for Γ_j in Γ.

We define an action of Γ on I_a thus: for $x \in \Gamma$ and $j \in I_a$, $x.j$ is defined by the relation $\alpha_{x.j}\Gamma_f = x.\alpha_j \Gamma_f$ - this amounts to the obvious action of Γ on the left coset space Γ/Γ_f. We note that the stabilizer of $t \in I_a$ with respect to this action is Γ_t, and the action is independent of the coset representatives α_r chosen.

We are now able to define the whole action of Γ on Δ. For $x \in \Gamma$, we define $x.(j,r)$ to be $(k(j), y(j).r)$ where $x = \alpha_{k(j)} y(j) (\alpha_j)^{-1}$ for some (uniquely determined) $k(j) \in I_a$ and $y(j) \in \Gamma_1$. One can verify straightforwardly that this is a well-defined group action and has all the desired properties. It does depend on the α_r, though this does not matter.

We record the above construction in the following result.

Proposition 4.5.5.2 *(With the above notation.)*
The $*$-action of Γ on $\mathcal{D}$ is given in terms of that of Γ_f on $\mathcal{D}_1$ and the coset representatives α_r by the formula

$$x.(j,r) = (k(j), y(j).r)$$

for each $x \in \Gamma$, $j \in I_a$ and $r \in I_n^*$, where $x = \alpha_{k(j)} y(j) (\alpha_j)^{-1}$

Elementarily, each orbit $\mathcal{O}$ intersects each (Dynkin) component $\mathcal{D}_j$, and by symmetry, does so in the same number of nodes. Furthermore, if $(j,r) \in \mathcal{O} \cap \mathcal{D}_j$, then the orbit under action by Γ_j which contains (j,r) equals $\mathcal{O} \cap \mathcal{D}_j$:- in other words, $\mathcal{D}_j \cap \Gamma.(j,r) = \Gamma_j.(j,r)$. Hence the cardinality of $\mathcal{O}$ is one of a, $2a$, or $3a$.

If $\mathcal{D}_1$ is <u>not</u> of type E_6, we will call the orbit containing $(1,n)$ the *main orbit* M of the action: this is an orbit of maximal cardinality, and case-by-case verification shows that the action is determined completely by its restriction to M. (In the case of E_6, we take for M the orbit containing $(1,1)$.) Thus we have an effective transitive action of H_l on M.

Proposition 4.5.5.3 *If $\Gamma_f \lhd \Gamma$, then for $y \in \Gamma_f$, $y.(j,r) = (j, y(r))$ where $y(r)$ is independent of j. (*Viz. *Γ_f stabilizes all components and acts the same way on each $\mathcal{D}_j$.)*

Chapter 5

Reduction modulo Primes

5.1 Algebraic number theory

5.1.1 Algebraic number fields

We recall here some standard properties of and notations for algebraic number fields (henceforth 'number fields') which we will require. A suitable reference for this section is [Ma77].

A *number field* K is a finite extension of $\mathbb{Q}$. The subset $\mathbb{Z}_K$ consisting of elements which satisfy *monic* polynomials with coefficients in $\mathbb{Z}$ is called the *ring of integers of* K. $\mathbb{Z}_K$ is a Dedekind domain with field of fractions K, but not necessarily a principal ideal domain. In particular, all nonzero prime ideals of $\mathbb{Z}_K$ are maximal, and there is unique factorization of nonzero ideals into products of maximals. We will often call such maximal ideals *K-prime*, as there could rarely be confusion with the zero ideal of K, and the set of all K-primes will be denoted $\mathcal{M}_K$. Each K-prime $\mathfrak{p}$ induces a discrete valuation $||_\mathfrak{p}$ on K *via* the localization $(\mathbb{Z}_K)_\mathfrak{p}$ of $\mathbb{Z}_K$, and the units of the localized ring are called *$\mathfrak{p}$-units*. The (finite) residue field $\mathbb{Z}_K/\mathfrak{p}$ corresponding to $\mathfrak{p}$ will be denoted $\mathbb{F}_\mathfrak{p}$, and the cardinality of this field by $N\mathfrak{p}$. Recall that the absolute norm map N just defined extends multiplicatively to all nonzero ideals in $\mathbb{Z}_K$. We often use the fact that for each $x \in K \setminus \{0\}$, there are only finitely many K-primes $\mathfrak{p}$ such that x is not a $\mathfrak{p}$-unit.

Of interest in general is the behaviour of K-primes $\mathfrak{p}$ under an extension L of degree n over K. It can be shown that $\mathfrak{p}\mathbb{Z}_L$ is a proper ideal of $\mathbb{Z}_L$, and that (as the latter is Dedekind) $\mathfrak{p} = \mathfrak{q}_1^{e_1} \ldots \mathfrak{q}_r^{e_r}$, where the $\mathfrak{q}_i$ are L-primes, each with a corresponding *ramification index* e_i, and *residual degree* f_i, this latter being the degree of the extension $\mathbb{Z}_L/\mathfrak{q}_i \supseteq \mathbb{Z}_K/\mathfrak{p}$. Further, one has the relation $n = \sum_{i=1}^{i=r} e_i f_i$. The $\mathfrak{q}_i$ are said to *lie above* $\mathfrak{p}$. Some terminology (all relating to the extension L/K): $\mathfrak{p}$ is *split* if $r = n$, *inert* if $r = 1$ and $f_1 = n$, and *unramified* if each $e_i = 1$. We often say that an L-prime $\mathfrak{q}$ is *unramified* if the unique K-prime $\mathfrak{p}$ satisfying $\mathfrak{q} \cap \mathbb{Z}_K = \mathfrak{p}$ is unramified in L. If not unramified, it is *ramified*, and it is a standard fact that only finitely many K-primes are ramified in L (for each fixed L).

We now suppose in addition that L/K is Galois, with $A = Gal(L/K)$. Then for each fixed $\mathfrak{p}$ the $e_i = e$ are all the same, and the $f_i = f$ are all the same (though not the same for all K-primes $\mathfrak{p}$). It can be shown that A acts transitively on the $\mathfrak{q}_i$ which lie above a given $\mathfrak{p}$, and one defines the *decomposition group* D_i of $\mathfrak{q}_i$ to be its isotropy group with respect to this action. Clearly, the various $\mathfrak{q}_i$ have conjugate decomposition groups of order ef. One also has an induced surjection $D_i \longrightarrow Gal(\mathbb{F}_{q_i}/\mathbb{F}_\mathfrak{p})$, whose kernel is called the *inertia group* of $\mathfrak{q}_i$. In particular, if $\mathfrak{p}$ is unramified, then D_i is cyclic of order f, and, further, there is a distinguished generator of D_i, the Frobenius element of $\mathfrak{q}_i$. To describe this, we note that $Gal(\mathbb{F}_{q_i}/\mathbb{F}_\mathfrak{p})$ is generated by the mapping $x \mapsto x^{N\mathfrak{p}}$. The element of D_i corresponding to this is called the *Frobenius element* of $\mathfrak{q}_i$. Then the *Frobenius class* $Fr\,\mathfrak{p}$ of $\mathfrak{p}$ is the conjugacy class in A containing this element, and this does not depend on i.

We will refer later to the next two results. The *(Dirichlet) density* of a subset S of $\mathcal{M}_K$ is defined to be

$$D = \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in S} N\mathfrak{p}^{-s}}{\log \frac{1}{s-1}}$$

if this limit exists (in which case $0 \leq D \leq 1$). We only need to know that the density of finite sets S exists and is zero. For more details we refer to [La70, VIII,§4].

Proposition 5.1.1.1 *If M is an intermediate extension, Galois over K, then the image of*

D_i under the obvious map from A to $A/Gal(L/M)$ is the decomposition group for $\mathfrak{q}_i \cap \mathbb{Z}_M$ over $\mathfrak{p}$.

Theorem 5.1.1.2 (Čebotarev) *[La70, VIII,§4, Thm.10]*

Let A be the Galois group of the extension L/K of number fields. Then, for each conjugacy class C in A, the set of K-primes whose Frobenius class is C has a density, and this density is $\#C/\#A$.

5.2 Zeta and L-functions

Here we recall the definitions of the standard types of zeta function which we will require (and the pertinent properties thereconcerning). K is a number field throughout. The first thing to note is their independence of the choices of algebraically closed overfields made.

For $x \in \mathbb{R}$, we write H_x for $\{z \in \mathbb{C} : Re(z) > x\}$.

5.2.1 Dedekind zeta functions

The *Dedekind zeta function of K* is that function of the complex variable s defined by

$$\zeta_K(s) = \sum_{0 \neq I \lhd \mathbb{Z}_K} N(I)^{-s} \qquad (s \in H_1)$$

We refer to [He67, §2] for the following. The series converges absolutely on H_1, and extends to a meromorphic function on $\mathbb{C}$ with a simple pole at $s = 1$. Furthermore, there is an *Euler product* of the sum, which converges absolutely (and locally uniformly) to $\zeta_K(s)$ on H_1, given (*via* the multiplicative property of N) by

$$\prod_{\mathfrak{p} \in \mathcal{M}_K} (1 - N\mathfrak{p}^{-s})^{-1}.$$

There is a functional equation relating $\zeta_K(s)$ to $\zeta_K(1-s)$ *via* the gamma function Γ. We record this as

Proposition 5.2.1.1 *[La70, XIII§3]*

$$\zeta_K(s) = |D|^{1/2-s}\left(\frac{\pi^{s-1/2}\Gamma(1/2-s/2)}{\Gamma(s/2)}\right)^{r_1}\left(\frac{(2\pi)^{2s-1}\Gamma(1-s)}{\Gamma(s)}\right)^{r_2}\zeta_K(1-s)$$

where r_1,r_2 are the numbers of real (respectively complex) embeddings of K, and $|D|$ is the (absolute value of its) discriminant.

We write the functional equation as $\zeta_K(s) = Y(s)\zeta_K(1-s)$, though it could clearly be put in the form $X(s) = X(1-s)$ with X meromorphic.

5.2.2 Artin L-functions

Let X be a finite group and R be a principal ideal domain, assumed to be a subring of $\mathbb{C}$. For our purposes, an *R-representation of X* is a group homomorphism $\theta : X \longrightarrow Aut_R(V)$ for some finitely generated free R-module V whose rank is the *degree* of θ. We recall that $Aut_R(V) \cong GL(\text{rank}\, V, R)$ as abstract groups.

The *character of θ* is the map $\chi : X \longrightarrow \mathbb{C}$ given by $x \mapsto$ *(the trace of)* $\theta(x)$. The fibres of χ are unions of conjugacy classes of X. The conjugate $\overline{\chi}$ of χ is also a character of X, that of the *contragredient* representation to θ, of which we need know no more than the existence.

θ is called *trivial* (and the corresponding character *principal*) if X acts trivially on V. θ is said to be *reducible* if $V = V_1 \oplus V_2$ with the V_i being nonzero X-stable R-submodules of V. Otherwise θ is *irreducible* (and the corresponding character is *simple*). The R-representations $\theta_i : X \longrightarrow GL(V_i)$ $(i = 1, 2)$ are *R-equivalent* if there is an R-isomorphism $f : V_1 \longrightarrow V_2$ such that $\theta_2(x) = f \circ \theta_1(x) \circ f^{-1}$ $\forall x \in X$.

We will need the cases in which R is $\mathbb{C}$ or $\mathbb{Z}$, and adopt the convention that omission of mention of R signifies its adoption as $\mathbb{C}$. Finally, the r^{th} exterior power $\Lambda^r\theta$ of a representation θ is defined by $\Lambda^r\theta(x) = \theta(x) \wedge \cdots \wedge \theta(x)$.

The following is well-known.

Proposition 5.2.2.1

(i) Two irreducible representations of X are equivalent iff they have the same character.

(ii) There is a bijection between the conjugacy classes in X and its distinct simple characters.

Next, let M be a finite Galois extension of K with group Ξ. For a representation

$$\theta : \Xi \longrightarrow GL_n(\mathbb{C})$$

of Ξ with character χ, we define the *Artin L-function* by

$$L(\Xi, \chi, s) \text{ or } L(M/K, \chi, s) = (\dagger) \prod_{\substack{\mathfrak{p} \in \mathcal{M}_K \\ \mathfrak{p} \text{ unramified in } M}} \det(I - \theta(Fr\,\mathfrak{p})N\mathfrak{p}^{-s})^{-1} \qquad (s \in H_1)$$

where $(\dagger)$ is a product of modified factors for the K-primes which ramify in M, while I is the $n \times n$ identity matrix. These modified factors will not concern us. Note the simplification when Ξ is abelian, and that the principal character simply gives us $\zeta_K(s)$, or at least that part of it corresponding to the primes unramified in M.

It can be shown [He67, Thm 7] that $L(M/K, \chi, s)$ is holomorphic on H_1, and extends to a meromorphic function on $\mathbb{C}$. If χ is simple, $L(M/K, \chi, s)$ is nonzero on the closure of H_1 unless χ is principal (in which case there is a simple pole at 1). A famous conjecture of E. Artin *(loc.cit.)* asserts the non-existence of any other pole for any simple χ.

Proposition 5.2.2.2 *[He67, 3.10,Thm.7 ff] Let M be a Galois extension of K.*

(1) The (Dedekind) zeta functions for M and K are related by

$$\zeta_M(s) = \prod_{\chi} L(M/K, \chi, s)^{\chi(id)} \qquad (s \in H_1)$$

where χ runs through the simple characters of Ξ.

(2) $L(M/K, \chi, s)$ satisfies a functional equation relating it to $L(M/K, \overline{\chi}, 1-s)$.

Note that this last strictly only makes sense (as formulated so far) for the local factors corresponding to unramified K-primes, but the modified factors are so constructed as to make [5.2.2.2] hold in general *(loc.cit.)*. We shall not need such a refinement.

5.2.3 Weil and Hasse-Weil zeta functions

The Weil zeta function is defined for 'schemes of finite type' over a finite field $\mathbb{F}_q$ of q elements [Se65], but we will only need it for affine varieties over $\mathbb{F}_q$, when it is defined thus: recall [2.5] that if we have $\mathbb{F}_q \subseteq \mathbb{F}_{q^r} \subseteq \mathbb{E}$, and an affine variety V over $\mathbb{F}_q$, the $\mathbb{F}_{q^r}$-rational points of V can be identified with the finite set $\mathrm{Hom}_{\mathbb{F}_q-alg}(\mathbb{F}_q[V], \mathbb{F}_{q^r})$. If N_r denotes the cardinality of this set, then the *Weil zeta function* for V over $\mathbb{F}_q$ is defined to be

$$Z(V, \mathbb{F}_q, t) = \exp \sum_{r=1}^{\infty} N_r t^r / r$$

and it is easily seen that $Z(V, \mathbb{F}_q, t) \in \mathbb{Q}[[t]]$ (a power series in t over $\mathbb{Q}$). There is an obvious extension of the notion to projective V over $\mathbb{F}_q$. One also has the following elementary 'base-change' formula

$$Z(V, \mathbb{F}_{q^s}, t^s) = \prod_{j=0}^{s-1} Z(V, \mathbb{F}_q, \rho^j t)$$

where ρ is a primitive s^{th} root of unity.

To form the *Hasse-Weil zeta function* of a K-variety V, one performs the operation of 'reducing it mod $\mathfrak{p}$' for each $\mathfrak{p}$ in $\mathcal{M}_K$ (this process is described separately in [5.3]), so obtaining a variety $V_\mathfrak{p}$ over the residue field $\mathbb{F}_\mathfrak{p}$, and forms the product of the corresponding Weil zeta functions, *viz.*

$$\zeta(V, K, s) := (\dagger) \prod_{\forall^* \mathfrak{p} \in \mathcal{M}_K} Z(V_\mathfrak{p}, \mathbb{F}_\mathfrak{p}, (N\mathfrak{p})^{-s})$$

where

(a) the convenient notation $\forall^* \mathfrak{p}$ means 'for all but finitely many $\mathfrak{p}$'; and

(b) we denote by $(\dagger)$ factors corresponding to a finite subset of $\mathcal{M}_K$ which it is necessary to omit.

Implicit in the definition is the identification of Hasse-Weil zeta functions whose local factors are the same $\forall^* \mathfrak{p}$.

5.3 Reduction mod $\mathfrak{p}$

5.3.1 Definitions

Given an affine K-variety V where K is a number field, we define, for each discrete valuation ring $R_\mathfrak{p}$ of K, where $\mathfrak{p}$ is the corresponding K-prime, a variety $V_\mathfrak{p}$ over the residue class field $\mathbb{F}_\mathfrak{p}$. We note that one often has that properties of V pass to $V_\mathfrak{p}$ $\forall^*\mathfrak{p}$ [*viz.* there may be finitely many primes for which the property does not hold], rather than for every $\mathfrak{p}$. We will ignore the archimedean primes of K completely.

Though the process of reduction mod $\mathfrak{p}$ has an intrinsic description as a fibre product of schemes [Mu88, II.4], this does not seem well suited to calculation, and we will present an earlier approach due to Shimura [Sh55]. His terminology has been superseded, so a little care is needed in reading his paper.

Shimura defines reduction mod $\mathfrak{p}$ as follows (we specialize his construction to the case of number fields). Pick a universal domain over K and over each of its residue fields $\mathbb{F}_\mathfrak{p}$. Denote these by S and $\Sigma_\mathfrak{p}$ respectively. (Following Shimura, we use Roman letters in number fields and Greek letters in finite fields.) We take all of our varieties as being embedded in affine spaces over these fields and of course assume that all fields considered are contained in these latter.

Take now a point $x \in S^n$, say $x = (x_1, \ldots, x_n)$, and $\xi = (\xi_1, \ldots, \xi_n) \in (\Sigma_\mathfrak{p})^n$. We say that ξ *is a specialization of* x *(over* $R_\mathfrak{p}$*)* if the natural map $R_\mathfrak{p} \twoheadrightarrow \mathbb{F}_\mathfrak{p}$ has an extension to a ring morphism

$$R_\mathfrak{p}[x_1, \ldots, x_n] \twoheadrightarrow \mathbb{F}_\mathfrak{p}[\xi_1, \ldots, \xi_n] \text{ with } x_i \to \xi_i \ \forall i \in \{1, \ldots, n\}.$$

We will again follow Shimura in using the convenient notation $(x) \xrightarrow{R_\mathfrak{p}} (\xi)$ to describe this situation.

This property is equivalent to the following: whenever

$$g(X) \in R_\mathfrak{p}[X_1, \ldots, X_n] \text{ satisfies } g(x_1, \ldots, x_n) = 0, \text{ then } \gamma(\xi_1, \ldots, \xi_n) = 0,$$

where γ denotes the class of g mod $\mathfrak{p}$. Clearly this shows that the transcendence degree of $K(x_1, \ldots, x_n)$ over K is at least that of $\mathbb{F}_\mathfrak{p}(\xi_1, \ldots, \xi_n)$ over $\mathbb{F}_\mathfrak{p}$. In other words, dimension

cannot increase along a specialization. An essential tool in Shimura's formulation is the *specialization ring* $[(x) \xrightarrow{R_\mathfrak{p}} (\xi)]$, namely

$$\{F(x_1,\ldots,x_n)/G(x_1,\ldots,x_n) : F,G \in R_\mathfrak{p}[x_1,\ldots,x_n] \text{ such that } G_\mathfrak{p}(\xi_1,\ldots,\xi_n) \neq 0\}$$

which is just the maximal localization of $R_\mathfrak{p}[x_1,\ldots,x_n]$ *via* which the extended ring homomorphism above will factor. This characterizes (for a given specialization) the rational functions $H[\{x_i\}]$ which reduce mod $\mathfrak{p}$ to the corresponding $H_\mathfrak{p}[\{\xi_i\}]$: note that this holds in particular for polynomials satisfied by $\{x_1,\ldots,x_n\}$.

Next, given a variety V $(\subseteq S^n)$ as above, we define its *reduction mod* $\mathfrak{p}$, denoted $V_\mathfrak{p}$, to be that subset of $\Sigma_\mathfrak{p}^n$ consisting of all points which are specializations of points of V over $R_\mathfrak{p}$. We remark that $V_\mathfrak{p}$ may be empty even if V is not.

Analogous to the above is the notion of a *generic point (over K)*, where one uses the zero ideal of $\mathbb{Z}_K$: note that $K = R_0$ in our notation. Taking $(x) \in S^n$, the affine variety in which x is generic (over K) is the subset of S^n consisting of all points which are specializations of x over R_0. This is the approach which is adopted in [We46]. Weil specializes over fields: Shimura extends Weil's theory to local domains (which we can always take as Noetherian).

5.3.2 Basic facts

We will use the following elementary result.

Proposition 5.3.2.1 *[Sh55, §1] (With the above notations.)*

(a) *If we have* $(x) \xrightarrow{K} (y)$ *and* $(y) \xrightarrow{R_\mathfrak{p}} (\eta)$ *then* $(x) \xrightarrow{R_\mathfrak{p}} (\eta)$.

(b) *If we have* $(x) \xrightarrow{R_\mathfrak{p}} (\eta)$ *and* $(\eta) \xrightarrow{\mathbb{F}_\mathfrak{p}} (\upsilon)$ *then* $(x) \xrightarrow{R_\mathfrak{p}} (\upsilon)$.

We now start to assemble the properties of reduction mod $\mathfrak{p}$ required, and will either prove or adduce a source of proof in each case. In fact, most of the properties of linear algebraic groups which we will require are almost always preserved by reduction mod $\mathfrak{p}$. The best source of proofs of this sort of result known to the author is [Ono58], though we will also need some results merely asserted in the literature.

Proposition 5.3.2.2 *[Sh55]*

Let V and W be non-empty affine K-varieties (K a number field) (and K-subvarieties of ambient spaces S^m, S^n as necessary for the hypotheses of the statements following).

(i) If V is absolutely irreducible, so is $V_\mathfrak{p}$ $\forall^*\mathfrak{p}$ [§6, Thm.26]Sh.

(ii) If the components of V all have the same dimension d, then all components of $V_\mathfrak{p}$ have dimension d also $\forall^*\mathfrak{p}$ [Sh55, §3,Prop.19].

(iii) If L is a finite extension of K, and $\mathfrak{q}$ a prime of L, with $\mathfrak{p}$ its restriction to $\mathbb{Z}_K$, then $V_\mathfrak{p}$ and $V_\mathfrak{q}$ coincide as varieties over $\Sigma_\mathfrak{p}$ [Sh55, §3,Thm.7].

(iv) Reduction mod $\mathfrak{p}$ commutes with the formation of finite products and unions [Sh55, §3,Prop.18].

(v) $(V \cap W)_\mathfrak{p} \subseteq V_\mathfrak{p} \cap W_\mathfrak{p}$ [Sh55, §3,Prop.18].

(vi) If $f : V \longrightarrow W$ is a K-morphism of varieties, then $\forall^*\mathfrak{p}$, $f_\mathfrak{p}$ is an $\mathbb{F}_\mathfrak{p}$-morphism from $V_\mathfrak{p}$ to $W_\mathfrak{p}$.

Part *(vi)* of the last result is not in [Sh55], but is easily seen.

Proposition 5.3.2.3 *[Ono58]*

Let G and H be K-groups (which we take as K-subgroups of $GL_n(\mathbb{C})$), and A a K-subgroup of G.

(i) For almost all $\mathfrak{p}$ of $\mathcal{M}_K$, $G_\mathfrak{p}$ is an algebraic group over $\mathbb{F}_\mathfrak{p}$ [Ono58, 1.1].

(ii) If G is unipotent, so is $G_\mathfrak{p}$ [Ono58, 1.10].

(iii) $\dim(G_\mathfrak{p} \cap H_\mathfrak{p}) = \dim(G \cap H)_\mathfrak{p} = \dim(G \cap H)$ $\forall^*\mathfrak{p}$ *[Ono58, 2.3].*

(iv) $\mathcal{Z}_G(A)_\mathfrak{p} \subseteq \mathcal{Z}_{G_\mathfrak{p}}(A_\mathfrak{p})$ and $\mathcal{N}_G(A)_\mathfrak{p} \subseteq \mathcal{N}_{G_\mathfrak{p}}(A_\mathfrak{p})$ $\forall^*\mathfrak{p}$ [Ono58, 1.2 and 1.4].

(v) If G is solvable (respectively, nilpotent), so is $G_\mathfrak{p}$ [Ono58, 1.8].

(vi) If A is a torus (respectively, a maximal torus) in G, so is $A_\mathfrak{p}$ in $G_\mathfrak{p}$ $\forall^*\mathfrak{p}$ [Ono58, 2.4,2.15].

(vii) If A is a Borel subgroup of G, so is $A_\mathfrak{p}$ in $G_\mathfrak{p}$ $\forall^*\mathfrak{p}$ [Ono58, 2.10].

Many of the converses [at least $\forall^*\mathfrak{p}$] to the statements above are also true , though we will not need them. One should note that, in *(vii)*, the existence of such Borel subgroups cannot be guaranteed.

5.4 Preservation theorems

We include here some results and some proofs which do not appear to be in the literature. Recall that $\#G$ denotes the number of components of the group G.

5.4.1 Irreducible components

Proposition 5.4.1.1 (Preservation of components)
If G is a K-group, then $\#G_{\mathfrak{p}} = \#G$ $\forall^*\mathfrak{p}$.

Proof: We write $G = \coprod_{i\in I} a_i G^0$. By (finitely) extending K, we can assume that each a_i is K-rational, and that each of these components reduces $\forall^*\mathfrak{p}$ to an irreducible $\mathbb{F}_{\mathfrak{p}}$-variety, of the same dimension as G^0, and these latter are components of $G_{\mathfrak{p}}$. It only remains to show them disjoint, for which it suffices to show (taking an affine embedding) that if $u, v \in K^n$ satisfy $u_{\mathfrak{p}} = v_{\mathfrak{p}}$ $\forall^*\mathfrak{p}$, then $u = v$. But if $u \neq v$, then for some i (say) the i^{th} coordinates of u, v cannot agree mod $\mathfrak{p}$ for infinitely many $\mathfrak{p}$. □

5.4.2 Exactness and isogenies

The first clause of the following is asserted in [Ono65, 1.2], but the present author has not been able to locate proofs of either part in the literature.

Proposition 5.4.2.1 (Preservation of exactness and isogenies)
Let $1 \to A \xrightarrow{f} B \xrightarrow{g} C \to 1$ be a K-sequence.

(i) If A and B (therefore also C) are connected, then $1 \to A_{\mathfrak{p}} \xrightarrow{f_{\mathfrak{p}}} B_{\mathfrak{p}} \xrightarrow{g_{\mathfrak{p}}} C_{\mathfrak{p}} \to 1$ is an $\mathbb{F}_{\mathfrak{p}}$-sequence, $\forall^*\mathfrak{p}$.

(ii) If B is connected and g is a K-isogeny, $g_{\mathfrak{p}}$ is a central $\mathbb{F}_{\mathfrak{p}}$-isogeny $\forall^*\mathfrak{p}$, and, further, $\#\ker g = \#\ker g_{\mathfrak{p}}$ $\forall^*\mathfrak{p}$.

Proof: (i) Ignoring finitely many $\mathfrak{p}$, we can suppose that $A_{\mathfrak{p}}$, $B_{\mathfrak{p}}$ and $C_{\mathfrak{p}}$ are connected, have the same dimensions as A, B, C (respectively), and that $f_{\mathfrak{p}}$ and $g_{\mathfrak{p}}$ are $\mathbb{F}_{\mathfrak{p}}$-group homomorphisms. Clearly $f_{\mathfrak{p}}$ is injective, and trivially $g_{\mathfrak{p}} \circ f_{\mathfrak{p}}$ is the zero map $\forall^*\mathfrak{p}$. We prove first that $g_{\mathfrak{p}}$ is surjective. To do this, we introduce the corresponding sequence of

Lie algebras, namely

$$0 \to \mathcal{L}(A) \xrightarrow{\partial f} \mathcal{L}(B) \xrightarrow{\partial g} \mathcal{L}(C) \to 0.$$

We first prove that this latter sequence is exact.

Firstly, as g is a dominant morphism of irreducible varieties, we know [1.11.0.1] that ∂g is surjective iff g is separable: since $\operatorname{char} K = 0$, this is automatic.

It is easy to see that, if $h : V \longrightarrow W$ is a K-morphism of K-groups, then $(\partial h)_{\mathfrak{p}} = \partial(h_{\mathfrak{p}})$ $\forall^*\mathfrak{p}$ - to see this note that a linear map (which we can suppose is given by a reduced echelon matrix) will reduce mod $\mathfrak{p}$ to a linear map; moreover the bracket operations on $\mathcal{L}(V)$ and $\mathcal{L}(W)$ (K-bilinear, anticommutative maps satisfying the Jacobi identity) certainly can be reduced mod $\mathfrak{p}$, and we get structures of Lie algebra on each of $\mathcal{L}(V)_{\mathfrak{p}}$ and $\mathcal{L}(W)_{\mathfrak{p}}$, and of a homomorphism thereof on $(\partial h)_{\mathfrak{p}}$. Indeed, considering the non-singular minors of the reduced echelon matrix, we see that the rank and nullity of the map are also preserved $\forall^*\mathfrak{p}$.

Applying this last result to f and g, we get that, $\forall^*\mathfrak{p}$,

$$0 \to \mathcal{L}(A_{\mathfrak{p}}) \xrightarrow{\partial(f_{\mathfrak{p}})} \mathcal{L}(B_{\mathfrak{p}}) \xrightarrow{\partial(g_{\mathfrak{p}})} \mathcal{L}(C_{\mathfrak{p}}) \to 0$$

is exact, and so $\dim g_{\mathfrak{p}}(B_{\mathfrak{p}}) = \dim C_{\mathfrak{p}}$, for if these were different then the linear map $\partial g_{\mathfrak{p}}$ would have to factor *via* a linear map to a space of dimension lower than the rank of $\partial g_{\mathfrak{p}}$. Thus $g_{\mathfrak{p}}$ is surjective, and also $(\ker g)_{\mathfrak{p}}$ has finite index $t_{\mathfrak{p}}$ (say) in $\ker(g_{\mathfrak{p}})$ $\forall^*\mathfrak{p}$.

To verify that we can $\forall^*\mathfrak{p}$ take $t_{\mathfrak{p}} = 1$, we argue as follows: if we have (for any field F) an F-isomorphism of F-varieties $f : X \longrightarrow Y$, then, as is readily verified, $\forall x \in X$, we have a specialization $(x) \xrightarrow{F} (f(x))$.

Fix any of the remaining primes $\mathfrak{p}$, and suppose the residue field $\mathbb{F}_{\mathfrak{p}}$ extended so that each component of $\ker(g_{\mathfrak{p}})$ has a rational point. Thus these components are pairwise $\mathbb{F}_{\mathfrak{p}}$-isomorphic. If $a : (\ker g)_{\mathfrak{p}} \longrightarrow X$ is such an isomorphism for some component X of $\ker(g_{\mathfrak{p}})$ then we clearly have, for each point $\xi \in X$, a specialization $(\eta) \xrightarrow{\mathbb{F}_{\mathfrak{p}}} (\xi)$ from some $\eta \in (\ker g)_{\mathfrak{p}}$ by definition of $(\ker g)_{\mathfrak{p}}$. But then we have $(x) \xrightarrow{R_{\mathfrak{p}}} (\eta)$ for some $x \in \ker g$, so we can use part *(ii)* of [5.3.2.1] to get $(x) \xrightarrow{R_{\mathfrak{p}}} (\xi)$ and so $\ker(g_{\mathfrak{p}}) \subseteq (\ker g)_{\mathfrak{p}}$, proving (i).

(ii) Under the hypothesis of (ii), a similar argument gives the surjectivity of $\partial g_{\mathfrak{p}} = \partial(g_{\mathfrak{p}})$ and so of $g_{\mathfrak{p}}$: that $g_{\mathfrak{p}}$ is central $\forall^*\mathfrak{p}$ follows from (1) of [3.1.0.2]. By passing to a finite

extension of K, we may assume that $\ker g$ consists of K-rational points, so that, $\forall^* \mathfrak{p}$, each of them has a unique reduction mod $\mathfrak{p}$ and is in the kernel of $g_{\mathfrak{p}}$, while these points are distinct: hence $\#\ker g \leq \#\ker g_{\mathfrak{p}}\ \forall^* \mathfrak{p}$. Conversely, we use [1.9.0.2] to get that

$$\#\ker g_{\mathfrak{p}} \leq [\mathbb{F}_{\mathfrak{p}}(B_{\mathfrak{p}}) : \mathbb{F}_{\mathfrak{p}}(C_{\mathfrak{p}})] \leq [K(B) : K(C)] = \#\ker g.$$

□

Corollary 5.4.2.2

Under the hypothesis of (ii), B and C have the same Hasse-Weil zeta function.

Proof: This now follows from the corresponding local statement, which is given in [4.4.0.2]. □

5.4.3 Centralizers of tori

Let G be a connected K-group, and S a K-torus acting K-morphically thereon. Recall that if Φ denotes the set of roots of S in G, then there is a decomposition

$$\mathfrak{g} = \mathfrak{g}^S \oplus (\oplus_{\alpha \in \Phi} \mathfrak{g}_\alpha)$$

where $\mathfrak{g}_\alpha$ and $\mathfrak{g}^S$ are as at [3.3.3].

Proposition 5.4.3.1 (Preservation of centralizers of tori)

$\forall^* \mathfrak{p}$ of K, $\mathcal{Z}_{G_{\mathfrak{p}}}(S_{\mathfrak{p}}) = \mathcal{Z}_G(S)_{\mathfrak{p}}$

Proof: Since G is connected, so is $\mathcal{Z}_G(S)$ [3.4.1.3], and, $\forall^* \mathfrak{p}$, so are $G_{\mathfrak{p}}$, $S_{\mathfrak{p}}$, $\mathcal{Z}_G(S)_{\mathfrak{p}}$ and $\mathcal{Z}_{G_{\mathfrak{p}}}(S_{\mathfrak{p}})$: we will henceforth assume these so. By part (iv) of [5.3.2.3], we know that $\mathcal{Z}_{G_{\mathfrak{p}}}(S_{\mathfrak{p}}) \supseteq \mathcal{Z}_G(S)_{\mathfrak{p}}$ so need only show that these two groups have the same dimension. Recall too the correspondence between global and infinitesimal centralizers of tori [3.3.3.2]. Thus $\mathfrak{g}^S = \mathcal{L}(\mathcal{Z}_G(S))$ and $\mathfrak{g}_{\mathfrak{p}}^{S_{\mathfrak{p}}} = \mathcal{L}(\mathcal{Z}_{G_{\mathfrak{p}}}(S_{\mathfrak{p}}))\ \forall^* \mathfrak{p}$. We write $\mathfrak{g}^S$ as

$$\mathfrak{g}^S = \bigcap_{s \in S} \{X \in \mathfrak{g} : (Ad\ s)X = X\}$$

Note that, for each $s \in S$, $\{X \in \mathfrak{g} : (Ad\ s)X = X\}$ is a connected unipotent (additive) K-subgroup of $\mathfrak{g}$ (regarded merely as vector space). It follows from part (*iii*) of [5.3.2.3] that, provided we can replace the intersection over S by intersection over a finite subset A of $S(K)$, then $\forall^* \mathfrak{p}$

$$(\mathfrak{g}^S)_{\mathfrak{p}} = (\bigcap_{s \in A} \{X \in \mathfrak{g} : (Ad\ s)X = X\})_{\mathfrak{p}} \cong \bigcap_{\sigma \in A_{\mathfrak{p}}} \{X \in \mathfrak{g}_{\mathfrak{p}} : (Ad\ \sigma)X = X\}$$
$$\supseteq \bigcap_{\sigma \in S_{\mathfrak{p}}} \{X \in \mathfrak{g}_{\mathfrak{p}} : (Ad\ \sigma)X = X\} = {\mathfrak{g}_{\mathfrak{p}}}^{S_{\mathfrak{p}}}$$

so $\dim \mathcal{Z}_G(S) \geq \dim \mathcal{Z}_{G_{\mathfrak{p}}}(S_{\mathfrak{p}})$ and we will be done. It remains to verify that we can find such an $A \subseteq S(K)$. Let us write

$$\mathfrak{l} = \bigcap_{s \in S(K)} \{X \in \mathfrak{g} : (Ad\ s)X = X\}$$

so clearly $\mathfrak{l} \supseteq \mathfrak{g}^S$ and $\mathfrak{l}$ is a connected unipotent subgroup of $\mathfrak{g}$. There is a map

$$h : S \times \mathfrak{l} \longrightarrow \mathfrak{g} \text{ given by } h(s, X) = (Ad\ s)X - X,$$

for $s \in S$, $X \in \mathfrak{g}$. Thus $h(S(K) \times \mathfrak{l}) = 0$. K being perfect, it follows that $\mathfrak{l}$ is K-isomorphic to an affine space, and so K-unirational [4.3.0.4]. S being connected and reductive, with K infinite, it follows that S is also K-unirational and so $S(K)$ is (globally) dense in S [2.7.0.1]. Then $C := S \times \mathfrak{l}$ is again K-unirational, so $C(K) = S(K) \times \mathfrak{l}(K)$ is dense in C. Hence $S(K) \times \mathfrak{l}$ is dense in C, so $h(S(K) \times \mathfrak{l})$ is dense in the closure of $h(C)$. So h is the zero map, and $\mathfrak{l} = \mathfrak{g}^S$. That we can choose a *finite* subset A of $S(K)$ with the claimed property simply follows by induction. □

5.4.4 The radical and unipotent radical

The following is asserted in [Ono66, p122], but not proved.

Proposition 5.4.4.1 (Preservation of radicals)
Let G be a connected K-group. Then, $\forall^* \mathfrak{p}$, the following hold.

(i) $u(G)_{\mathfrak{p}} = u(G_{\mathfrak{p}})$.

(ii) $r(G)_{\mathfrak{p}} = r(G_{\mathfrak{p}})$.

Proof: That $u(G)_{\mathfrak{p}}$ and $r(G)_{\mathfrak{p}}$ are connected normal subgroups of the connected group $G_{\mathfrak{p}}$, with the former unipotent and the latter solvable, $\forall^* \mathfrak{p}$, follows from [5.3.2.3]. Thus $u(G)_{\mathfrak{p}} \subseteq u(G_{\mathfrak{p}})$ and $r(G)_{\mathfrak{p}} \subseteq r(G_{\mathfrak{p}})$. By making a finite extension of K, we may assume [4.3.0.2] that G has a K-split maximal torus T, that all elements of $\mathcal{B}^{\mathrm{T}}$ are defined over K, that $T_{\mathfrak{p}}$ is an $\mathbb{F}_{\mathfrak{p}}$-split maximal torus of $G_{\mathfrak{p}}$, and that $B_{\mathfrak{p}}$ is a Borel subgroup of $G_{\mathfrak{p}}$ for each $B \in \mathcal{B}^{\mathrm{T}}$ [5.3.2.3]. For any connected group H, we have the standard theorem [3.4.7.1] that $u(H) = u(I(S))$, where S is a maximal torus of H and

$$I(S) = (\bigcap_{B \in \mathcal{B}^S} B)^0$$

as usual. Applying this to $G_{\mathfrak{p}}$ and $T_{\mathfrak{p}}$, we get that

$$u(G_{\mathfrak{p}}) = u(I(T_{\mathfrak{p}})) \subseteq u((\bigcap_{\substack{B \in \mathcal{B}^{(T_{\mathfrak{p}})} \\ \text{s.t. } \exists C \in \mathcal{B}^{\mathrm{T}} \\ \text{with } B = C_{\mathfrak{p}}}} B)^0)$$

the inclusion passing to unipotent parts because the groups are connected and solvable.

Now, $\forall^* \mathfrak{p}$, each $C \in \mathcal{B}^{\mathrm{T}}$ passes to some $B \in \mathcal{B}^{(T_{\mathfrak{p}})}$ by reduction mod $\mathfrak{p}$: thus, $\forall^* \mathfrak{p}$, all the elements of $\mathcal{B}^{\mathrm{T}}$ are in the last index set. By [3.4.7.1] again, one gets that

$$\dim u(G_{\mathfrak{p}}) \leq \dim u(G)$$

verifying (i).

For (ii), observe first that we can suppose that G is reductive, for if this case is done, we have that

$$\dim r(G) = \dim r(G/u(G)) + \dim u(G) = \dim r(G_{\mathfrak{p}}/u(G)_{\mathfrak{p}}) + \dim u(G)_{\mathfrak{p}}$$

and know that $u(G)_{\mathfrak{p}} = u(G_{\mathfrak{p}})$, so have $\dim r(G) = \dim r(G_{\mathfrak{p}})$.

We henceforth assume that G is reductive. Under this hypothesis, let $\Phi(G,T)$ be the (finite) set of roots of G with respect to T, so that for $\alpha \in X(T)$ with $T_\alpha := (\ker \alpha)^0$,

$$\alpha \in \Phi(G,T) \Leftrightarrow \mathcal{Z}_G(T_\alpha) \text{ is not solvable}$$

by [3.4.6.1]. Recall that the $\mathcal{Z}_G(T_\alpha)$ are connected reductive K-subgroups of G which strictly contain T [3.4.7.3]. Dimensional considerations, (i), and the finiteness of $\Phi(T,G)$, then guarantee that $\mathcal{Z}_G(T_\alpha)_\mathfrak{p}$ is not solvable for any α, $\forall^*\mathfrak{p}$. Our result [5.4.3.1] says that

$$\mathcal{Z}_G(T_\alpha)_\mathfrak{p} = \mathcal{Z}_{G_\mathfrak{p}}((T_\alpha)_\mathfrak{p})$$

so the latter are all nonsolvable $\forall^*\mathfrak{p}$, and thus for each $\alpha \in \Phi(G,T)$

$$(T_\alpha)_\mathfrak{p} = (\ker\beta)^0$$

for some $\beta \in \Phi(G_\mathfrak{p}, T_\mathfrak{p})$, $G_\mathfrak{p}$ being reductive. We use now the last assertion of [4.2.1.4]

$$r(H) = (\bigcap_{\alpha\in\Phi(H,S)} S_\alpha)^0$$

(for any connected reductive group H with maximal torus S). Applying this to $G_\mathfrak{p}$, $T_\mathfrak{p}$ we have

$$r(G_\mathfrak{p}) = \left(\bigcap_{\alpha\in\Phi(G_\mathfrak{p},T_\mathfrak{p})} T_\alpha\right)^0 \subseteq \left(\bigcap_{\substack{\alpha\in\Phi(G_\mathfrak{p},T_\mathfrak{p}) \\ \text{and } T_\alpha=S_\mathfrak{p} \\ \text{for some } S\leq T}} T_\alpha\right)^0 \subseteq \left(\bigcap_{\substack{\alpha\in\Phi(G_\mathfrak{p},T_\mathfrak{p}) \\ T_\alpha=S_\mathfrak{p} \text{ for some } S\leq T \\ \text{and } \mathcal{Z}_G(S) \text{ nonsolvable}}} T_\alpha\right)^0$$

and the argument above shows that all the (connected components of the) kernels of roots of G with respect to T actually occur in this last index set. So by [4.2.1.4] again, we get $\dim r(G_\mathfrak{p}) \leq \dim r(G)_\mathfrak{p}$ $\forall^*\mathfrak{p}$ and are done. □

5.4.5 Roots and weights

Proposition 5.4.5.1 (Preservation of root systems)

Let G' be a connected reductive K-group with maximal K-torus T', with Θ as the set of weights of T' in G' and Φ as the corresponding set of roots. Then, identifying Θ and

Φ *with subsets of* $X' = X(T')$, *one has,* $\forall^*\mathfrak{p}$, $\Theta_\mathfrak{p}$ *(respectively,* $\Phi_\mathfrak{p}$*) as the set of weights (respectively, roots) of the maximal torus* $T'_\mathfrak{p}$ *of* $G'_\mathfrak{p}$.

Furthermore, $\forall^*\mathfrak{p}$, $\Phi_\mathfrak{p}$ *is a root system in* $X(T'_\mathfrak{p}/r(G'_\mathfrak{p})) \otimes_\mathbb{Z} \mathbb{Q}$, *and these root systems are isomorphic to* Φ $\forall^*\mathfrak{p}$.

Proof: By [3.4.3.4], $T = T'/r(G')$ is a maximal torus of the connected semisimple group $G = G'/r(G')$, and *(loc.cit.)* there is an isomorphism induced from the Weyl group W' associated to $\Phi(T', G')$ to the Weyl group W of $\Phi(T, G)$. Since $r(G')$ is contained in the kernel of each root of T' in G', a map is induced from $\Phi(T', G')$ to $\Phi(T, G)$. These are sets of the same cardinality by [4.2.1], and the map is certainly an injection (considering kernels of roots) so is a bijection. Indeed, it extends to an isomorphism of root systems (as the Cartan integers are preserved too). As $\mathcal{Z}_G(T) = \mathcal{Z}_{G'}(T')/r(G')$ by [3.4.3.1], by preservation of the radical [5.4.4.1], preservation of centralizers of tori [5.4.3.1], and the correspondence of global to infinitesimal centralizers of tori [3.3.3.2], it follows that we need only prove the result for T and G.

The subalgebra $\mathfrak{g}_\mathfrak{p}^{T_\mathfrak{p}}$ of $\mathfrak{g}_\mathfrak{p}$ has the same dimension as $\mathfrak{g}^T$ $\forall^*\mathfrak{p}$, so the rank and cardinality of Φ are preserved $\forall^*\mathfrak{p}$.

We extend K to a splitting field L for G, and work in L henceforth. Recall [4.3.0.1] that each component of $\mathcal{N}_G(T)$ then has an L-rational point, and these reduce mod $\mathfrak{p}$ to the same number of distinct irreducible components of $\mathcal{N}_{G_\mathfrak{p}}(T_\mathfrak{p})$ - the dimension of the normalizer being preserved mod $\mathfrak{p}$ $\forall^*\mathfrak{p}$ by rigidity. Thus we get $\#W_\mathfrak{p} \leq \#W$, where these are the obvious Weyl groups. The reverse inequality follows from the fact that these groups act simply transitively on the sets of Borel subgroups of G (resp. $G_\mathfrak{p}$) containing T (resp. $T_\mathfrak{p}$) [4.2.1.4].

Given $\alpha, \beta \in \Phi(G, T)$, one has

$$< \alpha, \beta^* > = < \alpha_\mathfrak{p}, (\beta^*)_\mathfrak{p} >$$

$\forall^*\mathfrak{p}$, where the coroot α^* of α and $< \alpha, \beta^* > \in \mathbb{Z}$ are defined by the usual relations

$$\alpha \circ \beta^* : \mathbb{G}_m \longrightarrow \mathbb{G}_m$$
$$x \longmapsto x^{<\alpha,\beta^*>}$$
and $< \alpha, \alpha^* > = 2$.

Put $T_\alpha = (\ker \alpha)^0$ as usual: this is defined over L as T is L-split. Clearly, $\forall^* \mathfrak{p}$, $\alpha_\mathfrak{p}$ is well-defined, and is a character of the maximal torus $T_\mathfrak{p}$ of the connected semisimple group $G_\mathfrak{p}$. Moreover, by [3.4.6.1], for $\beta \in X = X(T)$, $\beta \in \Phi$ iff $\mathcal{Z}_G(T_\beta)$ is not solvable. Now, $\mathcal{Z}_G(T_\beta)_\mathfrak{p} = \mathcal{Z}_{G_\mathfrak{p}}((T_\mathfrak{p})_{\beta_\mathfrak{p}})$ $\forall^* \mathfrak{p}$ by [5.4.3.1], so when $\beta \in \Phi$, $\beta_\mathfrak{p} \in \Phi_\mathfrak{p}$ $\forall^* \mathfrak{p}$.

Clearly, $\forall^* \mathfrak{p}$, one gets $(\beta^*)_\mathfrak{p} = (\beta_\mathfrak{p})^*$, and so the coroots are also preserved $\forall^* \mathfrak{p}$. This proves preservation of the Cartan integers $\forall^* \mathfrak{p}$, which demonstrates that all of the following are preserved: root lengths, orthogonality of roots (and so irreducibility of subsystems), and the (abstract) Weyl group because the relations in a (Coxeter) presentation thereof are derived therefrom. This verifies that $\Phi_\mathfrak{p}$ is $\forall^* \mathfrak{p}$, the set of roots of $G_\mathfrak{p}$. Then [5.4.3.1] implies preservation of the weights, and the final assertion follows from [4.2.1.4]. □

In particular, the Dynkin diagram is preserved $\forall^* \mathfrak{p}$.

Chapter 6

Zeta Functions: Split and Simple Groups

6.1 Preliminaries and notation

The key idea in the passage from the number field case to the local case is an action by decomposition groups on characters. Except where otherwise specified, we only consider connected groups. Moreover, we confine our attention to connected reductive groups, not only because there is no loss of generality in doing so, as we will see in a moment, but also because such a group is split iff it has a split maximal torus.

The following notation is fixed throughout this chapter. K is a number field. G always denotes a connected semisimple K-group with inner field l and splitting field m. For any field n such that $K \subseteq n \subseteq K^s$, $\Gamma_n := Gal(K^s/n)$ and H_n denotes the left coset space Γ/Γ_n. We omit the subscript n when $n = K$. H_n is identified with $Gal(n/K)$ when n/K is normal.

T is a maximal torus of G, defined over K, of dimension n and with character module X. The Dynkin diagram of G will be denoted $\mathcal{D}$, and its (graph) components $\mathcal{D}_1, \mathcal{D}_2, \ldots$ or by notation like ${}^g X_{n,r}$ as at [4.5.4]. We also use [4.5.2], [4.5.3] the notations $An(G)$ and '$*$-action', for various groups. By default their use is relative to K. Finally we introduce the convenient notation Ξ for $\dim G + \#\Phi^+$ (where Φ^+ is the set of positive roots with

respect to some ordering).

Occasionally additional hypotheses will be imposed. We remark that the zeta function of the trivial group (over K) is the Dedekind zeta function $\zeta_K(s)$ for K.

6.1.1 Reductification

Proposition 6.1.1.1 *If J is a connected K-group, with $\dim u(J) = b$, and reductification R, then $\zeta(J, K, s) = \zeta(R, K, s - b)$.*

Proof: This is immediate from the preservation of $u(J)$ [5.4.4.1], exactness of $\mathbb{F}_\mathfrak{p}$-rational points for $\mathbb{F}_\mathfrak{p}$-sequences [4.4.0.2], and the $\mathbb{F}_\mathfrak{p}$-isomorphism of $u(J)$ with $\mathbb{A}^b$ [4.3.0.4], all $\forall^*\mathfrak{p}$ of course. □

In particular, for connected unipotent J, we have $\zeta(J, K, s) = \zeta_K(s - \dim J)$ - or more precisely almost all of their local factors agree.

6.1.2 General remarks about reduction mod $\mathfrak{p}$

As usual [5.3.2.3], [5.4.4.1], if $\mathfrak{p} \in \mathcal{M}_K$, and has residual degree $f_\mathfrak{p}$ in m, then we may assume that $T_\mathfrak{p}$ is a maximal $\mathbb{F}_\mathfrak{p}$-torus in the connected semisimple $\mathbb{F}_{\mathfrak{p}^{f_\mathfrak{p}}}$-split $\mathbb{F}_\mathfrak{p}$-group $G_\mathfrak{p}$, and that $\mathfrak{p}$ is unramified in m. Thus X is isomorphic to $X_\mathfrak{p} := X(T_\mathfrak{p})$ (say) as abelian groups, $\forall^*\mathfrak{p}$.

If $\mathfrak{q} \in \mathcal{M}_m$ lies above $\mathfrak{p}$, then $D_\mathfrak{q}$ denotes the corresponding decomposition group in H_m.

Proposition 6.1.2.1 *Reduction mod $\mathfrak{p}$ induces an isomorphism (of abelian groups)*

$\theta_\mathfrak{p} : X \longrightarrow X_\mathfrak{p}$ $\forall^*\mathfrak{p}$.

If $\mathfrak{p}$ is a K-prime, unramified in m, for which $\theta_\mathfrak{p}$ is an isomorphism, then $\theta_\mathfrak{p}$ is also $D_\mathfrak{q}$-equivariant for each $\mathfrak{q}$ above $\mathfrak{p}$.

Proof: We choose a basis $x_1, \ldots, x_n$ for X. Since any two such bases are related by an integer matrix of determinant ± 1, the following discussion does not depend on the basis chosen. Thus $X = \sum_i \mathbb{Z}x_i$, and, $\forall^*\mathfrak{p}$, $(x_i)_\mathfrak{p} \in X_\mathfrak{p}$ for each i.

We only consider such primes subsequently. Clearly there is a group homomorphism from X to $X_{\mathfrak{p}}$. Since both are free abelian groups of rank n, it is enough to show surjectivity (as the kernel will then be of rank zero and so trivial).

Choose $\alpha \in X_{\mathfrak{p}}$. So $\alpha : T_{\mathfrak{p}} \longrightarrow \mathbb{G}_m$, and α is defined over $\mathbb{F}_{\mathfrak{q}}$ (this being a splitting field for $T_{\mathfrak{p}}$). Hence there is an m-morphism $s : T \longrightarrow \mathbb{G}_m$ of varieties such that $s_{\mathfrak{p}} = \alpha$ and $s(e_T) = y$ (say) with $y \in \mathbb{G}_m(m)$. Now take $t : T \longrightarrow \mathbb{G}_m$ given by $t(x) = y^{-1}s(x)$. Again t is an m-morphism of varieties while $t_{\mathfrak{p}} = \alpha$ still holds $\forall^*\mathfrak{p}$. But then by [3.3.1.1], $t \in X$.

Under the hypothesis of the second clause, we recall that we have a canonical isomorphism of $D_{\mathfrak{q}}$ with $Gal(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}})$, so we can regard $\theta_{\mathfrak{p}}$ as a bijection of $D_{\mathfrak{q}}$-sets. If σ is a generator for $D_{\mathfrak{q}}$ and $x \in X$ then $\theta_{\mathfrak{p}}(\sigma.x) = \sigma.\theta_{\mathfrak{p}}(x)$ since σ stabilizes $\mathfrak{q}$. □

6.1.3 Property (Z) for K-groups

We will say, for a K-group J, and a finite Galois extension n of K, that J *has property (Z) for* n, *or for* n/K if $\zeta(J, K, s)$ is an alternating product of Artin L-functions for characters of H_n. We will say that J *has property (Z)* if there exists some finite Galois extension n of K such that J has property (Z) with respect to n. We write this down in a slightly more convenient form.

Proposition 6.1.3.1 *Let C be the set of simple characters of H_n.*

The K-group J has property (Z) for n iff there exist, for each $\chi \in C$, integers $a_{\chi,j}$ for $j \geq 0$ (almost all of which are zero) such that

$$\#J_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}^t}) = \sum_{\chi \in C} \sum_{j} a_{\chi,j} N\mathfrak{p}^{jt} \chi([Fr\,\mathfrak{p}]^t). \qquad (\forall t\ \forall^*\mathfrak{p})$$

We now assemble some simplification theorems for the problem of determining which connected groups have property (Z).

Proposition 6.1.3.2

(1) Let $D \xrightarrow{f} E$ be a K-isogeny of connected K-groups. Then $\zeta(D, K, s) = \zeta(E, K, s)$.

(2) Let $1 \to A_1 \to B \to A_2 \to 1$ be a K-sequence, with all groups connected. Suppose that each A_i has property (Z) for n_i. Then B has property (Z) for $n = n_1 n_2$.

(3) If $A_1, \ldots, A_t$ are such that each A_i has property (Z) for n_i, then $A = A_1 \times \cdots \times A_t$ has property (Z) for $n = n_1 \ldots n_t$.

Proof: *(1)* By [5.4.2.1], $\forall^* \mathfrak{p} \in \mathcal{M}_K$, $D_{\mathfrak{p}} \xrightarrow{f_{\mathfrak{p}}} E_{\mathfrak{p}}$ is a central $\mathbb{F}_{\mathfrak{p}}$-isogeny. But then the corresponding local factors in $\zeta(D, K, s)$ and $\zeta(E, K, s)$ are the same by [4.4.0.2].

(2) That n is a finite Galois extension of K is a standard and elementary result. By Galois theory, each $Gal(n_i/K)$ is a quotient group of H_n, say $\theta_i : H_n \twoheadrightarrow Gal(n_i/K)$. Put C_i (respectively, C) for the set of simple characters of $Gal(n_i/K)$ (respectively, of H_n). By [4.4.0.2], we have

$$\#(A_1)_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}^t})\#(A_2)_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}^t}) = \#B_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}^t}) \qquad (\forall t\ \forall^* \mathfrak{p})$$

and by hypothesis, for each $i = 1, 2$

$$\#(A_i)_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}^t}) = \sum_{\chi \in C_i} \sum_j a_{i,\chi,j} \chi([Fr\,\mathfrak{p}]^t) N\mathfrak{p}^{jt}$$

for some collection of integers $a_{i,\chi,j}$. The elements of each C_i can be lifted to elements of C without changing their degrees - *viz.* $\chi \in C_i$ passes to $\chi' \in C$ *via* the definition $\chi'(y) = \chi(\theta_i(y))$. Thus one can write

$$\#(B)_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}^t}) = \sum_{\chi \in C} \sum_j a_{\chi,j} \chi([Fr\,\mathfrak{p}]^t) N\mathfrak{p}^{jt}$$

for some collection of integers $a_{\chi,j}$, and the result follows from [6.1.3.1].

(3) This follows from *(2)* and induction. □

Recall [4.5.1.3] that a connected semisimple K-group is an almost direct product of connected (semisimple) almost K-simple normal K-subgroups, its *almost K-simple factors.*

Corollary 6.1.3.3 *Suppose that the almost K-simple factors $G_1, \ldots, G_t$ of G are such that each G_i has property (Z) for the extension n_i.*

(a) G has property (Z) for $n = n_1 \ldots n_t$.

(b) If n_i is the inner field for G_i for each i, then n is the inner field for G.

Proof: Recall [4.5.1.2] that the product map $G_1 \times \cdots \times G_t \longrightarrow G$ is a central K-isogeny. Then (a) follows from (1) and (3) of [6.1.3.2].

Recall that the Dynkin diagram $\mathcal{D}$ of G is the disjoint union of the Dynkin diagrams $\mathcal{E}_i$ for the G_i and each $\mathcal{E}_i$ is a union of orbits under the $*$-action. If e is any field such that $K \subseteq e \subseteq K^s$, then e is an inner field for G iff Γ_e acts trivially on $\mathcal{D}$. Equivalently, iff Γ_e acts trivially on each of the $\mathcal{E}_i$. Thus any inner field for G contains all the n_i, and the converse is clear. □

6.2 Connected solvable groups

By [3.3.4.1], if we have a connected solvable K-group J, then we have a K-sequence

$$1 \longrightarrow u(J) \longrightarrow J \longrightarrow R \longrightarrow 1$$

where R is a K-torus - (that this is a semi-direct product decomposition for J is not germane, and the section $J \longleftarrow R$ would not necessarily be defined over K anyway). By [5.4.4.1], the decomposition is preserved under reduction mod $\mathfrak{p}$ $\forall^* \mathfrak{p}$. By [6.1.1.1], we can actually assume that J is a K-torus T of dimension n, with Galois splitting field m (say). We now look more closely at this situation.

6.2.1 Tori over finite fields

We consider in this subsection, a torus T of dimension n defined over $F_1 = \mathbb{F}_q$ and F_a-split for some $a \geq 1$, where $F_a = \mathbb{F}_{q^a}$. We write $M_n(\mathbb{Z})$ for the $n \times n$ integer matrices, identified with the ring of (algebraic group) endomorphisms of $\mathbb{G}_m^n$ [3.3.3.1]. Fix an F_a-isomorphism $\theta : T \longrightarrow \mathbb{G}_m^n$. We use the following well-known result.

Theorem 6.2.1.1 (Smith normal form (for $\mathbb{Z}$)) *[Ja74, Thm 3.8]*
Let $A' \in M_n(\mathbb{Z})$. Then there exist P, Q and A, all in $M_n(\mathbb{Z})$, with $A = QA'P^{-1}$, $|\det Q| = |\det P| = 1$, and A diagonal, with diagonal entries $a_1, \ldots, a_n$ satisfying the following conditions.

(1) for $1 \leq i \leq r = \operatorname{rank} A'$, $a_i \geq 1$ and further $a_1 | a_2 | \ldots | a_r$.

(2) $a_{r+1} = a_{r+2} = \cdots = a_n = 0$.

A is uniquely determined by A' and these conditions.

In the notation of the theorem, A is the *Smith normal form* of A', and the a_i are the *invariant factors* of A'.

Now if G' is a Frobenius map on T (for F_1), we have the set of F_1-rational points of $T(F_1) = \{x \in T : G'(x) = x\}$ - this does not depend on the choice of G'. Since G' is also an endomorphism of T, it follows that $\theta \circ G' \circ \theta^{-1} =: G \in M_n(\mathbb{Z})$; also $G^a = q^a I$ where I is the $n \times n$ identity matrix since T is F_a-split. An argument in Serre [Se59, §VI.2] shows that in fact $G = q.M$ where $M \in M_n(\mathbb{Z})$ (and therefore $M^a = I$). We now use θ to transform the determination of $T(F_1)$ into a problem in the standard torus $\mathbb{G}_m^n$. Identifying G to the corresponding matrix M shows that we require to find the solutions of $\{y \in \mathbb{G}_m^n : M.y = qy\}$ where qy means $(qI).y$. Returning to additive notation (recall that $\mathbb{G}_m^n$ is a module over $M_n(\mathbb{Z})$) we see that we require to find the set S (say) which results from solving the 'linear system of equations'

$$S := \{\mathbf{x} \in \mathbb{G}_m^n : N.\mathbf{x} = \mathbf{0}\},$$

where we have written N for $M - qI$.

A necessary condition for some $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{G}_m^n$ to lie in S is the following. If $\mathbf{y} \in S$, then $(\det N)\mathbf{y} = \mathbf{0}$, as one sees by multiplying the system through by the adjoint matrix to N. Hence each y_i is a $(\det N)^{th}$ root of unity - note that $\det N \equiv \pm 1 \bmod q$, so there exists some minimal $b \in \mathbb{Z}^+$ such that all coordinates y_i of all $y \in S$ lie in $\mathbb{G}_m^n(F_b)$. More exactly, we take b to be the least positive solution of the congruence $q^b \equiv 1 \bmod (\det N)$. Let α be a primitive element of F_b (that is, a generator of its multiplicative group F_b^*). Then, taking discrete logarithms with respect to α, we see that for each $x \in F_b^*$ there is a unique integer $i_x \in \{1, 2, \ldots, q^b - 1\}$ such that $\alpha^{i_x} = x$. As we can now restrict our attention to elements of $\mathbb{G}_m^n(F_b)$, putting $m = q^b - 1$ and $\mathbb{Z}_m$ for the integers $\bmod m$, we see that now we can identify S with the set

$$\{y = (y_1, \ldots, y_n) \in \mathbb{Z}_m \times \cdots \times \mathbb{Z}_m : Ny \equiv 0 \bmod m\}.$$

Of course the vector congruence here simply means componentwise congruence mod m. We seek now the cardinality of S. For the purpose of counting the solutions, we can also assume that N is in its Smith normal form, with invariant factors n_i (say) - these are all nonzero. Suppose first that m were a prime power p^a. Then the number of solutions of the system would be $\prod_i (n_i, p^a)$.

Return now to the case of a general m - we use here a version of the Chinese remainder theorem. Since $(\prod_i n_i)|m$ and p^a is the highest power of p which divides m, it follows that $\prod_i (n_i, p^a) = (\prod_i n_i, p^a) = |(\det N, p^a)|$, and taking the product over the prime powers which exactly divide $q^b - 1$ gives $(|\det N|, m) = |\det N|$ for the total number of solutions. Similarly, the number of F_c-rational points of T will be $|\det(M^c - q^c I)|$ for each $c \geq 1$.

6.2.2 Tori over K and connected solvable groups

The discussion in this subsection appears in [Se59, VI,§1,no.3]: we return to the general notation of the chapter. Since H_m acts on X, each element induces an automorphism of $\mathbb{Z}^n$, yielding a representation $A : H_m \longrightarrow GL(n, \mathbb{Z})$ [4.3.0.2]. The discussion [6.1.2.1] shows that $\forall^* \mathfrak{p}$, the corresponding representation for $T_{\mathfrak{p}}$ is $\mathbb{Z}$-equivalent to the restriction of A to the decomposition group (since the various decomposition groups for primes above $\mathfrak{p}$ are mutually conjugate, one obtains $\mathbb{Z}$-conjugate representations therefrom).

We have seen in the last subsection how to find the number of $\mathbb{F}_{\mathfrak{p}^n}$-rational points of $T_{\mathfrak{p}}$: this is $|\det(M^n - q^n I)|$ where $q = N\mathfrak{p}$ and M is $A(Fr\,\mathfrak{p})$. We can now write down the zeta function of $T_{\mathfrak{p}}$ $\forall^* \mathfrak{p}$.

Let $\lambda_1, \ldots, \lambda_n$ be the set of eigenvalues of $A(Fr\,\mathfrak{p})$ (in some order: these are roots of unity as H_m is finite); let I be an appropriate identity matrix, and Φ_h the h^{th} exterior power [Ja74, 7.2] of the diagonal matrix whose entries are $\lambda_1, \ldots, \lambda_n$. Then the zeta function [5.2.3] for $T_{\mathfrak{p}}$ over $\mathbb{F}_{\mathfrak{p}}$ is

$$Z(T_{\mathfrak{p}}, \mathbb{F}_{\mathfrak{p}}, t) = \prod_{h=0}^{h=n} \prod_{i_1<i_2<\cdots<i_h} (1 - \lambda_{i_1}\lambda_{i_2}\ldots\lambda_{i_h}(N\mathfrak{p})^{n-h}t)^{(-1)^{h+1}}$$
$$= \prod_{h=0}^{h=n} \det(I - (N\mathfrak{p})^{n-h}t\Phi_h)^{(-1)^{h+1}}$$

If we write $L_h(s)$ for the Artin L-function corresponding to the h^{th} exterior power $\Lambda^h A$ of (the representation) A, then the Hasse-Weil zeta function for T over K [5.2.3] is

$$\zeta(T, K, s) = (\dagger) \prod_{\mathfrak{p}} Z(T_{\mathfrak{p}}, \mathbb{F}_{\mathfrak{p}}, (N\mathfrak{p})^{-s})$$
$$= (\dagger) \prod_{h=0}^{n} \prod_{\mathfrak{p}} \det(I - (N\mathfrak{p})^{n-h-s}\Phi_h)^{(-1)^{h+1}}$$
$$= (\dagger) \prod_{h=0}^{n} L_h(s + h - n)^{(-1)^h}$$
$$= (\dagger) \prod_{h=0}^{n} L(H_m, \Lambda^h\chi, s + h - n)^{(-1)^h}$$

where we denote by $\Lambda^h\chi$ the character of $\Lambda^h A$. From this, and [6.1.1.1], one can in principle write down the Hasse-Weil zeta function for a connected solvable K-group, and so of $r(G)$.

Proposition 6.2.2.1

(1) Every connected solvable K-group has property (Z) for the splitting field of some maximal K-torus over K.

(2) If every connected almost K-simple K-group has property (Z) over K, then every connected K-group has property (Z) over K.

Proof: *(1)* has just been shown. Let J be a connected K-group, so there is a K-sequence of connected groups $1 \to r(J) \to J \to S \to 1$, with S semisimple. By hypothesis the almost K-simple factors of S have property (Z) over K, and so by [6.1.3.3], S has property (Z) over K also. But then by (1) and [6.1.3.2], J has property (Z) over K. □

6.3 Split groups

While we do not need to consider these cases separately, the formulas obtained are of interest, and we will use them later.

Proposition 6.3.0.1 *Let J be a K-group. Then there is a finite extension M of K, and $P(X) \in \mathbb{Z}[X]$ such that $\forall^* \mathfrak{p}$ of M, $\forall r \geq 1$, $P((N\mathfrak{p})^r)$ is the number of $\mathbb{F}_{(N\mathfrak{p})^r}$-rational points of $J_{\mathfrak{p}}$.*

Proof: We can extend K to an M so that (i) each component of J has an M-rational point, (ii) $r(J)$ is M-split, and (iii) for some maximal K-torus T of $I := J^0/r(J)$, T is contained in a Borel subgroup B of I with B split over M. Each of these requirements can be realized over some finite extension of K [3.1.0.3], [4.3.0.2] and [4.3.0.1]. If I is trivial, we are finished (see the end of this proof); otherwise it is a connected semisimple M-split group, and this we henceforth assume. Our choice of M guarantees that the (absolutely) almost simple factors of I are (defined over M and) M-split. Write W for the Weyl group of I with respect to T, namely the finite group $\mathcal{N}_I(T)/\mathcal{Z}_I(T)$. Then W is also preserved by reduction mod $\mathfrak{p}$ $\forall^* \mathfrak{p}$ [5.4.5.1], and our choice of B and T gives a canonical basis for Φ and corresponding length function on W, $l : W \longrightarrow \mathbb{N}$ [4.1.0.1].

The above hypotheses are sufficient to guarantee that each double coset BwB (for $w \in W$) in the Bruhat decomposition [4.2.2.3] for I, namely

$$I = \coprod_{w \in W} BwB$$

(disjoint union) can be taken as defined over M, and further that the canonical isomorphism of varieties [4.3.0.4] $BwB \cong B \times \mathbb{A}^{l(w)}$ is also defined over M (for each $w \in W$). Assembling all of the above, we introduce the notation $a = \#J$, $b = \dim u(J)$, $c = \dim u(B)$, $d = \dim T$, $e = \dim r(J)/u(J)$, and take

$$P(X) = aX^{b+c}(X-1)^{d+e} \sum_{w \in W} X^{l(w)}$$

The group W is also the Weyl group of the root system $\Phi(I,T)$ which is associated to I, and is the direct product of the Weyl groups corresponding to the irreducible root subsystems of $\Phi(I,T)$. We can show from this that the polynomial $\sum_{w\in W} X^{l(w)}$ is the product of those corresponding to these irreducible subsystems: these latter polynomials can be found in the earlier part of table after [4.5.4.1] (except that we have incorporated powers of $X-1$ and of X into the expression $aX^{b+c}(X-1)^{d+e}$). This gives an explicit description of $P(X)$: it is interesting that the nonzero roots of P are roots of unity. [Had I been trivial, we would have had $c=d=0$ and $\sum_{w\in W} X^{l(w)}=1$.] □

Corollary 6.3.0.2 *The (Hasse-Weil) zeta function for J over M is an alternating product of integer translates of $\zeta_M(s)$ (and in particular J has property (Z) for M/M).*

Explicitly,

$$\zeta(J,M,s) = (\dagger) \prod_{i=b+c}^{i=\dim J} \zeta_M(s-i)^{\alpha_i}$$

where $P(X)=\sum_i \alpha_i X^i$. □

Corollary 6.3.0.3 *$\zeta(J,M,s)$ has a functional equation relating it to $\zeta(J,M,1+r-s)$, where $r=b+c+\dim J$.*

Proof: Let $\Phi_t(X)$ denote the (monic) irreducible polynomial over $\mathbb{Q}$ for the primitive t^{th} roots of unity: its degree is $\phi(t)$. It is implicit above that the sum $\sum_{w\in W} X^{l(w)}$ in the expression for $P(X)$ is a product of such factors for $t>1$. One easily verifies that $X^{\phi(t)}\Phi_t(X^{-1}) = \Phi_t(X)$ for $t>1$, (for $t=1$, a minus sign is needed). Hence, $X^r P(X^{-1}) = CP(X)$ where $C=(-1)^{d+e}$ and so we have the relation $\alpha_i = C\alpha_{r-i}$ among the coefficients of P. Recalling the functional equation [5.2.1.1] for the Dedekind zeta function, which we write as $\zeta_M(s-i) = Y(s-i)\zeta_M(1+i-s)$, with Y meromorphic, we have

$$\zeta(J,M,s) = (\dagger) \prod_{i=b+c}^{i=\dim J} [Y(s-i)\zeta_M(1+i-s)]^{\alpha_i}$$
$$= (\dagger) \prod_{i=b+c}^{i=\dim J} Y(s-i)^{\alpha_i} \cdot \prod_{j=b+c}^{j=\dim J} \zeta_M(1+r-j-s)^{\alpha_{r-j}}$$

then we get

$$\zeta(J,M,s) = (\dagger) \left[\prod_{i=b+c}^{i=\dim J} Y(s-i)^{\alpha_i} \right] \cdot \zeta(J,M,1+r-s)^C$$

We can of course choose the finitely many hitherto undetermined factors to fit into this pattern. □

Note that the r which occurs in the last corollary is equal to $\dim u(J) + \Xi$: this is a point which will recur later.

6.4 Almost simple groups

Throughout this section [6.4], G is an almost simple K-group.

6.4.1 Notations and statement of the Main Result *(AS)*

Recall [4.5.4] that G is connected and has a connected Dynkin diagram ${}^gX_{n,r}$ (say) [*loc.cit*]. We write again n for the rank, and r for the K-rank. Recall that $H_l \cong Gal(l/K)$ acts effectively on ${}^gX_{n,r}$ [4.5.2]. For $\mathfrak{p} \in \mathcal{M}_K$, $\mathfrak{p}$ unramified in l, let $Fr\,\mathfrak{p}$ be its Frobenius class in H_l. Recall the notation Ξ for $\dim G + \#\Phi^+$: observe that for a split almost simple group, we would have, in the notation of [6.3], $X^{\Xi}P(X^{-1}) = CP(X)$ where $P(X)$ is the rationality formula and C is $(-1)^n$.

By [6.1.2.1], we can identify the strict $\mathbb{F}_\mathfrak{p}$-isogeny class of $G_\mathfrak{p}$ $\forall^*\mathfrak{p}$. (The fact that we are now dealing with the *inner* field rather than the *splitting* field is a minor detail, settled by [5.1.1.1].) The table following gives, for each diagram of outer type ${}^gX_{n,r}$, the density of that subset S_h of $\mathcal{M}_K$ which is defined by the condition that $({}^gX_{n,r})_\mathfrak{p}$ has type ${}^hX_n$ for

$\mathfrak{p} \in S_h$. The entries in the table were found by applying the Čebotarev density theorem [5.1.1.2] to [6.1.2.1]. The corresponding cardinalities are given too.

K-type	Density	$\mathbb{F}_p$-type	Cardinality
${}^2A_{n,r}$	$1/2$	${}^1A_{n,n}$	$q^{n(n+1)/2}\prod_{i=1}^{n}(q^{i+1}-1)$
	$1/2$	${}^2A_{n,[\frac{n+1}{2}]}$	$q^{n(n+1)/2}\prod_{i=1}^{n}(q^{i+1}-(-1)^{i+1})$
${}^2D_{n,r}$	$1/2$	${}^1D_{n,n}$	$q^{n(n-1)}(q^n-1)\prod_{i=1}^{n-1}(q^{2i}-1)$
	$1/2$	${}^2D_{n,n-1}$	$q^{n(n-1)}(q^n+1)\prod_{i=1}^{n-1}(q^{2i}-1)$
${}^2E_{6,r}$	$1/2$	${}^1E_{6,6}$	$q^{36}(q^{12}-1)(q^9-1)(q^8-1)(q^6-1)(q^5-1)(q^2-1)$
	$1/2$	${}^2E_{6,4}$	$q^{36}(q^{12}-1)(q^9+1)(q^8-1)(q^6-1)(q^5+1)(q^2-1)$
${}^3D_{4,r}$	$1/3$	${}^1D_{4,4}$	$q^{12}(q^4-1)\prod_{i=1}^{3}(q^{2i}-1)$
	$2/3$	${}^3D_{4,2}$	$q^{12}(q^8+q^4+1)(q^6-1)(q^2-1)$
${}^6D_{4,r}$	$1/6$	${}^1D_{4,4}$	$q^{12}(q^4-1)\prod_{i=1}^{3}(q^{2i}-1)$
	$1/2$	${}^2D_{4,3}$	$q^{12}(q^4+1)\prod_{i=1}^{3}(q^{2i}-1)$
	$1/3$	${}^3D_{4,2}$	$q^{12}(q^8+q^4+1)(q^6-1)(q^2-1)$

The rest of [6.4] is devoted to the proof of the following result.

Theorem 6.4.1.1 *(For G an almost simple K-group.)*
(1) G has property (Z) for l/K.
(2) There is a field f, with $K \subseteq f \subseteq l$ and $[f : K]$ equal to 1 or 2, such that $\zeta(G, f, s)$ satisfies a functional equation relating it to $\zeta(G, f, 1+\Xi-s)$. We can choose $f = K$ unless ${}^gX_{n,r}$ is one of ${}^2A_{n,r}$ for $n \equiv 2$ or 3 mod 4, ${}^2D_{n,r}$ for any $n \geq 4$, or ${}^6D_{4,r}$.

6.4.2 Dependence on l and X_n alone

The first observation to make is the following.

Theorem 6.4.2.1 *(For G an almost simple K-group.)*
The Hasse-Weil zeta function $\zeta(G, K, s)$ depends only on l and X_n.

Proof: We begin by considering an almost simple $\mathbb{F}_\mathfrak{p}$-group J, with ${}^gX_n$ given. In fact, we claim that the strict $\mathbb{F}_\mathfrak{p}$-isogeny class of J is already determined by this information. Recall [4.5.3.2] that to show this, we must prove that the strict $\mathbb{F}_\mathfrak{p}^s$-isogeny class, the $\mathbb{F}_\mathfrak{p}$-index and the anisotropic kernel are determined uniquely (up to $Gal(\mathbb{F}_\mathfrak{p}^s/\mathbb{F}_\mathfrak{p})$-set isomorphism or $\mathbb{F}_\mathfrak{p}$-isomorphism as appropriate). The relative $\mathbb{F}_\mathfrak{p}$-rank r of J is well-defined by [4.5.4.1], though we do not need this explicitly.

J is $\mathbb{F}_\mathfrak{p}$-quasisplit, so the anisotropic kernel is trivial by [4.5.3.1]. Further, the strict $\mathbb{F}_\mathfrak{p}^s$-isogeny class of J is just that of X_n. Finally, the $\mathbb{F}_\mathfrak{p}$-index is determined by the following data. All orbits are distinguished, since J is $\mathbb{F}_\mathfrak{p}$-quasisplit. The inner field for J is the (unique) extension l_1 of $\mathbb{F}_\mathfrak{p}$ of degree g. The group $C = Gal(l_1/\mathbb{F}_\mathfrak{p})$ acts effectively on X_n. But elementary considerations regarding possible (directed-)graph automorphisms of X_n show that there is a unique structure of C-(directed-)graph which can be put on X_n, which is effective in the sense of C-sets. This lifts to a unique action of $Gal(\mathbb{F}_\mathfrak{p}^s/\mathbb{F}_\mathfrak{p})$ on X_n, such that $Gal(\mathbb{F}_\mathfrak{p}^s/l_1)$ acts trivially. Hence the $\mathbb{F}_\mathfrak{p}$-index is also uniquely determined by the data ${}^gX_n$.

This verifies the claim that the strict $\mathbb{F}_\mathfrak{p}$-isogeny class of J is specified by the data $\{g, X_n\}$: the Weil zeta function of J depends only on this, by [4.4.0.2]. This justifies

notation like $Z({}^gX_n, \mathbb{F}_\mathfrak{p}, t)$ for $Z(J, \mathbb{F}_\mathfrak{p}, t)$.

We return to the almost simple K-group G. Recall that the Dynkin diagram is preserved under reduction mod $\mathfrak{p}$ $\forall^*\mathfrak{p}$ [5.4.5.1]. We also observe that if $Fr\,\mathfrak{p}$ is the identity class of H_l, then $G_\mathfrak{p}$ is $\mathbb{F}_\mathfrak{p}$-split: thus for $g = 1$, $G_\mathfrak{p}$ is necessarily $\mathbb{F}_\mathfrak{p}$-split and almost simple ($\forall^*\mathfrak{p}$), so the local factors are known.

Next suppose $g = 2$. If $Fr\,\mathfrak{p}$ is *not* the identity class of H_l, $G_\mathfrak{p}$ is (for almost all such primes) strictly $\mathbb{F}_\mathfrak{p}$-isogenous to an $\mathbb{F}_\mathfrak{p}$-group of type ${}^2X_{n,r}$ (for the same X_n as G, and r as in the table [4.5.4.1]); the Hasse-Weil zeta function is again determined by this information, in which knowledge of l is implicit.

For $g = 3$, if $Fr\,\mathfrak{p}$ is either of the non-identity classes, then $G_\mathfrak{p}$ must have the same Weil zeta function as the group ${}^3D_{4,2}$.

Finally for $g = 6$, if $Fr\,\mathfrak{p}$ has elements of order 2, then we have the local factor $Z({}^2D_4, \mathbb{F}_\mathfrak{p}, t)$. If $Fr\,\mathfrak{p}$ has elements of order 3, then we get $Z({}^3D_4, \mathbb{F}_\mathfrak{p}, t)$. □

The above result suggests that the Hasse-Weil zeta function is in some sense a rather 'crude' invariant of the group.

Next is an elementary result for which the author does not know a source: it will be used in some of the existence proofs for functional equations. A special case was used already in [6.3].

Lemma 6.4.2.2 *Let $A(X) \in \mathbb{C}[X]$, $A \not\equiv 0$, of degree d. For $z \in \mathbb{C}$, let m_z be the multiplicity of z as a root of A. Suppose further that there exist $\alpha \in \mathbb{Z}$ and $C \in \mathbb{C}$ such that $CX^\alpha A(X^{-1}) = A(X)$. Then $\alpha = d + m_0$ and $C = (-1)^{m_1}$.*

Proof: Write $A(X) = X^{m_0}(X-1)^{m_1}Q(X)$ where $Q(0)Q(1) \neq 0$. Then

$$CX^\alpha X^{-m_0}(X^{-1}-1)^{m_1}Q(X^{-1}) = X^{m_0}(X-1)^{m_1}Q(X),$$

so

$$C(-1)^{m_1}X^{\alpha-2m_0-m_1}(X-1)^{m_1}Q(X^{-1}) = (X-1)^{m_1}Q(X).$$

Dividing by $(X-1)^{m_1}$, and evaluating at $X = 1$ gives $C = (-1)^{m_1}$, and the assertion about α follows by comparing terms of degree zero. □

6.4.3 Proof of *(AS)* for groups of inner type

The computations here almost follow from those in [6.3]. If G is of inner type over K so that $l = K$, then so is $G_{\mathfrak{p}}$ $\forall^*\mathfrak{p}$, and thus $G_{\mathfrak{p}}$ can be taken as $\mathbb{F}_{\mathfrak{p}}$-split (being necessarily $\mathbb{F}_{\mathfrak{p}}$-quasisplit). Hence one takes for rationality formula the polynomial $P(X)$ given in [4.5.4.1], giving $\zeta(G, K, s)$ as an alternating product of translates of Dedekind zeta functions [6.3.0.2] (so G has property (Z) for K/K) with a functional equation over K as at [6.3.0.3].

6.4.4 Unification of rationality formulas

In the next few subsections, we record again the explicit expressions [4.5.4.1] for numbers of $\mathbb{F}_{\mathfrak{p}^t}$-rational points for the various almost simple $\mathbb{F}_{\mathfrak{p}}$-groups of outer type, and 'unify' these formulas to get at the number field case by introducing characters of (the current group) H_l, which we recall can be identified with $Gal(l/K)$.

We recall that H_l is isomorphic to a subgroup of S_3. For convenience, we refer below to the presentation $<\sigma, \tau|\sigma^2, \tau^3, (\sigma\tau)^2>$ for S_3 and subgroups $C_2 :=<\sigma|\sigma^2>$, $C_3 :=<\tau|\tau^3>$ thereof.

Subsequently in this section, χ, sundrily annotated, denotes various simple non-principal characters of H_l (which we recall are constant on conjugacy classes), and e denotes the identity element of H_l. We use $A(X)$ and $B(X)$, sometimes annotated, to denote (various) elements of $\mathbb{Z}[X]$, and use C to denote various combinations of the functions which appear in the functional equations for Artin L-functions. The exact form of C is not important: it could readily be written down in any given case if required.

Recall that the rationality formula to be used for $P(N\mathfrak{p}^t)$ in the case of an $\mathbb{F}_{\mathfrak{p}}$-group of outer type depends on the degree t of extension being considered. In all subsequent cases, an expression for $\#G_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}^t})$ is obtained which is valid for all $t \geq 1$ and $\forall^*\mathfrak{p}$. We will see that characters of H_l are involved, and the formulas are found by a little experimentation.

6.4.5 General remarks about *(AS)* for cases in which $g = 2$

We use here the character χ of C_2 such that $\chi(\sigma) = -1$ and $\chi(e) = 1$. We note that $\chi(\sigma^a) = \chi(\sigma)^a$ for each $a \in \mathbb{Z}$ as χ is linear, and that $\chi(\sigma^a)^2 = 1$. The three types of

diagram are considered separately: in each case, the 'unifying' formula is readily verified. We will see that, in each of the three cases, we can choose polynomials $A(X)$ and $B(X)$ in $\mathbb{Z}[X]$, with coefficients independent of t, such that $\#G_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}^t}) = A(N\mathfrak{p}^t)+\chi([Fr\,\mathfrak{p}]^t)B(N\mathfrak{p}^t)$ for all t and $\forall^*\mathfrak{p}$. The calculations for the case ${}^2A_{n,r}$ will be carried out in full, as these are the most complicated: the others will be abridged.

6.4.6 Verification of *(AS)* for the cases ${}^2A_{n,r}$

$$\#({}^2A_{n,r})_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}^t}) = \begin{cases} N\mathfrak{p}^{tn(n+1)/2}\prod_{i=1}^{n}(N\mathfrak{p}^{t(i+1)}-1) & \text{if } 1 \in Fr\,\mathfrak{p} \ \underline{\text{or}} \\ & (\sigma \in Fr\,\mathfrak{p} \text{ and } (2,t)=2), \\ N\mathfrak{p}^{tn(n+1)/2}\prod_{i=1}^{n}(N\mathfrak{p}^{t(i+1)}-(-1)^{i+1}) & \text{if } \sigma \in Fr\,\mathfrak{p} \text{ and } (2,t)=1. \end{cases}$$

$$= N\mathfrak{p}^{tn(n+1)/2}\prod_{i=1}^{n}(N\mathfrak{p}^{t(i+1)}-\chi([Fr\,\mathfrak{p}]^{t(i+1)})) \qquad (\forall t,\ \forall^*\mathfrak{p})$$

As only the *parity* of the exponent to which $Fr\,\mathfrak{p}$ is raised is significant, we can simplify this to

$$N\mathfrak{p}^{tn(n+1)/2}\prod_{\substack{i=1\\(i \text{ odd})}}^{n}(N\mathfrak{p}^{t(i+1)}-1)\cdot\prod_{\substack{j=1\\(j \text{ even})}}^{n}(N\mathfrak{p}^{t(j+1)}-\chi([Fr\,\mathfrak{p}]^t))$$

and so

$$\#({}^2A_{n,r})_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}^t}) = A(N\mathfrak{p}^t)+\chi([Fr\,\mathfrak{p}]^t)B(N\mathfrak{p}^t)$$

with $A(X)$ and $B(X)$ being in $\mathbb{Z}[X]$ (and independent of t). We write $A(X) = \sum_i a_iX^i$ and $B(X) = \sum_j b_jX^j$.

Hence, by the definitions [5.2.3] of the Artin L-function and Hasse-Weil zeta function we get

$$\zeta({}^2A_{n,r}, K, s) = (\dagger) \prod_{\mathfrak{p}} \exp(\sum_{t=1}^{\infty} \frac{A(N\mathfrak{p}^t)N\mathfrak{p}^{-st}}{t}) \cdot \prod_{\mathfrak{p}} \exp(\sum_{t=1}^{\infty} \frac{\chi([Fr\,\mathfrak{p}]^t)B(N\mathfrak{p}^t)N\mathfrak{p}^{-st}}{t})$$

$$= (\dagger) \prod_i \zeta_K(s-i)^{a_i} \cdot \prod_j L(H_l, \chi, s-j)^{b_j}.$$

verifying (1) of [6.4.1.1] for this case. We can clearly get a functional equation of the required form over l; however if we can find $c \in \mathbb{Z}$ and $w \in \mathbb{C}$ such that

$$X^c A(X^{-1}) = wA(X) \text{ and } X^c B(X^{-1}) = wB(X)$$

we get a functional equation over K of the form

$$\zeta({}^2A_{n,r}, K, s) = C(s)\zeta({}^2A_{n,r}, K, 1+c-s)^w$$

as follows. Observe that χ is a *real* character. We use the functional equations for $\zeta_K(s)$ and $L(H_l, \chi, s)$ [5.2.1.1, 5.2.2.2].

$$\zeta({}^2A_{n,r}, K, s) = (\dagger) \prod_i \zeta_K(s-i)^{a_i} \cdot \prod_j L(H_l, \chi, s-j)^{b_j}$$
$$= (\dagger)C(s) \prod_i \zeta_K(1+i-s)^{a_i} \cdot \prod_j L(H_l, \overline{\chi}, 1-s+j)^{b_j}$$

Now $wa_{c-i} = a_i$ and $wb_{c-j} = b_j$ for all $i, j \in \mathbb{Z}$: furthermore, i runs through the same index set as $c-i$, and j runs through the same index set as $c-j$ by construction. Replacing i by $c-i$ and j by $c-j$ in the last expression gives

$$\zeta({}^2A_{n,r}, K, s) = (\dagger)C(s)\zeta({}^2A_{n,r}, K, 1+c-s)^w$$

as required. (Recall that w is ± 1.)

We now seek sufficient conditions for the existence of c and w with the required properties. Recall that, by [6.4.2.2], we necessarily have $c = \deg A + m_0(A) = \deg B + m_0(B)$ and $w = (-1)^{m_1(A)} = (-1)^{m_1(B)}$, where (almost as before) $m_z(Q)$ denotes the multiplicity of z as a root of the nonzero polynomial $Q(X) \in \mathbb{C}[X]$.

We can certainly find such a c, w for the polynomial $T_n(X)$ (say) with constant coefficients

$$T_n(X) = X^{n(n+1)/2} \prod_{\substack{i=1 \\ (i \text{ odd})}}^{n} (X^{i+1} - 1)$$

whose degree is d (say), and which has 1 as a root of multiplicity $\left[\frac{n+1}{2}\right]$ - namely

$$c = d + \frac{n(n+1)}{2} \text{ and } w = (-1)^{\left[\frac{n+1}{2}\right]}$$

T_n divides both A and B, so we can remove this common factor, and suppose that $A(X)$ and $B(X)$ are such that

$$A(N\mathfrak{p}^t) + \chi([Fr\,\mathfrak{p}]^t)B(N\mathfrak{p}^t) = \prod_{\substack{j=1 \\ (j \text{ even})}}^{n} (N\mathfrak{p}^{t(j+1)} - \chi([Fr\,\mathfrak{p}]^t)) \qquad (*)$$

Write

$$I = \{j \in \mathbb{Z} | j \text{ is even and } 1 \leq j \leq n\}, \text{ and } c = \#I + \sum_{j \in I} j$$

- thus c is the degree of (*) (the degree in $N\mathfrak{p}^t$). We note next that (with our new A and B), $m_1(A) = m_1(B) = 0$ for all n. We know, of course, that both A and B have integer coefficients, but in fact both A and $-B$ (are nonzero and) have nonnegative coefficients so cannot have 1 as a root. To see this, observe that as $\chi([Fr\,\mathfrak{p}]^t)^2 = 1$, on expanding (*), terms coming from the product of an even (respectively, odd) number of $\chi([Fr\,\mathfrak{p}]^t)$ terms only contribute to the expression for A (respectively, B). Hence the nonnegativity of A and $-B$, and we must take $w = 1$ for the new A and B.

We write y for $\chi([Fr\,\mathfrak{p}]^t)$ from now on in this subsection, and recall again that $y = y^{-1}$. Then we have (in which all subscripts j run over I)

$$A(X)+yB(X)=\prod_j(X^{(j+1)}-y)=X^c\prod_j(1-yX^{-j-1})=(-y)^{\#I}X^c\prod_j(X^{-j-1}-y)$$
$$=(-y)^{\#I}X^c[A(X^{-1})+yB(X^{-1})]$$

$$=\begin{cases}X^c[A(X^{-1})+yB(X^{-1})] & \text{for } \#I \text{ even},\\ X^c[-yA(X^{-1})-B(X^{-1})] & \text{for } \#I \text{ odd}.\end{cases}$$

For $\#I$ even (equivalently, $n\equiv 0$ or $1 \bmod 4$) we have

$$A(X)+yB(X)=X^c[A(X^{-1})+yB(X^{-1})];$$

since this must hold for both $y=1$ and $y=-1$, we get

$$A(X)=X^cA(X^{-1}) \text{ and } B(X)=X^cB(X^{-1}).$$

Adding this value for c to the value $\frac{n(n+1)}{2}+d$ obtained for the polynomial $T_n(X)$ and multiplying w by w' gives $c=\dim G+\frac{n(n+1)}{2}=\Xi$ as required, and we have a functional equation for $n\equiv 0$ or $1 \bmod 4$ as claimed in [6.4.1.1]. We record this explicitly.

$$\zeta({}^2A_{n,r},K,s)=(\dagger)C(s)\zeta({}^2A_{n,r},K,1+\Xi-s)^{\left((-1)^{\left[\frac{n+1}{2}\right]}\right)}$$
$$(n\equiv 0 \text{ or } 1 \mod 4.)$$

For $\#I$ odd, (equivalently, $n\equiv 2$ or $3 \bmod 4$), we get similarly,

$$A(X)=-X^cB(X^{-1}) \text{ and } B(X)=-X^cA(X^{-1}).$$

However $\deg A+m_0(A)=c+3$ and $\deg B+m_0(B)=c-3$, so we cannot 'reciprocate' A and B simultaneously and therefore cannot find a functional equation over K by this method, also as claimed [*loc.cit.*].

This verifies all of the assertions of [6.4.1.1] about groups of type ${}^2A_{n,r}$.

6.4.7 Verification of *(AS)* for the cases ${}^2D_{n,r}$

$$\#({}^2D_{n,r})_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}^t}) = \begin{cases} N\mathfrak{p}^{tn(n-1)}(N\mathfrak{p}^{tn}-1)\prod_{i=1}^{n-1}(N\mathfrak{p}^{2it}-1) & \text{if } 1 \in Fr\,\mathfrak{p} \text{ or} \\ & (\sigma \in Fr\,\mathfrak{p} \text{ and } (2,t)=2), \\ N\mathfrak{p}^{tn(n-1)}(N\mathfrak{p}^{tn}+1)\prod_{i=1}^{n-1}(N\mathfrak{p}^{2it}-1) & \text{if } \sigma \in Fr\,\mathfrak{p} \text{ and } (2,t)=1. \end{cases}$$

$$= N\mathfrak{p}^{tn(n-1)}(N\mathfrak{p}^{tn} - \chi([Fr\,\mathfrak{p}]^t))\prod_{i=1}^{n-1}(N\mathfrak{p}^{2it}-1)$$

all of this holding $\forall t$, $\forall^*\mathfrak{p}$ of course. By a similar, but easier argument, we get polynomials A and B such that

$$\#({}^2D_{n,r})_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}^t}) = A(N\mathfrak{p}^t) + \chi([Fr\,\mathfrak{p}]^t)B(N\mathfrak{p}^t)$$

and hence that

$$\zeta({}^2D_{n,r}, K, s) = (\dagger)\prod_i \zeta_K(s-i)^{a_i} \cdot \prod_j L(H_l, \chi, s-j)^{b_j}$$

This time, we find that

$$A(X) = X^{n^2}\prod_{i=1}^{n-1}(X^{2i}-1) = (-1)^{n-1}X^{3n^2-n}A(X^{-1})$$

$$B(X) = -X^{n^2-n}\prod_{i=1}^{n-1}(X^{2i}-1) = (-1)^{n-1}X^{3n^2-3n}B(X^{-1})$$

so that no functional equation over K can be found by the method above. However, we do again have a functional equation over l.

6.4.8 Verification of *(AS)* for the cases ${}^2E_{6,r}$

Due to constraints of space, this time we write the actual conditions for the two different rationality formulas after the formulas themselves.

$$\#({}^2E_{6,r})_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}^t}) = \begin{cases} \left\{ \begin{array}{r} N\mathfrak{p}^{36t}(N\mathfrak{p}^{12t}-1)(N\mathfrak{p}^{9t}-1)(N\mathfrak{p}^{8t}-1)\cdot \\ (N\mathfrak{p}^{6t}-1)(N\mathfrak{p}^{5t}-1)(N\mathfrak{p}^{2t}-1) \end{array} \right\} & \text{if 'A'} \\ \left\{ \begin{array}{r} N\mathfrak{p}^{36t}(N\mathfrak{p}^{12t}-1)(N\mathfrak{p}^{9t}+1)(N\mathfrak{p}^{8t}-1)\cdot \\ (N\mathfrak{p}^{6t}-1)(N\mathfrak{p}^{5t}+1)(N\mathfrak{p}^{2t}-1) \end{array} \right\} & \text{if 'B'} \end{cases}$$

where

'A' is: $1 \in Fr\,\mathfrak{p}$ *or* $(\sigma \in Fr\,\mathfrak{p}$ *and* $(2,t)=2)$; and

'B' is: $\sigma \in Fr\,\mathfrak{p}$ *and* $(2,t)=1$.

We unify the formulas as

$$N\mathfrak{p}^{36t}(N\mathfrak{p}^{12t}-1)(N\mathfrak{p}^{9t}-\chi([Fr\,\mathfrak{p}]^t))(N\mathfrak{p}^{8t}-1)(N\mathfrak{p}^{6t}-1)(N\mathfrak{p}^{5t}-\chi([Fr\,\mathfrak{p}]^t))(N\mathfrak{p}^{2t}-1)$$

$\forall t$, $\forall^*\mathfrak{p}$. The same argument again gives

$$\#({}^2E_{6,r})_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}^t}) = A(N\mathfrak{p}^t) + \chi([Fr\,\mathfrak{p}]^t)B(N\mathfrak{p}^t)$$

with

$$\begin{aligned} A(X) &= X^{36}(X^{12}-1)(X^8-1)(X^6-1)(X^2-1)(X^{14}+1) = X^{114}A(X^{-1}) \\ B(X) &= -X^{41}(X^{12}-1)(X^8-1)(X^6-1)(X^2-1)(X^4+1) = X^{114}B(X^{-1}) \end{aligned}$$

and hence

$$\zeta({}^2E_{6,r},K,s) = (\dagger)\prod_i \zeta_K(s-i)^{a_i}\cdot\prod_j L(H_l,\chi,s-j)^{b_j}$$

in an obvious notation.

The constant 114 which appears is the value of $\Xi = \dim G + \#\Phi^+$ as usual. Thus

$$\zeta({}^2E_{6,r},K,s) = C(s)\zeta({}^2E_{6,r},K,115-s)$$

where $C(s)$ is meromorphic. We have now verified [6.4.1.1] for $g=2$.

6.4.9 Verification of *(AS)* for cases in which $g = 3$

We write here ω for $\exp\frac{2\pi i}{3}$ and use the following characters χ' and χ'' of C_3.

Class	e	τ	τ^2
χ'	1	ω	ω^2
χ''	1	ω^2	ω

$$\#({}^3D_{4,r})_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}^t}) = \begin{cases} \left\{ N\mathfrak{p}^{12t}(N\mathfrak{p}^{4t}-1)\cdot \prod_{i=1}^{3}(N\mathfrak{p}^{2it}-1) \right\} & \text{if } 1 \in Fr\,\mathfrak{p} \text{ or} \\ & (\tau \in Fr\,\mathfrak{p} \text{ and } (3,t)=3) \text{ or} \\ & (\tau^2 \in Fr\,\mathfrak{p} \text{ and } (3,t)=3), \\ \left\{ N\mathfrak{p}^{12t}(N\mathfrak{p}^{8t}+N\mathfrak{p}^{4t}+1)\cdot (N\mathfrak{p}^{6t}-1)(N\mathfrak{p}^{2t}-1) \right\} & \text{if } (\tau \in Fr\,\mathfrak{p} \text{ and } (3,t)=1) \text{ or} \\ & (\tau^2 \in Fr\,\mathfrak{p} \text{ and } (3,t)=1). \end{cases}$$

$$= N\mathfrak{p}^{12t}(N\mathfrak{p}^{6t}-1)(N\mathfrak{p}^{2t}-1)(N\mathfrak{p}^{8t}-[\chi'([Fr\,\mathfrak{p}]^t)+\chi''([Fr\,\mathfrak{p}]^t)]N\mathfrak{p}^{4t}+1)$$

$\forall t$, $\forall^*\mathfrak{p}$ as usual.

This time we have $\#({}^3D_{4,r})_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}^t}) = A(N\mathfrak{p}^t)+\chi'([Fr\,\mathfrak{p}]^t)B(N\mathfrak{p}^t)+\chi''([Fr\,\mathfrak{p}]^t)B(N\mathfrak{p}^t)$ with the same function $B(X)$ multiplying each of χ' and χ'' so that we only have to consider the *real* character $\chi'+\chi''$. Explicitly,

$$\begin{aligned} A(X) &= X^{12}(X^6-1)(X^2-1)(X^8+1) = X^{40}A(X^{-1}) \\ B(X) &= -X^{16}(X^6-1)(X^2-1) = X^{40}B(X^{-1}) \end{aligned}$$

with $\Xi = 40$ for this case, and we get

$$\zeta({}^3D_{4,r}, K, s) = (\dagger) \prod_i \zeta_K(s-i)^{a_i} \cdot \prod_j L(H_l, \chi', s-j)^{b_j} \cdot \prod_j L(H_l, \chi'', s-j)^{b_j}$$

Hence we get the functional equation over K

$\zeta({}^3D_{4,r}, K, s) = C(s)\zeta({}^3D_{4,r}, K, 41-s)$,

and this verifies [6.4.1.1] for $g = 3$.

6.4.10 Verification of *(AS)* for cases in which $g = 6$

This time we use the following characters χ_1 and χ_2 of S_3.

Class	e	σ	τ
χ_1	1	-1	1
χ_2	2	0	-1

$$\#({}^6D_{4,r})_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}^t}) = \begin{cases} \left\{ N\mathfrak{p}^{12t}(N\mathfrak{p}^{4t}-1) \cdot \prod_{i=1}^{3}(N\mathfrak{p}^{2it}-1) \right\} & \text{if } 1 \in Fr\,\mathfrak{p} \text{ or} \\ & (\sigma \in Fr\,\mathfrak{p} \text{ and } (2,t)=2) \text{ or} \\ & (\tau \in Fr\,\mathfrak{p} \text{ and } (3,t)=3), \\ \left\{ N\mathfrak{p}^{12t}(N\mathfrak{p}^{4t}+1) \cdot \prod_{i=1}^{3}(N\mathfrak{p}^{2it}-1) \right\} & \text{if } \sigma \in Fr\,\mathfrak{p} \text{ and } (2,t)=1, \\ \left\{ N\mathfrak{p}^{12t}(N\mathfrak{p}^{8t}+N\mathfrak{p}^{4t}+1) \cdot (N\mathfrak{p}^{6t}-1)(N\mathfrak{p}^{2t}-1) \right\} & \text{if } \tau \in Fr\,\mathfrak{p} \text{ and } (3,t)=1. \end{cases}$$

which is $\forall t$, $\forall^* \mathfrak{p}$ as usual,

$$N\mathfrak{p}^{12t}(N\mathfrak{p}^{6t}-1)(N\mathfrak{p}^{2t}-1)(N\mathfrak{p}^{8t} - \chi_2([Fr\,\mathfrak{p}]^t)N\mathfrak{p}^{4t} + \chi_1([Fr\,\mathfrak{p}]^t))$$

In the usual way we can find A, B_1 and B_2 such that

$$\#({}^6D_{4,r})_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}^t}) = A(N\mathfrak{p}^t) + \chi_1([Fr\,\mathfrak{p}]^t)B_1(N\mathfrak{p}^t) + \chi_2([Fr\,\mathfrak{p}]^t)B_2(N\mathfrak{p}^t).$$

with

$$\begin{aligned} A(X) &= X^{20}(X^6-1)(X^2-1) = X^{48}A(X^{-1}) \\ B_1(X) &= X^{12}(X^6-1)(X^2-1) = X^{32}B_1(X^{-1}) \\ B_2(X) &= -X^{16}(X^6-1)(X^2-1) = X^{40}B_2(X^{-1}) \end{aligned}$$

For the record, we get

$$\zeta({}^6D_{4,r}, K, s) = (\dagger)\prod_i \zeta_K(s-i)^{a_i} \cdot \prod_j L(H_l, \chi_1, s-j)^{b_{1,j}} \cdot \prod_k L(H_l, \chi_2, s-k)^{b_{2,k}}$$

in a notation which should be self-explanatory. Thus we do not have (by the above method) a functional equation over K: however, by passing to a quadratic extension f such that G has type ${}^3D_{4,r'}$ (for some $r' \geq r$) over f, we can get a functional equation over f. Such an extension exists by the fundamental theorem of Galois theory.

This verifies the assertions for the case $g = 6$, and indeed concludes the proof of [6.4.1.1].

Chapter 7

Two Dynkin Components and Future Work

7.1 Virtual characters and notation

$\mathbb{Z}$-linear combinations of characters of a finite group J are usually called *virtual characters* of J. In particular, the virtual characters of J then form a commutative ring with unit. Though not in general characters of representations of J, some of the formal theory of characters still applies. A character which *is* afforded by a representation is said to be *effective*. If χ is effective and J is a Galois group then $L(J, -\chi, s) = L(J, \chi, s)^{-1}$.

In [7], we use again the 2-element group $C_2 = <\sigma|\sigma^2>$ with simple characters $\{\chi_0, \chi\}$, χ_0 being principal. We also put $\mathbb{Z}C$ for their $\mathbb{Z}$-span, which in this case consists of $\mathbb{Z}$-valued functions on C_2. In addition to the usual notations and hypotheses at the start of the last chapter, all of which we retain, suppose that G is almost K-simple (and therefore semisimple), such that its Dynkin diagram $\mathcal{D}$ has two components, both X_n. The nodes of these components will be denoted $\{1, \ldots, n\}$ and $\{1', \ldots, n'\}$.

By [4.5.5.1] there is a quadratic extension f of K, and a connected almost simple f-group M such that $G \sim_K R_{f/K}(M)$. We will often use the fact that f is a normal extension of K, and contained in the inner field l. The main result is as follows.

Theorem 7.1.0.1 *(For G connected almost K-simple with two Dynkin components.)*

*$\zeta(G,K,s)$ is an alternating product of Artin L-functions for characters of H_l (*viz. *G has property (Z) for l/K).*

7.2 The case where M has inner f-type

We suppose that M has Dynkin diagram ${}^1X_{n,r}$ and corresponding rationality formula $P(X)$ (*viz.* $P(N\mathfrak{p}^t) = \#M_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}^t})$ for all $t \geq 1$, $\forall^* \mathfrak{p}$).

Lemma 7.2.0.1 *There exists (a unique) $Q(X) \in \mathbb{Z}C[X]$ such that the induced map Q : $C_2 \longrightarrow \mathbb{Z}[X]$ given by evaluating the coefficients at elements of C_2 satisfies*

$$Q(\sigma^i) = \begin{cases} P(X^2) & i = 1, \\ \\ P(X)^2 & i = 2. \end{cases}$$

Proof: We construct $Q(X)$ directly. We want (if possible) to find $Q(X) = \sum_i (a_i\chi_0 + b_i\chi)X^i$ such that Q satisfies the hypotheses above, with each a_i and b_i being integers. We have $P(X) = \sum_{j=s}^{d} p_j X^j$ (say) with $d = \dim M$ and $s = \frac{\dim M - n}{2}$ as usual [4.5.4.1].

By our hypotheses, we must have $\sum_i (a_i + b_i)X^i = P(X)^2$ and $\sum_i (a_i - b_i)X^i = P(X^2)$, so that the relations

$$\sum_i 2a_i X^i = P(X)^2 + P(X^2)$$

$$\sum_i 2b_i X^i = P(X)^2 - P(X^2)$$

show the existence of a unique $Q(X) \in \mathbb{C}C[X]$ with the required properties: it remains to show that the a_i and b_i are all integers. Now $P(X^2) = \sum_{j=s}^{d} p_j X^{2j}$ and $P(X)^2 = \sum_{k=2s}^{2d} X^k \sum_{j=s}^{k} p_j p_{k-j}$. The summation range $s, \ldots, k$ in the inner sum is not minimal, but this will not matter (of course p_j is taken as zero for $j \notin \{s, \ldots, d\}$).

$$2a_i = \begin{cases} \sum_{j=s}^{i} p_j p_{i-j} + p_{(\frac{i}{2})} & \text{for } i \text{ even,} \\ \\ \sum_{j=s}^{i} p_j p_{i-j} & \text{for } i \text{ odd.} \end{cases}$$

$$2b_i = \begin{cases} \sum_{j=s}^{i} p_j p_{i-j} - p_{(\frac{i}{2})} & \text{for } i \text{ even,} \\ \\ \sum_{j=s}^{i} p_j p_{i-j} & \text{for } i \text{ odd.} \end{cases}$$

Since $2a_i - 2b_i$ is an even integer for all i, it follows that a_i is an integer iff b_i is. We only consider the $\{a_i\}$ from now on, and take the cases 'i odd' and 'i even' separately.

For i odd:

$$2a_i = \sum_{j=s}^{i} p_j p_{i-j} = \sum_{j=s}^{\frac{i-1}{2}} p_j p_{i-j} + \sum_{j=\frac{i+1}{2}}^{i} p_j p_{i-j}$$

These summation ranges are all nonempty by construction; replacing the dummy j by $i-j$ under the last summation sign shows that the last two sums are the same. Hence $a_i \in \mathbb{Z}$ for all odd i.

For i even: This time, we have

$$2a_i = \sum_{j=s}^{i} p_j p_{i-j} + p_{(\frac{i}{2})} = p_{(\frac{i}{2})} + (p_{(\frac{i}{2})})^2 + \sum_{j=s}^{\frac{i}{2}-1} p_j p_{i-j} + \sum_{j=\frac{i}{2}+1}^{i} p_j p_{i-j}$$

Interchanging j and $i-j$ under the second summation sign again gives the result. Hence a_i is an integer for all even i. □

Proposition 7.2.0.2 *With the already established notation in this section, we have that,* $\forall^{*}\mathfrak{p}$, $Q(\sigma^{ir})(N\mathfrak{p}^r) = \#G_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}^r})$, *where* $\sigma^i = Fr\,\mathfrak{p}$ *and this holds* $\forall r \geq 1$.

Proof: For $i = 2$, we know that $G_{\mathfrak{p}} \sim_{\mathbb{F}_{\mathfrak{p}}} M_{\mathfrak{p}} \times M_{\mathfrak{p}}$, verifying this case. Otherwise, $i = 1$, and we have then $G_{\mathfrak{p}} \sim_{\mathbb{F}_{\mathfrak{p}}} R_{\mathbb{F}_{\mathfrak{p}^2}/\mathbb{F}_{\mathfrak{p}}}(M_{\mathfrak{p}})$, and so by [2.8.0.3], $\#G_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}^r}) = P(q^{lcm(2,r)})^{(2,r)}$

with $q = N\mathfrak{p}$ as usual. But for $i = 1$, $Q(\sigma^{ir})(q^r) = P(q^r)^2$ when r is even, and is $P(q^{2r})$ when r is odd, as required. □

Theorem 7.2.0.3 *(G as at the start of the chapter.)*

The Hasse-Weil zeta function $\zeta(G, K, s)$ is

$$(\dagger) \prod_i L(f/K, q_i, s - i),$$

where $Q(X) = \sum_i q_i X^i$.

Proof: This is now an elementary calculation. □

7.3 The case where M has f-type ${}^2X_{n,r}$

We recall that f/K is Galois. Suppose that the main orbit M (whose definition is immediately before [4.5.5.3]) is $\{u, v, u', v'\}$. We note that any subgroup of Γ_f which acts trivially on one Dynkin component (*via* the $*$-action) does so on the other as well because by [4.5.5.3] Γ_f acts in the same way on the components (more precisely, the components are isomorphic Γ_f-sets). Thus (recall the inner field l for G) $[l : K] = 4$, and moreover, $H_l \cong C_2 \times C_2$ (and not C_4) since it must contain (regarded as permutations on the underlying set of M) $\sigma = (uv)(u'v')$, which generates $\Gamma_f/\Gamma_l = Gal(l/f)$ (a subgroup of H_l), and $\rho = (uu')(vv')$ which interchanges the components.

We can just about identify the strict $\mathbb{F}_\mathfrak{p}$-isogeny class of $G_\mathfrak{p}$ immediately, as given in the following table. We remark that the uniqueness of the quadratic extension of $\mathbb{F}_\mathfrak{p}$ has been used. Let $P(X)$ be the rationality formula for X_n; recall that by [6.4.5] there exist $A(X)$ and $B(X)$ (with constant coefficients) such that $P(X) = A(X) + B(X)$ and $\#{}^2X_{n,r}(\mathbb{F}_{\mathfrak{p}^t}) = A(N\mathfrak{p}^t) + (-1)^t B(N\mathfrak{p}^t)$ (where ${}^2X_{n,r}$ temporarily denotes a group over $\mathbb{F}_\mathfrak{p}$). Using this and [2.8.0.3] gives the table which follows.

In this table, and subsequent similar ones, the second column gives either an almost $\mathbb{F}_\mathfrak{p}$-simple $\mathbb{F}_\mathfrak{p}$-group, or the Dynkin diagram of such a group, which is strictly $\mathbb{F}_\mathfrak{p}$-isogenous to $G_\mathfrak{p}$. The third column gives a rationality formula.

$$\begin{array}{llll} Fr\,\mathfrak{p} = e & X_n \coprod X_n & P^2(N\mathfrak{p}^t) \\ Fr\,\mathfrak{p} = \sigma & {}^2X_{n,r} \coprod {}^2X_{n,r} & [A(N\mathfrak{p}^t) + (-1)^t B(N\mathfrak{p}^t)]^2 \\ Fr\,\mathfrak{p} = \rho & R_{\mathbb{F}_{\mathfrak{p}^2}/\mathbb{F}_{\mathfrak{p}}}(X_n) & P^{(2,t)}(N\mathfrak{p}^{lcm(2,t)}) \\ Fr\,\mathfrak{p} = \sigma\rho & R_{\mathbb{F}_{\mathfrak{p}^2}/\mathbb{F}_{\mathfrak{p}}}(X_n) & P^{(2,t)}(N\mathfrak{p}^{lcm(2,t)}) \end{array}$$

The absence of $R_{\mathbb{F}_{\mathfrak{p}^2}/\mathbb{F}_{\mathfrak{p}}}({}^2X_{n,r})$ is due to the noncyclicity of H_l. We now need to reconcile these with the character table, and settle on the following simple characters of H_l.

Class	e	σ	ρ	$\sigma\rho$
χ_0	1	1	1	1
χ_1	1	1	−1	−1
χ_2	1	−1	1	−1
χ_3	1	−1	−1	1

We then put A and B into the rationality formulas, to obtain

$$Fr\,\mathfrak{p} = e \qquad X_n \coprod X_n \qquad A^2(N\mathfrak{p}^t) + 2A(N\mathfrak{p}^t)B(N\mathfrak{p}^t) + B^2(N\mathfrak{p}^t)$$

$$Fr\,\mathfrak{p} = \sigma \qquad {}^2X_{n,r} \coprod {}^2X_{n,r} \qquad A^2(N\mathfrak{p}^t) + 2(-1)^t A(N\mathfrak{p}^t)B(N\mathfrak{p}^t) + B^2(N\mathfrak{p}^t)$$

$$Fr\,\mathfrak{p} = \rho \qquad R_{\mathbb{F}_{\mathfrak{p}^2}/\mathbb{F}_{\mathfrak{p}}}(X_n) \qquad \begin{cases} A(N\mathfrak{p}^{2t}) + B(N\mathfrak{p}^{2t}) & \text{for } t \text{ odd}, \\ A^2(N\mathfrak{p}^t) + 2A(N\mathfrak{p}^t)B(N\mathfrak{p}^t) + B^2(N\mathfrak{p}^t) & \text{for } t \text{ even}. \end{cases}$$

$$Fr\,\mathfrak{p} = \sigma\rho \qquad R_{\mathbb{F}_{\mathfrak{p}^2}/\mathbb{F}_{\mathfrak{p}}}(X_n) \qquad \begin{cases} A(N\mathfrak{p}^{2t}) + B(N\mathfrak{p}^{2t}) & \text{for } t \text{ odd}, \\ A^2(N\mathfrak{p}^t) + 2A(N\mathfrak{p}^t)B(N\mathfrak{p}^t) + B^2(N\mathfrak{p}^t) & \text{for } t \text{ even}. \end{cases}$$

We have seen already in [7.2.0.1] how to find integers a_i and a_i' such that $A(X^2) = \sum_i (a_i - a_i')X^i$ and $A^2(X) = \sum_i (a_i + a_i')X^i$, and similarly b_i and b_i' for $B(X)$. We now observe that we require an $A(X^2)$ or a $B(X^2)$ precisely when $\chi_1([Fr\,\mathfrak{p}]^t) = -1$. Hence the terms which do not involve AB are

$$\sum_i (a_i + \chi_1([Fr\,\mathfrak{p}]^t)a_i')N\mathfrak{p}^t \text{ and } \sum_i (b_i + \chi_1([Fr\,\mathfrak{p}]^t)b_i')N\mathfrak{p}^t.$$

Finally, to get the terms involving AB, inspection shows that we should take

$$[\chi_2([Fr\,\mathfrak{p}]^t) + \chi_3([Fr\,\mathfrak{p}]^t)]A(N\mathfrak{p}^t)B(N\mathfrak{p}^t).$$

The final rationality formula is then

$$\#G_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}^t}) = \sum_i (a_i + b_i)N\mathfrak{p}^t + \sum_i (a_i' + b_i')\chi_1([Fr\,\mathfrak{p}]^t)N\mathfrak{p}^t + [\chi_2([Fr\,\mathfrak{p}]^t) + \chi_3([Fr\,\mathfrak{p}]^t)]A(N\mathfrak{p}^t)B(N\mathfrak{p}^t)$$

yielding zeta function

$$\zeta(G, K, s) = (\dagger) \prod_i \zeta_K(s-i)^{a_i+b_i} \cdot \prod_j L(H_l, \chi_1, s-j)^{a_j'+b_j'} \cdot \prod_k L(H_l, \chi_2, s-k)^{c_k} \cdot \prod_k L(H_l, \chi_3, s-k)^{c_k},$$

where $\sum_k c_k X^k = A(X)B(X)$.

7.4 The case where $M \sim_f {}^3D_{4,r}$

Since $\Gamma_f \lhd \Gamma$, we have $[l : K] = 6$, and indeed $H_l \cong C_2 \times C_3 \cong C_6$ since H_l contains $(134)(1'3'4')$ (generating $Gal(l/f)$), $(11')(33')(44')$ which interchanges the components, and their product (say) $\rho = (13'41'34')$. As usual we seek to classify $G_{\mathfrak{p}}$ according to $Fr\,\mathfrak{p}$. Let $P(X) = X^{12}(X^4-1)\prod_{i=1}^3(X^{2i}-1)$ be the rationality formula for $D_4 = {}^1D_{4,4}$. We use the following notation for the simple characters of H_l, where we write $\tau = \exp\frac{2\pi i}{6}$.

Class	e	ρ	ρ^2	ρ^3	ρ^4	ρ^5
χ_0	1	1	1	1	1	1
χ_1	1	τ	τ^2	-1	τ^4	τ^5
χ_2	1	τ^2	τ^4	1	τ^2	τ^4
χ_3	1	-1	1	-1	1	-1
χ_4	1	τ^4	τ^2	1	τ^4	τ^2
χ_5	1	τ^5	τ^4	-1	τ^2	τ

Considering the various conjugacy classes in H_l, putting $\omega = \exp\frac{2\pi i}{3} = \tau^2$, and abbreviating $lcm(2,t)$ by L we get

$$Fr\,\mathfrak{p} = e \qquad D_4 \coprod D_4 \qquad P^2(N\mathfrak{p}^t)$$

$$Fr\,\mathfrak{p} = \rho \qquad R_{\mathbb{F}_{\mathfrak{p}^2}/\mathbb{F}_{\mathfrak{p}}}({}^3D_{4,2}) \qquad \left\{ \begin{array}{r} [N\mathfrak{p}^{12L}(N\mathfrak{p}^{6L}-1)(N\mathfrak{p}^{2L}-1)\cdot \\ (N\mathfrak{p}^{8L}-(\omega^L+\omega^{2L})N\mathfrak{p}^{4L}+1)]^{(2,t)} \end{array} \right\}$$

$$Fr\,\mathfrak{p} = \rho^2 \qquad {}^3D_{4,2} \coprod {}^3D_{4,2} \qquad \left\{ \begin{array}{r} [N\mathfrak{p}^{12t}(N\mathfrak{p}^{6t}-1)(N\mathfrak{p}^{2t}-1)\cdot \\ (N\mathfrak{p}^{8t}-(\omega^t+\omega^{2t})N\mathfrak{p}^{4t}+1)]^2 \end{array} \right\}$$

$$Fr\,\mathfrak{p} = \rho^3 \qquad R_{\mathbb{F}_{\mathfrak{p}^2}/\mathbb{F}_{\mathfrak{p}}}(D_4) \qquad [N\mathfrak{p}^{12L}(N\mathfrak{p}^{4L}-1)\textstyle\prod_i(N\mathfrak{p}^{2iL}-1)]^{(2,t)}$$

$$Fr\,\mathfrak{p} = \rho^4 \qquad {}^3D_{4,2} \coprod {}^3D_{4,2} \qquad \left\{ \begin{array}{r} [N\mathfrak{p}^{12t}(N\mathfrak{p}^{6t}-1)(N\mathfrak{p}^{2t}-1)\cdot \\ (N\mathfrak{p}^{8t}-(\omega^t+\omega^{2t})N\mathfrak{p}^{4t}+1)]^2 \end{array} \right\}$$

$$Fr\,\mathfrak{p} = \rho^5 \qquad R_{\mathbb{F}_{\mathfrak{p}^2}/\mathbb{F}_{\mathfrak{p}}}({}^3D_{4,2}) \qquad \left\{ \begin{array}{r} [N\mathfrak{p}^{12L}(N\mathfrak{p}^{6L}-1)(N\mathfrak{p}^{2L}-1)\cdot \\ (N\mathfrak{p}^{8L}-(\omega^L+\omega^{2L})N\mathfrak{p}^{4L}+1)]^{(2,t)} \end{array} \right\}$$

where the formulas corresponding to $\rho^{\pm a}$ are the same.

We note that $\forall t$, $\omega^t+\omega^{2t} = \omega^L+\omega^{2L} = \tau^{2t}+\tau^{4t}$. Looking at the factors in the various rows which correspond to the factor $N\mathfrak{p}^{8t} - (\tau^t+\tau^{2t})N\mathfrak{p}^{4t}+1$ in the third row of the last table, and comparing with the character table shows that we should take this in general as

$$N\mathfrak{p}^{8t} - [\chi_2([Fr\,\mathfrak{p}]^t) + \chi_4([Fr\,\mathfrak{p}]^t)]N\mathfrak{p}^{4t} + 1.$$

We will adjust this now to take account of the parity of t. Define

$$Q(X,Y,Z) = X^{12}(X^6-1)(X^2-1)(X^8-(Y+Z)X^4+1) = A(X)+(Y+Z)B(X)$$

(say), so suitable evaluations of Q will give numbers of rational points. By an obvious extension of [7.2.0.1], there exist a finite set $I \subseteq \mathbb{N}\times\mathbb{N}\times\mathbb{N}$ and *integers* c_i and d_i (i in I) such

that $Q(X,Y,Z)^2 = \sum_{i\in I}(c_i+d_i)X^{i_1}Y^{i_2}Z^{i_3}$ and $Q(X^2,Y^2,Z^2) = \sum_{i\in I}(c_i-d_i)X^{i_1}Y^{i_2}Z^{i_3}$. Then by inspection, (recall that all the χ_j are linear characters), we get

$$\#G_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}^t}) = \begin{cases} Q(N\mathfrak{p}^t, \chi_2([Fr\,\mathfrak{p}]^t), \chi_4([Fr\,\mathfrak{p}]^t))^2 & \text{when } \chi_3([Fr\,\mathfrak{p}]^t) = +1, \\ Q(N\mathfrak{p}^{2t}, \chi_2([Fr\,\mathfrak{p}]^{2t}), \chi_4([Fr\,\mathfrak{p}]^{2t})) & \text{when } \chi_3([Fr\,\mathfrak{p}]^t) = -1. \end{cases}$$

$$= \sum_{i\in I}(c_i + \chi_3([Fr\,\mathfrak{p}]^t)d_i)N\mathfrak{p}^{i_1 t}\chi_2([Fr\,\mathfrak{p}]^t)^{i_2}\chi_4([Fr\,\mathfrak{p}]^t)^{i_3}$$

$(\forall t,\ \forall^*\mathfrak{p})$

verifying that $\zeta(G,K,s)$ is an alternating product of Artin L-functions for characters of H_l - *sciz.* has property (Z) for l/K.

7.5 The case where $M \sim_f {}^6D_{4,r}$

By the usual argument, we get $H_l \cong S_3 \times C_2$, with C_2 generated by $\sigma := (11')(33')(44')$. We observe that $\sigma(= \{1\}\times\sigma)$ is central in H_l, so that the conjugacy classes in H_l are those of $S_3 \times \{1\}$ and their translates by σ. Thus H_l has six simple characters. Now the characters of the direct product $A \times B$ of finite groups are readily determined as induced characters from A and B: the simple characters of $A\times B$ are the characters of representations $\theta_i \otimes_{\mathbb{C}} \phi_j$, where $\{\theta_i\}$ (respectively, $\{\phi_j\}$) runs over the irreducible representations of A (respectively, B). Thus the character table for $A\times B$ is the Kronecker product of those for A and B (*viz.* tensor product as matrices), with respect to a suitable ordering on the simple characters. Hence we have the following character table for H_l (where we merely list an element of each conjugacy class).

Class	e	$(13)(1'3')$	$(134)(1'3'4')$	σ	$(13)(1'3')\sigma$	$(134)(1'3'4')\sigma$
χ_0	1	1	1	1	1	1
χ_1	1	-1	1	1	-1	1
χ_2	2	0	-1	2	0	-1
χ_3	1	1	1	-1	-1	-1
χ_4	1	-1	1	-1	1	-1
χ_5	2	0	-1	-2	0	1

We write again $\omega = \exp\frac{2\pi i}{3}$ and $l = lcm(2,t)$; as usual $P(X)$ is the rationality formula

$$X^{12}(X^4-1)\prod_{i=1}^{3}(X^{2i}-1)$$

of D_4, and $P(X) = A(X) + B(X)$ where A and B are as in the rationality formula for ${}^2D_{4,3}$.

$$Fr\,\mathfrak{p} = e \qquad D_4 \coprod D_4 \qquad P^2(N\mathfrak{p}^t)$$

$$Fr\,\mathfrak{p} = (13)(1'3') \qquad {}^2D_{4,3} \coprod {}^2D_{4,3} \qquad [A(N\mathfrak{p}^t) + (-1)^t B(N\mathfrak{p}^t)]^2$$

$$Fr\,\mathfrak{p} = (134)(1'3'4') \qquad {}^3D_{4,2} \coprod {}^3D_{4,2} \qquad \left\{ \begin{array}{r} [N\mathfrak{p}^{12t}(N\mathfrak{p}^{6t}-1)(N\mathfrak{p}^{2t}-1)\cdot \\ (N\mathfrak{p}^{8t} - (\omega^t+\omega^{2t})N\mathfrak{p}^{4t}+1)]^2 \end{array} \right\}$$

$$Fr\,\mathfrak{p} = \sigma \qquad R_{\mathbb{F}_{\mathfrak{p}^2}/\mathbb{F}_{\mathfrak{p}}}(D_4) \qquad P(N\mathfrak{p}^l)^{(2,t)}$$

$$Fr\,\mathfrak{p} = (13)(1'3')\sigma \qquad R_{\mathbb{F}_{\mathfrak{p}^2}/\mathbb{F}_{\mathfrak{p}}}({}^2D_{4,3}) \qquad [A(N\mathfrak{p}^l) + (-1)^l B(N\mathfrak{p}^l)]^{(2,t)}$$

$$Fr\,\mathfrak{p} = (134)(1'3'4')\sigma \qquad R_{\mathbb{F}_{\mathfrak{p}^2}/\mathbb{F}_{\mathfrak{p}}}({}^3D_{4.2}) \qquad \left\{ \begin{array}{r} [N\mathfrak{p}^{12l}(N\mathfrak{p}^{6l}-1)(N\mathfrak{p}^{2l}-1)\cdot \\ (N\mathfrak{p}^{8l} - (\omega^l+\omega^{2l})N\mathfrak{p}^{4l}+1)]^{(2,t)} \end{array} \right\}$$

We observe that the top half of the last table is the same as that for the case ${}^6D_{4,r}$ [6.4.10] (except for the squaring of the rationality formula). In [6.4.10], we had

$$\#({}^6D_{4,r})_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}^t}) = A(N\mathfrak{p}^t) + \chi'([Fr\,\mathfrak{p}]^t)B_1(N\mathfrak{p}^t) + \chi''([Fr\,\mathfrak{p}]^t)B_2(N\mathfrak{p}^t)$$

where χ' and χ'' are the simple characters of S_3 denoted χ_1 and χ_2 there, and $A(X)$, $B_1(X)$ and $B_2(X)$ are polynomials with constant coefficients. Now put $Q(X,Y,Z) = A(X) + YB_1(X) + ZB_2(X)$. By the usual method, we apply [7.2.0.1] to find integers c_i and d_i such that

$$Q(X,Y,Z)^2 = \sum_i (c_i + d_i)X^{i_1}Y^{i_2}Z^{i_3}$$
$$Q(X^2,Y^2,Z^2) = \sum_i (c_i - d_i)X^{i_1}Y^{i_2}Z^{i_3}$$

and observe that

$$\#G_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}^t}) = \begin{cases} Q(N\mathfrak{p}^t, \chi_1([Fr\,\mathfrak{p}]^t), \chi_2([Fr\,\mathfrak{p}]^t))^2 & \text{if } \chi_3([Fr\,\mathfrak{p}]^t) = +1, \\ Q(N\mathfrak{p}^{2t}, \chi_1([Fr\,\mathfrak{p}]^t)^2, \chi_2([Fr\,\mathfrak{p}]^t)^2) & \text{if } \chi_3([Fr\,\mathfrak{p}]^t) = -1. \end{cases}$$

Hence we again get $\zeta(G,K,s)$ as an alternating product of Artin L-functions for characters of H_l.

7.6 Remarks about further work

We have seen that, to verify that all connected K-groups have property (Z), it would suffice to verify that every connected almost K-simple group has property (Z) [6.2.2.1].

In this chapter, we have verified that every such group which has up to two components in its Dynkin diagram has this property. The simplifying feature in this situation is that for such a group G, there exists a connected almost simple f-group M such that $G \sim_K R_{f/K}(M)$ with f being *normal* over K.

However, the general case ought not to be intractable in view of the systematization outlined in [4.5.5], which will hopefully form the basis of future work. There may be consequences for the Langlands program.

References

[AM69] Atiyah, M.F. and Macdonald, I.G., *Introduction to Commutative Algebra*, Addison-Wesley, (1969).

[Bor91] Borel, A., *Linear Algebraic Groups* (2nd enlarged edition), Springer Graduate Texts, **126** (1991).

[BT65] Borel, A. and Tits, J., Groupes Réductifs, *I.H.E.S. Publications Mathematiques* **27** (1965) *pp55-150.*

[BT72] Borel, A. and Tits, J., Compléments à l'article 'Groupes Réductifs', *I.H.E.S. Publications Mathematiques* 41 (1972) *pp253-276.*

[Bou68] Bourbaki, N., *Groupes et algèbres de Lie*, Hermann (Paris), (1968).

[Ca85] Carter, R., *Finite Groups of Lie Type*, John Wiley and Sons, 1985.

[DG70] Demazure, M. and Gabriel, P., *Groupes Algébriques*, Masson et Cie., Paris (1970).

[He67] Heilbronn, H., Zeta-Functions and L-Functions, *Algebraic Number Theory* (*eds.* Cassels, J.W.S. and Fröhlich, A.), Academic Press, London (1967).

[Hi74] Higgins, P. J., *An Introduction to Topological Groups*, L.M.S. Lecture Note Series **15**, Cambridge University Press (1974).

[Hu75] Humphreys, J.E., *Linear Algebraic Groups*, Springer Graduate Texts, **21** (1975).

[Ja64] Jacobson, N., *Lectures in Abstract Algebra* III, D. Van Nostrand (1964)

[Ja74] Jacobson, N., *Basic Algebra I*, W.H. Freeman, (1974).

[La56] Lang, S., Algebraic Groups over Finite Fields, *American Journal of Mathematics* **78** (1956), *pp555-563.*

[La70] Lang, S., *Algebraic Number Theory*, Addison-Wesley (1970).

[Ma77] Marcus, D.A., *Number Fields*, Springer-Verlag Universitext (1977).

[Mo56] Mostow, G.D., Fully Reducible Subgroups of Algebraic Groups, *American Journal of Mathematics* **78** (1956), *pp200-221.*

[Mu88] Mumford, D., The Red Book of Varieties and Schemes, *Springer Lecture Notes in Mathematics* **1358** (1988).

[Ono58] Ono, T., Sur la Réduction Modulo $\mathfrak{p}$ des Groupes Linéaires Algébriques, *Osaka Mathematical Journal* **10** (1958), *pp57-73.*

[Ono65] Ono, T., On the Relative Theory of Tamagawa Numbers, *Annals of Mathematics (2nd series)* **82** (1965), pp88-111.

[Ono66] Ono, T., On Tamagawa Numbers, *Proceedings of Symposia in Pure Mathematics* **IX**, A.M.S. (1966), *pp122-132.*

[Ros57] Rosenlicht, M., Some Rationality Questions on Algebraic Groups, *Annali di Matematica Pura ed Applicata* **43** (1957), *pp25-50.*

[Sa71] Satake, I., *Classification Theory of Semi-simple Algebraic Groups*, Marcel Dekker, (1971).

[Se59] Serre, J.-P., *Groupes Algébriques et Corps de Classes*, Hermann (Paris), (1959).

[Se65] Serre, J.-P., Zeta and L Functions, *Arithmetical Algebraic Geometry* (ed. O.F.G. Schilling), Harper's Series in Modern Mathematics, Harper and Row, New York (1965).

[Sh55] Shimura, G., Reduction of Algebraic Varieties with respect to a Discrete Valuation of the Basic Field, *American Journal of Mathematics* **77** (1955), *pp134-176.*

[Ti66] Tits, J., Classification of Algebraic Semisimple Groups, *Proceedings of Symposia in Pure Mathematics* **IX** A.M.S. (1966), *pp33-62.*

[We46] Weil, A., *Foundations of Algebraic Geometry*, A.M.S. Colloquium Publications, **XXIX** (1946).

Index of Definitions