ISRAEL JOURNAL OF MATHEMATICS 103 (1998), 207–235

INTEGRATING ON p-ADIC LIE GROUPS*

BY

M. P. F. DU SAUTOY

Department of Pure Mathematics and Mathematical Statistics
16 Mill Lane, Cambridge, CB2 1SB, England
e-mail: dusautoy@pmms.cam.ac.uk

AND

G. R. EVEREST

School of Mathematics, University of East Anglia
Norwich, Norfolk, NR4 7TJ, England
e-mail: g.everest@uea.ac.uk

ABSTRACT

Inspired by the classical Mahler measure of a polynomial, we study the integral of the order of an arithmetic polynomial on a compact p-adic Lie group. A result of Denef and van den Dries guarantees this is always a rational number. Integrals of this kind arise naturally; for example, the local canonical height of a rational point on an elliptic curve is given by a Mahler measure. Also, the mean valuation of the normal integral generators in a finite Galois extension arises as a Mahler measure. There is interest in being able to calculate the value of this measure. We show that for some classical groups, it is possible to reduce the integral to a simpler form, one where explicit computations are feasible. The motivation comes from the calculus trick of integration by substitution, also from Weyl's criterion. Applications are given to Galois Module Theory. Also, a close encounter with Leopoldt's conjecture is recorded. We deduce our results on the Mahler measure from the more general setting of local zeta functions defined for p-adic Lie groups. Our techniques apply to certain zeta functions, so we state and prove our results at that level of generality in our main theorem.

* Thanks go to Steve Wilson, the SERC and the London Mathematical Society for the Durham Galois Modules Workshop, which inspired the results in §5. Thanks go to Alex Lubotzky and the Royal Society for making possible the visit of the second author to the Hebrew University in Jerusalem which lead to the zeta-function point of view in §1 and §2.

Received October 4, 1994 and in revised form November 20, 1996

§1. Introduction

Let $K/\mathbb{Q}$ denote a finite extension of the rational numbers and suppose v is a non-archimedean valuation of K extending the p-adic valuation of $\mathbb{Q}$. Let $L = K_v$ denote the completion of K with respect to the v-adic topology. Write $\mathrm{ord}_v : L \to \mathbb{Q}$ for the usual v-adic order function defined as follows. Let π denote a generator for the non-zero prime ideal $\mathfrak{p}$ in the ring of integral elements ϑ_L in L. Given any non-zero element x, write $x = \pi^{\mathrm{ord}_v(x)}u$, where u is an element of ϑ_L^*, the group of units of ϑ_L. Let $\mathfrak{G}$ denote any compact v-adic Lie group and suppose F: $\mathfrak{G} \to L$ denotes any analytic map. Consider the following integral,

$$m_{\mathfrak{G}}(F) = \int_{\mathfrak{G}} \underset{v}{\mathrm{ord}}(F) d\mu_{\mathfrak{G}}. \tag{1.1}$$

In (1.1), $\mu_{\mathfrak{G}}$ denotes the Haar measure on the compact group $\mathfrak{G}$. We define this to be the **Mahler measure** of F on $\mathfrak{G}$, so named because of the classical Mahler measure of a polynomial, which is the integral of its logarithm over the torus. The classical Mahler measure has many wonderful properties and some outstanding questions also remain about its values. Many of these results and questions are collected in Boyd's paper [2]. The temptation to experiment by replacing the torus by other compact groups is irresistible. It is justified too on the grounds that these integrals arise naturally in quite concrete arithmetic situations. For example, in [14] we considered an elliptic analogue of the classical Mahler measure of a polynomial. The success of the venture hinged upon a local to global decomposition for the measure, where the local contributions are precisely integrals of the kind in (1.1). Another example arises where an integral such as (1.1) describes the distribution of normal integral bases in tame extensions of number fields, both locally and globally. In a different direction, integrals defined on compact p-adic groups are the key to understanding zeta functions counting subgroups of finite index in a large class of finitely generated groups (see [7]–[11], [16]). Integrals such as (1.1) arise in the Laurent coefficients of the zeta functions. In particular, (1.1) is a constant multiple of the coefficient of s in the Laurent expansion about $s = 0$ of the function defined in (1.4) of this paper. Our interest in the values of the general measure is further heightened by the following result:

PROPOSITION A: *$m_{\mathfrak{G}}(F)$ is a rational number.*

This follows by applying the results in [8] on the rationality of zeta functions associated to v-adic Lie groups. This in turn makes use of the deep results of Denef and van den Dries in [5] on zeta functions. The main theorem in

this paper is a step towards understanding the numerical analysis of integrals of the kind in (1.1). The motivation comes on two counts from the theory of real integration. Firstly, the calculus technique of integration by substitution to transform integrals into simpler forms. The basic aim is to realise the "$d\mu$" in (1.1) in a quite literal calculus-type manner as the local tangent space. Secondly, the discovery due to Weyl, that certain functions on bounded intervals may be integrated by averaging their values on a uniformly distributed sequence. Always, we will be in an arithmetic situation so that our groups and functions will be defined over an algebraic number field, labelled K. We propose the following as definitions.

Definitions: We say an arithmetic integral of the form in (1.1) is **linear** if it can be represented as a finite $(\mathbb{Q})$-linear combination of integrals of the following kind,

$$I = \int_{\mathbb{Z}_p^k} \operatorname*{ord}_v(f) d\mu_{\mathbb{Z}_p^k}, \quad f \in L[x_1, \ldots, x_k]. \tag{1.2}$$

In (1.2), $\mu_{\mathbb{Z}_p^k}$ denotes the Haar measure on the compact group $\mathbb{Z}_p^k$. We say an arithmetic integral of the form in (1.1) is K-**linear** if it can be represented as a finite $(\mathbb{Q})$-linear combination of integrals of the kind in (1.2) but where f has coefficients in K,

$$I = \int_{\mathbb{Z}_p^k} \operatorname*{ord}_v(f) d\mu_{\mathbb{Z}_p^k}, \quad f \in K[x_1, \ldots, x_k]. \tag{1.3}$$

We aim to show that these definitions provide useful theoretical and practical means for understanding better the integral in (1.1). Our main theorem proves that a very large class of integrals are K-linear. In §4, we will demonstate that a K-linear integral can be computed effectively as a limit of Riemann sums via an asymptotic formula. For some of the applications in mind in this paper, the resulting errors are about as good as they could be. Linearity of integrals is more likely to be of theoretical interest, as we indicate in the discussion around (1.4). See also Proposition 1.2 below, where we demonstrate a link between the value of a linear integral and the singular behaviour of the polynomial concerned.

The motivation for transforming integrals over Lie groups to integrals over linear spaces comes from two sources. Firstly the observation in a number of concrete arithmetic situations ([12]–[14]) that integrals arising on compact Lie groups $\mathfrak{G}$ can often be calculated by working in some way with the Lie algebra. Part of the explanation for this lies with the nature of effective results in the

theory of diophantine approximation. The non-trivial effective results take place within a Lie algebra. The most obvious example is Baker's Theorem about logarithms of algebraic numbers. In its p-adic and elliptic manifestations also, Baker's Theorem gives bounds for linear forms in objects lying inside the appropriate Lie algebra. They tend to be applied in arithmetic situations when the problem in hand can be worked out in the image of the logarithm map. Non-effective approximation tends to take place in the Lie group proper. For example, the Subspace Theorem of Schmidt ([21]) and Faltings Theorem on abelian varieties ([15]) are examples of this latter kind of theorem.

Secondly, the same basic technique is used in [9] where uniformity results are established for the zeta functions counting subgroups in compact Lie groups. There, the counting of subgroups is effected by the counting of subalgebras in the associated Lie algebra.

In fact, the results in [6]–[11], and the foundational paper [16], suggest that we should apply our definitions to the v-adic integrals defined as follows. With the notation as above, let

$$I(s, F, \mathfrak{G}) = \int_{\mathfrak{G}} |F|_v^s d\mu_{\mathfrak{G}}, \quad s \in \mathbf{C}, \quad \mathrm{Re}(s) > 0. \tag{1.4}$$

In the case, where $\mathfrak{G} = \mathbb{Z}_p^k$ and F is a polynomial, the integral $I(s, F, \mathfrak{G})$ is known as an **Igusa integral**. In tandem with our earlier definitions, we call $I(s, F, \mathfrak{G})$ **linear** if it can be represented as a finite $(\mathbb{Q})$-linear combination of Igusa integrals. If the resulting polynomials are all defined over K then we say $I(s, F, \mathfrak{G})$ is K-linear. Our main techniques show that a large class of zeta functions are linear. To try to gauge the potential of this observation, recall that several authors (see [6], [11]) have recognised functional equations satisfied by zeta functions. In [6], this is proved for certain types of Igusa integrals. Our observation may lead to a theoretical step in the proof that more general classes of zeta functions satisfy functional equations. The assumption on $\mathrm{Re}(s)$ prevails in the sequel. The results in [8] show that the function $I(s, F, \mathfrak{G})$ is a rational function in $|\pi|_v^s$. Thus, in particular, $I(s, F, \mathfrak{G})$ has a meromorphic continuation to the whole s-plane. Note that formally, (1.1) arises as $(\log |\pi^{-1}|_v)^{-1}$ times the coefficient of s in the Laurent expansion of (1.4) about $s = 0$. Thus (K-) linearity of $m_{\mathfrak{G}}(F)$ follows from (K-) linearity of $I(s, F, \mathfrak{G})$.

To state our theorem, let G denote a reductive algebraic group defined over the field L and $\phi\colon G \to \mathrm{GL}_n$ an L-rational representation of G. We shall suppose in addition that G is L-split. (This implies that $G(L)$ is an almost direct product of an L-split central torus and an L-split semi-simple group i.e. a Chevalley group.)

Suppose H is any subgroup of $\mathrm{GL}_n(L)$ which is commensurable with $G(\vartheta_L)$, i.e. $H \cap G(\vartheta_L)$ has finite index in H and $G(\vartheta_L)$. We will assume that we have taken $L/\mathbb{Q}_p$ to be a Galois extension. The elements of the Galois group Δ act on H. We will say F is a **polynomial on** H if it is a polynomial on the entries of the matrices in H, together with their Galois images. (Thus F is a polynomial defined on the space whose elements are vectors $(h^\delta)_{\delta\in\Delta}$, $h \in H$.) We wish to obtain some idea of the typical valuation of F on this compact group. The measure $m_H(F)$ does just that.

THEOREM 1.1: *Let G denote an L-split reductive algebraic group, defined over the local field L and ϕ: $G \to \mathrm{GL}_n$ an L-rational representation of G. Let H denote a subgroup of $\mathrm{GL}_n(L)$ which is commensurable with the maximal compact subgroup $G(\vartheta_L)$ of $G(L)$. (1) If F is a polynomial on H with coefficients in L then the integrals defining $I(s,F,H)$ and $m_H(F)$ are linear. (2) Suppose that L is the completion of the algebraic number field K. If G, F and ϕ are defined over the field K and G is K-split, then $I(s,F,H)$ and $m_H(F)$ are K-linear.*

In §2, we will prove this theorem. It is sufficient to prove this for the integrals defining $I(s,F,H)$ by our remarks after (1.4) concerning the relationship between $I(s,F,H)$ and $m_H(F)$. This paper is *really* about measures like $m_H(F)$; they are actual rational numbers that people might wish to calculate and we present several approaches to that problem.

In §3 we gather together some miscellaneous results around the calculation of $m_H(F)$ in various examples not covered by Theorem 1.1 but which arise naturally in various contexts. This includes the special case where H is an open subgroup of $\mathrm{SL}_n(D)$ where D is a division algebra over $\mathbb{Q}_p$. This is in fact a non-split reductive group except in the case where D is a commutative division algebra, i.e. when D is a field. In another direction, examples (ii) and (iii) concern the harder problem of averaging the values of F over the local closure of a group defined over the global ring ϑ_K. The group in question is an example of an analytic torus which is not represented algebraically. This does occur naturally, see §5. Some interesting obstructions are encountered at both levels, linearity and K-linearity; we consider integrals which are linear but apparently not K-linear. The obstructions arise from some interesting quarters. For example, the ramification and the lack of proof for an unproven conjecture due to Leopoldt about the non-vanishing of the p-adic regulator, which we will define in §3. This is related to the way global algebraic units embed locally.

In §4, we present a theorem which shows that K-linear integrals $m_H(F)$ are effectively computable via Riemann sums. This is in fact the raison d'être of

this paper. In terms of practicability, there now exist packages such as PARI-GP which are able to compute the standard objects in algebraic number theory very quickly. Our results make it feasible to actually compute what would otherwise be intractable integrals.

In §5, we show how Theorem 1.1 and the examples in §3 apply to the study of normal integral bases, both in finite extensions of $\mathbb{Q}_p$ and in finite extensions of $\mathbb{Q}$. In this instance, the Mahler measure gives a sort of average v-adic valuation for the set of normal integral bases.

We conclude the introduction with the following calculation of the value of a linear integral. This shows that the linearisation methods we espouse may yield fruitful insights into the relationship between the value of $m_H(F)$ and the singular behaviour of F on H.

PROPOSITION 1.2: *Suppose $f \in \mathbb{Z}_p[x_1, \dots, x_k]$ which has non-zero reduction $\overline{f}$ mod p. Let*

$$\theta = \int_{\mathbb{Z}_p^k} \operatorname{ord}_p(f) d\mu_{\mathbb{Z}_p^k}. \tag{1.5}$$

If $|\theta|_p > p^{k-1}$ then $\overline{f}$ has a singular point on $\mathbb{F}_p^k$.

For example, the integral of $\operatorname{ord}_p(x^2 - p)$ over $\mathbb{Z}_p$ is easily computed to be $1/p$. The proposition predicts singular behaviour of the polynomial modulo p and we do not have to look far to find it. The statement of Proposition 1.2 looks weak but is actually the strongest possible of its type. For example, the polynomial $f = x^3 + y^2 + 1$ is non-singular over $\mathbb{F}_7$ and the integral of $\operatorname{ord}_7(f)$ over $\mathbb{Z}_7^2$ is $1/14$.

To prove Proposition 1.2, it is easier to prove a stronger statement. Let $\underline{a} \in \mathbb{Z}_p^k$ denote a fixed vector. Let $\mathbf{C}_{\underline{a}}$ denote the coset $\underline{a} + (p\mathbb{Z}_p)^k$. Consider the integral

$$\rho = \int_{\mathbb{C}_{\underline{a}}} \operatorname{ord}_p(f) d\mu, \tag{1.6}$$

where $f \in \mathbb{Z}_p[x_1, \dots x_k]$ does not reduce to zero mod p, and where μ denotes Haar measure on $\mathbb{Z}_p^k$.

PROPOSITION 1.3: *If $\overline{f}$ has no singular points on $\mathbb{F}_p^k$ then the rational number in* (1.6) *satisfies $|\rho|_p \leq p^{k-1}$.*

Proof: After relabelling if necessary, we may suppose that $\overline{f}(x_1, x_2, \dots, x_k)$ is non-singular in x_1, for any choice of $x_2, \dots, x_k$ with $x_i \equiv a_i$ for $i = 2, \dots, r$.

Evaluating the integral by Fubini's Theorem, we obtain the value 0 (if $f(\underline{a})$ does not vanish mod p) or

$$\int dx_2 \cdots dx_r \int_{x_1 \equiv a_1 \bmod p} \operatorname*{ord}_p(x_1 - \alpha_1) d\mu = \frac{1}{p^{k-1}(p-1)},$$
$$\text{where } \alpha_1 \equiv a_1 \bmod p.$$

This is because the non-singularity condition, together with Hensel's Lemma guarantees that the simple root of $f(x_1)$ congruent to a_1 modulo p, can always be lifted to a simple root α_1 in $\mathbb{Z}_p$ with $\alpha_1 \equiv a_1 \bmod p$. ∎

The statement in Proposition 1.2 follows trivially from the ultrametric inequality because θ is a finite sum of integrals of the kind in (1.6).

§2. Split reductive groups

Throughout this section L denotes a finite Galois extension of $\mathbf{Q}_p$ with Galois group Δ, ϑ_L the ring of integers of L, $\mathfrak{p}$ the maximal ideal in ϑ_L and π a uniformizing parameter for $\mathfrak{p}$. The field K will always denote a finite extension of $\mathbb{Q}$ whose completion with respect to some non-archimedean valuation v is L. Recall that a group H is **commensurable** with a group G if $H \cap G$ has finite index in H and G. In this section we prove that certain integrals over split reductive groups can be transformed into linear and K-linear integrals as defined in (1.2) and (1.3).

Let G denote an L-split reductive algebraic group defined over L and let $\phi\colon G \to \mathrm{GL}_n$ be an L-rational representation of G. Let H denote a subgroup of $\mathrm{GL}_n(L)$ which is commensurable with the maximal compact subgroup $G(\vartheta_L)$ of $G(L)$. We first prove a lemma which allows us to make various reductions.

LEMMA 2.1: *Let H_0 be a subgroup of finite index in H. Suppose that for every polynomial F on H_0 with coefficients in L, $I(s, F, H_0)$ is linear. Then $I(s, F, H)$ is linear for every polynomial F defined on H. If in addition everything is defined over K and $I(s, F, H_0)$ is always K-linear then the same is true of $I(s, F, H)$.*

Proof: By choosing coset representatives $g_i \in \mathrm{GL}_n(L)$ for H_0 in H we can write

$$I(s, F, H) = \sum_{i=1}^{[H:\, H_0]} I(s, F_i, H_0) \cdot \mu_H(H_0)$$

where $F_i(\mathbb{X}) = F(g_i \mathbb{X})$. This suffices to prove linearity.

To prove K-linearity we must check that we can choose the representatives g_i such that $\phi(g_i) \in \mathrm{GL}_n(K)$. Now $\phi(G(K)) \leq \mathrm{GL}_n(K)$ and $G(K)$ is Zariski-dense

inside $G(L)$. Thus $G(K)$ meets any coset of the subgroup H_0. Hence we can choose a representative for that coset from $G(K)$. ∎

We can apply Lemma 2.1 immediately to reduce to the case that G is a connected reductive algebraic group since if G^0 denotes the connected component of G then $H^0 = H \cap G^0(L)$ has finite index in H. We shall apply this lemma a number of times to reduce our integral. A connected reductive algebraic group is an almost direct product of its central torus S and its derived group G' which is semi-simple. Recall that an almost direct product means that $S(L) \cap G'(L)$ is finite (see [1], Proposition 2.2).

By descending to a subgroup of finite index we may suppose that H is a direct product of a subgroup H_1 of $S(\vartheta_L)$ and a subgroup H_2 of the semi-simple group $G'(\vartheta_L)$. Thus we may write the integral $I(s, F, H)$ as a product $I(s, F, H_1)I(s, F, H_2)$. We may therefore consider separately the two cases where (1) G is an L-split torus and (2) G is a connected L-split semi-simple group.

§2.1. Tori.

THEOREM 2.2: *Suppose that G is an L-split torus and ϕ: $G \to \mathrm{GL}_n$ is an L-rational homomorphism. Let H be a subgroup commensurable with $G(\vartheta_L)$. (1) Then $I(s, F, H)$ is linear. (2) If ϕ and G are defined over K and G is K-split then $I(s, F, H)$ is K-linear.*

Proof: By conjugating with an element from $\mathrm{GL}_n(L)$ (or from $\mathrm{GL}_n(K)$ if G is K-split) we may suppose that $\phi(G(L)) \leq \mathrm{diag}_n(L)$. We can also identify G with l copies of the multiplicative group $\mathbb{G}_m$ such that $G(L) = \mathrm{diag}_l(L)$. Each diagonal entry $\phi_i(t)$ $(i = 1, \ldots, n)$ of $\phi(t) \in \phi(G(L))$ is then given by some character of $G(L)$. Hence there exist $n_{1i}, \ldots, n_{li} \in \mathbb{Z}$ such that, if $t = \mathrm{diag}_l(x_1, \ldots, x_l)$ then

$$\phi_i(t) = x_1^{n_{1i}} \cdots x_l^{n_{li}}. \tag{2.1}$$

The subgroups $G(1 + \pi^i \vartheta_L) = \mathrm{diag}_l(1 + \pi^i \vartheta_L)$ are a base of neighbourhoods of the identity of $G(\vartheta_L)$. Since H is commensurable with $G(\vartheta_L)$, H contains some $S(1 + \pi^i \vartheta_L)$ as a subgroup of finite index. By Lemma 2.1 we may suppose that $H = G(1 + \pi^i \vartheta_L)$. The map $\vartheta_L^l \to G(1 + \pi^i \vartheta_L)$ is a measure-preserving bijection which we may use to write

$$I(s, F, H) = \int_{\vartheta_L^l} |F^*((1 + y_1 \pi^i), \ldots, (1 + y_l \pi^i))|_v^s d\mu_{\vartheta_L^l}$$

where, by (2.1) above, F^* is a polynomial in $(1 + y_j \pi^i)$ and $(1 + y_j \pi^i)^{-1}$ and their Galois conjugates. Since $|1 + y_j \pi^i|_v = 1$, we can multiply F^* through by

$(1 + y_j\pi^i)$ without altering the value of $|F^*|_v$ and hence we may assume that F^* is in fact a polynomial in $(1 + y_j\pi^i)$ and its Galois conjugates.

We almost have a linear integral except for the complication that F^* is a polynomial in the Galois conjugates of $(1 + y_j\pi^i)$. The following lemma shows that the Galois conjugation does not cause any problem once we have linearized an integral as above over ϑ_L:

LEMMA 2.3: *Suppose the function $F(x_1, \ldots, x_n)$ is given by a polynomial (with coefficients from L) in $(x_1, \ldots, x_n) \in \vartheta_L^n$ and their Galois conjugates $x_i^{\tau_j}$ where $\tau_1, \ldots, \tau_d$ are Galois automorphisms of L. Then*

$$\int_{\vartheta_L^n} |F(x_1, \ldots, x_n)|_v^s d\mu_{\vartheta_L^n}$$

is linear. If the function F is given by a polynomial with coefficients from K then the integral is K-linear.

Proof: Take a basis for ϑ_K over $\mathbb{Z}$ which extends then to a basis for ϑ_L over $\mathbb{Z}_p$. We can transform the integral above into an integral over $\mathbb{Z}_p^{dn}$ where $d = [L\colon \mathbb{Q}_p]$. The Galois automorphisms then become linear maps over K with respect to this basis and hence there is a polynomial $F^*(y_1, \ldots, y_{dn})$ such that the integral has the following form:

$$\int_{\mathbb{Z}_p^{dn}} |F^*(y_1, \ldots, y_{dn})|_v^s d\mu_{\mathbf{Z}_p^{dn}}.$$

Linearity is then clear. Also, K-linearity follows since our choice of a basis for ϑ_K over $\mathbb{Z}$ ensures that $F^*(y_1, \ldots, y_{dn})$ has coefficients in K if F was given by a polynomial with coefficients in K. ∎

Lemma 2.3 suffices then to conclude the proof of Theorem 2.2 of the linearity (or K-linearity) of $I(s, F, H)$. ∎

§2.2. SPLIT SEMI-SIMPLE ALGEBRAIC GROUPS. Suppose now that G is a connected k-split semi-simple algebraic group. Then G has the structure of a Chevalley group, i.e. there is an isomorphism (defined over the field k which splits G) between G and a Chevalley group (see [1]). We recall the definition of a Chevalley group.

Let $\mathcal{L}$ be a semi-simple Lie algebra over the field $\mathbb{C}$, and $\mathcal{H}$ a Cartan subalgebra of $\mathcal{L}$, i.e. a self-normalizing nilpotent subalgebra. Let

$$\mathcal{L} = \mathcal{H} \oplus \sum_{\alpha \in \Phi} \mathcal{L}_\alpha$$

denote the Cartan decomposition of $\mathcal{L}$ where $\mathcal{L}_\alpha = \{x \in \mathcal{L}: [h,x] = \alpha(h)x$ for all $h \in \mathcal{H}\}$ is a one-dimensional subspace and Φ is the associated root system. Let $\{h_\beta, e_\alpha: \beta \in \Pi, \alpha \in \Phi\}$ denote a Chevalley basis for $\mathcal{L}$ where Π is a basis for the root system and $\mathcal{H} = \langle h_\beta | \beta \in \Pi\rangle$. Let $\mathcal{U}_\mathcal{L}$ denote the universal enveloping algebra and $\mathcal{U}_\mathbb{Z}$ the $\mathbb{Z}$-algebra generated by all $e_\alpha^m/m!$ ($m \in \mathbb{N}$, $\alpha \in \Phi$). Let V be a representation space for $\mathcal{L}$ such that we have a homomorphism $\phi: \mathcal{L} \to \mathrm{End}(V)$. This representation extends to define an action of the universal enveloping algebra $\mathcal{U}_\mathcal{L}$ on V. Consider the decomposition into weight spaces V^λ with respect to $\mathcal{H}$:

$$V = \sum_{\lambda \in \Lambda(\phi)} V^\lambda,$$

where $\Lambda(\phi)$ denotes the set of all non-trivial weights corresponding to the representation ϕ. Then V contains a **$\mathbb{Z}$-admissable lattice** $V_\mathbb{Z}$, that is a $\mathbb{Z}$-lattice such that:

(i) $V_\mathbb{Z}$ is stable under the action of $\mathcal{U}_\mathbb{Z}$, i.e. stable under each $\phi(e_\alpha)^m/m!$ for all $\alpha \in \Phi, m \in \mathbb{N}$;

(ii) $V_\mathbb{Z} = \sum_{\lambda \in \Lambda(\phi)} V_\mathbb{Z}^\lambda$ where we define $V_\mathbb{Z}^\lambda = V_\mathbb{Z} \cap V^\lambda$.

The **Chevalley group** $G(k)$ over the field $k/\mathbb{Q}$ is then defined to be the following subgroup of the automorphisms of $V_\mathbb{Z} \otimes_\mathbb{Z} k$:

$$G(k) = \langle x_\alpha(t): \alpha \in \Phi, t \in L\rangle. \tag{2.2}$$

In (2.2),

$$x_\alpha(t) = \exp(t\phi(e_\alpha)) = \sum_{n=0}^{\infty} t^n \phi(e_\alpha)^n/n! \tag{2.3}$$

for $t \in k$ and $\alpha \in \Phi$. Note that $\phi(e_\alpha)^n$ acts as zero for n sufficiently large so the sum in (2.3) is actually finite.

We consider the case now where $k = L$. Let $G(\vartheta_L)$ denote the group generated by $x_\alpha(t)$ for all $\alpha \in \Phi$ and $t \in \vartheta_L$. Then $G(\vartheta_L)$ is a maximal compact subgroup of G. Let μ denote the Haar measure on $G(L)$ normalized such that $G(\vartheta_L)$ has measure 1.

THEOREM 2.4: *Let ϕ: $G \to \mathrm{GL}_n$ be an L- rational representation of the Chevalley group G. Let F denote a polynomial with coefficients in L on the entries of $h \in \mathrm{GL}_n(L)$ and their Galois conjugates h^δ where δ ranges over the Galois group of $L/\mathbb{Q}_p$. Let $H \leq \mathrm{GL}_n(L)$ be commensurable with $G(\vartheta_L)$. Then*

the integral $I(s, F, H)$ is linear. If ϕ and F are defined over the global field K then $I(s, F, H)$ is K-linear.

Proof: By choosing a basis for the admissable $\mathbb{Z}$-lattice $V_{\mathbb{Z}}$ we can define a faithful $\mathbb{Q}$-rational representation of G denoted

$$\phi\colon G \to \mathrm{GL}_n, \tag{2.4}$$

where $\dim_{\mathbb{C}} V = n$. Such a representation ϕ we shall call a **defining representation**. (Note that it is not to be confused with the natural representation for the classical groups like SL_m.) The following lemma shows that it suffices to prove the theorem for this defining representation:

LEMMA 2.5: *Suppose that G is a connected semi-simple algebraic group defined over a field k of characteristic zero. Let $\phi_1\colon G \to \mathrm{GL}_{n_1}$ and $\phi_2\colon G \to \mathrm{GL}_{n_2}$ be two k-rational representations of G and suppose that ϕ_1 is faithful. Then there exist polynomials $p_{ij}(X_{kl})$ $(i, j = 1, \ldots, n_2$ and $k, l = 1, \ldots, n_1)$ with coefficients in k such that*

$$\phi_2(g) = (p_{ij}(\phi_1(g)))$$

for all $g \in G(k)$.

Proof: See Theorem 14.4 of [24] which ensures that the entries $\phi_2(g)$ are polynomials in the entries of $\phi_1(g)$ and $(\det \phi_1(g))^{-1}$. Since G is semi-simple, it is equal to its own derived group and hence $\det \phi_1(g) = 1$. Alternatively, for a proof in the case of Chevalley groups see Lemma 69 of [22]. ∎

We define $w_\alpha(t) = x_\alpha(t)x_{-\alpha}(-t^{-1})x_\alpha(t)$ and $h_\alpha(t) = w_\alpha(t)w_\alpha(1)^{-1}$ for each $\alpha \in \Phi$ and $t \in L$. Define for each $m \in \mathbb{N}$ the following congruence subgroups:

$$G_m = \langle x_\alpha(t_\alpha), h_\beta(1 + t_\beta)\colon t_\alpha, t_\beta \in \mathfrak{p}^m, \alpha \in \Phi, \beta \in \Pi\rangle. \tag{2.5}$$

In (2.5), G_m is the normal closure of the group generated by $x_\alpha(t_\alpha)$, $t_\alpha \in \mathfrak{p}^m$. The set $\{G_m\}_{m\in\mathbb{N}}$ forms a system of neighbourhoods of the identity for the topology on $G(\vartheta_L)$. Hence any subgroup of finite index in $G(\vartheta_L)$ contains a subgroup G_m for some m. The groups $G(\vartheta_L)$ and G_m have the following alternative description with respect to the representation ϕ:

$$G(\vartheta_L) = \phi^{-1}(\phi(G) \cap \mathrm{GL}_n(\vartheta_L)),$$
$$G_m = \{g \in G(\vartheta_L)\colon \phi(g) \equiv I_n (\mathrm{mod}\ \mathfrak{p}^m)\}.$$

(See, for example, [19], Corollary 4.4.)

By Lemma 2.1 it suffices to consider the case where $H = G_m$ for some m. The group G_m can be parameterized in a simple manner: let $l =$ card Π and $k =$ card Φ^+ where Φ^+ denotes the positive roots. Define the map θ: $\pi^m \vartheta_L^{2k+l} \to G_m$ by

$$\theta((t_\alpha)_{\alpha<0}, (t_\beta)_{\beta\in\Pi}, (t_\alpha)_{\alpha>0}) = \prod_{\alpha<0} x_\alpha(t_\alpha) \prod_{\beta\in\Pi} h_\beta(1+t_\beta) \prod_{\alpha>0} x_\alpha(t_\alpha), \tag{2.6}$$

where the product is taken with respect to some chosen ordering on the root system. In (2.6), θ is an isomorphism of varieties over L. For a proof see [22], Theorem 7 (b) and Theorem 22. In Lemma 1.20 of [8] we considered the Haar measure on a uniformly powerful pro-p group, that is a finitely generated torsion-free pro-p group for which G/G^p is abelian for p odd and G/G^4 is abelian for $p = 2$. For example the congruence subgroups G_m defined as the kernels of the natural maps from $\mathrm{GL}_n(\mathbb{Z}_p)$ onto $\mathrm{GL}_n(\mathbb{Z}_p/p^m\mathbb{Z}_p)$ are uniformly powerful pro-p groups. It was shown that a certain parametrization of a uniformly powerful pro-p group is measure-preserving. In a similar fashion, we can prove:

LEMMA 2.6: *Let ν denote the additive Haar measure on ϑ_L^{2k+l} normalized at $\pi^m\vartheta_L^{2k+l}$ and μ the Haar measure on G_m normalized such that G_m has measure 1. Let $X \subseteq G_m$, then X is a measurable subset if and only if $\theta^{-1}(X)$ is a measurable subset of ϑ_L^{2k+l}. In this case $\mu(X) = \nu(\theta^{-1}(X))$.*

Proof: The additive Haar measure ν on ϑ_L^{2k+l} induces a measure via θ on G_m and hence on G_m/G_{m+n} for each $n \in \mathbb{N}$. This measure coincides with the measure induced by μ on G_m/G_{m+n} (since both just measure the cardinality of subsets). By Bourbaki's Integration VII §1.6 this implies that the measures ν and μ coincide on G_m. ∎

Note that in fact G_m is a uniformly powerful pro-p group for m sufficiently large. In [25], Weigel proves that, under certain conditions on the Chevalley group G and the prime p, one can characterize the largest open normal uniformly powerful pro-p subgroup of $G(\vartheta_L)$ as the subgroup G_e where e is the ramification index of the field L.

We can now use our parameterization of G_m and Lemma 2.6 to rewrite the integral $m_{G_m}(F)$ as an additive integral:

$$\int_{\pi^m\vartheta_L^{2k+l}} |F(\phi(\theta(\mathbf{t})))|_v^s d\mu, \tag{2.7}$$

where $\mathbf{t} = ((t_\alpha)_{\alpha<0}, (t_\beta)_{\beta\in\Pi}, (t_\alpha)_{\alpha>0})$.

LEMMA 2.7:

(1) *The entries of* $\phi(x_\alpha(t_\alpha))$ *are polynomials in* t_α *with integer coefficients.*

(2) *The entries of* $\phi(h_\beta(1+t_\beta))$ *are polynomials in* $1+t_\beta$ *and* $(1+t_\beta)^{-1}$ *with integer coefficients.*

Proof: Part (2) will follow from (1) since we have defined $w_\alpha(t) = x_\alpha(t)$ $x_{-\alpha}(-t^{-1})x_\alpha(t)$ and $h_\alpha(t) = w_\alpha(t)w_\alpha(1)^{-1}$ for each $\alpha \in \Phi$ and $t \in L$. For part (1) we must check how $x_\alpha(t_\alpha)$ acts on a $\mathbb{Z}$- basis for the $\mathbb{Z}$-admissable lattice $V_\mathbb{Z}$. Now $\phi(e_\alpha)^m/m!$ acts as zero for m sufficiently large and therefore

$$\phi(x_\alpha(t_\alpha)) = \sum_{m=0}^{M} \phi(e_\alpha)^m t_\alpha^m/m!.$$

Since $\phi(e_\alpha)^m/m!$ stabilizes the $\mathbb{Z}$-lattice $V_\mathbb{Z}$, it is given by a matrix with integer entries. Hence the entries of $\phi(x_\alpha(t_\alpha))$ are given by polynomials in t_α with integer coefficients. ∎

Lemma 2.7 implies that $F(\phi(\theta(\mathbf{t})))$ is a polynomial (with coefficients in K if F is defined over K) in t_α and $(1+t_\beta)^{-1}$ and their Galois conjugates. But $(1+t_\beta^{\sigma_j})^{-1}$ always takes values which are units since $t_\beta \in \mathfrak{p}^m$. Thus

$$|F(\phi(\theta(\mathbf{t})))|_v = |(1+t_\beta)^N F(\phi(\theta(\mathbf{t})))|_v$$

for any N and so we can assume in fact that $F(\phi(\theta(\mathbf{t})))$ is a polynomial (with coefficients in K if F is defined over K) in t_α together with its Galois conjugates.

Finally, we can apply Lemma 2.3 to the integral in (2.7) to conclude the proof of Theorem 2.4. ∎

§3. Examples

In this section, we will present some examples of the Mahler measure which arise from a more number theoretic perspective. These integrals are not covered by the examples of §2. However, we see that in some circumstances we are able to prove linearity and K-linearity yielding integrals that in some cases can be computed explicitly. This is the case in example (i) where we consider an integral over a subgroup of the local units ϑ_L^* of the local field L.

In examples (ii) and (iii) we consider integrals over the p-adic closure of a subgroup of the global unit group ϑ_K^* where we embed these units into L^l using the $l = [K\colon \mathbf{Q}]$ distinct embeddings of K into L. These integrals we shall show can be written as integrals of the value of exponential polynomials over $\mathbf{Z}_p^r$.

These exponential polynomials, which are finite sums of constant multiples of exponentials, are defined via the local embeddings of the global units. In these examples we see how obstructions can arise in either the linearity or K-linearity. The difference with the examples in §2 is that we are led to consideration of an integral of a polynomial on non-algebraic representations of the torus.

Now let $L/\mathbf{Q}_p$ denote a Galois extension, with Galois group Δ.

(i) Let $\rho \in L$ then we say ρ is **primitive** if it has the property that $\rho^\delta \equiv 0 \bmod \pi$ does not hold for all $\delta \in \Delta$. Write T_ρ for the trace map, $T_\rho(u) = \sum_{\delta\in\Delta}(\rho u)^\delta$. Given $1 \leq m \in \mathbf{N}$, let H denote the subgroup of ϑ_L^* defined by

$$H = \{u \in \vartheta_L^* | u^\delta \equiv 1 \bmod \pi^m \text{ for all } \delta \in \Delta\}.$$

Also let $N_{L|\mathbf{Q}_p}(\pi) = P$, where $N_{L|\mathbf{Q}_p}\colon L \to \mathbf{Q}_p$ denotes the field norm. It is easy to prove that $m_H(T_\rho) = m + 1/(P-1)$ if $T_\rho(1) \equiv 0 \bmod \pi^m$. Otherwise $m_H(T_\rho)$=ord$_v(T_\rho(1))$.

(ii) Suppose L is large enough so that there are $l = [K\colon \mathbf{Q}]$ distinct embeddings of K into L. Label these $\tau_j, j = 1, \ldots, l$. We have then a map $\vartheta_K^* \to \vartheta_L^{*l}$. Rather than considering an integral with respect to the closure of the global units inside ϑ_L^{*l}, we define the following subgroup U_1 of finite index in ϑ_K^* whose closure has a slightly easier description:

$$U_1 = \{u \in \vartheta_K^* | \tau_j(u) \equiv 1 \bmod \pi \text{ for all } j\}.$$

The more general setting of the closure of ϑ_K^* follows then by applying the technique of Lemma 2.1. Let $\overline{U_1}$ denote the closure of U_1 as a subgroup of ϑ_L^{*l}. By taking a basis $e_1, \ldots, e_r$ for the torsion-free rank of U_1 (where r is given by Dirichlet's Unit Theorem) we may write $\overline{U_1} = \prod_{i=1}^r e_i^{\mathbf{Z}_p}$. (Note that our definition of U_1 implies that the p-adic exponential of e_i is defined, where we think of e_i embedded in ϑ_L^{*l}.)

The integrals we wish to consider have the following form

$$I = \int_{\overline{U_1}} \operatorname{ord}_v(F(u_1, \ldots, u_l))d\mu$$

where F is a polynomial with coefficients in $\mathbf{Q}$ and $d\mu$ is the additive Haar measure on the $\mathbf{Z}_p$-module $\overline{U_1} \cong \mathbf{Z}_p^r$. Using this isomorphism we can write this integral as an integral of an exponential polynomial

$$I = \int_{\mathbf{Z}_p^r} \operatorname{ord}_v(F(u_1(\mathbf{x}), \ldots, u_l(\mathbf{x})))d\mu$$

where $u_i(\mathbf{x}) = \tau_i(e_1)^{x_1} \cdots \tau_i(e_r)^{x_r}$. We shall try to linearise such an integral.

The special case where $r = 1$ and K totally real (hence $l = 2$ by Dirichlet's Theorem) reveals three interesting possibilities.

(a) Since $\tau_1(e_1)\tau_2(e_1) = 1$, we may clear any reference to $\tau_2(e_1)$ and assume τ_1 is the identity. Then we have an exponential polynomial in the exponent of e_1 and the methods in [12] can be brought to bear. In particular, expand $F(e_1^x)$ as a convergent power series in x. We can now apply Strassman's Theorem which says that a convergent power series in one variable is the product of a polynomial and a function with order 0 everywhere. See [20] for a very elegant proof of Strassman's Theorem. That is, any convergent power series $F(x)$ has $\mathrm{ord}_v(F(x)/f(x)) = 0$ for all $x \in \mathbf{Z}_p$, where $f(x)$ is a polynomial. We do indeed produce a linear integral. However, it is not at all certain that we produce a K-linear integral, for any K as we cannot guarantee that the coefficients of $f(x)$ will be algebraic.

(b) Alternatively we can factorise $F(e_1^x) = a\Pi_k(e_1^x - \alpha_k)$. Then it is sufficient to suppose $F(e_1^x) = e_1^x - \alpha$, for some algebraic α. We might as well assume $\alpha \equiv 1 \bmod \pi$. Then $\mathrm{ord}_v(e_1^x - \alpha) = \mathrm{ord}_v(e_1^x\alpha^{-1} - 1) = \mathrm{ord}_v(\log(e_1^x\alpha^{-1}))$. Thus the integral collapses to that of $\mathrm{ord}_v(x\log_p(e_1) - \log_p(\alpha))$ which is clearly linear. Equally clearly, this can fail to be K-linear, for any algebraic number field K, since the p-adic version of Baker's Theorem guarantees that $\log_p(e_1)/\log_p(\alpha)$ is transcendental, whenever e_1/α is not a root of unity times a power of p. (See chapter IV of [17] for a statement and another application of the p-adic version of Baker's Theorem.)

(c) An alternative is to try the change of variable $e_1^x = 1 + \pi^m y$. However, since e_1 is not necessarily an element of $\mathbf{Z}_p$, we cannot guarantee that y is in $\mathbf{Z}_p$. Progress comes by making an assumption about the ramification. If p is totally split in K then K embeds in $\mathbf{Q}_p$. The uniformising parameter is defined only up to unit multiple and is an associate of p. Thus, we choose p as this uniformising parameter. We can then make the change of variables $e_1^x = 1 + p^m y$, where m=ord$_v(e_1 - 1)$. This induces a filtration-preserving bijection so counting cosets is the same for either variable, just as in the proof of the theorem. Clearly, this method yields a $\mathbf{Q}$-linear integral.

Methods (a) and (b) offer little hope for generalisation so we turn to method (c). The technical assumptions we make are that $K/\mathbf{Q}$ is totally real and p splits completely in K. By our first assumption, Dirichlet's Unit Theorem relates l and r by the formula $r = l - 1$. Let p^m denote the conductor of U_1, the largest power p^m of p with $\tau_j(u) \equiv 1 \bmod p^m$, for all j. Write $\tau_j(u) = 1 + p^m y_j$, for

all $1 \leq j \leq r$. Let R_p denote the matrix $(\log_p(\tau_j(e_i)))$ for $1 \leq i, j \leq r$ where j ranges over the rows. This is a matrix in $M_r(\mathbf{Z}_p)$ and we suppose without loss of generality that the invariant factors are all equal to p^m. If this were not the case, we could replace U_1 by a subgroup of finite index where this property does hold. Write $u = e_1^{x_1} \dots e_r^{x_r}$ for $x_i \in \mathbf{Z}, 1 \leq i \leq r$. The variables $\underline{x} = (x_1, \dots, x_r)$ and $\underline{y} = (y_1, \dots, y_r)$ are related by the formula

$$R_p \underline{x} = (\log_p(1 + p^m \underline{y})). \tag{3.1}$$

In (3.1), the right hand side denotes the column vector $(\log_p(1 + p^m y_j))_{1 \leq j \leq r}$. Provided the matrix R_p is non-singular, it induces a filtration-preserving bijection between the x and y variables. Thus the integral of $\mathrm{ord}_v(F(u_1(\mathbf{x}), \dots, u_l(\mathbf{x})))$ is the same as that of $\mathrm{ord}_v(F(1+p^m y_1, \dots, 1+p^m y_r, ((1+p^m y_1) \cdots (1+p^m y_r))^{-1}))$ using the fact that $u_1(\mathbf{x}) \dots u_l(\mathbf{x}) = 1$. Clearly we produce a $\mathbf{Q}$-linear integral under the condition of the non-singularity of R_p. This condition is actually the statement of a celebrated conjecture due to Leopoldt (see [17], [18]).

CONJECTURE (Leopoldt): *The matrix R_p is non-singular.*

The determinant of the matrix R_p is now known as Leopoldt's p-adic regulator. Leopoldt's Conjecture has been proved in the case where the Galois closure of $K/\mathbf{Q}$ is either an abelian group or one of a small number of non-abelian groups. The Conjecture can be reformulated as saying that $\overline{U_1}$ has finite index as a subgroup in $\{(u_1, \dots, u_l) \in \vartheta_L^{*l} | u_1 \cdots u_l = 1\}$. With this approach we can formulate Leopodt's conjecture for fields which are not totally real. However as the next paragraph illustrates this does not help us in getting a linear integral. For a good account of the p-adic regulator, together with a proof of Leopoldt's conjecture in the abelian case, consult chapter IV of [17].

If this conjecture fails, write r' for the rank of R_p. Choose r' linearly independent rows in R_p and extend to a non-singular matrix which we can then use to change variables. However we begin to sink rapidly. For example, suppose the conjecture fails for $r = 2$ (it can't in reality). Then $u_2 = u_1^\lambda$ for some $\lambda \in \mathbf{Z}_p$. Now λ is necessarily transcendental, by the p-adic version of Baker's Theorem. Thus y_2 is related to the variable y_1 by the formula $(1 + p^m y_1)^\lambda = 1 + p^m y_2$. With this transformation, we do not even appear to be able to secure linearity. Note that the same problem arises if we are not in the totally real case where we will have to write u_j for $j > r$ as transcendental expressions in the first u_i, $i \geq r$.

(iii) Continuing with the closure of the global units, we now do an explicit example after the manner of that in (i), assuming p is totally split in K. In

this case K embeds in $\mathbf{Q}_p$ and v is the usual p-adic valuation twisted by the embedding. We keep the notation v for the valuation and note that the norm of the prime ideal is p. Let $\rho \in K$, and define $S_\rho(u) = \sum_j \rho_j u_j$, for $u \in U_1$, with the suffix denoting image under τ_j. As before, we consider $S_\rho(u)$ as an exponential polynomial on $\mathbf{Z}_p^r$. We also need to make the additional assumption in this case that l is coprime to p. As in (i), consider ρ to be primitive if it has the property that $\rho_j \equiv 0 \bmod p$ does not hold for every j.

THEOREM 3.1:

(1) *If* $\mathrm{ord}_v(S_\rho(1)) < m$ *then* $m_{\mathbf{Z}_p^r}(S_\rho) = \mathrm{ord}_v(S_\rho)$.

(2) *If* $\mathrm{ord}_v(S_\rho(1)) \geq m$ *then* $m_{\mathbf{Z}_p^r}(S_\rho) = m + 1/(p-1)$ *for all primitive* ρ *if and only if Leopoldt's Conjecture is true.*

This theorem has some geometric appeal. If we think of $S_\rho(u)$ as a measure of the local distance between ρ and u, i.e. a distance which takes account of all the local embeddings above p, then we may interpret part (2) of Theorem 3.1 as saying that the global units ought to lie at a uniform mean distance from any random element. This ties in with the interpretation of Leopoldt's Conjecture that the p-adic closure of the global units has p-adic rank equal to the torsion-free rank of the global unit group. Perhaps this is easier to visualise in the archimedean context. Suppose we consider a discrete additive subgroup $\mathfrak{L}$ of $\mathbf{R}^2$. We are in a non-compact situation so compactify by projecting elements of $\mathfrak{L}$ centrally onto the edge of the unit circle, by dividing each non-zero element by its length. Clearly the distribution of these images will be uniform if the $\mathbf{R}$-rank of the group is 2 whilst being very non-uniform (consisting of two points) if the $\mathbf{R}$-rank is 1.

Proof of Theorem 3.1: (1) is clear. To prove (2), notice that the primitivity condition means we may assume one of $\rho_i \equiv 0 \bmod p$ fails for some i in the range $1 \leq i \leq r$. We write $u_j = \tau_j(u)$ then we may write $u_l = u_{r+1} = 1/u_1 \cdots u_r$. Clear the denominator and write $v_i = u_1 \cdots u_i^2 \cdots u_r$ so the polynomial is $S_\rho(v) = \rho_1 v_1 + \cdots + \rho_r v_r + \rho_{r+1}$. The matrix of the transformation has determinant $l = r+1$ which is a p-adic unit by our assumption on l. As in example (ii), write $v_i = 1 + p^m y_i$. Then the truth of the conjecture enables the integrand to be simplified to that of $\mathrm{ord}_v(S_\rho(1) + p^m(\rho_1 y_1 + \cdots + \rho_r y_r)) = \mathrm{ord}_v(S_\rho(\underline{y}))$. Write $N(t) = \#\{\underline{y} \bmod p^{t+1} \colon \mathrm{ord}_v(S_\rho(\underline{y})) = t\}$. Clearly $N(t) = 0$ for $t < m$. The primitivity condition ensures that $N(t) = (p-1)p^{(t+1-m)(r-1)}$ for $t \geq m$. Thus the integral simplifies to

$$\sum_{t=m}^{\infty} tN(t)/p^{(t+1-m)r}.$$

Inserting the formula for $N(t)$ and summing the resulting geometric progression gives the value $m + 1/(p-1)$.

Conversely, assume the conjecture is false. Now the $v_i, i = 1, \dots, r$ generate $\overline{U_1}$ and we take $g_i, i = 1, \dots, r$ to be a basis, where $g_i = e_1 \cdots e_i^2 \cdots e_r$. We may therefore write $v = g_1^{z_1} \dots g_r^{z_r}$ for $z_1, \dots, z_r \in \mathbf{Z}_p^r$. Writing $g_i^{\tau_j} = g_{ij} = 1 + p^m w_{ij}$, and working modulo p^{m+1}, the expression $S_\rho(v)$ simplifies to

$$S_\rho(v) = \rho_{r+1} + \sum_{j=1}^{r} \rho_j (1 + p^m w_{1j})^{z_1} \cdots (1 + p^m w_{rj})^{z_r}$$

$$\equiv S_\rho(1) + p^m \sum_{i=1}^{r} z_i \sum_{j=1}^{r} \rho_j w_{ij} \bmod p^{m+1}.$$

Viewing the ρ_j and the $w_{ij} \bmod p$, we can find a vector $(\rho_1, \dots, \rho_{r+1})$ which does not reduce to zero modulo p, with $\sum_{j=1}^{r} \rho_j w_{ij} \equiv 0 \bmod p$, for every $i = 1, \dots, r$. This is because the failure of Leopoldt's conjecture guarantees the matrix (w_{ij}) is singular modulo p. Simultaneously, we can guarantee that $S_\rho(1) \equiv 0 \bmod p^m$. Now these congruences for the conjugates of ρ can be lifted to produce an element $\rho \in K$ which is clearly primitive and satisfies $\mathrm{ord}_v(S_\rho(u)) \geq m+1$ for all $u \in \overline{U_1}$. The integral of this function cannot help inheriting the same inequality. ∎

(iv) The proof of Theorem 1.1 involves parametrising the Lie group via the root system. This is not always the only way of parametrising the group. We present another way in the case where G is the general or special linear group with entries coming from a division algebra D over $\mathbf{Q}_p$. These groups are only split if the division algebra is actually commutative, i.e. a field. In §5 we shall want to consider these non-split examples when we make an application to the theory of Galois modules.

By choosing a basis for D as an m-dimensional vector space over $\mathbf{Q}_p$ we can define the regular representation $\rho\colon D \to \mathrm{M}_m(\mathbf{Q}_p)$ of D where $x \in D$ is sent to the matrix corresponding to the $\mathbf{Q}_p$-linear transformation $y \mapsto xy$ of D. (Note that $m = d^2 m_1$ where $[K\colon \mathbf{Q}_p] = m_1$ and $K = Z(D)$ since then D is a central division algebra over K.) Using the representation ρ we can consider the simple algebra $A = \mathrm{M}_n(D)$ as a linear subspace of $\mathrm{M}_{nm}(\mathbf{Q}_p)$. We have a reduced norm $N_{A/\mathbf{Q}_p}\colon A \to \mathbf{Q}_p$ defined on the algebra A which reduces to the determinant map when D is a field. The invertible elements of A are then

$$A^* = \mathrm{GL}_n(D) = \{x \in \mathrm{M}_n(D)\colon N_{A/\mathbf{Q}_p}(x) \neq 0\}. \tag{3.2}$$

Let $\mathbf{M}$ be a maximal order inside D and suppose that H is commensurable with $\mathrm{GL}_n(\mathbf{M})$, the group of units inside the maximal order $\mathrm{M}_n(\mathbf{M})$ of A. The repre-

sentation of A as a subspace of $\mathrm{M}_{nm}(\mathbf{Q}_p)$ gives rise then to a $\mathbf{Q}_p$-rational representation ϕ: $\mathrm{GL}_n(D) \to \mathrm{GL}_{nm}(\mathbf{Q}_p)$. We can define a system of neighbourhoods U_i of the identity for $\mathrm{GL}_n(D)$ via the congruence kernels in $\mathrm{GL}_{nm}(\mathbf{Q}_p)$:

$$U_i = \{g \in \mathrm{GL}_n(D)\colon \phi(g) \in \mathrm{M}_{nm}(\mathbf{Z}_p) \text{ and } \phi(g) \equiv 1_{nm} \bmod p^i\}. \tag{3.3}$$

The group H is then commensurable with such an open subgroup. Suppose that F is a polynomial over K in the entries of the image of H under the representation ϕ. We shall prove that the integral $m_H(F)$ is linear. Note that by the same argument as in Lemma 2.5, we may consider the more general setting of taking a polynomial defined on the entries of H under an arbitrary $\mathbf{Q}_p$-rational representation.

As before, since H contains U_i as a subgroup of finite index for some i, we may suppose that $H = U_i$ by choosing coset representatives and changing the polynomial a finite number of times.

Now $\phi(U_i)$ is equal to $I_{nm} + p^i V$ where V is some $\mathbf{Z}_p$-submodule inside $\mathrm{M}_{nm}(\mathbf{Z}_p)$. We can use V as a way to coordinatize U_i. Choosing a basis for V, we may identify it with $\mathbf{Z}_p^N$ for some N.

Make the change of variable $u \mapsto 1 + p^i v$. We claim that

$$\int_{U_i} \operatorname*{ord}_v(F) d\mu_{U_i} = \int_{\mathbf{Z}_p^N} \operatorname*{ord}_v(F^*) d\mu_{\mathbf{Z}_p^N}. \tag{3.4}$$

This follows because $\mathrm{card}(U_i/U_{i+k}) = \mathrm{card}(p^i V/p^{i+k}V)$ which implies that the Haar measure $d\mu_{U_i}$ is the same as the Haar measure $d\mu_{\mathbf{Z}_p^N}$ induced on U by the change of variable. Thus we have proved:

THEOREM 3.2: *Suppose that D is a division algebra over $\mathbf{Q}_p$ and that $\mathbf{M}$ is a maximal order inside D. If H is commensurable with $\mathrm{GL}_n(\mathbf{M})$ and F is a polynomial over L in the matrix entries of H, then the integral $m_H(F)$ is linear.*

We can refine the example above to allow us to consider the group $\mathrm{SL}_n(D) = \{x \in \mathrm{M}_n(D)\colon N_{A/\mathbf{Q}_p}(x) = 1\}$. Define a system of neighbourhoods of the identity for $\mathrm{SL}_n(D)$:

$$W_i = \{g \in \mathrm{SL}_n(D)\colon \phi(g) \in \mathrm{M}_{nm}(\mathbf{Z}_p) \text{ and } \phi(g) \equiv 1_{nm} \bmod p^i\}. \tag{3.5}$$

Again we can reduce the integral over the subgroup H commensurable with some such neighbourhood to the case where $H = W_i$.

With U_i as in (3.3), define the following map $U_i \to 1 + p^i\mathbf{Z}_p \times W_i$:

$$u \mapsto (N_{A/\mathbf{Q}_p}(u), \mathrm{diag}_{nm}(N_{A/\mathbf{Q}_p}(u)^{-1}, I_m, \ldots, I_m) \cdot u). \tag{3.6}$$

The multiplicativity of the norm map guarantees that

$$\mathrm{diag}_{nm}(N_{A/\mathbf{Q}_p}(u)^{-1}, I_m, \ldots, I_m) \cdot u \in W_i.$$

This map is a bijective map and preserves the filtrations on each group which implies that it is measure preserving.

Let F be a polynomial defined on the entries of W_i. Using the above measure-preserving bijection and the fact that $1 = \int_{1+p^i\mathbf{Z}_p} d\mu_{1+p^i\mathbf{Z}_p}$ we have

$$\begin{aligned} m_{W_i}(F) &= \int_{W_i} \operatorname*{ord}_v(F) d\mu_{W_i} \\ &= \left(\int_{W_i} \operatorname*{ord}_v(F) d\mu_{W_i}\right)\left(\int_{1+p^i\mathbf{Z}_v} d\mu_{1+p^i\mathbf{Z}_p}\right) \\ &= \int_{U_i} \mathrm{ord}(F^*) d\mu_{U_i} \end{aligned} \tag{3.7}$$

where $F^*(u) = F(\mathrm{diag}_{nm}(N_{A/\mathbf{Q}_p}(u)^{-1}, I_m, \ldots, I_m) \cdot u) = F(u^*)$. Evaluating F on u^* introduces denominators but these all specialise to π-adic units so they can be cleared without affecting the value of $\mathrm{ord}_v(F)$. Thus F^* can be thought of as a polynomial in $(nm)^2$ variables and we integrate over U_i. We can therefore apply the above theorem to deduce the same result for $\mathrm{SL}_n(D)$:

THEOREM 3.3: *Suppose that D is a division algebra over $\mathbf{Q}_p$ and that $\mathbf{M}$ is a maximal order inside D. If H is commensurable with $\mathrm{SL}_n(\mathbf{M})$ and F is a polynomial over L in the matrix entries of H, then the integral $m_H(F)$ is linear.*

What about the question of the K-linearity of these integrals? Suppose that the division algebra $D = D_0 \otimes_K \mathbf{Q}_p$ for some division algebra D_0, defined over an algebraic subfield K of $\mathbf{Q}_p$. Then in Theorems 3.2 and 3.3 we can deduce K-linearity for the integral $m_H(F)$. This happens for example in the case where the division algebra D is just the matrix algebra $\mathrm{M}_m(\mathbf{Q}_p)$.

§4. Effective computation of K-linear integrals

It was Weyl who noticed that certain real integrals can be computed by averaging their values over a sequence which is uniformly distributed in the domain of integration. This is usually applied to the case where the function is continuous but functions with logarithmic singularities are also amenable to this method. The p-adic analogue is perfectly valid and we demonstrate this now, in the case of a K-linear integral, obtaining a good bound for the error term.

THEOREM 4.1: *Let $L/\mathbb{Q}_p$ denote a finite extension and suppose $f \in L[x_1, \dots, x_k]$ has coefficients in $L \cap \overline{\mathbb{Q}}$. Then the following effective asymptotic formula holds as $X \to \infty$,*

$$\int_{\mathbb{Z}_p^k} \operatorname*{ord}_v(f) d\mu = (2X)^{-k} \sum_{\substack{\underline{x} \in \mathbb{Z}^k \\ |\underline{x}| \leq X}} \operatorname*{ord}_v(f(\underline{x})) + O(X^{-C}), \tag{4.1}$$

where in (4.1), $0 < C < 1$ is an effective constant.

Look ahead to (4.12), (4.13) and the corollary to this theorem for some commentary on the nature of C. In (4.1), $|\ \ |$ denotes the usual 'max'-norm on Euclidean space. It should be noted that here, and throughout the paper, we ignore the zero values of the argument. This will always constitute a small set in the appropriate sense. In the example above, there can be at most $O(X^{k-1})$ values of $\underline{x} \in \mathbb{Z}^k$ with $|\underline{x}| \leq X$ which cause $f(\underline{x})$ to vanish. These cause no interference with the kind of statement made in Theorem 4.1.

Proof: Let π denote a prime element of O_L. Multiplying by a suitable power of π, we may suppose the coefficients of f are π-integral and that $\operatorname{ord}_v(f)$ is non-negative on $\mathbb{Z}_p^k$. Since the coefficients of $f(\underline{x})$ are algebraic we can take the norm down to $\mathbb{Q}$ and suppose f has coefficients in $\mathbb{Z}$. Thus, consider the values of $\operatorname{ord}_p(f(\underline{x}))$ as $\underline{x}$ runs over $\mathbb{Z}^k$ with $|\underline{x}| \leq X$. As a further reduction step, notice that the application of an element $A^{-1} \in \mathrm{SL}_k(\mathbb{Z})$ to the integrating variable preserves the integral. Alternatively, we could view A itself as acting on f. Let f_A denote the resulting polynomial. We may choose A with the property f_A is monic in x_1 (say) of degree d. Assume A has been chosen thus and drop all reference to it in the sequel. Decompose the sum in (4.1) over the values of f as follows,

$$\sum_{t=0}^{T_X} t \#\{\underline{x} \in \mathbb{Z}^k : |\underline{x}| \leq X, \operatorname*{ord}_p(f(\underline{x})) = t\}. \tag{4.2}$$

In (4.2), T_X denotes the maximum value of $\operatorname{ord}_p(f(\underline{x}))$ allowed by the condition $|\underline{x}| \leq X$. The first step is to prove that the sum in (4.2) converges and we begin along this road by giving a bound for T_X. Clearly $f(\underline{x})$ is bounded in absolute value by $c_1 |\underline{x}|^{c_2}$, where c_1, c_2 are positive constants. The p-part can be no greater than this, so taking logs and using the bound for $|\underline{x}|$ we find the p-adic order of $f(\underline{x})$ is bounded by $c_3 \log X$. This is the bound required for T_X. Given t with $1 \leq t \leq T_X$, define $N(t)$ as follows,

$$N(t) = \#\{\underline{x} \in (\mathbb{Z}/p^{t+1}\mathbb{Z})^k : \operatorname*{ord}_p(f(\underline{x})) = t\}. \tag{4.3}$$

Also define $N(t, X)$ by

$$N(t, X) = \#\{\underline{x} \in \mathbb{Z}^k : |\underline{x}| \leq X, \operatorname{ord}_p(f(\underline{x})) \geq t\}. \tag{4.4}$$

LEMMA 4.2: *With d denoting the degree of f in x_1, we have the bounds:*

$$N(t) = O(p^{t(k-1/d)}), \tag{4.5}$$

$$N(t, X) = O(X^{k-1}(Xp^{-t/d} + 1)). \tag{4.6}$$

Notice that (4.5) follows from (4.6) upon setting $X = p^t$. Thus it suffices to prove (4.6) only. Let $x_2, \ldots, x_k$ take any value in the allowable range. The result is a monic polynomial in the variable x_1 of degree d. Suppose first that $p^t \leq X^d$. The worst that can happen is for a single x_1 to be a good approximation to all of the roots of $f(x_1)$. This fixes approximately $p^{t/d}$ of the first p-adic coefficients of x_1. There remain $O(Xp^{-t/d})$ choices for the tail-end of x_1. Now suppose $p^t > X^d$. For any specialisation, there is only one value of x_1 which yields a solution of the inequality $\operatorname{ord}_p(f(x_1)) \geq t$. If there were two, x_1 and x_1' then their difference would satisfy $\operatorname{ord}_p(x_1 - x_1') \geq t > \log X / \log p$. But this is impossible because they both lie in the range $|x_1, x_1'| \leq X$. Putting the two types of bound together yields the form of (4.6) and completes the proof of the lemma. ∎

To prove Theorem 4.1, decompose the range of summation for the t-variable by defining

$$T_X' = [\log X / \log p], \qquad T_X'' = [d \log X / \log p]. \tag{4.7}$$

Let the corresponding sums be denoted $\sum$, $\sum'$ and $\sum''$. Now deal with them in turn. Given $1 \leq t \leq N(t)$, let $\underline{a}_j, j = 1, \ldots, N(t)$ denote representatives for the cosets mod p^{t+1} in the definition of $N(t)$. We may suppose they are chosen with the property $|\underline{a}_j| \leq p^{t+1}$. Then the first sum is

$$\sum = \sum_{t=1}^{T_X'} t \sum_{j=1}^{N(t)} \#\{\underline{x} \in \mathbf{Z}^k : |\underline{x}p^{t+1} + \underline{a}_j| \leq X\}. \tag{4.8}$$

In the range $1 \leq t \leq T_X'$ we can estimate the inner expression in (4.8) as follows:

$$\begin{aligned} \#\{\underline{x} \in \mathbb{Z}^k : |\underline{x}p^{t+1} + \underline{a}_j| \leq X\} &= \#\{\underline{x} \in \mathbb{Z}^k : |\underline{x}| \leq \frac{X}{p^{t+1}} + O(1)\} \\ &= \left(\frac{2X}{p^{t+1}}\right)^k + O\left(\left(\frac{X}{p^t}\right)^{k-1}\right). \end{aligned} \tag{4.9}$$

The choice of $\underline{a}_j$ guarantees that the error term in (4.9) is uniform. Using the bound for $N(t)$ in (4.5), (4.8) becomes

$$(4.10) \qquad (2X)^k \sum_{t=1}^{T'_X} \frac{tN(t)}{p^{(t+1)k}} + O\left(X^{k-1} \sum_{t=1}^{T'_X} t p^{t(k-1/d)} \right).$$

The error term in (4.10) is $O(T'_X X^{k-1/d}) = O(\log X \cdot X^{k-1/d})$. The main term differs from the full sum,

$$(4.11) \qquad (2X)^k \sum_{t=1}^{\infty} \frac{tN(t)}{p^{(t+1)k}},$$

by an amount which is

$$(4.12) \qquad O\left(X^k \sum_{t=T'_X}^{\infty} t p^{-1/d} \right) = O(\log X \cdot X^{k-1/d}).$$

Clearly the sum in (4.11) converges, later we will identify it with an integral. Thus $\sum$ satisfies the form of (4.1). Now we move on to $\sum'$ and apply (4.6).

(4.13)

$$\sum{}' = O\left(\sum_{t=T'_X}^{T''_X} tN(t,X) \right) = O\left(T''_X \cdot X^k \sum_{t=T'_X}^{T''_X} p^{-t/d} \right) = O(\log X \cdot X^{k-1/d}).$$

Thus (4.13) shows the second sum to be lying within the error term. Finally, consider $\sum''$ and apply (4.6) once again. Having fixed $x_2, \ldots, x_k$, (4.6) guarantees at most finitely many contributions to the sum in x_1. This number is uniformly bounded independently of the specialisation. For each contribution, we take the most pessimistic view for t of T_X and deduce

$$(4.14) \qquad \sum{}'' = O(T_X \cdot X^{k-1}) = O(\log X \cdot X^{k-1}).$$

Thus (4.14) shows $\sum''$ to be lying considerably well within the error term. Putting these formulae together shows that the sum in (4.1) converges to the expression in (4.11) with an error term equal to $O(\log X \cdot X^{k-1/d})$.

Finally, we need to make some statement recognising (4.11) as the integral in (4.1). The definition of the integral is

$$(4.15) \qquad \lim_{N \to \infty} p^{-Nk} \sum_{\substack{x_i = 1 \\ i = 1, \ldots, k}}^{p^N} \operatorname{ord}_p(f(\underline{x})).$$

This is clearly equal to

$$\lim_{N\to\infty}(2p^N)^{-k}\sum_{\substack{|\underline{x}|\le p^N\\ \underline{x}\in\mathbb{Z}^k}}\operatorname{ord}_p(f(\underline{x})). \tag{4.16}$$

Replacing X by p^N, we deduce that if the expression on the right in (4.1) converges then it must converge to the integral. This completes the proof of Theorem 4.1. ∎

COROLLARY 4.3: *If f is linear and monic in one variable then the error term in (4.1) is $O(\log X/X)$.*

This gives a class of examples where the error term is about as good as it could be. The polynomials arising from the estimation of the mean valuation of the normal integral bases in certain extensions (see §5) belong to this class.

Note: The formulae obtained so far are completely uniform in all except one respect. The only point at which the coefficients of the polynomial play any role is the bound for T_X.

§5. Applications to Galois module theory

Let $K/\mathbb{Q}$ denote a finite Galois extension and let Γ denote the Galois group. The Hilbert Normal Basis Theorem asserts that an element $a \in K$ may be found with the property that its conjugates under Γ form a $\mathbb{Q}$-basis for K. It is known that for most tame extensions, the corresponding statement holds at the integral level. Let ϑ_K denote the ring of algebraic integers in K. In [23], Taylor shows that the only potential obstruction to the existence of an integral version of this statement is the presence of symplectic characters for Γ.

It will suit our purposes to think in terms of the actions of the various group algebras. Let $\mathbb{Q}\Gamma$ denote the rational group algebra, acting linearly on K. Then Hilbert's Theorem is the formula,

$$K = a.\mathbb{Q}\Gamma, \qquad \text{for some } a \in K. \tag{5.1}$$

At the integral level, we are interested in the action of $\mathbb{Z}\Gamma$ upon ϑ_K and a is said to generate a **normal integral basis** if the following formula is true,

$$\vartheta_K = a.\mathbb{Z}\Gamma. \tag{5.2}$$

In this notation, we obtain a very neat expression for the set of all the normal integral generators for the extension $K/\mathbb{Q}$. It is precisely the orbit

$$a.\mathbb{Z}\Gamma^*, \tag{5.3}$$

where in (5.3), the * indicates the group of units of the group ring $\mathbb{Z}\Gamma$.

In [3], Bushnell introduced the idea of taking the integral average of the norms of normal integral bases in the archimedean case. We now try to apply our definitions in the non-archimedean analogue. Let v extend the p-adic valuation on $\mathbb{Q}$, where p is a prime number and write $\overline{\mathbb{Z}\Gamma^*}$ for the p-adic closure of the group of units of the integral group ring, with respect to the p-adic topology on $\mathbb{Z}\Gamma$. Let F denote any polynomial in $K[x_\gamma]_{\gamma\in\Gamma}$, where $x = \sum_{\gamma\in\Gamma} x_\gamma\gamma \in \overline{\mathbb{Z}\Gamma^*}$. The object of our interest is $m_{\overline{\mathbb{Z}\Gamma^*}}(F)$.

Example: Let a generate a normal integral basis for $K/\mathbb{Q}$ and take $f(g) = a.g$, with $g \in \overline{\mathbb{Z}\Gamma^*}$. Then the measure $m_{\overline{\mathbb{Z}\Gamma^*}}(f)$ represents the average v-adic order of the set of normal integral bases for the extension $K/\mathbb{Q}$. It follows from Proposition A that this quantity is a rational number and there is some interest in being able to calculate its value. We have some mixed success trying to apply our definitions in this case; in fact we see illustrated many of the points raised in §3. Recall that the group algebra $\mathbb{Q}\Gamma$ has a Wedderburn decomposition according to the irreducible representations of Γ. (It may help to have a copy of [4] to hand.) Write

$$\mathbb{Q}\Gamma \simeq \Pi_i A_i(\mathbb{Q}). \tag{5.4}$$

In (5.4), the factor $A_i(\mathbb{Q})$ represents a simple $\mathbb{Q}$- algebra. Let $\mathfrak{M}$ denote the maximal order of $\mathbb{Q}\Gamma$ containing $\mathbb{Z}\Gamma$. There is a corresponding decomposition of maximal orders $\mathfrak{M}_i$ in A_i,

$$\mathfrak{M} \simeq \Pi_i \mathfrak{M}_i. \tag{5.5}$$

This decompositon even respects units,

$$\mathfrak{M}^* \simeq \Pi_i \mathfrak{M}_i^*.$$

It is known that $\mathbb{Z}\Gamma^*$ is contained with finite index inside $\mathfrak{M}^*$. This statement is then true upon closure with respect to the p-adic valuation.

For example, let Γ denote the cyclic group of order q, where q denotes an odd prime. The group algebra decomposes in the following way,

$$\mathbb{Q}\Gamma \simeq \mathbb{Q} \times \mathbb{Q}(\zeta_q). \tag{5.6}$$

In (5.6), $\mathbb{Q}(\zeta_q)$ denotes the cyclotomic field obtained by adjoining a primitive qth root of unity, ζ_q to $\mathbb{Q}$. It is sufficient to work with units inside the maximal real

subfield of $\mathbb{Q}(\zeta_q)$. Leopoldt's Conjecture is known to be true for this field. If $p \equiv 1 \bmod q$ then p is totally split in this field. Thus, the methods in §3(ii)(c) apply to produce a $\mathbb{Q}$-linearity statement for $m_{\overline{\mathbb{Z}\Gamma^*}}(f)$. However, in the general abelian case we encounter the potential difficulties of §3(ii)(b). This happens whenever one of the factors $A_i(\mathbb{Q})$ is a number field in which p does not split totally. For example, this happens when Γ is the cyclic group of order p. It might yet be possible to overcome this difficulty and obtain a result for general abelian groups. At least we have the reasurrance of knowing Leopoldt's Conjecture is true for the maximal real subfields of each of the $A_i(\mathbb{Q})$ since they are all abelian extensions.

The second example is much more heartening. With q as above, let $\Gamma = D_{2q}$, the dihedral group of order $2q$. (This is a group for which the inverse Galois problem is known to be true.) The group algebra $\mathbb{Q}\Gamma$ decomposes in the following way,

$$\mathbb{Q}\Gamma \simeq \mathbb{Q} \times \mathbb{Q} \times M_2(E). \tag{5.7}$$

In (5.7), $E = \mathbb{Q}(\zeta_q)^+$ denotes the maximal real subfield of the cyclotomic field. Suppose that $p \equiv 1 \bmod q$. Taking the closure, we find ourselves working with a polynomial on $(q-1)/2$ copies of $\mathrm{SL}_2(\mathbb{Z}_p)$. A K-linearity statement follows from Theorem 1.1 or example 3(iv). At the other extreme, suppose q is coprime with $p-1$. Then we are working with a polynomial on a single copy of $\mathrm{SL}_2(O_E)$ and we need to integrate over the p-adic closure. Again Theorem 1.1 or Example 3(iv) implies K-linearity.

Thus, for the moment, all we can say is that if p splits totally inside E, the smallest field over which the characters of Γ are defined then we may deduce K-linearity.

We have more unqualified success in the local case. Complete K to an extension $L/\mathbb{Q}_p$ which is tame and Galois with Galois group Δ. Emmy Noether showed that a local normal integral basis always exists, which statement we write as

$$\vartheta_L = a.\mathbb{Z}_p\Delta. \tag{5.8}$$

The set of all such is the orbit of the compact group $\mathbb{Z}_p\Delta^*$ given by

$$a.\mathbb{Z}_p\Delta^*. \tag{5.9}$$

Suppose F is a polynomial on $\mathbb{Z}_p\Delta^*$ with coefficients in K. This means that F is an element of $K[x_\delta]_{\delta\in\Delta}$, where $x = \sum_{\delta\in\Delta} x_\delta\delta \in \mathbf{Z}_p\Delta^*$. Let v denote the valuation on L extending that on $\mathbb{Q}_p$. Consider the measure $m_{\mathbb{Z}_p\Delta^*}(F)$. Again Proposition A implies that this measure is a rational number.

THEOREM 5.1:

(1) *The integral defining the Mahler measure $m_{\mathbb{Z}_p\Delta^*}(F)$ is linear.*

(2) *If the Eichler condition is satisfied then the Mahler measure $m_{\mathbb{Z}_p\Delta^*}(F)$ is K-linear.*

Example: Suppose a generates a local normal integral basis and we take $f(h) = a.h$. The integral defining $m_{\mathbb{Z}_p\Delta^*}(f)$ gives the average v-adic order of all the local normal integral bases. Once again, the result of Denef and van den Dries applies to show the rationality of this measure. Perhaps it is worth pointing out that in the abelian case, the corresponding polynomials in Theorem 4.1 are all linear. Thus the corollary to that theorem guarantees that the error terms for the Riemann sums are as good as they could be. Suppose we take $\Delta = D_{2q}$ and $p \equiv 1 \bmod q$ as above. Then we find ourselves working with a polynomial on two copies of $\mathbb{Z}_p^*$ and $(q-1)/2$ copies of $\mathrm{GL}(2, \mathbb{Z}_p)$. If q is coprime with $p-1$ then we are working with two copies of $\mathbb{Z}_p^*$ and one copy of $\mathrm{GL}_2(\vartheta_L)$, where $L = \mathbb{Q}_p(\zeta_q)$.

Proof of Theorem 5.1: There is a decomposition

$$\mathbb{Q}_p\Delta \simeq \Pi_j B_j \tag{5.10}$$

of $\mathbb{Q}_p\Delta$ into a product of simple $\mathbb{Q}_p$- algebras. Let $\mathfrak{M}_p$ denote the maximal order of $\mathbb{Q}_p\Delta$. There is a corresponding decomposition which we label as follows:

$$\mathfrak{M}_p \simeq \Pi_j \mathfrak{M}_{p,j}. \tag{5.11}$$

At the level of maximal orders, the isomorphism in (5.11) preserves units

$$\mathfrak{M}_p^* \simeq \Pi_j \mathfrak{M}_{p,j}^*. \tag{5.12}$$

It always happens that $\mathbb{Z}_p\Delta^*$ is contained with finite index inside $\mathfrak{M}_p^*$. Equality holds except for at most a finite number of primes p.

Thus we see that the group $\mathbb{Z}_p\Delta^*$ is contained with finite index inside a product of groups of invertible elements of the rings of integral elements of simple, finite-dimensional $\mathbb{Q}_p$-algebras. What does a simple, finite-dimensional $\mathbb{Q}_p$-algebra look like? It is a full matrix algebra over a division algebra $M_n(D), D/\mathbb{Q}_p$. (Note, n could be 1 and D could be a field.) Integrals over a product of groups of invertible elements of algebras of this kind are considered in 3, example (iv). We can deduce from that example the linearity of the integral. This proves (i). If the Eichler condition is satified then the division algebra D is in fact a matrix algebra. By the comment following Theorem 3.3 this implies that the integral is K-linear. ∎

References

[1] A. Borel and J. Tits, *Groupes réductifs*, Publications Mathématiques de l'Institut des Hautes Études Scientifiques **27** (1965), 55–151.

[2] D. Boyd, *Speculations concerning the range of Mahler's measure*, Canadian Mathematical Bulletin **24** (1980), 453–469.

[3] C. Bushnell, *Norm distribution in Galois orbits*, Journal für die reine und angewandte Mathematik **310** (1979), 81–99.

[4] C. Curtis and I. Riener, *Representation Theory of Finite Groups and Associative Algebras*, Wiley, New York, 1962.

[5] J. Denef and L. van den Dries, *p-adic and real subanalytic sets*, Annals of Mathematics **128** (1988), 79–138.

[6] J. Denef and D. Meuser, *A functional equation of Igusa's local zeta function*, American Journal of Mathematics **113** (1991), 1135–1152.

[7] J. Dixon, M. du Sautoy, A. Mann and D. Segal, *Analytic pro-p Groups*, London Mathematical Society Lecture Notes # 157, Cambridge University Press, 1991.

[8] M. P. F. du Sautoy, *Finitely generated groups, p-adic analytic groups and Poincaré series*, Annals of Mathematics **137** (1993), 639–670.

[9] M. P. F. du Sautoy, *Zeta functions of groups and Lie algebras: uniformity*, Israel Journal of Mathematics **86** (1994), 1–23.

[10] M. P. F. du Sautoy, *Counting congruence subgroups in arithmetic groups*, The Bulletin of the London Mathematical Society **26** (1994), 255–262.

[11] M. P. F. du Sautoy and A. Lubotzky, *Functional equations and uniformity for local zeta functions of nilpotent groups*, American Journal of Mathematics **118** (1996), 39–90.

[12] G. R. Everest, *On the p-adic integral of an exponential polynomial*, The Bulletin of the London Mathematical Society **27** (1995), 334–340.

[13] G. R. Everest, *The mean value of a sum of S-units*, Journal of the London Mathematical Society (2) **51** (1995), 417–428.

[14] G. R. Everest and Bríd ní Fhlathúin, *The elliptic Mahler measure*, Mathematical Proceedings of the Cambridge Philosophical Society **120** (1996), 13–25.

[15] G. Faltings, *Diophantine approximation on abelian varieties*, Annals of Mathematics **133** (1991), 549–576.

[16] F. J. Grunewald, D. Segal and G. C. Smith, *Subgroups of finite index in nilpotent groups*, Inventiones Mathematicae **93** (1988), 185–223.

[17] N. Koblitz, *p-adic Analysis: A Short Course on Recent Work*, London Mathematical Society Lecture Notes # 46, Cornell Univ. Press, Ithaca, NY, 1980.

[18] H.-W. Leopoldt, *Eine p-adische Theorie der Zetawerte II*, Journal für die reine und angewandte Mathematik **274/75** (1975), 224–239.

[19] M. Matsumoto, *Sur les sous-groupes arithmetiques des groupes semisimple déployés*, Annales Scientifiques de l'Écolee Normale Supérieure **2** (1969), 1–62.

[20] A. J. van der Poorten, *Zeroes of p-adic exponential polynomials*, Indagationes Mathematicae **38** (1976), 46–49.

[21] W. M. Schmidt, *Diophantine Approximations and Diophantine Equations*, Lecture Notes in Mathematics #1467, Springer, Berlin, 1991.

[22] R. Steinberg, *Lectures on Chevalley Groups*, Yale University, 1967.

[23] M. J. Taylor, *On Fröhlich's conjecture for rings of integers of tame extensions*, Inventiones Mathematicae **63** (1981), 41–79.

[24] B. A. F. Wehrfritz, *Infinte Linear Groups*, Springer, Berlin, Heidelberg, New York, 1973.

[25] T. Weigel, *On the profinite completion of arithmetic groups of split type*, to appear.