J. Austral. Math. Soc. (*Series A*) **62** (1997), 198–216

DUALITY ON TORI AND MULTIPLICATIVE DEPENDENCE RELATIONS

DANIEL BERTRAND

(Received 22 March 1996; revised 5 June 1996)

Communicated by W. W. L. Chen

Abstract

In this paper, we give multihomogeneous estimates for the group of relations linking multiplicatively dependent algebraic numbers. In the process, we raise a question in the style of Lehmer's problem, concerning multidimensional covolumes in the lattice of units. The proofs are based on the Brill-Gordan duality theorem on orthogonal lattices, and the paper closes with an algebraic version of this theorem, concerning orthogonal abelian subvarieties of an arbitrarily polarized abelian variety.

1991 *Mathematics subject classification* (*Amer. Math. Soc.*): primary 11H41; secondary 11S10, 14K05.
Keywords and phrases: geometry of numbers, regulators, abelian varieties.

The aim of this article is two-fold. On the one hand, we describe a new approach to the problem of controlling the set of relations between multiplicatively dependent elements in a number field. On the other hand, we establish a formula for the degrees of orthogonal abelian subvarieties in a given polarized abelian variety. The linking thread is provided by the classical theory of duality for lattices in the euclidean space $\mathbb{R}^n$, according to which a pair of rational orthogonal subspaces of complementary dimensions cut $\mathbb{Z}^n$ along two sublattices of equal covolume.

For the convenience of the reader, we have recalled in the first section of the paper a proof of this well-known result (cf. [8] for some historical comments, tracing it back to Brill-Gordan, and [17] for an adelic translation). With an eye to non-principal polarizations in Section 3, and also because such a generalization provides a proof of the (equally classical) multihomogeneous version on which Section 2 is based, we do not assume in this discussion unimodularity of the ambient lattice.

The second section deals with multiplicative dependence relations. Our method is inspired by [1] (where we computed the covolume of the set of relations in terms of

https://doi.org/10.1017/S1446788700000768 Published online by Cambridge University Press

the degree of an algebraic subgroup of a split torus ($(G_m)^n$), but no algebraic geometry is needed in the present description. The result itself is close to those obtained by Matveev in [12], generalizing the multihomogeneous bound of Loxton and van der Poorten [10] (see also Chen [4]). However, we elaborate on these works firstly by taking into account the multihomogeneous character of the relation group itself (actually, this simplifies the proof), and secondly by analysing in more detail the dependence of the results in the number field under study. In the process, we come across a natural question on minima of covolumes in the lattice of units, which may be viewed as an extrapolation between the still open problem of Lehmer on minimal heights, and known lower bounds for regulators.

In our last section, we state and prove the 'exact formula' alluded to in [11] for orthogonal subvarieties in a polarized abelian variety. Over $\mathbb{C}$, this boils down to the study of dual subtori in $(\mathbb{R}/\mathbb{Z})^{2n}$, and it is not surprising that such results as in Section 1 should apply. However, we have here preferred to use a more algebraico-geometric approach. The resulting proof is not fundamentally different, but has the advantage of working in any characteristic. Here again, we also deduce from our result its multihomogeneous version.

The author thanks the Number Theory Research Centre of Macquarie University, where this paper was initiated.

1. Orthogonal lattices

(a) Notation We begin by recalling standard notation and results on lattices (as a general reference, see [3]). If M is a lattice, that is, a discrete $\mathbb{Z}$-module of maximal rank in an $\mathbb{R}$-vector space W of finite dimension, say r, and if $b(x, y)$ is a non-degenerate symmetric or antisymmetric bilinear form on W, we denote by $\mathrm{Vol}(M) = \mathrm{Vol}_b\, M$ the absolute value of the discriminant of b with respect to M. In terms of a basis $(m_1, \ldots, m_r)$ of M over $\mathbb{Z}$, $\mathrm{Vol}(M)$ is given by the square root of the absolute value of the determinant of the matrix

$$B(M) := (b(m_i, m_j);\ 1 \le i,\ j \le r).$$

(When b is a scalar product on W, $\mathrm{Vol}(M)$ is the volume of the torus W/M for the metric induced by b, or equivalently, the r-dimensional volume of a fundamental domain for M in W, hence our notation.)

To M and b as above, we associate the set

$$M^* := \{x \in W,\ b(x, m) \in \mathbb{Z} \text{ for all } m\text{'s in } M\},$$

which is again a discrete $\mathbb{Z}$-module of rank r in W, called the lattice dual to M (with respect to b). One easily checks that in terms of the basis $(m_1, \ldots, m_r)$ of W over $\mathbb{R}$,

https://doi.org/10.1017/S1446788700000768 Published online by Cambridge University Press

a basis of M^* over $\mathbb{Z}$ is given by the columns of the transpose of the matrix $B(M)^{-1}$, so that $\mathrm{Vol}(M^*)^2 = \det(B(M))^{-1}$, and

$$\mathrm{Vol}(M)\,\mathrm{Vol}(M^*) = 1.$$

Since $(M^*)^*$ contains M, we deduce from this formula that any lattice coincides with its bidual.

If N is a lattice containing M, its dual N^* lies in M^*, and the map

$$\mathbf{e}(b) : M^* \times N \to \mathbb{C}^*,$$

sending an element (m^*, n) of $M^* \times N$ to the root of unity $\exp(2i\pi b(m^*, n))$, induces an exact pairing between M^*/N^* and N/M. In other words, these groups are in Pontryagin duality. That their orders $[N : M] = [M^* : N^*]$ coincide can also be deduced from the index formula

$$\mathrm{Vol}(M)/\,\mathrm{Vol}(N) = [N : M].$$

We finally note that M^* contains M if and only if b assumes integral values on M (by which we henceforth mean : on $M \times M$). Then, M^*/M is self-dual, and its order

$$[M^* : M] = \mathrm{Vol}(M)/\,\mathrm{Vol}(M^*) = \mathrm{Vol}(M)^2.$$

(b) The duality formula Let now L be a lattice in a $\mathbb{R}$-vector space V of finite dimension, endowed with a non-degenerate symmetric or antisymmetric bilinear form b. A subgroup M of L can be viewed as a lattice in the $\mathbb{R}$-vector space W it generates in V. Recall that W is *regular* (for b) if the restriction $b_{|W}$ of b to $W \times W$ is again non-degenerate, that is, if V is the direct sum of W and the orthogonal subspace $W^\perp = \{x \in V,\ b(x, W) = 0\}$ (for instance, all W's are regular if b is a scalar product). We may then consider the lattice M^* of W, dual to M with respect to $b_{|W}$; it contains the intersection with W of the lattice L^* of V, dual to L with respect to b. Suppose furthermore that M is a direct factor in L (this holds if and only if M coincides with the intersection of L with W, in which case we say that M is a *primitive* subgroup of L), and that b assumes integral values on L; then $M = W \cap L$ is contained in $W \cap L^*$. Under these hypotheses, our general formula can be stated as follows.

PROPOSITION 1. *Let b be a non-degenerate symmetric or antisymmetric bilinear form on a finite-dimensional real vector space V, assuming integral values on a lattice L in V. Let further M be a primitive subgroup of L, cut out by a regular $\mathbb{R}$-subspace W of V, and let $M^\perp$ be the primitive subgroup of L cut out by the orthogonal complement $W^\perp$ of W in V. Then:*

https://doi.org/10.1017/S1446788700000768 Published online by Cambridge University Press

(i) *the lattices $M \hookrightarrow W \cap L^* \hookrightarrow M^*$ of W, the lattices $M^\perp \hookrightarrow W^\perp \cap L \hookrightarrow (M^\perp)^*$ of $W^\perp$ and the lattices $M \oplus M^\perp \hookrightarrow L \hookrightarrow L^*$ of V are related by the index relations*

$$[L^* : M \oplus M^\perp] = [(M^\perp)^* : (M^\perp)].[W \cap L^* : M] = [M^* : M].[W^\perp \cap L^* : M^\perp];$$

in particular: $\mathrm{Vol}(M)/[W \cap L^* : M]^{1/2} = \mathrm{Vol}(M^\perp)/[W^\perp \cap L^* : M^\perp]^{1/2}$;

(ii) *furthermore, we have* $[L^* : L] = [W \cap L^* : M].[W^\perp \cap L^* : M^\perp]$, *so that*

$$\mathrm{Vol}(M^\perp) = \mathrm{Vol}(M)\,\mathrm{Vol}(L)/[W \cap L^* : M].$$

[When L is unimodular, that is, when $\mathrm{Vol}(L) = 1$, L^* coincides with L and the whole lemma reduces to the classical equality : $\mathrm{Vol}(M) = \mathrm{Vol}(M^\perp)$.]

PROOF. (i) Since $b(M \oplus M^\perp, (M^\perp)^*)$ and $b(L^*, M^\perp)$ lie in $\mathbb{Z}$, the bilinear map:

$$\mathbf{e}(b) : (L^*/M \oplus M^\perp) \times ((M^\perp)^*/M^\perp) \to \mathbb{C}^*$$

sending a pair (x, y) to $\exp(2i\pi b(x, y))$ is well defined. Its right kernel consists of classes of elements in $W \cap L^{**} = M^\perp$, and is thus trivial. To compute its left kernel, let p be the orthogonal projection from V to $W^\perp$. Since $b(x, y) = b(p(x), y)$ for all (x, y) in $V \times W^\perp$, that kernel consists of all classes of elements in $p^{-1}((M^\perp)^{**}) = p^{-1}(M^\perp)$, and is thus equal to $((W \oplus M^\perp) \cap L^*)/M \oplus M^\perp$. But this group is isomorphic to $(W \cap L^*)/M$, while $(M^\perp)^*/M^\perp$ is self-dual. The above pairing therefore yields an isomorphism:

$$(L^*/M \oplus M^\perp)/((W \cap L^*)/M) \approx (M^\perp)^*/M^\perp.$$

(An alternative way to prove this isomorphism consists in showing that $p(L^*)$ coincides with $(W^\perp \cap L)^* = (M^\perp)^*$.) In particular :

$$[L^* : M \oplus M^\perp] = [(M^\perp)^* : (M^\perp)].[W \cap L^* : M].$$

Now, (W, M) and $(W^\perp, M^\perp)$ play symmetric roles, because M is primitive. In particular, $(M^\perp)^\perp := L \cap (W^\perp)^\perp = L \cap W = M$. Our first formula is therefore established. Its corollary then follows from our introductory remarks.

(ii) Since $b(L, W^\perp \cap L)$ and $b(L^*, M^\perp)$ lie in $\mathbb{Z}$, the bilinear map:

$$\mathbf{e}(b) : (L^*/L) \times ((W^\perp \cap L^*)/M^\perp) \to \mathbb{C}$$

sending a pair (x, y) to $\exp(2i\pi b(x, y))$ is well defined. Its right kernel consists of classes of elements in $W^\perp \cap L^{**} = M^\perp$, and is thus trivial. Its left kernel is represented by the inverse image under the projection p of $(W^\perp \cap L^*)^*$. Let us check that this latter group coincides with $p(L)$: it obviously contains $p(L)$; conversely, if an element w

of $W^\perp$ satisfies $b(w, p(x)) \in \mathbb{Z}$ for all x's in L, then $b(w, L)$ lies in $\mathbb{Z}$ and w belongs to L^*; therefore, $p(L)^*$ is contained in $W^\perp \cap L^*$; thus, by biduality, $(W^\perp \cap L^*)^*$ lies in, and so is equal to, $p(L)$.

The left kernel of our pairing may now be written as $(L^* \cap p^{-1}(p(L))))/L = (L^* \cap (L \oplus W))/L$, and is thus isomorphic to $(L^* \cap W)/(L \cap W) = (L^* \cap W)/M$. From the induced exact pairing

$$((L^*/L)/(W \cap L^*/M)) \times (W^\perp \cap L^*)/M^\perp \to C^*$$

we get:

$$[L^* : L] = [W \cap L^* : M].[W^\perp \cap L^* : M^\perp],$$

and this concludes the proof of Lemma 1.

REMARK 1. Although its source and target have the same order, it is not true in general that the natural map from $(W \cap L^*/M) \times (W^\perp \cap L^*/M^\perp)$ to L^*/L induced by addition in L^* is an isomorphism. For a counterexample, consider $L = \mathbb{Z}.(2, 0) \oplus \mathbb{Z}.(0, 1)$ in $V = \mathbb{R}^2$, with its standard scalar product, and $M = \mathbb{Z}.(2, 2)$.

(c) Complementary minors Suppose now that (V, b) is $\mathbb{R}^n$, endowed with its standard scalar product, and that L is the unimodular lattice $\mathbb{Z}^n$. For any subset J of the set $\{1, \dots, n\}$, of cardinality, say, r, denote by p_J the orthogonal projection of $\mathbb{R}^n$ to its r-dimensional face $\mathbb{R}^J$. Given a subgroup M of L of rank r, we set :

$$\mathrm{Vol}_J(M) = \mathrm{Vol}(p_J(M)) = \text{covolume of } p_J(M) \text{ in } \mathbb{R}^J \text{ if } p_J(M) \text{ has rank } r,$$
$$\mathrm{Vol}_J(M) = 0 \text{ if } rk(p_J(M)) < r.$$

Thus, $\mathrm{Vol}_J(M))$ is in both cases the absolute value of the $Jx\{1, \dots, r\}$-minor of any $(n \times r)$-matrix expressing a base of M over $\mathbb{Z}$ in the canonical basis of $\mathbb{R}^n$. By Pythagoras' theorem (also known as Cauchy-Binet in this case), the square of the volume of an r-dimensional parallelotope in $\mathbb{R}^n$ is the sum of the squares of the r-dimensional volumes of its projections to the different r-faces of $\mathbb{R}^n$, that is,

$$(\mathrm{Vol}(M))^2 = \sum_J (\mathrm{Vol}_J(M))^2,$$

where J runs through the $\binom{r}{n}$ subsets of cardinality r in $\{1, \dots, n\}$. Thus, at least in this setting, the following classical 'corollary' (see, for example, [2, Lemme 2.iii]) would immediately have implied Proposition 1. But, in preparation for its geometric analogue in Section 3, we shall now deduce it from Proposition 1, rewritten in the shape :

$$\mathrm{Vol}(M) = \mathrm{Vol}(W^\perp \cap L^*)).\,\mathrm{Vol}(L)$$

(reverse the roles of M and $M^\perp$ in Proposition 1(ii), and use the index formula).

https://doi.org/10.1017/S1446788700000768 Published online by Cambridge University Press

COROLLARY. *Let M be a primitive subgroup of rank r of $\mathbb{Z}^n$, let $M^\perp$ be its orthogonal complement with respect to the standard scalar product on $\mathbb{R}^n$, and let $J \cup J'$ be a partition of $\{1, \dots, n\}$ in two subsets of cardinality r, $n - r$. Then*

$$\mathrm{Vol}_J(M) = \mathrm{Vol}_{J'}(M^\perp).$$

PROOF. To any n-tuple of variable positive integers $z = \{z_1, \dots, z_n\}$, we associate the self-adjoint automorphism $\xi_z = \mathrm{diag}(z_1, \dots, z_n)$ of $\mathbb{R}^n$, and the twist b_z of the standard scalar product b given by :

$$b_z(x, y) = b(\xi_z(x), y) = \sum_{i=1,\dots,n} z_i x_i y_i.$$

We shall denote by Vol_z covolumes with respect to b_z (and to its restrictions to the faces of $\mathbb{R}^n$), by W the $\mathbb{R}$-subspace generated by M, by L^z the lattice dual to $L = \mathbb{Z}^n$ with respect to b_z and by W^z the orthogonal complement of W with respect to the scalar product b_z. Applying Proposition 1(ii) in the above shape to b_z, we obtain:

$$\mathrm{Vol}_z(M) = \mathrm{Vol}_z(W^z \cap L^z). \mathrm{Vol}_z(L).$$

Now, the (standard) orthogonal complement $W^\perp$ of W is the image under ξ_z of W^z; similarly, L^z is mapped by ξ_z onto the lattice L^* dual to L with respect to b, which coincides with L (unimodularity of $\mathbb{Z}^n$). Therefore, $\xi_z(W^z \cap L^z) = W^\perp \cap L = M^\perp$. Since the p_J's are still orthogonal projections with respect to b_z, Pythagoras' theorem reads :

$$(\mathrm{Vol}_z(M))^2 = \sum_J (\mathrm{Vol}_{z,J}(M))^2 = \sum_J (\mathrm{Vol}_J(M))^2 z^J,$$

where $z^J = \prod_{i \in J} z_i$, and

$$(\mathrm{Vol}_z(W^z \cap L^z))^2 = (\mathrm{Vol}_z((\xi_z)^{-1}(M^\perp)))^2 = \sum_{J'} (\mathrm{Vol}_{z,J'}((\xi_z)^{-1}(M^\perp)))^2,$$

where J' runs through the subsets of $\{1, \dots, n\}$ of cardinality $n - r = rk(M^\perp)$. But $(\mathrm{Vol}_{J'}(M^\perp))^2 = (\mathrm{Vol}_{z,J'}(M^\perp))^2 (z^{J'})^{-1} = (\mathrm{Vol}_{z,J'}((\xi_z)^{-1}(M^\perp)))^2 z^{J'}$, and $\mathrm{Vol}_z(L))^2 = \mathrm{Vol}(L)^2 z_1 \cdots z_n = z^J z^{J'}$. Gathering these different equalities, we get:

$$\sum_J (\mathrm{Vol}_J(M))^2 z^J = \sum_{J'} (\mathrm{Vol}_{J'}(M^\perp))^2 z^J.$$

Since this formula holds for any choice of positive integer z, we may view it as an equality of polynomials in n variables, each of whose coefficients must therefore coincide.

https://doi.org/10.1017/S1446788700000768 Published online by Cambridge University Press

2. Multiplicative dependence relations

Let n and d be two positive integers. In this section, we consider a number field k of degree d over $\mathbb{Q}$, and for any n-tuple $\boldsymbol{\alpha}$ of non-zero elements $(\alpha_1, \dots, \alpha_n)$ in k, we study the covolume of the subgroup

$$M = M(\boldsymbol{\alpha}) := \{(b_1, \dots, b_n) \in \mathbb{Z}^n, \alpha_1^{b_1} \dots \alpha_n^{b_n} = 1\}$$

of the lattice $L = Z^n$ in the euclidean space $\mathbb{R}^n$. We refer to [4] and [12] for a historical survey on this 'relation group'. In view of Proposition 1, we may equivalently study its orthogonal complement $M^{\perp}$ in $\mathbb{Z}^n$, which, for reasons which will soon appear, could be called the parametrizing group. In a nutshell : we estimate Plücker coordinates instead of equations.

(a) Notation We express our result in terms of relative (rather than absolute) logarithmic heights, defined, for an element α in k^*, by

$$h_k(\alpha) = \Sigma_v d_v \max(0, \operatorname{Log}|\alpha_v|),$$

where v runs through the different places of k, and d_v, $|\ |_v$ are the local degree of k at v and the v-adic absolute value on k, normalized by $|p|_v = p^{-1}$ if v lies above a prime number p, and $|2|_v = 2$ if v is archimedean. (Thus, $h_{\mathbb{Q}(\alpha)}(\alpha) = h_k(\alpha)/[k : \mathbb{Q}(\alpha)]$ is the logarithm of the Mahler measure of α.) The cardinality of the set Σ of archimedean places of k is denoted by σ (with σ' complex places), so that the group U_k of units of k has rank $rk(U_k) = \sigma - 1$, and $d = \sigma + \sigma'$.

The height is related to an ℓ^1-norm as follows. Let S be a finite set of places of k, of cardinality s, containing Σ, and let k_S^* be the group of S-units in k^*. Consider be the logarithmic 'embedding' $\mathcal{L}$ of k_S^* into $\mathbb{R}^S$:

$$\alpha \to \mathcal{L}(\alpha) = \{d_v \operatorname{Log}|\alpha|_v; v \in S\},$$

whose kernel $\mu(k^*)$ consists of the roots of unity in k , and whose image is a lattice in a hyperplane of $\mathbb{R}^S$. For any q in $N \cup \{\infty\}$, denote by $\|.\|_q$ the ℓ^q-norm on $\mathbb{R}^S$. Thus, for α in k_S^*, we have

$$\|\mathcal{L}(\alpha)\|_q = \left(\sum_{v \in S} |d_v \operatorname{Log}|\alpha|_v|^q\right)^{1/q} \qquad (q \neq \infty),$$
$$\|\mathcal{L}(\alpha)\|_\infty = \max_{v \in S}(|d_v \operatorname{Log}|\alpha|_v|),$$

and it follows from the product formula $h(\alpha) = h(\alpha^{-1})$ that

$$\|\mathcal{L}(\alpha)\|_1 = 2h_k(\alpha),$$

https://doi.org/10.1017/S1446788700000768 Published online by Cambridge University Press

and that $\|\mathcal{L}(\alpha)\|_q \leq 2^{1/q} h_k(\alpha)$ (cf. [1, 6, 12]). Furthermore, the ℓ^2-norm enables us to speak of the covolume $\mathrm{Vol}(\Lambda)$ of any discrete subgroup Λ in the vector space it generates in $\mathbb{R}^S$. For instance, $\mathrm{Vol}(\mathcal{L}(U_k))$ is the regulator of the number field k, times $2^{\sigma'}\sqrt{\sigma}$ (cf. (3.7) below). More generally, for any integer m with $0 \leq m \leq \mathrm{rk}(k_S^*) = s - 1$, we set:

$$(1.1) \qquad V_m(k, S) = \min_U\{\mathrm{Vol}(\mathcal{L}(U));\ U = \text{a subgroup of } k_S^* \text{ of rank } m\}.$$

By the properties of $\mathcal{L}$ recalled above, $V_m(k, S)$ is non-zero. Various effective lower bounds for this quantity will be given in the last part of this section. For instance, one has

$$(3.6) \qquad V_m(k, S) \geq (1/8d)^{3\,\inf(d,m)},$$

independently of S. We point out that $V_m(k, S)$ appears implicitly in [12] (where it is bounded in terms of ℓ^∞-norms; cf. [12, Lemma 5], and (3.3) below), and in [4] (where it is bounded in terms of ℓ^2-norms; see also [1, Proposition 2], and (3.4) below). Finally,

$$(3.3') \qquad V_m(k, S) \geq s^{-m} h_k[m],$$

where

$$(1.2) \quad h_k[m] = \min\left\{\prod_{i=1,\dots,m} h_k(\epsilon_i);\ \epsilon_1, \dots, \epsilon_m \text{ multipicatively independent in } k^*\right\}$$

denotes the product of the first m successive minima of the function h_k on k^*.

(b) A minor bound Recalling the notation $\mathrm{Vol}_J(M)$ from Section 1(c), we have:

THEOREM 2. *Let S be a finite set of places of k containing Σ, and let $\alpha_1, \dots, \alpha_n$ be S-units in k^*. Denote by r the rank of their relation group M and by $J \cup J'$ a partition of $\{1, \dots, n\}$ in two subsets of cardinality $r, n - r$. Then:*

$$\mathrm{Vol}_J(M) \leq (\sqrt{2})^{n-r}.|\mu(k^*)|^r.V_{n-r}(k, S)^{-1}.\prod_{i\in J'} h_k(\alpha_i).$$

[In order to apply this result efficiently, one should take S minimal with respect to the α_i's . Up to the factor $(\sqrt{2})^{n-r}$, it then cannot be improved, cf. (3.2') below. In the opposite direction, one can dispose of S in the statement of Theorem 2 by appealing to such bounds as (3.6), with $m = n - r$. As for $|\mu(k^*)|$, it is equal to 2 if $\sigma \neq \sigma'$, and is otherwise bounded from above by the largest integer N such that $\phi(N)$ divides d, cf. [4].]

https://doi.org/10.1017/S1446788700000768 Published online by Cambridge University Press

PROOF. We first compare M to the primitive subgroup M' given by the intersection of $\mathbb{Z}^n$ with the $\mathbb{R}$-subspace W generated by M in $\mathbb{R}^n$. For $(b_1, \dots, b_n)$ in M', $\alpha_1^{b_1} \cdots \alpha_n^{b_n}$ is a root of unity in k^*, so that the exponent of M'/M divides $|\mu(k^*)|$. Consequently, $[M' : M]$, and a fortiori $[p_J(M') : p_J(M)]$, divide $|\mu(k^*)|^r$. By the index formula, we are now reduced to the case where M is primitive.

Under this hypothesis, the group A generated by $\alpha_1, \dots, \alpha_n$ in k_S^* is torsion-free. Being finitely generated, it is free, of rank $n - \mathrm{rk}(M) = n - r$, and there exists a basis $\beta_1, \dots, \beta_{n-r}$ of A over $\mathbb{Z}$, in terms of which we may 'parametrize' $\alpha_1, \dots, \alpha_n$. More precisely, let

$$C = (c_{i,j})_{1 \le i \le n,\ 1 \le j \le n-r} (n \text{ rows}, n - r \text{ columns})$$

be the $n \times (n - r)$ matrix with integral coefficients, such that

$$\alpha_i = \prod_{j=1,\dots,n-r} \beta_j^{c_{i,j}} \quad \text{for all } i = 1, \dots, n. \tag{2}$$

For any element $(b_1, \dots, b_n)$ in the relation group M, we deduce from the multiplicative independence of the β_j's that $\sum_{i=1,\dots,n} b_i c_{ij} = 0$ for all $j = 0, \dots, n - r$. In other words, the $n - r$ columns of C belong to the orthogonal complement $M^\perp = W^\perp \cap \mathbb{Z}^n$ of M in $\mathbb{Z}^n$. We shall now show that they make up a basis of $M^\perp$.

Since the α_i's generate A, there exists an $n \times (n - r)$ integral matrix B' such that $(\beta_1, \dots, \beta_{n-r}) = (\alpha_1, \dots, \alpha_n)^{B'}$, hence: $(\beta_1, \dots, \beta_{n-r}) = (\beta_1, \dots, \beta_{n-r})^{{}^tC.B'}$, and the independence of the β_j's implies that ${}^tC.B'$ is the $(n - r) \times (n - r)$ identity matrix I_{n-r}. On the other hand, let c be a $n \times (n - r)$ integral matrix expressing a basis of $M^\perp$ in the canonical basis of $\mathbb{Z}^n$, and let P be the $(n - r) \times (n - r)$ integral matrix such that $C = cP$. Then, ${}^tC.B' ={}^t P.({}^tcB') = I_{n-r}$, so that P belongs to $GL_{n-r}(\mathbb{Z})$, and our claim is proved.

Thus, the absolute value of the $J' \times \{1, \dots, n - r\}$ minor of the matrix C coincides with $\mathrm{Vol}_{J'}(M^\perp) = \mathrm{Vol}_J(M)$, and we deduce from the relations (2) that the subgroup $A_{J'}$ of A generated by the α_j's for j in J' has rank $< n - r$ if and only if $\mathrm{Vol}_J(M)$ vanishes; otherwise, $\mathrm{Vol}_J(M)$ is the index of $A_{J'}$ in A .

Considering the logarithmic embedding of k_S^* into $\mathbb{R}^S$, and noticing that $\mathscr{L}$ is injective on the free group A, we now derive from the index formula:

$$\mathrm{Vol}(\mathscr{L}(A))\, \mathrm{Vol}_J(M) = \mathrm{Vol}(\mathscr{L}(A_{J'})).$$

By Hadamard's inequality, this expression is bounded from above by $\prod_{i \in J'} \|\mathscr{L}(\alpha_i)\|_2$, hence by $\prod_{i \in J'} \|\mathscr{L}(\alpha_i)\|_1$, and even by $(\sqrt{2})^{n-r} \prod_{i \in J'} h_k(\alpha_i)$. Since $\mathrm{Vol}(\mathscr{L}(A)) \ge V_{n-r}(k, S)$ by definition (cf. (1.1)), Theorem 2 is established.

REMARK 2. Theorem 2 holds even if some of the $h(\alpha_j)$'s are zero . Indeed, if J' contains an index with this property, the projection $p_J(M)$ will have rank $< r$, and

$\mathrm{Vol}_J(M)$ will also vanish. (If all $h(\alpha_j)$'s are 0, that is, if $r = n$, our formula is still valid, since the empty product 0^0 – just as the covolume of $\{0\}$ in $\{0\}$ – is equal to 1). This eventuality can create problems when dealing with only one relation as in [10, Theorem 3], which in fact holds in full generality only if $r = 1$.

In [12], Matveev expresses his bounds in terms of the twisted sup norm

$$|\mathbf{x}|_a = \max_{i=1,\dots,n} (a_i|x_i|) \quad \text{for } \mathbf{x} = (x_1, \dots, x_n) \text{ in } \mathbb{R}^n,$$

where $a = (a_1, \dots, a_n)$ is any n-tuple of real numbers satisfying $a_i > h_k(\alpha_i)$ for $i = 1, \dots, n$. We now show how to recover his results from Theorem 2 (and the bounds for $\mathrm{Vol}_{n-r}(k, S)$ given in Section 2(c)).

COROLLARY ([12, Theorem 4]). *Under the hypotheses of Theorem 2, there exists a set of r linearly independent elements* $\mathbf{b}_1, \dots, \mathbf{b}_r$ *of M such that:*

$$\prod_{j=1,\dots,r} |\mathbf{b}_j|_a \le (n_r)^{1/2}(\sqrt{2})^{n-r}|\mu(k^*)|^r V_{n-r}(k, S)^{-1} \prod_{i=1,\dots,n} a_i.$$

PROOF. Let $\| \ \|_{a^2}$ be the a^2-twist of the standard scalar product on $\mathbb{R}^n$, defined by:

$$\|\mathbf{x}\|_{a^2} = \sum_{i=1,\dots,n} a_i^2 x_i^2 \quad \text{for } \mathbf{x} = (x_1, \dots, x_n) \text{ in } \mathbb{R}^n.$$

Writing Vol_{a^2} for the corresponding volumes, we deduce from Theorem 2 and Pythagoras-Cauchy-Binet that

$$\mathrm{Vol}_{a^2}(M) \le (n_r)^{1/2}(\sqrt{2})^{n-r}.|\mu(k^*)|^r.h_{n-r}(k, S)^{-1}. \prod_{i=1,\dots,n} a_i.$$

We now proceed as in [12]. The $\| \ \|_{a^2}$-volume of the $|.|_a$ unit ball is equal to 2^n. By Vaaler's cube-slicing, its intersection with the vector-space W generated by M in $\mathbb{R}^n$ has volume $\ge 2^r$. Minkowski's theorem then yields a set of r linearly independent elements $\mathbf{b}_1, \dots, \mathbf{b}_r$ of M such that :

$$\prod_{j=1,\dots,r} |\mathbf{b}_j|_a \le 2^r\, \mathrm{Vol}_{a^2}(M)/2^r,$$

and the corollary follows from these two inequalities.

Finally, we point out that Chen's approach in [4] is also based on a parametrization process. But the vector space generated by $\mathscr{L}(A)$ over $\mathbb{Q}$ is used in place of A, and the resulting denominators which occur in the analogue of the matrix C can be controlled only with the help of geometry of numbers in $\mathscr{L}(k_S^*)$. It then becomes difficult to study each of its minors separately.

https://doi.org/10.1017/S1446788700000768 Published online by Cambridge University Press

(c) From regulators to Lehmer's problem We now list the lower bounds for $V_{n-r}(k, S)$ promised in Section 2(a), whose notation we resume. Since $\mathbb{R}^\Sigma \oplus (\bigoplus_{v \neq \Sigma} \mathbb{R}^{(v)})$ is an orthogonal decomposition of $\mathbb{R}^S$ with respect to the ℓ^2-norm, and since $|x|_v^{d_v} = |N_{k_v/\mathbb{Q}_p}(x)|_p$ for v above a prime p, orthogonal projection on the second factor gives

$$(3.1) \qquad V_m(k, S) \geq \min_{0 \leq \mu \leq \sigma - 1} \left\{ V_\mu(k, \Sigma) \prod_{i=1,\dots,[(m-\mu)/d]} \operatorname{Log} p_i \right\}$$

where p_i denotes the i-th prime number. For instance (cf. [12, example following Theorem 5]):

$$(3.2) \qquad V_m(\mathbb{Q}, S) \geq \prod_{i=1,\dots,m} \operatorname{Log} p_i.$$

More generally, let $S = \{p(1), \dots, p(n-1)\}$ be any set of $n-1$ increasing prime numbers, so that $V_{n-1}(\mathbb{Q}, S) = \prod_{i=1,\dots,n-1} \operatorname{Log} p(i)$, and consider the elements $\alpha_1 = p(1)$, $\alpha_2 = p(2)/p(1), \dots, \alpha_{n-1} = p(n-1)/p(n-2)$, $\alpha_n = -1/p(n-1)$ of $\mathbb{Q}^*$, for which $h_\mathbb{Q}(\alpha_i) = \operatorname{Log}(p(i))$ if $i < n$. Their relation group $M = \mathbb{Z}.(2, \dots, 2)$ has rank $r = 1$, and for $J = \{n\}$, we get the equality:

$$(3.2') \qquad \operatorname{Vol}_J(M) = 2 = |\mu(\mathbb{Q}^*)| V_{n-1}(\mathbb{Q}, S)^{-1} \prod_{i=1,\dots,n-1} h_\mathbb{Q}(\alpha_i).$$

In view of (3.1), we can now restrict to the crucial case $S = \Sigma$, that is, to the study of subgroups of the unit group U_k. But we prefer to postpone use of this remark to the final step of our discussion.

As was already suggested, practical lower bounds for $V_m(k, S)$ depend on the choice of a ℓ^q-norm on $\mathbb{R}^S$. We recall that the volume of the ℓ^q-unit ball in the standard space $\mathbb{R}^n$ is given by $(2\Gamma(1 + 1/q))^n / \Gamma(1 + n/q)$, and we first consider the case $2 \leq q \leq \infty$. Vaaler's cube-slicing inequality for $q = \infty$ (and the layman's sphere slicing equality for $q = 2$) have been extended to this full range by Meyer and Pajor in [13]. Accordingly, the intersection of the ℓ^q-unit ball in $\mathbb{R}^S$ with any m-dimensional subspace passing through the origin has volume at least equal to $2^m\Gamma(1+1/q))^m / \Gamma(1+m/q)$. On considering the subspaces generated by the different groups U in (1.1), we deduce from Minkowski's theorem the existence of a set of m multiplicatively independent elements $\epsilon_1, \dots, \epsilon_m$ in k_S^* such that:

$$\prod_{i=1,\dots,m} \|\mathscr{L}(\epsilon_i)\|_q \leq 2^m V_m(k, S)/(2^m\Gamma(1 + 1/q))^m / \Gamma(1 + m/q)),$$

hence

$$V_m(k, S) \geq (\Gamma(1 + 1/q))^m / \Gamma(1 + m/q))\omega(k, q, m),$$

https://doi.org/10.1017/S1446788700000768 Published online by Cambridge University Press

where

$$\omega(k,q,m)=\min\left\{\prod_{i=1,\dots,m}\|\mathscr{L}(\epsilon_i)\|_q;\ \epsilon_1,\dots,\epsilon_m \text{ multiplicatively indepdependent in } k^*\right\}.$$

For instance, we recover

$$(3.3)\qquad V_m(k,S)\geq\omega(k,\infty,m),$$

$$(3.4)\qquad V_m(k,S)\geq(\sqrt{\pi}/4m)^{m/2}\omega(k,2,m),$$

corresponding respectively to [12, Theorem 4], and to [4] (or [1, Prop. 2]).

But it seems more natural, in the context of Theorem 2, to express these lower bounds in terms of heights. From Hölder's inequality $\|x\|_1\leq\|x\|_q.s^{1-1/q}$ in $\mathbb{R}^S$, we get $\|\mathscr{L}(\epsilon)\|_q\geq 2h_k(\epsilon)/s^{1-1/q}$. Recalling the definition (1.2) of $h_k[m]$, we finally obtain with the latter choices of q:

$$(3.3')\qquad V_m(k,S)\geq(2/s)^m h_k[m],$$

$$(3.4')\qquad V_m(k,S)\geq(\sqrt{\pi}/ms)^{m/2}h_k[m].$$

We now consider the case $q=1$, where Hölder's inequality becomes an equality. Unfortunately, octahedra do not slice up as nicely as spheres, but by [13, Theorem 7], the volume X of the intersection of the ℓ^1-unit ball in $\mathbb{R}^S$ with any m-dimensional subspace passing through the origin still satisfies :

$$X\geq(s/\pi)^{(s-m)/2}(\Gamma((m+s)/2)/\Gamma(s)).2^m/\Gamma(1+m),$$

which is $\geq 2m.e^s/s^m$ if $s-m\leq\operatorname{Log}(s)$. Minkowski's theorem then yields a set of m multiplicatively independent elements $\epsilon_1,\dots,\epsilon_m$ in k_S^* such that:

$$\prod_{i=1,\dots,m}\|\mathscr{L}(\epsilon_i)\|_1\leq 2^m V_m(k,S)/X$$

and therefore, in terms of heights :

$$(3.5)\qquad V_m(k,S)\geq(2/s)^m e^s h_k[m]\quad\text{if } s-m\leq\operatorname{Log}(s).$$

(This is a slight sharpening on (3.2′) in the indicated range for m, which, in the setting of Theorem 2, would correspond to a relation group of small rank.)

A lazy way to conclude our discussion consists in bounding $h_k[m]$ from below by the mth power of any known bound for the first minimum $h_k[1]$ of h_k on k^*. For instance, $h_k[1]$ is at least $(16d)^{-2}$ (see, for example, [4]), and we deduce from (3.1), and (3.3) that

$$V_m(k,S)\geq\min_{0\leq\mu\leq\sigma-1}\left\{(2/\sigma)^\mu(16d)^{-2\mu}\prod_{i=1,\dots,[(m-\mu)/d]}\operatorname{Log}p_i\right\},$$

https://doi.org/10.1017/S1446788700000768 Published online by Cambridge University Press

hence

$$V_m(k, S) \geq (8d)^{-3\inf(d,m)}. \tag{3.6}$$

But this may be drastically improved in some situations. As an archimedean analogue of (3.2) , suppose for example that $S = \Sigma$, and that m is equal to the rank $\sigma - 1$ of U_k. Then, $V_{\sigma-1}(k, \Sigma) = \mathrm{Vol}(\mathscr{L}(U_k))$, and the lower bound for the regulator of k quoted in [6, p. 620] implies:

$$V_{\sigma-1}(k, \Sigma) \geq 10^{-3}\sqrt{d}|\mu(k^*)|e^{d/5}, \tag{3.7}$$

which grows exponentially with d. (To relate $\mathrm{Vol}(\mathscr{L}(U_k))$ to the regulator, take a basis of $\mathscr{L}(U_k)$, divide the components of the complex embeddings by 2, note that the regulator is the absolute value of each of the resulting $(\sigma - 1) \times (\sigma - 1)$ minors, and apply Cauchy-Binet.)

Rather than to Lehmer's classical 'conjecture' on the existence of a universal lower bound for $h_k[1]$, our approach thereby leads to the following problem. Let us say that an integer valued function N on the set of positive integers, satisfying $\mathcal{N}(\sigma) \leq \sigma - 1$ for all σ, is *Lehmer admissible* if

$$\inf_k\{\inf(V_n(k, \Sigma_k); \mathcal{N}(\sigma_k) \leq n \leq \sigma_k - 1\} > 0,$$

where k runs through all the number fields and Σ_k denotes the set of (σ_k) archimedean places of k. We then ask :

PROBLEM. (i) does there exist a Lehmer admissible function $\mathcal{N}$ such that $\limsup \mathcal{N}(\sigma)/\sigma < 1$?

(ii) does there exist a bounded Lehmer admissible function? In particular, does there exist a number $N \geq 2$ and a constant $c > 0$ such that all number fields k with $\sigma_k - 1 \geq N$ satisfy: $V_N(k, \Sigma_k) \geq c$?

(iii) does there exist a constant $c' > 0$ such that all number fields k with $\sigma_k \geq 2$ satisfy: $V_1(k, \Sigma_k) \geq c'/\sqrt{\sigma_k}$.

COMMENTS. (i) In view of (3.7), the function $\mathcal{N}(\sigma) = \sigma - 1$ is Lehmer admissible. But $\mathcal{N}(\sigma) = 1$ is not, since $\|\mathscr{L}(\epsilon^{1/d})\|_2 \ll 1/\sqrt{d}$.

(ii) The third question lies between the conjectures of Lehmer (on ℓ^1-norms) and of Schinzel-Zassenhaus (on ℓ^∞-norms).

(iii) In view of Hadamard's inequality $V_N(k, \Sigma) \leq (\sqrt{2})^N h_k[N]$, a positive answer to the second question would imply the existence of a constant $c'' > 0$ such that in any field k of sufficiently large degree, at least one amongst N independent units ϵ of k satisfies: $h_k(\epsilon) \geq c''$.

We mention in conclusion that an elliptic analogue of this last statement (concerning Lang's problem on minimal heights in terms of discriminants) has recently been proved, with $N = 5$, by David (cf. [5, Cor. 1.6]).

3. Orthogonal abelian subvarieties

We go back to the tori of Section 1(b), assuming now that b is antisymmetric (in particular, the dimension of V is an even number $n = 2a$), and that V has a complex structure, given by an endomorphism J symplectic with respect to b , such that the $\mathbb{R}$-bilinear form $b(Jx, y)$ is a scalar product. This ensures that any subspace W of V stable under J is regular for b . Then, $H(x, y) = b(Jx, y) + ib(x, y)$ is a Riemann form for the complex torus $A = V/L$, which is thus an abelian variety, and the complex subtori $B = W/M$, $B^\perp = W^\perp/M^\perp$ are abelian subvarieties of A. Furthermore, the covolume of L with respect to b, which can be described alternatively as the Pfaffian of $b = \mathrm{Im}(H)$ on $L \times L$, or as the covolume of L wih respect to the scalar product $\mathrm{Re}(H)$, satisfies:

$$[L^* : L]^{1/2} = \mathrm{Vol}(L) = (1/g!)\deg_H(A),$$

where $\deg_H(A)$ denotes the degree of the image of A in any of the projective embeddings attached to the Riemann form H (cf. [2, Proposition 3]). Thus, Proposition 1 translates into a formula (reproduced in Theorem 3 below) between the projective degrees of orthogonal abelian subvarieties. In this section, we give an algebraic proof of this formula, which allows to treat abelian varieties in any characteristic. Of necessity, we replace duals by Cartier duals, which, in our situation, can be computed as Hom or Ext groups.

(a) The duality formula Let thus A be an abelian variety over some field k, and let λ be a polarisation on A. For any abelian subvariety B of A, the abelian subvariety $B^\perp$ of A, orthogonal to B with respect to λ, can be described as follows: the polarization λ gives rise to an isogeny ϕ between A and its dual abelian variety A^v, while the transpose of the injection j from B into A is a surjection j^v from A^v onto the dual B^v of B. Then, $B^\perp$ is the connected component of 0 of the subgroup scheme $\phi^{-1}(\mathrm{Ker}(j^v))$ of A. As is well known (cf. [14, p. 173]), the natural map σ from $B \times B^\perp$ to A given by addition on A is an isogeny, and the orthogonal $(B^\perp)^\perp$ of $B^\perp$ coincides with B.

When very ample, the polarization λ also gives rise to an embedding of A in a projective space, and enables us to speak of the degree $\deg_\lambda(W) = W.\lambda^{\dim W}$ of the image in that space of any algebraic subvariety W of A. In fact, this notation makes sense in all cases. For instance, the degree of A itself is given by the Riemann-Roch theorem (cf. [14, Section 16]) :

$$\deg_\lambda(A) = \dim(A)!|K(\lambda)|^{1/2},$$

where $K(\lambda)$ is the kernel of the isogeny ϕ attached to λ (we still write $|.|$ for the order of a finite group scheme, cf. [15, p. 38]). The following formulae, which sharpen Lemmata 1.3 and 1.4 of [11], show how the degrees of two orthogonal abelian subvarieties are related.

https://doi.org/10.1017/S1446788700000768 Published online by Cambridge University Press

THEOREM 3. *Let (A, λ) be a polarized abelian variety over a field k, and let B, $B^\perp$ be a pair of orthogonal abelian subvarieties with respect to λ. Denote by b, b', $a = b + b'$ the respective dimensions of B, $B^\perp$, A. Then :*

(i) *the degree $|B \cap B^\perp|$ of the isogeny $\sigma : B \times B^\perp \to A$ satisfies the formula :*

$$|B \cap B^\perp|.|K(\lambda)| = (\deg_\lambda(B)/b!)^2.|B^\perp \cap K(\lambda)| = (\deg_\lambda(B^\perp)/b'!)^2.|B \cap K(\lambda)|;$$

in particular: $\deg_\lambda(B)/(b!.|B \cap K(\lambda)|^{1/2}) = \deg_\lambda(B^\perp)/(b'!.|B^\perp \cap K(\lambda)|^{1/2})$.

(ii) *furthermore, $K(\lambda)/(B^\perp \cap K(\lambda))$ is isomorphic to* $\mathrm{Hom}(B \cap K(\lambda), \mathbf{G}_m)$*;in particular, $|K(\lambda)| = |B \cap K(\lambda)|.|B^\perp \cap K(\lambda)|$, so that:*

$$deg_\lambda(B^\perp) = (b'!/a!b!) \deg_\lambda(B) \deg_\lambda(A)/|B \cap K(\lambda)|.$$

[When λ is a principal polarisation, that is, when the kernel $K(\lambda)$ of ϕ is trivial, Theorem 3 reduces to the easy equality: $\deg_\lambda(B)/b! = \deg_\lambda(B^\perp)/b'!$. For an analysis of the structure of the groups in that case, cf. [9, p. 368].]

PROOF. Without loss of generality, we assume that k is algebraically closed. We denote by B' the group scheme:

$$B' = \phi^{-1}(\mathrm{Ker}(j^v)),$$

whose component of the idendity is $B^\perp$.

(i) The restriction of λ to B is again a polarisation of B, whose associated isogeny from B to B^v is given by $j^v \cdot \phi \cdot j$. By Riemann-Roch on B and the definition of B', we therefore have:

$$(\deg_\lambda(B)/b!)^2 = |B \cap B'|.$$

Since the cycle associated to B' is equal to $|K(\lambda)/B^\perp \cap K(\lambda)|$ times that of $B^\perp$, this last expression is also equal to $|B \cap B^\perp|.\ |K(\lambda)|/|B^\perp \cap K(\lambda)|$, and our first formulae follow by biorthogonality.

(ii) Since $B^\perp$ is divisible and $B'/B^\perp$ is finite, the exact sequence

$$0 \to B^\perp \to B' \to B'/B^\perp \to 0$$

splits (cf. [14, Lemma 1, p. 223]), and there exists a finite group scheme

$$N \approx B'/B^\perp \approx K(\lambda)/(B^\perp \cap K(\lambda))$$

such that $B' \approx B^\perp \times N$. In the category of commutative group schemes over k, we then have, on denoting Cartier duals by ^{v}:

$$\mathrm{Hom}((B', \mathbf{G}_m) = \mathrm{Hom}(N, \mathbf{G}_m) = N^v, \mathrm{Ext}^1(B', \mathbf{G}_m) = \mathrm{Ext}^1(B^\perp, \mathbf{G}_m) = (B^\perp)^v.$$

Consider now the exact sequence: $0 \to B' \to A \to B^v \to 0$, where the second arrow is the natural injection, and the third one is given by $j^v \cdot \phi$. The long exact sequence associated to $\mathrm{Hom}(., \mathbf{G}_m)$ it induces reads:

$$0 \to \mathrm{Hom}(B', \mathbf{G}_m) \to \mathrm{Ext}^1(B^v, \mathbf{G}_m) \to \mathrm{Ext}^1(A, \mathbf{G}_m) \to \mathrm{Ext}^1(B', \mathbf{G}_m) \to 0$$

(cf. [14, Section 15], [15, p. 63], or [16, p. 166] if B' is reduced), that is,

$$0 \to N^v \to B^{vv} \to A^v \to (B^\perp)^v \to 0.$$

The second arrow of this exact sequence is $(j^v \cdot \phi)^v = \phi^v \cdot j$; but once B^{vv} is identifed to B, we have $\phi^v = \phi$ (cf. [14, pp. 130 and 188]), so that N^v coincides with the kernel of $\phi \cdot j$, which is $B \cap K(\lambda)$. In other words, the finite group schemes

$$K(\lambda)/(B^\perp \cap K(\lambda)) \quad \text{and} \quad B \cap K(\lambda)$$

are Cartier duals, and this concludes the proof of Theorem 3.

REMARK 3. B and $B^\perp$ may well intersect along $K(\lambda)$, so that once again (cf. Remark 1), it is not true in general that the natural map from $(B^\perp \cap K(\lambda)) \times (B \cap K(\lambda))$ to $K(\lambda)$ induced by the addition σ on A would be an isomorphism. For a counterexample, consider an elliptic curve with complex multiplication by $\pi = \sqrt{-2}$, with principal polarization (0), and set $A = E \times E$, polarized by $\lambda = p_1^*(0) + 2p_2^*(0)$. Let $B = \{x = \pi y\}$, so that $B^\perp = \{x = -\pi y\}$. On denoting by $E[f]$ the kernel of an endomorphism f of E, we see that $K(\lambda) = 0 \times E[2]$, which intersects both B and $B^\perp$ along $O \times E[\pi]$.

Finally, here is another way to state (or prove) Theorem 3, in terms of the e^λ pairing of Mumford ([14, Section 20]; over $\mathbb{C}$, and in the notation of the beginning of this section, $e^\lambda(x, y)$ is given by $\exp(-2i\pi(b(x', y'))$ for x', y' above points x, y in $K(\lambda)$). Since e^λ is non-degenerate on $K(\lambda)$, it is clear that the induced pairing

$$e^\lambda : K(\lambda) \times (K(\lambda) \cap B) \to \mu(k^*)$$

is right exact. Its left kernel contains $K(\lambda) \cap B^\perp$, and Theorem 3(ii) expresses the fact that they coincide.

(b) Complementary multidegrees We here suppose that A is the product of n polarized abelian varieties $(C_1, \lambda_1), \dots, (C_n, \lambda_n)$, and that $\lambda = p_1^*\lambda_1 + \cdots + p_n^*\lambda_n$, where p_i is the projection from A to C_i. Denote by c_i the dimension of C_i, so that $a = \dim A = c_1 + \cdots + c_n$, and let $J = \{r_1, \dots, r_n\}$ be a set of integers such that

https://doi.org/10.1017/S1446788700000768 Published online by Cambridge University Press

$0 \leq r_i \leq c_i$ for $i = 1, \dots, n$. In particular, $b := r_1 + \cdots + r_n \leq a$. For any subvariety W of A, of dimension b, we may then consider the intersection number

$$\deg_J(W) = W.(p_1^*\lambda_1)^{r_1}. \cdots .(p_n^*\lambda_n)^{r_n}.$$

When each λ_i is very ample, that is, yields an embedding of C_i in a projective space $\mathbf{P}(i)$, $\deg_J(W)$ may be interpreted as the multidegree with respect to J of the image of W in $\mathbf{P}(1) \times \cdots \times \mathbf{P}(n)$. But $\deg_J(W)$ makes sense in all cases, and for simplicity, we shall assume from now on that all the λ_i's, hence λ as well, are *principal* polarizations.

The relation between $\deg_\lambda(W)$ and the different multidegrees of W is given by Newton's formula:

$$\deg_\lambda(W) = W.\left(\sum_{i=1,\dots,n} p_i^*(\lambda_i)\right)^r = \sum_J c(J)\deg_J(W),$$

where J runs through all sets of n-tuples $\{r_1, \dots, r_n\}$ as above, and $c(J)$ is the binomial coefficient $b!/r_1! \cdots r_n!$. The following multihomogeneous version of Theorem 3, which, reversing the roles of B and $B^\perp$, we rewrite as $\deg_\lambda(B) = (b!/b'!a!)\deg_\lambda(B^\perp)\deg_\lambda(A)/|B^\perp \cap K(\lambda)|$, would therefore also imply it. For each $J = \{r_1, \dots, r_n\}$, we denote the 'complementary' set of J by $J' = \{r_1' = c_1 - r_1, \dots, r_n' = c_n - r_n\}$, with $r_1' + \cdots + r_n' := b' = a - b$.

COROLLARY. *Let* $(A, \lambda) = \prod_{i=1,\dots,n}(C_i, \lambda_i)$ *be a principally polarized abelian variety, let* B, $B^\perp$ *be a pair of orthogonal abelian subvarieties with respect to* λ, *of dimension* b, $b' = a - b$, *and let* J, J' *be complementary sets of indices as above. Then,*

$$\deg_J(B)/r_1! \dots r_n! = \deg_J'(B^\perp)/r_1'! \dots r_n'!$$

PROOF. To any n-tuple of variable positive integers $z = \{z_1, \dots, z_n\}$, we associate the polarization

$$\lambda_z = z_1 p_1^*\lambda_1 + \cdots + z_n p_n^*\lambda_n$$

on A. The corresponding isogeny from A to its dual A^v (which we identify with A thanks to the principal polarization λ) is the 'diagonal' map $\xi_z = \{z_1, \dots, z_n\}$ on $C_1 \times \cdots \times C_n$, whose kernel $A[\xi_z]$ has order $z_1^{2c_1} \cdots z_n^{2c_n}$. Applying Theorem 3 (in the shape above) to the orthogonal complement B^z of B with respect to λ_z, together with Newton's formula, we obtain:

$$\sum_J c(J)\deg_J(B)z^J = (b!/b'!a!)\left(\sum_{J'} c(J')\deg_{J'}(B^z)z^{J'}\right).a!|A[\xi_z]|^{1/2}/|B^z \cap A[\xi_z]|$$
$$= (b!/b'!)\left(\sum_{J'} c(J')\deg_{J'}(B^z)z^{J'}z^{J'}z^J\right)/|B^z \cap A[\xi_z]|$$

https://doi.org/10.1017/S1446788700000768 Published online by Cambridge University Press

where we have set: $z^J = z_1^{r_1} \cdots z_n^{r_n}$, and likewise for $z^{J'}$.

Now, $B^\perp$ is the set theoretic image of B^z under ξ_z, so that the cycles $(\xi_z)_* B^z$ and $|B^z \cap A[\xi_z]|.B^\perp$ coincide. On the other hand, $(\xi_z)^*(p_i^*\lambda_i) = z_i^2 p_i^*\lambda$. We therefore derive from the projection formula ([7, p. 426]) that:

$$|B_z \cap A[\xi_z]| \left(B^\perp . \prod_{i=1,\dots,n} (p_i^*\lambda_i)^{c_i - r_i} \right) = \left(B^z . \prod_{i=1,\dots,n} (z_i^2 p_i^*\lambda_i)^{c_i - r_i} \right)$$

for any subset $J' = (c_1 - r_1, \dots, c_n - r_n)$, that is,

$$|B^z \cap A[\xi_z]| \deg_{J'}(B^\perp) = \deg_{J'}(B^z) z^{2J'}.$$

Plugging this into the previous relation, we get:

$$\sum_J c(J) \deg_J(B) z^J = (b!/b'!) \sum_{J'} c(J') \deg_{J'}(B^\perp) z^J.$$

Since this formula holds for any choice of positive integers z, we may view it as an equality of polynomials in n variables, each of whose coefficients must therefore coincide.

References

[1] D. Bertrand, 'Minimal heights and polarizations on group varieties', *Duke Math. J.* **80** (1995), 223–250.

[2] D. Bertrand and P. Philippon, 'Sous-groupes algébriques de groupes algébriques commutatifs', *Illinois J. Math.* **32** (1988), 263–280.

[3] J. W. S. Cassels, *An introduction to the geometry of numbers* (Springer, Berlin, 1959).

[4] G.-L. Chen, 'Relations de dépendance linéaire entre des logarithmes de nombres algébriques', *Ann. Fac. Sc. Toulouse*, to appear.

[5] S. David, 'Points de petite hauteur sur les courbes elliptiques', *J. Number Theory*, to appear.

[6] E. Friedman, 'Analytic formulae for the regulator of a number field', *Invent. Math.* **98** (1989), 599–622.

[7] R. Hartshorne, *Algebraic geometry* (Springer, Berlin, 1977).

[8] R. Heath-Brown, 'Diophantine approximation with square-free numbers', *Math. Z.* **187** (1984), 335–344.

[9] H. Lange and C. Birkenhake, *Complex abelian varieties* (Springer, Berlin, 1992).

[10] J. Loxton and A. van der Poorten, 'Multiplicative dependence in number fields', *Acta Arith.* **42** (1983), 291–302.

[11] D. Masser and G. Wüstholz, 'Periods and minimal abelian subvarieties', *Ann. of Math. (2)* **137** (1993), 407–458.

[12] E. M. Matveev, 'On linear and multiplicative relations', *Russian Ac. Sci. Sbornik Math.* **78** (1994), 411–425.

[13] M. Meyer and A. Pajor's, 'Volume des sections de la boule unité de ℓ_n^p', *J. Funct. Anal.* **80** (1988), 109–123.

[14] D. Mumford, *Abelian varieties* (Oxford University Press, Oxford, 1970).

[15] S. Schatz, 'Group schemes, formal groups and p-divisible groups', in: *Arithmetic geometry* (ed. Cornell-Silverman) (Springer, Berlin, 1986).

[16] J-P. Serre, *Groupes algébriques et corps de classes* (Hermann, Paris, 1959).

[17] J. Thunder, 'Asymptotic estimates for rational points of bounded height on flag varieties', *Compositio Math.* **88** (1993), 155–186.

Université de Paris VI
Institut de Mathématiques, T. 46, C. 247
4, Place Jussieu
75 252 Paris Cédex 05
France
e-mail: bertrand@math.jussieu.fr

https://doi.org/10.1017/S1446788700000768 Published online by Cambridge University Press