Astérisque
312, 2007, p. 171–177

14. AN ALTERNATIVE APPROACH USING IDEAL BASES

by

Stefan Wewers

Abstract. — We give another approach to the proof of the Gross-Keating intersection formula. This approach is based on the concept of *ideal bases* in the theory of anisotropic quadratic forms over $\mathbb{Z}_p$, and in the case $p = 2$ is drastically simpler than the proof given in the previous chapter.

***Résumé* (Une approche alternative à l'aide des bases idéales).** — On donne une autre approche à la démonstration de la formule de Gross et Keating. Cette approche est basée sur la notion de *bases idéales* de la théorie des formes quadratiques anisotropes sur $\mathbb{Z}_p$, et est plus simple que la démonstration dans le chapitre précédent pour $p = 2$.

In this note we give an alternative proof of Proposition 1.5 and Proposition 1.6 of [**R**]. This proof uses the concept of *ideal bases* introduced in Section 6 of [**B**] and thus avoids the difficulties encountered in the case $p = 2$. In fact, our arguments work the same way for any p.

1. Homomorphisms between quasi-canonical lifts

1.1. Let p be a prime number and D the quaternion division algebra over $\mathbb{Q}_p$. The reduced norm gives an anisotropic $\mathbb{Q}_p$-valued quadratic form on D which we denote by Q. The function $v : D^\times \to \mathbb{Z}$, $\alpha \mapsto \mathrm{ord}_p\, Q(\alpha)$, is the standard normalized valuation on D.

Let $\boldsymbol{\psi} = (\psi_1, \dots, \psi_n)$ be an ordered tuple of linearly independent elements of D, and let $L \subset D$ be the $\mathbb{Z}_p$-lattice spanned by $\boldsymbol{\psi}$. The restriction of Q to L gives L the structure of an anisotropic quadratic $\mathbb{Z}_p$-module. We say that $\boldsymbol{\psi}$ is an *ideal basis* of L if

$$v(\psi_i) \leq v(\psi_j) \quad \text{for all } i \leq j$$

2000 ***Mathematics Subject Classification.*** — 14L05, 11F32.
Key words and phrases. — Formal $\mathcal{O}$-modules, quaternion algebras, modular intersection numbers.

and if

$$v\Big(\sum_i x_i\psi_i\Big) = \min_i v(x_i\psi_i)$$

for all $(x_i) \in \mathbb{Z}_p^n$. By [**B**], Lemma 6.4, this is equivalent to Definition 6.3 of *loc. cit.*. In particular, every sublattice $L \subset D$ has an ideal basis.

By [**B**, Proposition 6.6], an ideal basis is also optimal. Moreover, if $\boldsymbol{\psi}$ is ideal then the numbers $a_i := v(\psi_i)$, $i = 1, \ldots, n$, are the Gross-Keating invariants of L.

1.2. Let $K \subset D$ be a subfield which is a quadratic extension of $\mathbb{Q}_p$. Then there exists an element $\varphi \in K$ such that

$$\mathcal{O}_K = \mathbb{Z}_p \oplus \mathbb{Z}_p \cdot \varphi$$

and such that φ is a unit (resp. a uniformizer) if $K/\mathbb{Q}_p$ is unramified (resp. if $K/\mathbb{Q}_p$ is ramified). For such an element, we have

$$v(x + y\varphi) = \min\{2\operatorname{ord}_p x, 2\operatorname{ord}_p y + v(\varphi)\}, \tag{1.1}$$

for all $x, y \in \mathbb{Q}_p$. It follows that $(1, p^r\varphi)$ is an ideal basis of

$$\mathcal{O}_r = \mathbb{Z}_p \oplus \mathbb{Z}_p \cdot p^r\varphi,$$

the unique order in $\mathcal{O}_K$ of conductor p^r, for all $r \geq 0$.

1.3. Let G be the unique formal group of height 2 over $k = \bar{\mathbb{F}}_p$. We identify the ring of endomorphisms of G with the maximal order $\mathcal{O}_D$ of D. Note that for $\psi \in \mathcal{O}_D$ the integer $v(\psi)$ is equal to the *height* of the isogeny $\psi : G \to G$.

Fix two positive integers $r, s \geq 0$, and let F_r, F_s be quasi-canonical lifts of G of level r and s, with respect to the subfield $K \subset D$. We assume that F_r, F_s are defined over A, a complete discrete valuation ring which is a finite extension of the ring of Witt vectors over k. We denote by

$$H_{r,s} := \operatorname{Hom}_A(F_r, F_s)$$

the group of homomorphisms of formal groups $F_r \to F_s$. This is a free $\mathbb{Z}_p$-module of rank 2. It is also a right (resp. left) module under the order $\mathcal{O}_r = \operatorname{End}(F_r)$ (resp. the order $\mathcal{O}_s = \operatorname{End}(F_s)$).

Reducing a homomorphism $F_r \to F_s$ to the special fibre yields a $\mathbb{Z}_p$-linear embedding $H_{r,s} \hookrightarrow D$. Via this embedding we may consider $H_{r,s}$ as a quadratic $\mathbb{Z}_p$-module.

Proposition 1.1

1. *As a right $\mathcal{O}_r$-module, $H_{r,s}$ is free of rank* 1, *generated by a homomorphism $\psi_1 : F_r \to F_s$ of height $|s - r|$.*
2. *The Gross-Keating invariants of $H_{r,s}$ are $(|s - r|, r + s)$ if $K/\mathbb{Q}_p$ is unramified and $(|s - r|, r + s + 1)$ if $K/\mathbb{Q}_p$ is ramified.*

Proof. — Replacing all isogenies by their duals, we may assume that $r \leq s$. Let F/A be the canonical lift of G with respect to the embedding $K \subset D$. By [**Ww1**, §4], we may identify F_r with the quotient of F corresponding to the superlattice $T_r \supset T := \mathcal{O}_K$ defined by

$$T_r := \mathbb{Z}_p \cdot p^{-r} + \mathcal{O}_K$$

(and similarly for F_s). By [**Ww1**, Corollary 2.3], this presentation of F_r, F_s yields an isomorphism of right $\mathcal{O}_r$-modules

$$H_{r,s} \cong \{\alpha \in \mathcal{O}_K \mid \alpha T_r \subset T_s\}.$$

We let $\psi_1 \in H_{r,s}$ denote the element corresponding to 1 under this isomorphism. Clearly, the height of ψ_1 equals the index of T_r in T_s, which is $s - r$. To prove Part 1 of the proposition, it remains to show that $\alpha T_r \subset T_s$ if and only if $\alpha \in \mathcal{O}_r$. One direction is clear. For the other direction, fix $\alpha \in \mathcal{O}_K$ with $\alpha T_r \subset T_s$. In order to show that $\alpha \in \mathcal{O}_r$, we may add any element of $\mathbb{Z}_p$ to α. Hence we may assume that $\alpha = x\varphi$, where $x \in \mathbb{Z}_p$ and φ is as in Section 1.2. Our assumption implies that

$$\alpha p^{-r} = x p^{-r} \varphi \in T_s = \mathbb{Z}_p \cdot p^{-s} \oplus \mathbb{Z}_p \cdot \varphi.$$

We conclude that $p^r | x$ and hence $\alpha \in \mathcal{O}_r$. This proves Part 1.

Set $\psi_2 := p^r \varphi \psi_1$. Clearly, (ψ_1, ψ_2) is the basis of $H_{r,s}$ corresponding to the ideal basis $(1, \varphi)$ of $\mathcal{O}_r$ under the isomorphism $\mathcal{O}_r \cong H_{r,s}$. This isomorphism is not an isometry, but for $\psi = \alpha \cdot \psi_1 \in H_{r,s}$, with $\alpha \in \mathcal{O}_r$, we have

$$v(\psi) = v(\alpha) + (s - r).$$

Therefore, it follows from (1.1) that (ψ_1, ψ_2) is an ideal basis of $H_{r,s}$. By the choice of $\varphi \in K$ in Section 1.2, we get $v(\psi_2) = s + r$ (resp. $v(\psi_2) = s + r + 1$) if $K/\mathbb{Q}_p$ is unramified (resp. ramified). This completes the proof of Part 2 of the proposition. □

1.4. We choose a uniformizer λ of the discrete valuation ring A. For $n \geq 0$ we set $A_n := A/(\lambda^{n+1})$. Let $H_{r,s,n}$ denote the subgroup of $\mathcal{O}_D$ consisting of endomorphisms $\psi : G \to G$ which lift to a homomorphism $F_r \otimes A_n \to F_s \otimes A_n$.

Given an element $\psi \in \mathcal{O}_D - H_{r,s}$, we define two integers,

$$l_{r,s}(\psi) := \max\{v(\psi + \phi) \mid \phi \in H_{r,s}\}$$

and

$$n_{r,s}(\psi) := \max\{m \mid \psi \in H_{r,s,m}\}.$$

We let e denote the absolute ramification index of the discrete valuation ring A.

Proposition 1.2. — *There exists a constant $c_{r,s}$, only depending on (r, s), such that the following holds. If $l_{r,s}(\psi) \geq r + s - 1$ then*

$$n_{r,s}(\psi) = c_{r,s} + \frac{e}{2} \cdot l_{r,s}(\psi).$$

Proof. — First we consider the case $r = s$. Then we may assume that $F_r = F_s$. This is the case studied in [**Vl**]. By ăloc. cit., Proposition 3.1, we have for $l_{r,s}(\psi) \geq 2r - 1$

$$n_{r,s}(\psi) = a(r-1) + p^{r-1} + \Big(\frac{l_{r,s}(\psi)+1}{2} - r\Big)e + 1, \tag{1.2}$$

where $a(k) = (p^k - 1)(p+1)/(p-1)$. Hence the proposition is true for $r = s$.

For the general case, we may again assume that $r \leq s$. By induction on s, we will reduce to the case $r = s$. Suppose that the proposition is proved for some pair (r, s) with $r \leq s$. Let F_r, F_s, F_{s+1} be quasi-canonical lifts of level $r, s, s+1$. We want to prove the proposition for the pair $(r, s+1)$. By Proposition 1.1.1, the group $H_{s,s+1}$ is generated, as a right $\mathcal{O}_s$-module, by a homomorphism $\beta : F_s \to F_{s+1}$ of height one. Moreover, the map $\psi \mapsto \beta\psi$ is an isomorphism of $\mathbb{Z}_p$-modules $H_{r,s} \xrightarrow{\sim} H_{r,s+1}$.

Let $\psi \in \mathcal{O}_D - H_{r,s+1}$ with $l_{r,s+1}(\psi) \geq s+r$. In a first step we will assume in addition that either $r > 0$ or that $l_{r,s+1}(\psi) \geq r + s + 1$. It is no restriction of generality to assume that $v(\psi) = l_{r,s+1}(\psi)$. Then $v(\psi) > 0$ and we can write $\psi = \beta\psi'$, with $\psi' \in \mathcal{O}_D$. It follows from the assertions made in the preceding paragraph that we have

$$l_{r,s+1}(\psi) = l_{r,s}(\psi') + 1. \tag{1.3}$$

In particular, $l_{r,s}(\psi') \geq r + s$. On the other hand, [**Ww1**, Corollary 6.3], says that

$$n_{r,s+1}(\psi) = n_{r,s}(\psi') + e/e_{s+1}, \tag{1.4}$$

where we use the following notation. Let $M = K \cdot W[1/p]$, and let $\mathcal{O}_M$ be its ring of integers. By M_s we denote the ring class field of $O_s^\times \subset \mathcal{O}_K^\times$, by $\mathcal{O}_{M_s}$ its ring of integers, and by e_s its absolute ramification index. Then $\mathcal{O}_{M_s}$ is the minimal subring of A over which F_s can be defined. So for $r > 0$, the proposition follows from (1.3), (1.4) and induction.

Unfortunately, for $r = 0$ the above argument proves the claim only for the weaker bound $l_{r,s} \geq r + s = s$. The problem is that for $s = 1$ and $l = 0$ the element ψ is a unit in $\mathcal{O}_D$, and so we cannot divide by β and reduce to the case $s = 0$. However, the argument can be used to compute the value of the constant $c_{r,s}$. For instance, for $(r, s) = (0, 0)$ we have $c_{0,0} = e/2$ by (1.2), and so by (1.3) and (1.4) we get $c_{0,1} = e/e_1$. Therefore, the proposition is proved if we can show that for $l_{0,1}(\psi) = 0$ we have $n = n_{0,1}(\psi) = e/e_1$.

Since $l_{0,1}(\psi) = 0$, the endomorphism ψ is an automorphism of G. Let F_r^ψ denote the lift of G obtained from F_r by composing the isomorphism $F_r \otimes_A k \xrightarrow{\sim} G$ with ψ. Then ψ lifts to a homomorphism $F_r \to F_s$ modulo λ^n if and only if the two deformations $F_r^\psi \otimes A/(\lambda^n)$ and $F_s \otimes A/(\lambda^n)$ are isomorphic. This, in turn, means that $u(F_r^\psi) \equiv u(F_s) \pmod{\lambda^n}$ (here $u(F) \in A$ denotes the modulus of a lift of G defined over A). By [**Ww1**, Corollary 5.6], the valuation of $u(F_r^\psi)$ (resp. of $u(F_s)$) is equal to e/e_r (resp. equal to e/e_s). Since $e_r = e_0 < e_s = e_1$, the maximal value that n can take is e/e_1. This is what we still had to prove. □

2. The modular intersection number

2.1. Let p be an arbitrary prime and $k = \bar{\mathbb{F}}_p$. Let G be the (unique) formal group of height 2 over k. We identify $\mathrm{End}_k(G)$ with the maximal order $\mathcal{O}_D$ of the quaternion division algebra D over $\mathbb{Q}_p$. Let $W = W(k)$ denote the ring of Witt-vectors over k. Let (Γ, Γ') be the universal deformation of the pair of formal groups (G, G). It is defined over the universal deformation space $\mathcal{S} \cong \mathrm{Spf}\, W[[t, t']]$.

Let $L \subset \mathcal{O}_D$ be a sub-$\mathbb{Z}_p$-module of rank 3. We denote by Q the quadratic form induced on L by the reduced norm on $\mathcal{O}_D$. For $\psi \in L$ we define $v(\psi) := \mathrm{ord}_p\, Q(\psi)$. Choose an ideal basis (ψ_1, ψ_2, ψ_3) of (L, Q), see Section 1.1. Let $a_i := v(\psi_i)$. The numbers a_1, a_2, a_3 are the Gross–Keating invariants of L.

For $i = 1, 2, 3$, let $\mathcal{T}_i$ denote the closed subscheme of $\mathcal{S}$ corresponding to the ideal $I \lhd W[[t, t']]$ which is minimal for the property that ψ_i lifts to a homomorphism $\Gamma \to \Gamma'$ modulo I. The following proposition corresponds to Proposition 1.5 of [**R**].

Proposition 2.1. — *If $a_3 \leq 1$ then $a_3 = 1$ and*

$$(\mathcal{T}_1 \cdot \mathcal{T}_2 \cdot \mathcal{T}_3)_{\mathcal{S}} = \begin{cases} 1, & \text{for } a_2 = 0, \\ 2, & \text{for } a_2 = 1. \end{cases}$$

Proof. — Since Q is anisotropic, the a_i cannot have all the same parity. Therefore, $a_1 \leq a_2 \leq a_3 \leq 1$ implies $a_0 = 0$ and $a_3 = 1$. In particular, ψ_1 is an automorphism of G. It follows that $\mathcal{T}_1 \cong \mathrm{Spf}\, W[[t]]$, and that we may identify $\Gamma|_{\mathcal{T}_1}$ with $\Gamma'|_{\mathcal{T}_1}$ via ψ_1. So for the rest of the proof, we assume that $\psi_1 = 1 \in \mathcal{O}_D$ and consider $\mathcal{T}_2, \mathcal{T}_3$ as closed subschemes of $\mathcal{S}' = \mathrm{Spf}\, W[[t]]$, the universal deformation space of G. For $i = 2, 3$, $\mathcal{T}_i$ is defined by the condition that ψ_i lifts to an endomorphism of Γ.

Let $\mathcal{O} = \mathbb{Z}_p[\psi_2] \subset \mathcal{O}_D$ denote the subring generated by ψ_2. Since $(\psi_1 = 1, \psi_2)$ is an ideal basis of $\mathcal{O}$, we have

$$a_2 = v(\psi_2) = \max\{v(x + \psi_2) \mid x \in \mathbb{Z}_p\}.$$

If $a_2 = 0$, then it follows that $\mathcal{O} = \mathcal{O}_K$ is the maximal order of $K \subset D$, an unramified quadratic extension of $\mathbb{Q}_p$. Therefore, $\mathcal{T}_2 \cong \mathrm{Spf}\, W \subset \mathcal{S}'$ and $F := \Gamma|_{\mathcal{T}_2}$ is the canonical lift corresponding to the subfield $K \subset D$. Moreover, in the notation of §1.4 we have $l = l_{0,0}(\psi_3) = v(\psi_3) = a_3$. It follows from [**Ww1**], Theorem 3.3 (see the proof of Proposition 1.2) that $\mathcal{T}_3 \cap \mathcal{T}_2 \subset \mathcal{T}_2$ corresponds to the ideal $(p^n) \lhd W$, with

$$n = n_{0,0}(\psi_3) = \frac{l+1}{2} e = \frac{a_3 + 1}{2} = 1.$$

This proves the proposition for $a_2 = 0$.

If $a_2 = 1$, then $\mathcal{O} = \mathcal{O}_K$ is also the maximal order of K, but $K/\mathbb{Q}_p$ is ramified. With the same arguments as above, it follows that $\mathcal{T}_2 \cong \mathrm{Spf}\, \mathcal{O}_M \subset \mathcal{S}'$ is the canonical locus corresponding to the subfield $K \subset D$. Applying again [**Ww1**], Theorem 3.3, we get

$$n = n_{0,0}(\psi_3) = \frac{l+1}{2} e = a_3 + 1 = 2.$$

This proves the proposition for $a_2 = 1$. □