SIMPLE PROOFS OF CLASSICAL EXPLICIT RECIPROCITY LAWS ON CURVES USING DETERMINANT GROUPOIDS OVER AN ARTINIAN LOCAL RING

Greg W. Anderson
School of Mathematics
University of Minnesota
Minneapolis, MN 55455, USA
gwanders@math.umn.edu
and
Fernando Pablos Romo
Departamento de Matemáticas
Universidad de Salamanca
Plaza de la Merced 1-4
37008 Salamanca, España
fpablos@usal.es

Abstract. The notion of determinant groupoid is a natural outgrowth of the theory of the Sato Grassmannian and thus well-known in mathematical physics. We briefly sketch here a version of the theory of determinant groupoids over an artinian local ring, taking pains to put the theory in a simple concrete form suited to number-theoretical applications. We then use the theory to give a simple proof of a reciprocity law for the Contou-Carrère symbol. Finally, we explain how from the latter to recover various classical explicit reciprocity laws on nonsingular complete curves over an algebraically closed field, namely sum-of-residues-equals-zero, Weil reciprocity, and an explicit reciprocity law due to Witt. Needless to say, we have been much influenced by the work of Tate on sum-of-residues-equals-zero and the work of Arbarello-DeConcini-Kac on Weil reciprocity. We also build in an essential way on a previous work of the second-named author.

1. Introduction

In 1968 J. Tate [8] gave a definition of the residues of differentials on a curve in terms of traces of certain linear operators on infinite-dimensional vector spaces. Further, Tate deduced the residue theorem ("sum-of-residues-equals-zero") on a nonsingular complete curve X from the finite-dimensionality of the cohomology

The second-named author was partially supported by DGESYC research contract BFM2000-1327 and Castilla y León regional government contract SA064/01.
2000 *Mathematics Subject Classification*: 14H05, 11R37, 19F15.

groups $H^0(X, \mathcal{O}_X)$ and $H^1(X, \mathcal{O}_X)$. This work of Tate has been enormously influential.

In 1989 E. Arbarello, C. De Concini and V. G. Kac [1] interpreted the tame symbol at a point of a complete nonsingular algebraic curve X over an algebraically closed field as a commutator in a certain central extension of groups and then, in the style of Tate, deduced a reciprocity law on X for the tame symbol ("Weil reciprocity") from the finite-dimensionality of $H^0(X, \mathcal{O}_X)$ and $H^1(X, \mathcal{O}_X)$. Recently the second-named author of this paper has provided an interpretation [6] of the central extension of [1] in terms of determinants associated to infinite-dimensional vector subspaces valid for curves over a perfect field. The logical organization of this paper to a significant extent parallels that of [6].

In 1994 C. Contou-Carrère [3] defined a natural transformation greatly generalizing the tame symbol. In the case of an artinian local base ring k with maximal ideal m, the natural transformation takes the following form. Let $f, g \in k((t))^\times$ be given, where t is a variable. (Here and below $A^\times$ denotes the multiplicative group of a ring A with unit.) It is possible in exactly one way to write

$$f = a_0 \cdot t^{w(f)} \cdot \prod\nolimits_{i=1}^{\infty} (1 - a_i t^i) \cdot \prod\nolimits_{i=1}^{\infty} (1 - a_{-i} t^{-i})$$
$$g = b_0 \cdot t^{w(g)} \cdot \prod\nolimits_{i=1}^{\infty} (1 - b_i t^i) \cdot \prod\nolimits_{i=1}^{\infty} (1 - b_{-i} t^{-i})$$

with $w(f), w(g) \in \mathbb{Z}$, $a_i, b_i \in k$ for $i > 0$, $a_0, b_0 \in k^\times$, $a_{-i}, b_{-i} \in m$ for $i > 0$, and $a_{-i} = b_{-i} = 0$ for $i \gg 0$. By definition the value of the *Contou-Carrère symbol* is

$$\langle f, g \rangle := (-1)^{w(f)w(g)} \frac{a_0^{w(g)} \prod_{i=1}^{\infty} \prod_{j=1}^{\infty} \left(1 - a_i^{j/(i,j)} b_{-j}^{i/(i,j)}\right)^{(i,j)}}{b_0^{w(f)} \prod_{i=1}^{\infty} \prod_{j=1}^{\infty} \left(1 - a_{-i}^{j/(i,j)} b_j^{i/(i,j)}\right)^{(i,j)}} \in k^\times.$$

The definition makes sense because only finitely many of the terms appearing in the infinite products differ from 1. The symbol $\langle \cdot, \cdot \rangle$ is clearly antisymmetric and, although it is not immediately obvious from the definition, also bimultiplicative.

If k is a field, and hence $m = 0$, then the infinite products go away and the Contou-Carrère symbol reduces to the tame symbol. If $k = k_0[\epsilon]/(\epsilon^3)$, where k_0 is a field, then

$$\langle 1 - \epsilon f, 1 - \epsilon g \rangle \equiv 1 - \epsilon^2 \operatorname{Res}_{t=0}(g\, df) \bmod \epsilon^3$$

for all $f, g \in k_0((t))$, and so the Contou-Carrère symbol also contains the residue as a special case. If k is a $\mathbb{Q}$-algebra and $f \in 1 + m((t))$, then

$$\langle f, g \rangle = \exp(\operatorname{Res}_{t=0} \log f \cdot d \log g).$$

This last formula renders the bimultiplicativity of the Contou-Carrère symbol at least plausible and motivates the definition.

The main aims of this paper are (i) to interpret the Contou-Carrère symbol $\langle f, g \rangle$—up to signs—as a commutator of liftings of f and g to a certain central extension of a group containing $k((t))^\times$ (see Thm. 3.4.3) and then (ii) to exploit the commutator interpretation to prove in the style of Tate a reciprocity law for the Contou-Carrère symbol on a nonsingular complete curve defined over an algebraically closed field (see Thm. 4.2.1). The commutator interpretation of the Contou-Carrère symbol provided here formally resembles the commutator formula [7, Prop. 3.6] stated in Segal-Wilson.

In more detail, the general reciprocity law proved here takes the following form. Let F be an algebraically closed field. Let X/F be a complete nonsingular curve.

Let S be a finite nonempty set of (closed) points of X. For any ring or group A, put $A^S := \{(a_s)_{s\in S} | a_s \in A\}$. By choosing uniformizers at each point belonging to S, identify $R_0 := H^0(X \setminus S, \mathcal{O}_X)$ with an F-subalgebra of $F((t))^S$. Further, suppose now that the artinian local ring k considered above is a finite F-algebra. Put $R := R_0 \otimes_F k$ and make the evident identification of $R^\times$ with a subgroup of $k((t))^{\times S}$. We prove that

$$\prod_{s\in S} \langle f_s, g_s \rangle = 1$$

for all $f, g \in R^\times$. With $k = F$ we get back Weil reciprocity. With $k = F[\epsilon]/(\epsilon^3)$ we get back sum-of-residues-equals-zero. With F of characteristic $p > 0$ and $k = F[\epsilon]/(\epsilon^{p^{n-1}+1})$, we get back an explicit reciprocity law due to Witt [9].

The general reciprocity law proved here seems in principle to be known in the mathematical physics world, albeit no reference convenient for a number theorist can be cited. We claim novelty only for the simplicity and directness of our approach to the reciprocity law. We hope to popularize the reciprocity law among number theorists, and expect it to have many applications.

The backdrop for our constructions is provided by the theory of *determinant groupoids* over k. The notion of determinant groupoid is a natural outgrowth of the theory of the Sato Grassmannian and hence is quite familiar in mathematical physics. But inconveniently, in its native habitat, this notion is packaged with a lot of extra structure unneeded for studying reciprocity laws. We sketch here a "minimalist" version of the theory just adequate for the purposes we have in mind. We have taken pains to make the theory concrete and easy to apply, and also suitable for study by beginning graduate students in number theory and algebraic geometry. The theory very likely has applications beyond those discussed in this paper. We hope that our approach can be generalized to yield an "integrated version" of Beilinson's multi-dimensional generalization [2] of Tate's theory.

2. Determinant groupoids over an artinian local ring

We fix an artinian local ring k throughout the paper. We denote the maximal ideal of k by m and the multiplicative group of k by $k^\times$. Given a free k-module V of finite rank, we denote the rank of V over k by $\operatorname{rk} V$ and the maximal exterior power of V over k by $\det V$.

2.1. Background on k-modules.

Lemma 2.1.1. *A k-module V is flat if and only if for all integers $r > 0$, row vectors $x \in \mathrm{Mat}_{1\times r}(k)$ and column vectors $v \in \mathrm{Mat}_{r\times 1}(V)$ such that $xv = 0$, there exists an integer $s > 0$, a matrix $y \in \mathrm{Mat}_{r\times s}(k)$, and a column vector $w \in \mathrm{Mat}_{s\times 1}(V)$ such that $v = yw$ and $xy = 0$.*

Proof. This is a standard flatness criterion holding over any commutative ring with unit. See [5, (3.A), Thm. 1, part 6, pp. 17-18]. □

Lemma 2.1.2. *A family $\{v_i\}_{i\in I}$ of elements of a k-module V generates V over k if and only if the family $\{v_i \bmod mV\}_{i\in I}$ generates V/mV over k/m. (This is a version of Nakayama's Lemma. Note that V need not be finitely generated over k.)*

Proof. ($\Rightarrow$) Trivial. ($\Leftarrow$) Let V' be the k-span of $\{v_i\}_{i\in I}$. We have

$$V = V' + mV = V' + m^2V = ... = V'$$

because the ideal m is nilpotent. □

Lemma 2.1.3. *A family $\{v_i\}_{i\in I}$ of elements of a flat k-module V is k-linearly independent if and only if the family $\{v_i \bmod mV\}_{i\in I}$ of elements of V/mV is (k/m)-linearly independent.*

Proof. We may assume that $I = \{1, \ldots, r\}$. For convenience assemble the vectors v_i into a column vector $v \in \mathrm{Mat}_{r\times 1}(k)$. ($\Rightarrow$) Suppose that there exists $x \in \mathrm{Mat}_{1\times r}(k)$ such that $x \not\equiv 0 \bmod m$ but $xv \equiv 0 \bmod mV$. Let T be a minimal ideal of k and select $0 \neq t \in T$. Then $tm = 0$, hence $txv = 0$ but $tx \neq 0$, a contradiction. (Flatness of V was not needed to prove this implication.) ($\Leftarrow$) Suppose there exists $x \in \mathrm{Mat}_{1\times r}(k)$ such that $xv = 0$. By Lemma 2.1.1 there exists an integer $s > 0$, a matrix $y \in \mathrm{Mat}_{r\times s}(k)$ and a column vector $w \in \mathrm{Mat}_{s\times 1}(k)$ such that $v = yw$ and $xy = 0$. By hypothesis the matrix $y \bmod m \in \mathrm{Mat}_{r\times s}(k/m)$ must be of maximal rank. Therefore some maximal square submatrix of y is invertible and hence $x = 0$. (This argument comes from the proof of [5, (3.G), Proposition, p. 21].) □

Proposition 2.1.4. *(i) A k-module is free if and only if projective if and only if flat. (ii) If two of the k-modules in a short exact sequence of such are free, then so is the third. (iii) The k-linear dual of a free k-module is again free. (We frequently apply this proposition below but rarely cite it explicitly.)*

Proof. (i) It is necessary only to prove that flatness implies freeness, and for this purpose Lemmas 2.1.2 and 2.1.3 clearly suffice. (ii) Let

$$0 \to U \to V \to W \to 0$$

be a short exact sequence of k-modules. If U and W are free, then V is clearly free. If V and W are free then U is a direct summand of V, hence U is projective and hence U is free. If U and V are free, then any k-basis $\{u_i\}$ of U remains (k/m)-linearly independent in V/mV by Lemma 2.1.3, hence there exists a family of elements $\{v_j\}$ of V such that $\{u_i \bmod mV\} \coprod \{v_j \bmod mV\}$ is a (k/m)-basis of V/mV, hence $\{u_i\} \coprod \{v_j\}$ is a k-basis of V by Lemmas 2.1.2 and 2.1.3, and hence $\{v_j\}$ projects to a k-basis for W. (iii) This can be proved by straightforwardly applying Lemma 2.1.1 to verify flatness. We omit the details. □

Lemma 2.1.5. *Let V be a free k-module and let M be a finitely generated k-module. For every k-linear map $f : V \to M$ there exists a k-submodule $V' \subset V$ such that the quotient k-module V/V' is free of finite rank and $V' \subset \ker f$.*

Proof. By induction on the length of M as a k-module, we may assume that $M = k/m$ and $f \neq 0$. Since V is free, f is the reduction modulo m of a surjective k-linear functional $\tilde{f} : V \to k$. Put $V' := \ker \tilde{f}$. Then V' has the desired properties. □

Proposition 2.1.6. *Let V be a free k-module. Let $A, B \subset V$ be free k-submodules. The quotient $(A+B)/(A\cap B)$ is finitely generated if and only if there exists a free k-submodule $P \subset A \cap B$ such that the quotient k-modules A/P and B/P are free of finite rank. (We frequently apply this proposition below but rarely cite it explicitly.)*

Proof. ($\Rightarrow$) By Lemma 2.1.5 applied to the natural map $B \to B/(A\cap B)$ there exists a k-submodule $P \subset A \cap B$ such that the quotient k-module B/P is free of finite rank. It is then easily verified that P has all the desired properties. ($\Leftarrow$) Trivial. □

2.2. Commensurability and related notions.

2.2.1. *Commensurability.* Let V be a free k-module. Given free k-submodules $A, B \subset V$ we write $A \sim B$ and say that A and B are *commensurable* if the quotient $\frac{A+B}{A\cap B}$ is finitely generated over k. It is easily verified that commensurability is an equivalence relation.

2.2.2. *Relative rank.* Let V be a free k-module. Let $A, B \subset V$ be free k-submodules such that $A \sim B$. Put

$$\mathrm{Rk}^V(A,B) := \mathrm{rk}\, A/P - \mathrm{rk}\, B/P$$

where $P \subset A \cap B$ is any free k-submodule such that A/P and B/P are free of finite rank, thereby defining the *relative rank* of A and B. It is easily verified that $\mathrm{Rk}^V(A,B)$ is independent of the choice of P and hence well-defined. It follows that

$$\mathrm{Rk}^V(A,C) = \mathrm{Rk}^V(A,B) + \mathrm{Rk}^V(B,C)$$

for all free k-submodules $A, B, C \subset V$ such that $A \sim B \sim C$.

2.2.3. *The restricted general linear group.* Given a free k-module V and a free k-submodule $V_+ \subset V$, let $G^V_{V_+}$ denote the set of k-linear automorphisms σ of V such that $V_+ \sim \sigma V_+$. It is easily verified that $G^V_{V_+}$ is a subgroup of the group of k-linear automorphisms of V depending only on the commensurability class of V_+. We call $G^V_{V_+}$ the *restricted general linear group* associated to V and V_+.

2.2.4. *The index.* Let V be a free k-module and let $V_+ \subset V$ be a free k-submodule. Given $\sigma \in G^V_{V_+}$, put

$$\mathrm{ind}^V_{V_+}\,\sigma := \mathrm{Rk}(V_+, \sigma V_+),$$

thereby defining the *index* of σ. It is easily verified that $\mathrm{ind}^V_{V_+}\,\sigma$ depends only on the commensurability class of V_+. It follows that the function

$$\mathrm{ind}^V_{V_+} : G^V_{V_+} \to \mathbb{Z}$$

is a group homomorphism.

Lemma 2.2.5. *Let V be a free k-module equipped with a direct sum decomposition $V = V_+ \oplus V_-$. For all $\sigma \in G^V_{V_-} \cap G^V_{V_+}$ we have $\mathrm{ind}^V_{V_+}\,\sigma + \mathrm{ind}^V_{V_-}\,\sigma = 0$.*

Proof. We have

$$\begin{aligned}
& \mathrm{ind}^V_{V_+}\,\sigma + \mathrm{ind}^V_{V_-}\,\sigma \\
= \; & \mathrm{rk}\, V_+/P_+ - \mathrm{rk}\, \sigma V_+/P_+ + \mathrm{rk}\, V_-/P_- - \mathrm{rk}\, \sigma V_-/P_- \\
= \; & \mathrm{rk}(V_+ + V_-)/(P_+ + P_-) - \mathrm{rk}(\sigma V_+ + \sigma V_-)/(P_+ + P_-) \\
= \; & \mathrm{rk}\, V/(P_+ + P_-) - \mathrm{rk}\, V/(P_+ + P_-) = 0
\end{aligned}$$

for any free k-submodules $P_\pm \subset V_\pm \cap \sigma V_\pm$ such that $V_\pm/P_\pm$ and $\sigma V_\pm/P_\pm$ are free of finite rank. $\square$

2.3. **The construction** $\mathrm{Det}^V(A,B;P)$**.** Fix a free k-module V.

2.3.1. *Definition.* Given commensurable free k-submodules $A, B \subset V$ and a free k-submodule $P \subset A \cap B$ such that the quotient k-modules A/P and B/P are free of finite rank, put

$$\mathrm{Det}^V(A,B;P) := \left\{k\text{-linear isomorphisms } \det(A/P) \xrightarrow{\sim} \det(B/P)\right\}.$$

Note that we have at our disposal an operation of *scalar multiplication*

$$((x,\alpha) \mapsto x \cdot \alpha) : k^\times \times \mathrm{Det}^V(A,B;P) \to \mathrm{Det}^V(A,B;P)$$

with respect to which $\mathrm{Det}^V(A,B;P)$ becomes a $k^\times$-torsor.

2.3.2. *The composition law.* Given free k-submodules $A, B, C \subset V$ belonging to the same commensurability class and a free k-submodule $P \subset A \cap B \cap C$ such that the k-modules A/P, B/P and C/P are free of finite rank, we have a *composition law*

$$((\alpha,\beta) \mapsto \beta \circ \alpha) : \mathrm{Det}^V(A,B;P) \times \mathrm{Det}^V(B,C;P) \to \mathrm{Det}^V(A,C;P)$$

at our disposal. The composition law is compatible with scalar multiplication in the sense that

$$x \cdot (\beta \circ \alpha) = (x \cdot \beta) \circ \alpha = \beta \circ (x \cdot \alpha).$$

Clearly the composition law is associative.

2.3.3. *The cancellation rule.* Given commensurable free k-submodules $A, B \subset V$ and free k-submodules $Q \subset P \subset A \cap B$ such that the quotient k-modules A/Q and B/Q are free of finite rank, we have at our disposal a canonical isomorphism

$$\left((\wedge p_\ell) \wedge (\wedge \tilde{a}_i) \mapsto (\wedge p_\ell) \wedge \left(\wedge \tilde{b}_j\right)\right) \mapsto ((\wedge a_i) \mapsto (\wedge b_j)) :$$

$$\mathrm{Det}^V(A,B;Q) \xrightarrow{\sim} \mathrm{Det}^V(A,B;P)$$

where $\{a_i\}$, $\{b_j\}$ and $\{p_\ell\}$ are any ordered k-bases for A/P, B/P and P/Q, respectively, and $\{\tilde{a}_i\}$ and $\{\tilde{b}_j\}$ are any liftings to A/Q and B/Q, respectively, of $\{a_i\}$ and $\{b_j\}$, respectively. We refer to this isomorphism as the *cancellation rule.* It is easily verified that the cancellation rule commutes with the composition law and with scalar multiplication.

2.3.4. *Inverse system structure.* Let V be a free k-module and let $A, B \subset V$ be commensurable free k-submodules. Consider the family $\mathcal{P}$ of free k-submodules $P \subset A \cap B$ such that A/P and B/P are free of finite rank. Partially order the family $\mathcal{P}$ by reverse inclusion. Then $\mathcal{P}$ is a directed set and it is easily verified that the cancellation rule gives the family of sets $\mathrm{Det}^V(A,B;P)$ indexed by $P \in \mathcal{P}$ the structure of inverse system.

2.4. **The connected groupoid** $\mathrm{Det}^V_{V_+}$**.** Fix a free k-module V and a free k-submodule $V_+ \subset V$.

2.4.1. *Definition.* For all free k-submodules $A, B \subset V$ belonging to the commensurability class of V_+ put

$$\mathrm{Det}^V_{V_+}(A,B) := \lim_{\leftarrow} \mathrm{Det}^V(A,B;P),$$

the limit extended over the inverse system defined in §2.3.4. Since scalar multiplication commutes with the cancellation rule, we have at our disposal an operation of scalar multiplication

$$((x,\alpha) \mapsto x \cdot \alpha) : k^\times \times \mathrm{Det}^V_{V_+}(A,B) \to \mathrm{Det}^V_{V_+}(A,B)$$

endowing the set $\mathrm{Det}^V_{V_+}(A,B)$ with the structure of $k^\times$-torsor.

2.4.2. *The composition law.* Since the cancellation rule and the composition law commute, we obtain in the limit a composition law

$$((\alpha,\beta) \mapsto \beta \circ \alpha) : \mathrm{Det}^V_{V_+}(A,B) \times \mathrm{Det}^V_{V_+}(B,C) \to \mathrm{Det}^V_{V_+}(A,C)$$

for all free k-submodules $A, B, C \subset V$ belonging to the same commensurability class. The composition law is associative and moreover is compatible with scalar multiplication in the evident sense.

2.4.3. *Definition of* $\mathrm{Det}^V_{V_+}$. The rule sending each pair $A, B \subset V$ of free k-submodules commensurable to V_+ to the set $\mathrm{Det}^V_{V_+}(A,B)$ makes the commensurability class of V_+ into a category. We denote this category by $\mathrm{Det}^V_{V_+}$. It is easily verified that every morphism in $\mathrm{Det}^V_{V_+}$ is an isomorphism and that all the objects of $\mathrm{Det}^V_{V_+}$ are isomorphic. Thus $\mathrm{Det}^V_{V_+}$ is a connected groupoid. Note that $\mathrm{Det}^V_{V_+}$ depends only on the commensurability class of V_+.

2.4.4. *Abstract nonsense.* Fix $\sigma \in G^V_{V_+}$ and let σ_* be the functor from $\mathrm{Det}^V_{V_+}$ to itself induced in evident fashion by σ. A *natural transformation* Φ from the identity functor of $\mathrm{Det}^V_{V_+}$ to σ_* is a rule associating to each object A of $\mathrm{Det}^V_{V_+}$ a morphism $\Phi(A) \in \mathrm{Det}^V_{V_+}(A, \gamma A)$ such that for any two objects A and B of $\mathrm{Det}^V_{V_+}$ the diagram

$$\begin{array}{ccccc} & A & \xrightarrow{\Phi(A)} & \gamma A & \\ \alpha & \downarrow & & \downarrow & \gamma_*\alpha \\ & B & \xrightarrow{\Phi(B)} & \gamma B & \end{array}$$

commutes for all $\alpha \in \mathrm{Det}^V_{V_+}(A,B)$. It is easily verified that the natural transformations from the identity functor of $\mathrm{Det}^V_{V_+}$ to σ_* are in bijective correspondence with $\mathrm{Det}^V_{V_+}(V_+, \gamma V_+)$ via the map $\Phi \mapsto \Phi(V_+)$.

2.4.5. *The central extension* $\tilde{G}^V_{V_+}$. We define $\tilde{G}^V_{V_+}$ to be the set consisting of pairs (σ, Φ) where $\sigma \in G^V_{V_+}$ and Φ is a natural transformation from the identity functor of $\mathrm{Det}^V_{V_+}$ to σ_*. We compose elements of $\tilde{G}^V_{V_+}$ by the rule

$$(\sigma_1, \Phi_1)(\sigma_2, \Phi_2) := (\sigma_1\sigma_2, A \mapsto (\sigma_{1*}(\Phi_2(A))) \circ \Phi_1(A)).$$

It is easily verified that this composition law is a group law. The group $\tilde{G}^V_{V_+}$ thus defined depends only on the commensurability class of V_+. The group $\tilde{G}^V_{V_+}$ fits into a canonical exact sequence

$$1 \to k^\times \xrightarrow{x \mapsto (1, A \mapsto x \cdot 1_A)} \tilde{G}^V_{V_+} \xrightarrow{(\sigma,\Phi)\mapsto\sigma} G^V_{V_+} \to 1,$$

where $1_A \in \mathrm{Det}^V_{V_+}(A, A)$ denotes the identity map. The exact sequence identifies $k^\times$ with a subgroup of the center of $\tilde{G}^V_{V_+}$.

2.4.6. *Remark.* When k is a field, the central extension of the restricted general linear group $G^V_{V_+}$ constructed here has cohomology class in $H^2(G^V_{V_+}, k^\times)$ equal to the cohomology class associated to the central extension studied in the paper [1] and equal to the opposite of the cohomology class associated to the central extension studied in [6]. So what we study here should be regarded as the deformation theory of the central extensions of [1] and [6].

3. Study of the symbol $\{\sigma, \tau\}^V_{V_+}$

3.1. **Definition and basic properties of the symbol.** Fix a free k-module V and free k-submodule $V_+ \subset V$.

3.1.1. *Definition.* Given commuting elements $\sigma, \tau \in G^V_{V_+}$, put

$$\{\sigma, \tau\}^V_{V_+} := \tilde{\sigma}\tilde{\tau}\tilde{\sigma}^{-1}\tilde{\tau}^{-1} \in \ker\left(\tilde{G}^V_{V_+} \to G^V_{V_+}\right) = k^\times$$

where $\tilde{\sigma}, \tilde{\tau} \in \tilde{G}^V_{V_+}$ are any liftings of σ and τ, respectively. It is easily verified that $\{\sigma, \tau\}^V_{V_+}$ is independent of the choice of liftings and hence well-defined. By the definitions we have

$$(\sigma_*\beta) \circ \alpha = \{\sigma, \tau\}^V_{V_+} \cdot ((\tau_*\alpha) \circ \beta)$$

for all $\alpha \in \mathrm{Det}^V_{V_+}(V_+, \sigma V_+)$ and $\beta \in \mathrm{Det}^V_{V_+}(V_+, \tau V_+)$. The latter formula is the one we rely upon in practice to calculate $\{\sigma, \tau\}^V_{V_+}$.

Lemma 3.1.2. *Let G be a group. Write $[x, y] := xyx^{-1}y^{-1}$ for all $x, y \in G$. Now let $\alpha, \beta, \gamma \in G$ be given. Assume that $[\beta, \gamma]$ is central in G. Then we have $[\alpha, \gamma][\beta, \gamma] = [\alpha\beta, \gamma]$.*

Proof.

$$\begin{aligned}
[\alpha, \gamma][\beta, \gamma][\alpha\beta, \gamma]^{-1} &= \alpha\gamma\alpha^{-1}\gamma^{-1}[\beta, \gamma]\gamma\alpha\beta\gamma^{-1}\beta^{-1}\alpha^{-1} \\
&= \alpha\gamma[\beta, \gamma]\beta\gamma^{-1}\beta^{-1}\alpha^{-1} \\
&= \alpha[\beta, \gamma][\beta, \gamma]^{-1}\alpha^{-1} = 1.
\end{aligned}$$

□

3.1.3. *Basic properties.* Fix elements $\sigma, \sigma', \tau, \tau' \in G^V_{V_+}$ such that the σ's commute with the τ's. (But we need assume neither that $\sigma\sigma' = \sigma'\sigma$ nor that $\tau\tau' = \tau'\tau$.) The following relations hold:

- $\{\sigma, \sigma\}^V_{V_+} = 1.$
- $\{\sigma, \tau\}^V_{V_+} = \left(\{\tau, \sigma\}^V_{V_+}\right)^{-1}.$

- $\{\sigma\sigma', \tau\}^V_{V_+} = \{\sigma, \tau\}^V_{V_+}\{\sigma', \tau\}^V_{V_+}$.
- $\{\sigma, \tau\tau'\}^V_{V_+} = \{\sigma, \tau\}^V_{V_+}\{\sigma, \tau'\}^V_{V_+}$.
- $\sigma V_+ = V_+ = \tau V_+ \Rightarrow \{\sigma, \tau\}^V_{V_+} = 1$.
- If $V_+ = \{0\}$ or $V_+ = V$, then $\{\sigma, \tau\}^V_{V_+} = 1$.
- $\{\sigma, \tau\}^V_{V_+}$ depends only on the commensurability class of V_+.

For the most part these facts are straightforwardly deduced from the definitions. Only the proof of bimultiplicativity offers any difficulty and the essential point of that proof is contained in the preceding lemma.

3.2. **The four square identity.** Fix a free k-module V, a free k-submodule $V_+ \subset V$ and commuting elements $\sigma, \tau \in G^V_{V_+}$. We work out an explicit formula for the symbol $\{\sigma, \tau\}^V_{V_+}$ in terms of determinants.

3.2.1. *Choices.* Let

$$P \subset V_+ \cap \sigma V_+, \quad Q \subset V_+ \cap \tau V_+$$

be free k-submodules such that the quotient k-modules

$$V_+/P, \quad \sigma V_+/P, \quad V_+/Q, \quad \tau V_+/Q$$

are free of finite rank. Let

$$R \subset P \cap Q \cap \tau P \cap \sigma Q$$

be a free k-submodule such that the quotient k-modules

$$P/R, \quad Q/R, \quad \tau P/R, \quad \sigma Q/R$$

are free of finite rank. Fix finite sequences

$$\{a_i\}, \ldots, \{h_i\}$$

in V (not necessarily all of the same length) such that the corresponding finite sequences

$$\left.\begin{array}{l}\{a_i \bmod P\},\\ \{b_i \bmod P\},\\ \{c_i \bmod Q\},\\ \{d_i \bmod Q\},\\ \{e_i \bmod R\},\\ \{f_i \bmod R\},\\ \{g_i \bmod R\},\\ \{h_i \bmod R\},\end{array}\right\} \text{ are } k\text{-bases of } \left\{\begin{array}{l}V_+/P,\\ \sigma V_+/P,\\ V_+/Q,\\ \tau_+ V/Q,\\ P/R,\\ Q/R,\\ \tau P/R,\\ \sigma Q/R,\end{array}\right.$$

respectively. Fix morphisms

$$\alpha \in \mathrm{Det}^V_{V+}(V_+, \sigma V_+), \quad \beta \in \mathrm{Det}^V_{V_+}(V_+, \tau V_+).$$

3.2.2. *Construction of representations of the morphisms α, β.* Since our purpose is to calculate $\{\sigma,\tau\}_{V_+}^{V}$ by means of the last formula of §3.1.1, we may simply assume that α is represented by

$$(\wedge(a_i \bmod P) \mapsto \wedge(b_i \bmod P)) \in \mathrm{Hom}_k\left(\det(V_+/P), \det(\sigma V_+/P)\right)$$

and that β is represented by

$$(\wedge(c_i \bmod Q) \mapsto \wedge(d_i \bmod Q)) \in \mathrm{Hom}_k\left(\det(V_+/Q), \det(\tau V_+/Q)\right).$$

By the cancellation rule α is also represented by

$$\left((\wedge\bar{e}_i) \wedge (\wedge\bar{a}_i) \mapsto (\wedge\bar{e}_i) \wedge \left(\wedge\bar{b}_i\right)\right) \in \mathrm{Hom}_k\left(\det(V_+/R), \det(\sigma V_+/R)\right)$$

and β is also represented by

$$\left(\left(\wedge\bar{f}_i\right) \wedge (\wedge\bar{c}_i) \mapsto \left(\wedge\bar{f}_i\right) \wedge \left(\wedge\bar{d}_i\right)\right) \in \mathrm{Hom}_k\left(\det(V_+/R), \det(\tau V_+/R)\right),$$

where here and below $v \mapsto \bar{v}$ denotes reduction modulo R.

3.2.3. *Construction of representations of the morphisms $\tau_*\alpha$ and $\sigma_*\beta$.* By definition $\tau_*\alpha$ is represented by

$$\begin{aligned}&(\wedge(\tau a_i \bmod \tau P) \mapsto \wedge(\tau b_i \bmod \tau P))\\ &\in \mathrm{Hom}_k\left(\det(\tau V_+/\tau P), \det(\tau\sigma V_+/\tau P)\right)\end{aligned}$$

and $\sigma_*\beta$ is represented by

$$\begin{aligned}&(\wedge(\sigma c_i \bmod \sigma Q) \mapsto \wedge(\sigma d_i \bmod \sigma Q))\\ &\in \mathrm{Hom}_k\left(\det(\sigma V_+/\sigma Q), \det(\sigma\tau V_+/\sigma Q)\right).\end{aligned}$$

By the cancellation rule, $\tau_*\alpha$ is also represented by

$$\begin{aligned}&\left((\wedge\bar{g}_i) \wedge (\wedge\overline{\tau a}_i) \mapsto (\wedge\bar{g}_i) \wedge \left(\wedge\overline{\tau b}_i\right)\right)\\ &\in \mathrm{Hom}_k\left(\det(\tau V_+/R), \det(\tau\sigma V_+/R)\right)\end{aligned}$$

and $\sigma_*\beta$ is also represented by

$$\begin{aligned}&\left(\left(\wedge\bar{h}_i\right) \wedge (\wedge\overline{\sigma c}_i) \mapsto \left(\wedge\bar{h}_i\right) \wedge \left(\wedge\overline{\sigma d}_i\right)\right)\\ &\in \mathrm{Hom}_k\left(\det(\sigma V_+/R), \det(\sigma\tau V_+/R)\right).\end{aligned}$$

3.2.4. *Conclusion of the calculation.* We have now represented all the morphisms α, β, $\tau_*\alpha$ and $\sigma_*\beta$ in such a way that we can obtain representations for the compositions $(\sigma_*\beta)\circ\alpha$ and $(\tau_*\alpha)\circ\beta$ in the same rank one free k-module, namely

$$\mathrm{Hom}_k\left(\det(V_+/R), \det(\sigma\tau V_+/R)\right) = \mathrm{Hom}_k\left(\det(V_+/R), \det(\tau\sigma V_+/R)\right).$$

It is a straightforward matter to calculate the ratio. We find that

$$\begin{aligned}&\{\sigma,\tau\}_{V_+}^{V}\\ =\ &\frac{(\wedge\bar{h}_i) \wedge (\wedge\overline{\sigma d}_i)}{(\wedge\bar{g}_i) \wedge (\wedge\overline{\tau b}_i)}\frac{(\wedge\bar{e}_i) \wedge (\wedge\bar{b}_i)}{(\wedge\bar{h}_i) \wedge (\wedge\overline{\sigma c}_i)}\frac{(\wedge\bar{f}_i) \wedge (\wedge\bar{c}_i)}{(\wedge\bar{e}_i) \wedge (\wedge\bar{a}_i)}\frac{(\wedge\bar{g}_i) \wedge (\wedge\overline{\tau a}_i)}{(\wedge\bar{f}_i) \wedge (\wedge\bar{d}_i)}.\end{aligned}$$

The right side of the formula makes sense because in each of the fractions, both numerator and denominator generate the same rank one k-submodule of the exterior algebra over k of V/R. We call this result the *four square identity* because in an obvious way the diagram

$$\begin{array}{ccccccc}
V_+ & \{a_i\} & P & \{b_i\} & \sigma V_+ & & \\
\{c_i\} & & \{e_i\} & & \{\sigma c_i\} & & \\
Q & \{f_i\} & R & \{h_i\} & \sigma Q & & \\
\{d_i\} & & \{g_i\} & & \{\sigma d_i\} & & \\
\tau V_+ & \{\tau a_i\} & \tau P & \{\tau b_i\} & \sigma\tau V_+ & = \tau\sigma V_+ &
\end{array}$$

serves as a mnemonic. We call the diagram above a *template* for the calculation of $\{\sigma,\tau\}^V_{V_+}$ and we say that the right side of the four square identity is the *value* of the template.

3.3. **General rules of calculation.** Fix a free k-module V and a free k-submodule $V_+ \subset V$.

Proposition 3.3.1. *Fix commuting elements $\sigma,\tau \in G^V_{V_+}$. (i) Suppose there exists a free k-module W containing V as a k-submodule. Suppose further that σ,τ admit commuting extensions $\tilde\sigma,\tilde\tau \in G^W_{V_+}$, respectively. Then we have $\{\sigma,\tau\}^V_{V_+} = \{\tilde\sigma,\tilde\tau\}^W_{V_+}$. (ii) Suppose there exists a free k-submodule $U \subset V$ such that $\sigma U = U = \tau U$ and $U \cap V_+ = 0$. Put $\bar V := V/U$ and $\bar V_+ := (V_+ + U)/U$. Let $\bar\sigma$ and $\bar\tau$ be the k-linear automorphisms of $\bar V$ induced by σ and τ, respectively, and assume that $\bar\sigma,\bar\tau \in G^{\bar V}_{\bar V_+}$. Then we have $\{\sigma,\tau\}^V_{V_+} = \{\bar\sigma,\bar\tau\}^{\bar V}_{\bar V_+}$.*

Proof. We return to the setting of §3.2. Let T be the template above for calculating $\{\sigma,\tau\}^V_{V_+}$. The very same template T serves also to calculate $\{\tilde\sigma,\tilde\tau\}^W_{V_+}$. Therefore (i) holds. Let $\bar T$ be the projection of the template T into $\bar V$. Then $\bar T$ is a template for the calculation of $\{\bar\sigma,\bar\tau\}^{\bar V}_{\bar V_+}$ and moreover it is easily verified that the values of the templates T and $\bar T$ are equal. Therefore (ii) holds. □

Proposition 3.3.2. *Suppose V is equipped with a direct sum decomposition $V = V_0 \oplus V_1$. Put $V_{i+} := V_i \cap V_+$ for $i = 0,1$ and assume that $V_+ = V_{0+} \oplus V_{1+}$. Let commuting elements $\sigma_0,\sigma_1 \in G^V_{V_+}$ be given such that*

$$\sigma_i|_{V_0} \in G^{V_0}_{V_{0+}}, \quad \sigma_i|_{V_1} = 1$$

for $i = 0,1$. Then we have

$$\{\sigma_0|_{V_0},\sigma_1|_{V_0}\}^{V_0}_{V_{0+}} = \{\sigma_0,\sigma_1\}^V_{V_+}.$$

Proof. The proof is a straightforward application of the four square identity similar to that made in the proof of Proposition 3.3.1 and therefore omitted. □

Proposition 3.3.3. *Again suppose V is equipped with a direct sum decomposition $V = V_0 \oplus V_1$, put $V_{i+} := V_i \cap V_+$ for $i = 0,1$ and assume that $V_+ = V_{0+} \oplus V_{1+}$. Let $\sigma_0,\sigma_1 \in G^V_{V_+}$ be given such that*

$$\sigma_i|_{V_i} \in G^{V_i}_{V_{i+}}, \quad \sigma_i|_{V_{1-i}} = 1$$

for $i = 0, 1$. (Necessarily σ_0 and σ_1 commute.) Then we have

$$\{\sigma_0, \sigma_1\}^V_{V_+} = (-1)^{\nu_0\nu_1}$$

where

$$\nu_i := \mathrm{ind}^{V_i}_{V_{i+}} \sigma_i|_{V_i} = \mathrm{ind}^V_{V_+} \sigma_i$$

for $i = 0, 1$.

Proof. For $i = 0, 1$, choose a free k-submodule $P_i \subset V_{i+} \cap \sigma_i V_{i+}$ such that the quotient k-modules V_{i+}/P and $\sigma_i V_{i+}/P_i$ are free of finite rank and also choose finite sequences $\{e_{ij}\}$ and $\{f_{ij}\}$ in V_i (not necessarily of the same length) reducing modulo P_i to k-bases for V_{i+}/P_i and $\sigma_i V_{i+}/P_i$, respectively. Then the diagram

$$\begin{array}{ccccc}
V_{0+} \oplus V_{1+} & \{e_{0j}\} & P_0 \oplus V_{1+} & \{f_{0j}\} & \sigma_0 V_{0+} \oplus V_{1+} \\
\{e_{1j}\} & & \{e_{1j}\} & & \{e_{1j}\} \\
V_{0+} \oplus P_1 & \{e_{0j}\} & P_0 \oplus P_1 & \{f_{0j}\} & \sigma_0 V_{0+} \oplus P_1 \\
\{f_{1j}\} & & \{f_{1j}\} & & \{f_{1j}\} \\
V_{0+} \oplus \sigma_1 V_{1+} & \{e_{0j}\} & P_0 \oplus \sigma_1 V_{1+} & \{f_{0j}\} & \sigma_0 V_{0+} \oplus \sigma_1 V_{1+}
\end{array}$$

is a template for the calculation of $\{\sigma_0, \sigma_1\}^V_{V_+}$. The desired result now follows by the four square identity and the definitions. □

Proposition 3.3.4. *Let $V_- \subset V$ be a free k-submodule such that $V = V_+ \oplus V_-$. Let commuting elements $\sigma, \tau \in G^V_{V_+} \cap G^V_{V_-}$ be given. Then we have*

$$\{\sigma, \tau\}^V_{V_+} \{\sigma, \tau\}^V_{V_-} = 1.$$

Proof. We define

$$\sigma_0, \sigma_1, \tau_0, \tau_1 \in G^{V \oplus V}_{V_+ \oplus V_-}$$

by the block decompositions

$$\sigma_0 = \begin{bmatrix} \sigma & 0 \\ 0 & 1 \end{bmatrix}, \quad \sigma_1 = \begin{bmatrix} 1 & 0 \\ 0 & \sigma \end{bmatrix}, \quad \tau_0 = \begin{bmatrix} \tau & 0 \\ 0 & 1 \end{bmatrix}, \quad \tau_1 = \begin{bmatrix} 1 & 0 \\ 0 & \tau \end{bmatrix}.$$

Then we have

$$\begin{aligned}
&\{\sigma_0\sigma_1, \tau_0\tau_1\}^{V \oplus V}_{V_+ \oplus V_-} \\
&= \prod_{i=0}^{1} \prod_{j=0}^{1} \{\sigma_i, \tau_j\}^{V \oplus V}_{V_+ \oplus V_-} = \{\sigma, \tau\}^V_{V_+} \{\sigma, \tau\}^V_{V_-} (-1)^{\mu_-\nu_+ + \mu_+\nu_-}
\end{aligned}$$

by Propositions 3.3.2 and 3.3.3, where

$$\mu_\pm = \mathrm{ind}^V_{V_\pm} \sigma, \quad \nu_\pm = \mathrm{ind}^V_{V_\pm} \tau.$$

Put

$$U := \ker\left((v_0 \oplus v_1 \mapsto v_0 + v_1) : V \oplus V \to V\right).$$

Further, we have

$$\begin{aligned}\{\sigma_0\sigma_1,\tau_0\tau_1\}^{V\oplus V}_{V_+\oplus V_-} &= \{\sigma_0\sigma_1 \bmod U, \tau_0\tau_1 \bmod U\}^{(V\oplus V)/U}_{((V_+\oplus V_-)+U)/U}\\ &= \{\sigma,\tau\}^V_V = 1\end{aligned}$$

by part (ii) of Proposition 3.3.1. Finally, we have

$$(-1)^{\mu_-\nu_+ + \mu_+\nu_-} = (-1)^{2\mu_-\nu_+} = 1$$

by Lemma 2.2.5. The result follows. □

3.4. **The commutator interpretation of the Contou-Carrère symbol.**

3.4.1. *Preliminary discussion of the ring $k((t))$.* Let t be a variable. Let $k((t))$ be the ring obtained from the power series ring $k[[t]]$ by inverting t. It is easily verified that $k((t))$ is an artinian local ring with maximal ideal $m((t))$ and residue field $(k/m)((t))$. We have an additive direct sum decomposition

$$k((t)) = t^{-1}k[t^{-1}] \oplus k[[t]]$$

and a multiplicative direct sum decomposition

$$k((t))^\times = t^{\mathbb{Z}} \cdot (1+m[t^{-1}]) \cdot k^\times \cdot (1+tk[[t]])$$

at our disposal. The latter decomposition can be refined as follows. Each $f \in k((t))^\times$ has a unique presentation

$$f = t^{w(f)} \cdot a_0 \cdot \prod_{i=1}^{\infty}\left(1-a_{-i}t^{-i}\right) \cdot \prod_{i=1}^{\infty}\left(1-a_i t^i\right)$$

where

$$w(f)\in\mathbb{Z},\quad a_0 \in k^\times,\quad \begin{cases} a_i = 0 & \text{if } i \ll 0,\\ a_i \in m & \text{if } i<0,\\ a_i\in k^\times & \text{if } i=0,\\ a_i \in k & \text{if } i>0.\end{cases}$$

We call $w(f)$ the *winding number* of f and we call $\{a_i\}_{i=-\infty}^{\infty}$ the family of *Witt parameters* of f. Now view f as a k-linear automorphism of the free k-module $k((t))$. It is easily verified that $f \in G^{k((t))}_{k[[t]]}$ and that

$$\mathrm{ind}^{k((t))}_{k[[t]]} f = \mathrm{ind}^{(k/m)((t))}_{(k/m)[[t]]} f = -w(f \bmod m) = -w(f).$$

3.4.2. *Definition of the Contou-Carrère symbol.* Let $f, g \in k((t))^\times$ be given. Let $\{a_i\}$ and $\{b_j\}$ be the systems of Witt parameters associated to f and g, respectively. Put

$$\langle f,g\rangle := (-1)^{w(f)w(g)}\cdot\frac{a_0^{w(g)}}{b_0^{w(f)}}\cdot\frac{\prod_{i=1}^\infty\prod_{j=1}^\infty\left(1-a_i^{j/(i,j)}b_{-j}^{i/(i,j)}\right)^{(i,j)}}{\prod_{i=1}^\infty\prod_{j=1}^\infty\left(1-a_{-i}^{j/(i,j)}b_{j}^{i/(i,j)}\right)^{(i,j)}}.$$

The right side of the definition makes sense because all but finitely many factors in the infinite products differ from 1. This definition is due to Contou-Carrère [3]. We call the map

$$\langle\cdot,\cdot\rangle : k((t))^\times \times k((t))^\times \to k^\times$$

defined by the formula above the *Contou-Carrère symbol*. The symbol is clearly anti-symmetric:

$$\langle f, g\rangle = \langle g, f\rangle^{-1}.$$

Although it is not immediately evident from the definition, the symbol is also bimultiplicative:

$$\langle f', g\rangle = \langle f, g\rangle\langle f', g\rangle, \quad \langle f, gg'\rangle = \langle f, g\rangle\langle f, g'\rangle.$$

The following result establishes bimultiplicativity of the Contou-Carrère symbol as a byproduct.

Theorem 3.4.3. *For all $f, g \in k((t))^\times$ we have*

$$\langle f, g\rangle^{-1} = (-1)^{w(f)w(g)}\{f, g\}^{k((t))}_{k[[t]]}$$

where on the right side we view f and g as elements of the restricted general linear group $G^{k((t))}_{k[[t]]}$.

Before beginning the proof proper we prove a couple of lemmas. We say that a polynomial $f \in k[t]$ is *distinguished* if f is monic in t and $f \equiv t^{\deg f} \bmod m$, in which case necessarily $w(f) = \deg f$.

Lemma 3.4.4. *Fix a distinguished polynomial $f \in k[t]$ of degree n and $g \in k[[t]]^\times$. (i) The quotient of the power series ring $k[[t]]$ by its principal ideal (f) is free over k and the monomials $1, t, \ldots, t^{n-1}$ form a k-basis. (ii) We have*

$$\{f, g\}^{k((t))}_{k[[t]]} = \det(g|k[[t]]/(f)).$$

Proof. Statement (i) is a special case of the Weierstrass Division Theorem. From statement (i) it follows that the diagram

$$\begin{array}{ccccc}
k[[t]] & \emptyset & k[[t]] & \emptyset & k[[t]] \\
\emptyset & & \emptyset & & \emptyset \\
k[[t]] & \emptyset & k[[t]] & \emptyset & k[[t]] \\
\{f^{-1}t^i\}_{i=0}^{n-1} & & \{f^{-1}t^i\}_{i=0}^{n-1} & & \{gf^{-1}t^i\}_{i=0}^{n-1} \\
f^{-1}\cdot k[[t]] & \emptyset & f^{-1}\cdot k[[t]] & \emptyset & f^{-1}\cdot k[[t]]
\end{array}$$

is a template for the calculation of $\{g, f^{-1}\}^{k((t))}_{k[[t]]}$. Statement (ii) now follows from the four square identity. □

Lemma 3.4.5. *Let $f, g \in k[t]$ be distinguished polynomials. We have*

$$\{f, g\}^{k((t))}_{k[[t]]} = 1.$$

Proof. Since

$$f, g \in G^{k((t))}_{k[[t]]} \cap G^{k((t))}_{t^{-1}k[t^{-1}]},$$

we have

$$\{f, g\}^{k((t))}_{k[[t]]}\{f, g\}^{k((t))}_{t^{-1}k[t^{-1}]} = 1$$

by Proposition 3.3.4. Let p and q be the degrees of f and g, respectively. Now consider the template

$$\begin{array}{ccccccc}
t^{-1}k[t^{-1}] & \emptyset & t^{-1}k[t^{-1}] & \{t^i\}_{i=0}^{p-1} & t^{p-1}k[t^{-1}] \\
\emptyset & & \emptyset & & \emptyset \\
t^{-1}k[t^{-1}] & \emptyset & t^{-1}k[t^{-1}] & \{t^i\}_{i=0}^{p-1} & t^{p-1}k[t^{-1}] \\
\{t^i\}_{i=0}^{q-1} & & \{t^i\}_{i=0}^{q-1} & & \{ft^i\}_{i=0}^{q-1} \\
t^{q-1}k[t^{-1}] & \emptyset & t^{q-1}k[t^{-1}] & \{gt^i\}_{i=0}^{p-1} & t^{p+q-1}k[t^{-1}]
\end{array}$$

for the calculation of $\{f,g\}_{t^{-1}k[t^{-1}]}^{k((t))}$. By the four square identity we conclude that the latter symbol equals unity, and we are done. □

Lemma 3.4.6. *For all $f, g \in k[[t]]^\times$ we have*

$$\{f,g\}_{k[[t]]}^{k((t))} = 1.$$

Proof. In view of the formal properties noted in §3.1.3, this is clear. □

3.4.7. *Proof of Theorem 3.4.3.* Every element of $k((t))^\times$ factors as a power of t times a distinguished polynomial times a unit of $k[[t]]$. So after making the evident reductions based upon Lemmas 3.4.5 and 3.4.6, we may assume without loss of generality that f is a distinguished polynomial and that $g \in k[[t]]^\times$. By Lemma 3.4.4 we have

$$\{f,g\}_{k[[t]]}^{k((1/t))} = \det(g|k[[t]]/(f)).$$

The ratio of left and right sides above remains unchanged if we multiply g by any element of $k^\times$. We therefore may assume without loss of generality that $g(0) = 1$. Left and right sides above depend multiplicatively on g. Moreover, since t operates nilpotently on the quotient $k[[t]]/(f)$, there exists a positive integer N such that

$$\det(1 + t^N h|k[[t]]/(f)) = 1$$

for all $h \in k[[t]]$. We therefore may assume without loss of generality that

$$g = 1 - bt^q$$

for some positive integer q and $b \in k$. We may also assume without loss of generality that

$$f = t^p - a$$

for some positive integer p and $a \in m$. Finally, we have

$$\det\left(1 - bt^q|k[[t]]/(t^p - a)\right) = \left(1 - a^{q/(p,q)}b^{p/(p,q)}\right)^{(p,q)},$$

as can be verified by a straightforward calculation that we omit. We are done. □

3.4.8. *Reparameterization invariance.* It is easily verified that for any $\tau \in k((t))$ of winding number 1, the operation

$$(f(t) \mapsto f(\tau)) : k((t)) \to k((t)) \quad (\text{“substitution of } \tau \text{ for } t\text{”})$$

is a k-linear automorphism of $k((t))$ belonging to the restricted general linear group $G^{k((t))}_{k[[t]]}$. Via the commutator interpretation provided by Theorem 3.4.3, it follows that the Contou-Carrère symbol is invariant under reparameterization of $k((t))$.

3.4.9. *Recovery of the tame symbol and the residue.* If k is a field, the Contou-Carrère symbol obviously reduces to the tame symbol. It is possible also to recover the residue from the Contou-Carrère symbol, as follows. Take $k = F[\epsilon]/(\epsilon^3)$ where F is any field. Then we have

$$\langle 1 - \epsilon f, 1 - \epsilon g \rangle \equiv 1 - \epsilon^2 \operatorname{Res}_{t=0}(g\, df) \bmod \epsilon^3$$

for all $f, g \in F((t))$ as can be verified by a straightforward calculation. This last observation suggests an interpretation of our work as the “integrated version” of Tate's Lie-theoretic theory [8]. We hope that Beilinson's multidimensional generalization [2] of Tate's theory can analogously be integrated.

3.4.10. *The case in which k is a $\mathbb{Q}$-algebra.* Suppose k is a $\mathbb{Q}$-algebra. Let $f \in 1 + m((t))$ and $g \in k((t))^\times$ be given. We have

$$\langle f, g \rangle = \exp(\operatorname{Res}_{t=0} \log f \cdot d \log g)$$

as can be verified by a straightforward calculation. This is quite similar in form to the commutator formula given by Segal-Wilson [7, Prop. 3.6].

4. Reciprocity laws on curves

4.1. The common setting for the reciprocity laws.

4.1.1. *Basic data.* Let F be an algebraically closed field. Let X/F be a nonsingular complete algebraic curve. Let S be a finite nonempty set of closed points of X. For any ring or group A, put

$$A^S := \{(a_s)_{s \in S} | a_s \in A\} = (\text{product of copies of } A \text{ indexed by } S).$$

For each $s \in S$ select a uniformizer π_s at s.

4.1.2. *Construction of R_0.* For each meromorphic function f on X put

$$f^{(s)} := \sum_i a_i t^i \in F((t))$$

where

$$f = \sum_i a_i \pi_s^i \quad (a_i \in F)$$

is the Laurent expansion of f in powers of π_s. Put

$$R_0 := \{(f^{(s)})_{s \in S} \in F((t))^S \mid f \in H^0(X \setminus S, \mathcal{O}_X)\}.$$

The F-algebra R_0 is a copy of the affine coordinate ring of $X \setminus S$. We take for granted that

$$\dim_F F[[t]]^S \cap R_0 = \dim_F H^0(X, \mathcal{O}_X) = 1 < \infty$$

and

$$\dim_F \frac{F((t))^S}{R_0 \oplus F[[t]]^S} = \dim_F H^1(X, \mathcal{O}_X) = \text{genus of } X < \infty.$$

As in the papers [1], [6], [8], it is these finiteness statements from algebraic geometry that lead inevitably to reciprocity laws.

4.1.3. *Extension of scalars from F to k.* We assume now that the artinian local ring k taken as base for the theory of determinant groupoids is a finite F-algebra. We put

$$R := R_0 \otimes_F k = (k\text{-span of } R_0) \subset k((t))^S,$$

and

$$V := k((t))^S, \quad V_+ := k[[t]]^S.$$

Note that the k-modules $V_+ \cap R$ and $V/(R + V_+)$ are free of finite rank. Note that $R^\times$ acting in natural k-linear fashion on V is contained in the restricted general linear group $G^V_{V_+}$.

4.2. **A reciprocity law for the Contou-Carrère symbol.**

Theorem 4.2.1. *In the setting above, for all $f, g \in R^\times$ we have*

$$\prod_{s\in S} \langle f_s, g_s \rangle = 1.$$

Proof. Clearly there exists some F-subspace $M_0 \subset F((t))^S$ commensurable to $F[[t]]^S$ such that $F((t))^S = M_0 \oplus R_0$. Put $M := M_0 \otimes_F k$. Then we have

$$V = M \oplus R, \quad M \sim V_+$$

and hence we have

$$\{f, g\}^V_{V_+} = \{f, g\}^V_M = \{f, g\}^V_M \{f, g\}^V_R = 1.$$

The first two equalities are justified by the basic properties enumerated in §3.1.3 and the last by Proposition 3.3.4. We also have

$$\{f, g\}^V_{V_+} = \prod_{s\in S} \prod_{s'\in S} \{f_s, g_{s'}\}^{k((t))}_{k[[t]]} = (-1)^{(\sum_s w(f_s))(\sum_s w(g_s))} \cdot \prod_{s\in S} \langle f_s, g_s \rangle^{-1}.$$

The first equality is justified the basic properties enumerated in §3.1.3 and Propositions 3.3.2. The second equality is justified by Proposition 3.3.3 and Theorem 3.4.3. Finally, we have

$$\sum_{s\in S} w(f_s) = \sum_{s\in S} w(f_s \bmod m) = 0$$

because the second sum is the degree of a principal divisor on X. The result follows. $\square$

4.2.2. *Coordinate-independence of the local symbol $\langle f_s, g_s \rangle$.* In §3.4.8 we explained that the Contou-Carrère symbol is reparameterization invariant. In the present context, it follows that the value of the symbol $\langle f_s, g_s \rangle$ is independent of the choice π_s of uniformizer at s, and thus is coordinate-independent.

4.2.3. *Recovery of Weil reciprocity.* Take $k = F$. In this case the Contou-Carrère symbol reduces to the tame symbol, and hence Theorem 4.2.1 reduces to Weil reciprocity.

4.2.4. *Recovery of sum-of-residues-equals-zero.* Take $k = F[\epsilon]/(\epsilon^3)$. In this case, as explained in §3.4.9, the residue can be recovered from the Contou-Carrère symbol, and hence sum-of-residues-equals-zero can be recovered from Theorem 4.2.1.

4.3. Recovery of Witt's explicit reciprocity law.

4.3.1. *Quick review of Witt vectors.* Witt vectors were introduced in Witt's paper [9]. The basic theory—proofs omitted—takes the following form. For proofs, we recommend to the reader the exercises on this topic in Lang's algebra text [4]. Let

$$\{\epsilon\} \coprod \{\mathbf{x}_i, \mathbf{y}_i\}_{i=1}^{\infty}$$

be a family of independent variables. Write

$$\prod_{i=1}^{\infty}((1-\mathbf{x}_i\epsilon^i)(1-\mathbf{y}_i\epsilon^i)) = \prod_{i=1}^{\infty}(1-\mathbf{A}_i\epsilon^i),$$

$$\prod_{i=1}^{\infty}\prod_{j=1}^{\infty}\left(1-\mathbf{x}_i^{j/(i,j)}\mathbf{y}_j^{i/(i,j)}\epsilon^{ij/(i,j)}\right)^{(i,j)} = \prod_{i=1}^{\infty}(1-\mathbf{M}_i\epsilon^i),$$

thereby defining families of polynomials

$$\left\{\mathbf{A}_n, \mathbf{M}_n \in \mathbb{Z}\left[\{\mathbf{x}_i, \mathbf{y}_i\}_{i|n}\right]\right\}_{n=1}^{\infty}.$$

For any commutative ring A with unit and finite subset Δ of the set of positive integers closed under passage to divisors, let $\mathbb{W}_\Delta(A)$ denote the set of vectors with entries in A indexed by Δ. It can be shown that the $\mathbf{A}$'s and $\mathbf{M}$'s define addition and multiplication laws with respect to which $\mathbb{W}_\Delta(A)$ becomes a commutative ring with unit, functorially in commutative rings A with unit. Below we do not actually need to use the multiplication law in $\mathbb{W}_\Delta(A)$, but we mention its definition because it provides another way to see that the Contou-Carrère symbol is bimultiplicative.

4.3.2. *Ghost coordinates.* Consider the family of polynomials

$$\left\{\tilde{\mathbf{x}}_n := \sum_{d|n} d\mathbf{x}_d^{n/d}\right\}_{n=1}^{\infty}.$$

These polynomials are characterized by the power series identity

$$-\log\prod_{i=1}^{\infty}(1-\mathbf{x}_i\epsilon^i) = \sum_{\nu=1}^{\infty}\frac{\tilde{\mathbf{x}}_\nu\epsilon^\nu}{\nu}.$$

Given a ring A, a finite subset Δ of the set of positive integers closed under passage to divisors, $x = (x_i \in A)_{i\in\Delta} \in \mathbb{W}_\Delta(A)$ and an integer $i \in \Delta$, we write $\tilde{x}_i$ for the result of substituting x_d for $\mathbf{x}_d$ in $\tilde{\mathbf{x}}_i$ for all $d \in \Delta$, and we call $\tilde{x}_i$ the *ghost coordinate* of x indexed by i; in this context, for emphasis, we say that x_i is the *live coordinate* of x indexed by i. Addition and multiplication have a very simple expression in ghost coordinates:

$$\tilde{\mathbf{A}}_n = \tilde{\mathbf{x}}_n + \tilde{\mathbf{y}}_n, \quad \tilde{\mathbf{M}}_n = \tilde{\mathbf{x}}_n\tilde{\mathbf{y}}_n.$$

Clearly each variable $\mathbf{x}_n$ has a unique expansion as a polynomial in the $\tilde{\mathbf{x}}$'s with coefficients in $\mathbb{Q}$. It follows that for any $\mathbb{Q}$-algebra A the ring $\mathbb{W}_\Delta(A)$ decomposes in ghost coordinates as a product of copies of A indexed by Δ. But in general it is not possible to write $\mathbf{x}_n$ as a polynomial in the $\tilde{\mathbf{x}}$'s with integral coefficients, and hence in general $\mathbb{W}_\Delta(A)$ depends in a complicated way on A.

4.3.3. *Remark.* The focus in arithmetical applications of Witt vectors is usually on the case $\Delta \subset \{1, p, p^2, \dots\}$ for some rational prime p. In this case, for example, we have the striking fact that

$$\mathbb{W}_{\{1,p,\dots,p^{n-1}\}}(\mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}/p^n\mathbb{Z}.$$

But it is simpler to deal with the ring schemes of the form

$$\mathbb{W}_{\leq N} := \mathbb{W}_{\{1,\dots,N\}}.$$

The additive group scheme underlying the ring scheme $\mathbb{W}_{\leq N}$ is fairly easy to handle because the map

$$x = (x_i)_{i=1}^N \mapsto \prod_{i=1}^N (1 - x_i \epsilon) \bmod \epsilon^{N+1}$$

identifies the additive group underlying $\mathbb{W}_{\leq N}(A)$ with the group of units in $A[\epsilon]/(\epsilon^{N+1})$ congruent to 1 modulo (ϵ) functorially in commutative rings A with unit. Since the ring $\mathbb{W}_{\{1,p,\dots,p^{n-1}\}}(A)$ is a quotient of the ring $\mathbb{W}_{\leq p^{n-1}}(A)$ functorially in A, it turns out that we really lose no generality by thus restricting our focus.

4.3.4. *Definition of the symbol* $\mathrm{Res}^{\mathbb{W}}_{\leq N}$. Let us turn our attention back to the setting of Theorem 4.2.1. Fix a positive integer N. We now take

$$k := F[\epsilon]/(\epsilon^{N+1}).$$

We define a pairing

$$\mathrm{Res}^{\mathbb{W}}_{\leq N}(\cdot,\cdot) : F((t))^\times \times \mathbb{W}_{\leq N}(F((t))) \to \mathbb{W}_{\leq N}(F)$$

by the rule

$$\left\langle f, \prod_{i=1}^N \left(1 - x_i \epsilon^i\right) \right\rangle \equiv \prod_{i=1}^N \left(1 - \epsilon^i \left(\mathrm{Res}^{\mathbb{W}}_{\leq N}(f,x)\right)_i\right) \bmod (\epsilon^{N+1})$$

where $\langle \cdot,\cdot \rangle$ is the Contou-Carrère symbol.

4.3.5. *Comparison with Witt's original definition.* The pairing $\mathrm{Res}^{\mathbb{W}}_{\leq N}$ is essentially the pairing introduced in Witt's paper [9]. Without giving full details, we briefly explain this point as follows. Assume for the moment that F is of characteristic zero so that we can talk about ghost coordinates, and recall the remark of §3.4.10. We have

$$\left.\begin{array}{rl} & \log \left\langle f, \prod_{i=1}^N \left(1 - \epsilon^i x_i\right) \right\rangle \\ \equiv & \mathrm{Res}_{t=0} \left(-\log \left(\prod_{i=1}^N (1 - \epsilon^i x_i) \right) \cdot \dfrac{d \log f}{f} \right) \\ \equiv & \mathrm{Res}_{t=0} \left(\sum_{i=1}^N \dfrac{\tilde{x}_i \epsilon^i}{i} \cdot \dfrac{d\log f}{f} \right) \\ \equiv & \sum_{i=1}^N \left(\mathrm{Res}_{t=0} \left(\tilde{x}_i \dfrac{df}{f} \right) \right) \dfrac{\epsilon^i}{i} \end{array}\right\} \bmod (\epsilon^{N+1}).$$

In other words, we have

$$\widetilde{\mathrm{Res}^{\mathbb{W}}_{\leq N}(f,x)}_i = \mathrm{Res}_{t=0}\left(\tilde{x}_i \frac{df}{f}\right)$$

for $i = 1, \ldots, N$. This last formula for $i = 1, p, \ldots, p^{n-1}$ and F of characteristic $p > 0$ is exactly the expression in ghost coordinates of the rule used by Witt [9, p. 130] to define his pairing. But *a priori* Witt's definition is no good in characteristic p because live coordinates cannot in general be expressed as polynomials in the ghost coordinates with p-integral coefficients. Nevertheless, Witt succeeds in making the definition rigorous (see [9, Satz 4, p. 130]) by proving that the corresponding expression in live coordinates of his pairing is "denominator-free" and hence does make sense in arbitrary characteristic. Of course, with the hindsight afforded by Theorem 4.2.1, Witt's Satz 4 is not very difficult to check.

4.3.6. *Reciprocity for the symbol* $\mathrm{Res}^{\mathbb{W}}_{\leq N}$. We return to the situation in which the algebraically closed field F may be of any characteristic. As above, we fix a positive integer N. We then have

$$\sum_{s \in S} \mathrm{Res}^{\mathbb{W}}_{\leq N}(f_s, x_s) = 0$$

for all

$$f \in R_0^\times \subset F((t))^{\times S}, \quad x \in \mathbb{W}_{\leq N}(R_0) \subset \mathbb{W}_{\leq N}(k((t))^S) = \mathbb{W}_{\leq N}(k((t)))^S$$

by Theorem 4.2.1 and the definitions. We emphasize that the addition is to be performed in the group $\mathbb{W}_{\leq N}(F)$. From this last formula in the case that F is of characteristic p and $N = p^{n-1}$, it is not difficult to deduce the reciprocity law stated without proof on the last page of Witt's paper [9] in the case of an algebraically closed ground field of characteristic p. We omit further details.

5. Acknowledgements

The first-named author wishes to thank the mathematics department at the University of Salamanca for its hospitality during a two week period in May 2002 when much of the work on this paper was done. The first-named author became acquainted with determinant groupoids from the perspective of mathematical physics through some lectures on algebraic models of loop spaces by M. Kapranov in Spring 2002 at the University of Minnesota, and gratefully acknowledges that influence. The first-named author also wishes to thank the mathematics department at the University of Arizona for the opportunity to lecture on preliminary versions of some of these ideas at the Winter School of March 2000.

References

[1] Arbarello, E.; De Concini, C.; Kac, V. G.: *The infinite wedge representation and the reciprocity law for algebraic curves.* Theta functions—Bowdoin 1987, Part 1 (Brunswick, ME, 1987), 171–190, Proc. Sympos. Pure Math., **49**, Part 1, Amer. Math. Soc., Providence, RI, 1989.

[2] Beilinson, A. A.: *Residues and adèles. (Russian)* Funktsional. Anal. i Prilozhen. **14** (1980), no. 1, 44–45. {English translation: Functional Anal. Appl. **14** (1980), no. 1, 34–35.}

[3] Contou-Carrère, C.: *Jacobienne locale, groupe de bivecteurs de Witt universel, et symbole modéré. (French) [Local Jacobian, universal Witt bivector group, and tame symbol]* C. R. Acad. Sci. Paris Sér. I Math. **318** (1994), no. 8, 743–746.

[4] Lang, S.: *Algebra. Revised third edition.* Graduate Texts in Mathematics, **211**. Springer-Verlag, New York, 2002.

[5] Matsumura, H.: *Commutative algebra. Second edition.* Mathematics Lecture Note Series, **56**. Benjamin/Cummings Publishing Co., Inc., Reading, Mass., 1980.
[6] Pablos Romo, F.: *On the Tame Symbol of an Algebraic Curve.* Comm. Algebra. **30**(2002), no. 9, 4349–4368.
[7] Segal, G.; Wilson, G.: *Loop groups and equations of KdV type.* Inst. Hautes Etudes Sci. Publ. Math. **61**(1985), 5–65.
[8] Tate, J.: *Residues of differentials on curves.* Ann. Sci. Ecole Norm. Sup. (4) 1 1968 149–159.
[9] Witt, E.: *Zyklische Körper und Algebren der Charakteristik p vom Grad p^n.* J. Reine Angew. Math. **176**(1937), 126–140.