Journal of Generalized Lie Theory and Applications Vol. 3 (2009), No. 4, 297–310

Arithmetic Witt-hom-Lie algebras

Daniel LARSSON

Høgskolen i Oslo, Pb 4, St. Olavs plass, 0130 Oslo, Norway
E-mail: daniel.larsson@iu.hio.no

Abstract

This paper is concerned with explaining and further developing the rather technical definition of a hom-Lie algebra given in a previous paper which was an adaption of the ordinary definition to the language of number theory and arithmetic geometry. To do this we here introduce the notion of Witt-hom-Lie algebras and give interesting arithmetic applications, both in the Lie algebra case and in the hom-Lie algebra case. The paper ends with a discussion of a few possible applications of the developed hom-Lie language.

2000 MSC: 17B99, 14G99, 11G05, 11R99, 13F99

1 Introduction

The main purpose of this note is to explain the rather technical definition of a hom-Lie algebra given in [4] (in addition to motivating why I made that definition) and to provide a few novel examples of distinct number theoretical flavour.

Let me point out, however, that in order to draw any serious and deep conclusions of a number-theoretical nature from the association with hom-Lie algebras, one needs to know more of the finer structure of hom-Lie algebras, something that is yet to be investigated. On the other hand, a recent preprint [1] proves that hom-Lie algebras are actually Lie algebras in a suitably braided category[1]. This should certainly aid in the study of the structural characteristics of hom-Lie algebras. In fact, this result implies that every structural result on Lie algebras should have a precise hom-Lie analogue. Therefore, most results on Lie algebras should be transferrable (in principle, at least) to a hom-Lie version. This is something that certainly should be studied further.

The contents of the paper is as follows. Section 2 deals with the definition of hom-Lie algebra and hom-Lie structure, both as given in [4] and in a slightly different, but equivalent, way that might be more easily understood from a purely algebraic point of view. Section 3 introduces Witt-Lie algebras in a general way and shows that already this "un-twisted" case is full of potential number theory, such as Gauss sums and CM-elliptic curves. Section 4 generalizes the Witt-Lie algebras to Witt-hom-Lie algebras and this is then studied in some detail. Interspersed throughout the text are questions and suggestions for further study.

In the final few subsections of the paper, we give some "teasers" how the constructions introduced might be used in arithmetic. I am rather confident that there are interesting structures here waiting to be unveiled, both with respect to the study of hom-Lie algebras and the study of arithmetic and geometry.

Finally let me issue a warning: Some parts of this paper require more background than others and I do not always indicate what this background is. However, in most instances, I give pointers to the relevant literature where details may be found.

[1] This is something the present author has suspected for some time, see [4].

Notations. The following notations will be adhered to throughout.

- Λ will denote a commutative, associative integral domain with unity.
- $\mathsf{Com}(\Lambda)$ ($\mathsf{Com}(B)$, etc.) denotes the category of commutative, associative Λ-algebras (B-algebras, etc) with unity. Morphisms of Λ-algebras (B-algebras, etc.) are always unital, i.e., $\phi(1) = 1$.
- $A^\times$ is the set of units in A (i.e., the set of invertible elements).
- $\mathrm{End}_\Lambda(A)$ denotes the Λ-module of Λ-algebra morphisms on A.
- $\circlearrowleft_{a,b,c}(\cdot)$ will mean cyclic addition of the expression in bracket.
- Sch denotes the category of schemes; Sch/S denotes the category of schemes over S (i.e., the category of S-schemes) where S is some base scheme.
- When writing actions of group elements, we will alternatively use $\sigma(a)$ and a^σ, depending on the context.
- The notation A^g, A^G will denote the fixed ring of $g \in G$ and G, respectively, i.e.,
$$A^g := \big\{a \in A \mid a^g = a\big\}, \quad A^G := \big\{a \in A \mid a^g = a, \text{ for all } g \in G\big\}$$
- A will always denote an abelian group.

2 The basic constructions

Here we work "backwards" compared to the definition given in [4], as we feel that this might give a somewhat more natural (i.e., less "Bourbaki-ist") introduction going from the special to the general.

2.1 Hom-Lie structures

2.1.1 Hom-Lie algebras

Let A be a Λ-algebra and L an A-module. (Those who prefer can think of $\Lambda = A = \mathbb{F}$, a field, and L, an $\mathbb{F}$-vector space.) Assume that σ is a Λ-linear endomorphism on L.

Definition 2.1. A *hom-Lie algebra* on L is a tuple $(L, \langle\cdot,\cdot\rangle, \sigma)$, where $\langle\cdot,\cdot\rangle$ is Λ-bilinear product satisfying

(hL1.) $\langle a, a\rangle = 0$, for all $a \in L$;
(hL2.) $\circlearrowleft_{a,b,c}\big(\langle a^\sigma + a, \langle b, c\rangle\rangle\big) = 0$.

A morphism of hom-Lie algebras $(L, \langle\cdot,\cdot\rangle, \sigma)$ and $(L', \langle\cdot,\cdot\rangle', \sigma')$ is a Λ-module morphism $f : L \to L'$ such that $\sigma' \circ f = f \circ \sigma$.

Remark 2.2. One could wonder why the Λ-module A is there at all since everything in the definition is Λ-linear. But this is to allow greater flexibility as it will hopefully become clear later.

Let G be a group of endomorphisms on L. We define a *G-hom-Lie structure* on L to be a collection of hom-Lie algebras parametrized by the elements of G. More to the point, a G-hom-Lie structure on L is a family of hom-Lie algebras

$$\mathbf{L}(G) := \big\{(L, \langle\cdot,\cdot\rangle_\sigma, \sigma) \mid \sigma \in G\big\}$$

Morphisms of G-hom-Lie structures are bit more subtle to define: let $\mathbf{L}(G)$ and $\mathbf{L}'(G')$ be two G-hom-Lie structures (with different G's and underlying A-modules). Then a morphism $\mathbf{L}(G) \to \mathbf{L}'(G')$ is a pair (ϕ_L, ϕ_G) consisting of a Λ-module morphism $\phi_L : L \to L'$ and a group morphism $\phi_G : G \to G'$ such that

$$\phi_L \circ \sigma = \phi_G(\sigma) \circ \phi_L \quad \text{for all } \sigma \in G$$

and such that

$$\phi_L\big(\langle a, b\rangle_\sigma\big) = \big\langle \phi_L(a), \phi_L(b)\big\rangle_{\phi_G(\sigma)}$$

The fact that G is a group means that any G-hom-Lie structure includes a Lie algebra corresponding to the unit element of G. This Lie algebra may, or may not, be the abelian Lie algebra. In this way, the G-hom-Lie structure can be viewed as a family of "deformations" of the Lie algebra in $\mathbf{L}(G)$ (strictly speaking there could be Lie algebras in the family corresponding to group elements different from the unit), making the notion of G-hom-Lie structure a very pleasing and intuitive construction.

Let me also remark that the "deformations" in the hom-Lie families are *not* "quasi-deformations" in the sense of [5]. To recall, the quasi-deformation concept, can loosely be thought of as "deformations" of certain representations of Lie algebras. On the other hand, here the Lie algebras themselves are "deformed" (while not in any continuous, flat or other "geometric" ways) in the category of hom-Lie algebras.

The following base-change result was proved in [4]; here it is rephrased in the present usage of hom-Lie algebras.

Theorem 2.3. *Let $(L, \sigma, \langle\cdot,\cdot\rangle)$ be a hom-Lie algebra over a ring A and let $A \to B$ be a morphism of A-algebras. Then*

$$\big(L \otimes_A B, \sigma \otimes \mathrm{id}, \langle\cdot,\cdot\rangle \otimes (\,\circ\,)\big)$$

where $(\,\circ\,)$ denotes the multiplication in B, is a hom-Lie algebra over B.

It is very easy to prove this directly; we leave this to the reader.

2.1.2 Substructures

It is obvious what is to be meant by *sub-hom-Lie algebra*. However, there is another notion that is natural to consider here, namely, *sub-hom-Lie structures*.

Let (L, G) be a G-hom-Lie structure, where L is an A-module and G a group acting on L (and possibly also A). Then an **H-sub-hom-Lie structure** of (L, G) is a pair (K, H) together with two injections $K \hookrightarrow L$ and $H \hookrightarrow G$. Notice that this includes the cases where either of these is the identity.

2.1.3 Quotient structures

Dualizing, let (L, G) be a G-hom-Lie structure over A; then a **quotient hom-Lie structure** is an H-hom-Lie structure (K, H) and a pair of surjections $L \twoheadrightarrow K$ and $G \twoheadrightarrow H$.

2.1.4 Changing groups

Let $H \to G$ be a group morphism and L a G-hom-Lie structure. Notice that this means, in particular, that we have a representation $\rho : G \to \mathrm{End}(L)$. Clearly, restriction induces a H-hom-Lie structure on L via

$$\begin{tikzcd}
 & \mathrm{End}(L) \\
H \arrow[r] \arrow[ur, dashed] & G \arrow[u, "\rho"']
\end{tikzcd}$$

Hence, in particular, this holds for H a subgroup of G, thus inducing a sub-hom-Lie structure.

Similarly, for a surjection $\phi : G \twoheadrightarrow H$ and a G-hom-Lie structure L, we get an induced quotient H-hom-Lie structure on $L^{\ker(\phi)}$.

2.2 Global Hom-Lie structures

The "global" definition given in [4] was a bit more restrictive than necessary. Therefore, there is some discrepancies in the wording of the one below and the one from [4]. I think that the one given here should be inclusive enough for most arithmetic circumstances.

Fix a scheme $S \in \mathrm{ob}(\mathsf{Sch})$. Let $(S)_{\mathsf{fl}}$ denote the (big) flat site associated with S. To recall, this is the category of morphisms $U \to S$ (the "open sets" of S), locally of finite type, with the obvious morphisms, $U \in \mathrm{ob}(\mathsf{Sch})$. The covering families are families of flat morphisms $(U_i \to U)_i$, where $i \in I$ for some index set I. For more details on this see [6] for instance. By $\mathcal{G}$ we denote a sheaf of groups on $(S)_{\mathsf{fl}}$. Let $\mathcal{W}$ be a sheaf of $\mathcal{G}$-sets over $(S)_{\mathsf{fl}}$, i.e., a sheaf $\mathcal{W}$ over $(S)_{\mathsf{fl}}$ together with an action of $\mathcal{G}(U)$ on $\mathcal{W}(U)$ for $U \to S$.

The reason for this generality is that for arithmetic and geometric purposes, it is advantageous to allow for more general topologies than the Zariski topology; for instance étale topology [6] or the positive topology [8]. (Of course, we could use any topological space as base here, i.e., not necessarily restricting our discussion to schemes.)

Let $\mathcal{O}$ be the structure sheaf on $(S)_{\mathsf{fl}}$ in the sense that $\mathcal{O}_{U,\mathsf{fl}} := \mathcal{O}(U) := H^0(U, \mathcal{O}_U)$ for $U \in \mathrm{ob}((S)_{\mathsf{fl}})$ and let $\mathcal{A}$ be a sheaf of $\mathcal{O}$-algebras. We denote by $\mathcal{F}$ an $\mathcal{A}$-module. Let $\mathcal{G}$ be a sheaf of groups over $(S)_{\mathsf{fl}}$ acting $\mathcal{O}$-linearly on $\mathcal{F}$.

Definition 2.4. Given the above data, a *hom-Lie structure for* $\mathcal{G}$, or $\mathcal{G}$*-hom-Lie structure, on* $(S)_{\mathsf{fl}}$ is a $\mathcal{G}$-sheaf of $\mathcal{A}$-modules $\mathcal{F}$ together with, for each covering $(U_i \to U)_i$, $U \in \mathrm{ob}((S)_{\mathsf{fl}})$, an $\mathcal{O}(U_i)$-bilinear product $\langle\,\cdot,\cdot\,\rangle_i := \langle\,\cdot,\cdot\,\rangle(U_i)$ on $\mathcal{F}(U_i)$ such that

(hL1.) $\langle a, a\rangle_i = 0$, for all $a \in \mathcal{F}(U_i)$;

(hL2.) $\circlearrowleft_{a,b,c} \big(\langle a^g + a, \langle b, c\rangle_i\rangle_i\big) = 0$, for all $g \in \mathcal{G}(U_i)$.

A morphism of hom-Lie structures $(\mathcal{F}, \mathcal{G})$ and $(\mathcal{F}', \mathcal{G}')$ is a pair (f, ψ) consisting of a morphism of $\mathcal{O}$-modules $f : \mathcal{F} \to \mathcal{F}'$ and a morphism of group schemes $\psi : \mathcal{G} \to \mathcal{G}'$, such that $f \circ g = \psi(g) \circ f$, and $f_i(\langle a, b\rangle_{\mathcal{F},i}) = \langle f_i(a), f_i(b)\rangle_{\mathcal{F}',i}$, where we have put $f_i := f(U_i)$.

We thus get a category $\mathsf{HomLieStruc}_S$ of all hom-Lie structures on $(S)_{\mathsf{fl}}$ with morphisms given in the definition.

Hence, a hom-Lie structure is a family of (possibly isomorphic) products parametrized by $\mathcal{G}$. A product $\langle\,\cdot,\cdot\,\rangle_g$, for fixed $g \in \mathcal{G}$, is a *hom-Lie algebra on* $\mathcal{F}$.

In all cases, $\mathcal{G}$ is a constant sheaf of groups, i.e., $\mathcal{G}(U) = G$, for all $U \to S$, where G is a group (or group scheme over S). We will assume this from now on.

2.2.1 Specialization

When we only consider one open set $U = S$, Definition 2.4 specializes to

- $\mathcal{O}_X \rightsquigarrow \mathfrak{o} \in \mathrm{ob}(\mathsf{Com}(k))$;
- $\mathcal{A} \rightsquigarrow A \in \mathrm{ob}(\mathsf{Com}(\mathfrak{o}))$;
- $\langle\,\cdot,\cdot\,\rangle_{g,i} \rightsquigarrow \langle\,\cdot,\cdot\,\rangle_g$ (only one product for each $g \in G$).

When we need to specify the difference of the above case and Definition 2.4, we call this the *special case* and Definition 2.4 the *global case* (and so the global case includes the special).

3 Arithmetic Witt-Lie algebras

We will now introduce the notion of "arithmetic Witt algebras". These are graded Lie algebras coming endowed with obvious number-theoretical content. The notion of "generalized Witt algebras" have been around for a few decades and there are several more or less equivalent ways to define this; we have chosen one that is suitable for our present needs, namely, number theory. We have not been able to find this arithmetic application anywhere in the literature. In the next section we will generalize this to "Witt-hom-Lie algebras", taking into account "Galois structures".

3.1 Witt-Lie algebras

The classical Witt-Lie algebra $W_{\mathbb{C}}(\mathbb{Z},\underline{1})$ (the reason for the unorthodox notation will be clear from the discussion below) is defined as the complexified polynomial vector fields on the unit circle. More to the point

$$W_{\mathbb{C}}(\mathbb{Z},\underline{1})=\mathbb{C}\big[z,z^{-1}\big]\big[\partial_z\big]\quad\text{with}\quad\langle z^n\partial_z,z^m\partial_z\rangle=(m-n)z^{n+m}\partial_z$$

induced from the commutator. It is clearly $\mathbb{Z}$-graded.

This can be generalized as follows. Let A be an abelian group written additively and let $\chi^{\mathrm{a}}:\mathsf{A}\to\mathit{\Lambda}$, where $\mathit{\Lambda}$ is an integral domain (this assumption is kept throughout), be a 1-dimensional character, i.e., a group morphism into the additive group of $\mathit{\Lambda}$ (the superscript "a" is there to remind us that the character is additive). Denote by $W_{\mathbb{Z}}(\mathsf{A})$ the free $\mathbb{Z}$-module spanned by the formal symbols $\{\boldsymbol{w}(g)\mid g\in\mathsf{A}\}$. Let $\mathit{\Lambda}\to T$ be a $\mathbb{Z}$-algebra morphism, i.e., $T\in\mathrm{ob}(\mathsf{Com}(\mathit{\Lambda}))$. First define

$$\boldsymbol{w}(g)\cdot\boldsymbol{w}(h):=\alpha(g,h)\boldsymbol{w}(g+h)$$

where $\alpha:\mathsf{A}\times\mathsf{A}\to\mathit{\Lambda}$ is a $\mathit{\Lambda}$-valued, symmetric group 2-cocycle, i.e., a map $\alpha:\mathsf{A}\times\mathsf{A}\to\mathit{\Lambda}$ satisfying

$$\alpha(h,k)\alpha(g,h+k)=\alpha(g,h)\alpha(g+h,k),\quad\alpha(g,h)=\alpha(h,g)$$

Then define a $\mathit{\Lambda}$-linear product on the base extension to T,

$$W_T\big(\mathsf{A},\chi^{\mathrm{a}},\alpha\big):=W_{\mathbb{Z}}(\mathsf{A})\otimes_{\mathbb{Z}}T$$

as follows:

$$\big\langle a\boldsymbol{w}(g),b\boldsymbol{w}(h)\big\rangle:=\big(a\boldsymbol{w}(g)\big)^{\sigma}\cdot\big(b\boldsymbol{w}(h)\big)-\big(b\boldsymbol{w}(h)\big)^{\sigma}\cdot\big(a\boldsymbol{w}(g)\big),\quad a,b\in T\tag{3.1}$$

where $(a\boldsymbol{w}(g))^{\sigma}:=-a\chi^{\mathrm{a}}(g)\boldsymbol{w}(g)$ and similarly for $(b\boldsymbol{w}(h))^{\sigma}$. Notice that $(\cdot)^{\sigma}$ does not define a multiplicative map unless χ^{a} is multiplicative[2]. The above construction gives the structure constants

$$\big\langle a\boldsymbol{w}(g),b\boldsymbol{w}(h)\big\rangle=ab\chi^{\mathrm{a}}(h-g)\alpha(h,g)\boldsymbol{w}(g+h)\tag{3.2}$$

and it is easy to check that this defines an A-graded Lie algebra called the *Witt algebra of* $(\mathsf{A},\chi^{\mathrm{a}},\alpha)$.

[2] The reason for introducing this slightly awkward construction is to keep a suitable analogy with a later one; see Section 4.

As to not be drown in awkward notation we will most often, instead of the correct $\chi^{\mathrm{a}}(g)$, simply write g, remembering that g is strictly an element of a group and not of the ring T. This will certainly not cause any severe confusion. When confusion does lurk, χ^{a} is favored and used. Consequently, we also drop χ^{a} from the notation $W_T(\mathsf{A}, \chi^{\mathrm{a}}, \alpha)$.

Notice that the above $W_T(\mathsf{A}, \alpha)$ actually is, as a T-*module*, the (twisted) group algebra

$$T[\mathsf{A}] = \left\{ \sum_{\text{finite}} a_g \boldsymbol{w}(g) \mid g \in \mathsf{A},\ a_g \in T,\ \boldsymbol{w}(g)\boldsymbol{w}(h) = \alpha(g,h)\boldsymbol{w}(g+h) \right\}$$

We will find this description more suitable in what follows. Therefore, it is strongly graded and crystalline in the sense of [7].

Remark 3.1. The above can be considered the "rank one" case of the following construction. Let S be an A-set (i.e., a set together with an action of A). Form the set of formal symbols $\{\boldsymbol{w}_s(g) \mid s \in S,\ g \in \mathsf{A}\}$. Define the multigraded Lie product

$$\big\langle \boldsymbol{w}_s(g), \boldsymbol{w}_t(h) \big\rangle := h(s)\boldsymbol{w}_s(g+h) - g(t)\boldsymbol{w}_t(g+h)$$

We will however stick to the "rank one" case.

Remark 3.2. We remark also that this construction is functorial. Indeed, define the category $\mathsf{Ab}^{(3)}$ as the category whose objects are triples $(\mathsf{A}, \chi^{\mathrm{a}}, \alpha)$ and morphisms group morphisms $\mathsf{A} \xrightarrow{f} \mathsf{B}$ such that $\chi^{\mathrm{a}}_{\mathsf{B}} \circ f = \chi^{\mathrm{a}}_{\mathsf{A}}$ and $\alpha_{\mathsf{B}} \circ (f \times f) = \alpha_{\mathsf{A}}$. Then W_T is a functor from $\mathsf{Ab}^{(3)}$ to the category Lie of Lie algebras.

To show that this is actually a very general notion (although we will generalize further), let us give a few simple examples.

Example 3.3. We first consider two simple examples.

(a) The classical case is the Witt algebra for $(\mathbb{Z}, \underline{1})$ with $T = \mathit{\Lambda} = \mathbb{C}$, the unit (principal) character $\mathbb{Z} \to \mathbb{C}$ and α the constant 2-cocycle $\underline{1} : (g,h) \mapsto 1$.

(b) Take $\mathsf{A} = \mathbb{F}_p$ and $T = \mathit{\Lambda} = \mathbb{F}_p$, $\alpha = \underline{1}$. Now, $W_{\mathbb{F}_p}(\mathbb{F}_p, \underline{1})$ is the algebra that E. Witt actually studied. This can be given the following more conventional description. Consider the following $\mathbb{F}_p$-vector space:

$$\operatorname{Der}_{\mathbb{F}_p}\big(\mathbb{F}_p[t]/(t^p)\big) = \bigoplus_{i=0}^{p-1} \mathbb{F}_p t^i \partial_t$$

This is a Lie algebra under the commutator. In fact, we have the following isomorphism of Lie algebras:

$$W_{\mathbb{F}_p}(\mathbb{F}_p, \underline{1}) \xrightarrow{\simeq} \operatorname{Der}_{\mathbb{F}_p}\big(\mathbb{F}_p[t]/(t^p)\big), \quad a\boldsymbol{w}(i) \longmapsto a t^i \partial_t, \quad \text{for } i \in \mathbb{F}_p$$

When $p \neq 2$, these are simple (modular) Lie algebras.

Clearly, more elaborate versions of these examples can be constructed by varying A and/or α.

We will now give two more sophisticated examples coming from arithmetic.

3.1.1 Witt algebras from elliptic curves

Let K be a field and let $\mathscr{E}$ be an elliptic curve over K. Let $\mathbf{D}$ be a K-algebra.

By the Mordell-Weil theorem, the group of L-rational points $\mathscr{E}(L)$, for L/K a finite extension of number fields, is a finitely generated abelian group. In addition, the group of N-torsion points $\mathscr{E}[N] := \mathscr{E}(K^{\mathrm{alg}})[N]$, where K^{alg} denotes the algebraic closure of K, i.e., the group of all points $p \in \mathscr{E}(K^{\mathrm{alg}})$ such that $N \cdot p = p + p + \cdots + p = 0$ (N times), is isomorphic to $(\mathbb{Z}/N\mathbb{Z})^2$. This holds in general when K is a field of characteristic prime to N. The full group of torsion points $\mathscr{E}_{\mathrm{tors}}$ is the union of all $\mathscr{E}[N]$ (we assume here that $\mathrm{char}(K) = 0$).

Using these groups we can now form three natural Witt algebras. Namely,

- $W_{\mathbf{D}}(\mathscr{E}(L), \alpha) = \mathbf{D}[\mathscr{E}(L)]$, with $\chi^{\mathrm{a}} : \mathscr{E}(L) \to K$, $\alpha : \mathscr{E} \times \mathscr{E} \to K$;
- $W_{\mathbf{D}}(\mathscr{E}[N], \alpha) = \mathbf{D}[\mathscr{E}[N]]$, with $\chi^{\mathrm{a}} : \mathscr{E}[N] \to K$, $\alpha : \mathscr{E}[N] \times \mathscr{E}[N] \to K$;
- $W_{\mathbf{D}}(\mathscr{E}_{\mathrm{tors}}, \alpha) = \mathbf{D}[\mathscr{E}_{\mathrm{tors}}]$, with $\chi^{\mathrm{a}} : \mathscr{E}_{\mathrm{tors}} \to K$, $\alpha : \mathscr{E}_{\mathrm{tors}} \times \mathscr{E}_{\mathrm{tors}} \to K$.

There are several interesting possibilities for the K-algebra $\mathbf{D}$. For instance, (a) $\mathbf{D} = L$, a field over K; (b) $\mathbf{D} = \mathfrak{o}_L$, considered as an $\mathfrak{o}_K$-algebra; (c) $\mathbf{D} = \mathrm{End}(\mathscr{E})$, where $K = \mathbb{Z}$; (d) $\mathbf{D} = K_\nu$, where ν is a (discrete) valuation of K, and K_ν the completion of K with respect to ν; of course, we could also consider the ring of integers $\mathfrak{o}_\nu$.

The case (c) is interesting only when $\mathrm{End}(\mathscr{E}) \supset \mathbb{Z}$, the *complex multiplication* (CM) case.

Remark 3.4. Assume that K is a field. Since $\mathbf{D}$ is an $\mathfrak{o}_K$-algebra, $W_{\mathbf{D}}(\mathscr{E}[N], \alpha)$ (for instance) is also an $\mathfrak{o}_K$-module. This means that $W_{\mathbf{D}}(\mathscr{E}[N], \alpha)$ sheafifies to a quasi-coherent sheaf $\widetilde{W_{\mathbf{D}}(\mathscr{E}[N], \alpha)}$ on the 1-dimensional arithmetic scheme $\mathrm{Spec}(\mathfrak{o}_K)$. Therefore, we get a sheaf of Lie algebras over $\mathrm{Spec}(\mathfrak{o}_K)$.

This example will be even more interesting in the context of hom-Lie algebras.

3.1.2 A cyclotomic Witt-Lie algebra

Let $\mathsf{A} = \mathbb{Z}/p\mathbb{Z}$, where p is prime. We will also consider the multiplicative group $\mathsf{A}^\times = (\mathbb{Z}/p\mathbb{Z})^\times$ of units. In this case, a natural choice of additive character will be $\chi^{\mathrm{a}}(a \pmod p) := a \in \mathbb{Z}$.

Furthermore, let $\underline{\boldsymbol{\mu}}_n$ be the group of nth roots of unity. Take $T = \Lambda = \mathbb{Q}(\underline{\boldsymbol{\mu}}_n)$, the nth cyclotomic field, and pick a Dirichlet character $\vartheta : \mathsf{A}^\times \to \underline{\boldsymbol{\mu}}_n \subset \mathbb{Q}(\underline{\boldsymbol{\mu}}_n)$, i.e., a character ϑ such that $\vartheta(gh) = \vartheta(g)\vartheta(h)$. Extend ϑ to a character on the whole A by defining $\vartheta(0) = 0$, unless ϑ is the principal (unit) character ϑ_0 in which case we define $\vartheta_0(0) = 1$. There is nothing stopping us from letting $T \neq \Lambda$ below. In fact, convenience is the only reason for assuming equality here.

We get

$$W_{\mathbb{Q}(\underline{\boldsymbol{\mu}}_n)}(\mathsf{A}, \alpha) = W_{\mathbb{Z}}(\mathsf{A}) \otimes_{\mathbb{Z}} \mathbb{Q}(\underline{\boldsymbol{\mu}}_n) = \left\{ \sum_{\text{finite}} a_g \boldsymbol{w}(g) \mid a_g \in \mathbb{Q}(\underline{\boldsymbol{\mu}}_n) \right\}$$

where α is a 2-cocycle, with the $\mathbb{Q}(\underline{\boldsymbol{\mu}}_n)$-linear Lie algebra structure given by (3.2). Inside this $\mathbb{Q}(\underline{\boldsymbol{\mu}}_n)$-vector space there is an element on the form

$$\mathsf{G}(\vartheta) := -\sum_{g \in \mathsf{A}} \vartheta(g) \boldsymbol{w}(g)$$

a so-called *Gauss sum.* Recall that $(h-g)$ is actually $\chi^{\mathrm{a}}(h-g)$. Letting ϑ^* be another character, we can compute

$$\big\langle \mathsf{G}(\vartheta), \mathsf{G}\big(\vartheta^*\big)\big\rangle = \sum_g \sum_h \vartheta(g)\vartheta^*(h)(h-g)\alpha(h,g)\boldsymbol{w}(g+h)$$

Introducing the anti-symmetric pairing

$$\cdot\perp\cdot : \mathsf{A} \times \mathsf{A} \longrightarrow \mathbb{Q}\big(\underline{\boldsymbol{\mu}}_n\big)$$

defined by

$$(\cdot\perp\cdot)(a,b) := a\perp b := \vartheta(a)\vartheta^*(b) - \vartheta(b)\vartheta^*(a),$$

we have the following nice description of $\langle \mathsf{G}(\vartheta), \mathsf{G}(\vartheta^*)\rangle$.

Proposition 3.5. *Given the above, we have*

$$\big\langle \mathsf{G}(\vartheta), \mathsf{G}\big(\vartheta^*\big)\big\rangle = \sum_{k\in\mathsf{A}} \left(\sum_{g+h=k} (h-g)\alpha(g,h)(g\perp h) \right) \boldsymbol{w}(k)$$

Proof. The proof is a simple computation and is omitted. □

Example 3.6. For an explicit example consider the two Dirichlet characters on $(\mathbb{Z}/5\mathbb{Z})^\times$ (extended to $\mathbb{Z}/5\mathbb{Z}$) defined by

$$\vartheta := \big\{\vartheta(1) = 1,\ \vartheta(2) = i,\ \vartheta(3) = -i,\ \vartheta(4) = -1\big\}$$

and

$$\vartheta^* := \big\{\vartheta^*(1) = 1,\ \vartheta^*(2) = -1,\ \vartheta^*(3) = -1,\ \vartheta^*(4) = 1\big\}$$

Now we compute

$$\left\{ \begin{array}{lll} 1\perp 2 = -(1+i), & 1\perp 3 = i-1, & 1\perp 4 = 2, \\ 2\perp 3 = -2i, & 2\perp 4 = i-1, & 3\perp 4 = -(1+i) \end{array} \right\}$$

and so, using the proposition, we get

$$\begin{aligned} \big\langle \mathsf{G}(\vartheta), \mathsf{G}\big(\vartheta^*\big)\big\rangle &= \big(3\alpha(1,4)(1\perp 4) + \alpha(2,3)(2\perp 3)\big)\boldsymbol{w}(0) + \alpha(2,4)(2\perp 4)\boldsymbol{w}(1) \\ &\quad + \alpha(3,4)(3\perp 4)\boldsymbol{w}(2) + \alpha(1,2)(1\perp 2)\boldsymbol{w}(3) + \alpha(1,3)(1\perp 3)\boldsymbol{w}(4) \\ &= \big(6\alpha(1,4) - 2i\alpha(2,3)\big)\boldsymbol{w}(0) + (i-1)\alpha(2,4)\boldsymbol{w}(1) - (1+i)\alpha(3,4)\boldsymbol{w}(2) \\ &\quad - (1+i)\alpha(1,2)\boldsymbol{w}(3) + (i-1)\alpha(1,3)\boldsymbol{w}(4) \end{aligned}$$

Notice that, even in the case $\alpha = \underline{1}$, $\langle \mathsf{G}(\vartheta), \mathsf{G}(\vartheta^*)\rangle$ is not a Gauss sum, since the coefficients are not the image of some Dirichlet character (the images of which are all roots of unity). But there is more: even though, by definition, $\mathsf{G}(\vartheta)$ and $\mathsf{G}(\vartheta^*)$ have no $\boldsymbol{w}(0)$ term, their product $\langle \mathsf{G}(\vartheta), \mathsf{G}(\vartheta^*)\rangle$ in general has. Hence, this product is in general not even a $\mathbb{Q}(\underline{\boldsymbol{\mu}}_n)$-linear combination of Gauss sums.

Remark 3.7. Normally, when computing with Gauss sums, the symbols $\boldsymbol{w}(g)$ are powers of some primitive mth root of unity ζ_m, e.g., $\boldsymbol{w}(g) = \zeta_m^g$. Therefore, the Gauss sums are elements in the relative extension $\mathbb{Q}(\underline{\boldsymbol{\mu}}_n)(\zeta_m)$. These extensions are rather cumbersome to work with, even when $\gcd(m, n) = 1$, so working with symbols, as we have done, clarifies computations in our opinion.

We will use a generalization of Gauss sums further on. Therefore, let L/K be a finite Galois extension. Choose a multiplicative character $\vartheta : \mathrm{Gal}(L/K) \to L^\times$ such that $\vartheta^n = 1$, $n \leq [L/K]$. Then the so-called *resolvent* is the group algebra element

$$\big(\cdot \mid \vartheta\big) := \sum_{\sigma \in \mathrm{Gal}(L/K)} \vartheta(\sigma)\boldsymbol{w}(\sigma) \in L\big[\mathrm{Gal}(L/K)\big] = W_L\big(\mathrm{Gal}(L/K), \alpha\big)$$

(where the last equality is as vector spaces). We consider $(\cdot \mid \vartheta)$ as an operator on L:

$$\big(\cdot \mid \vartheta\big)(x) := \big(x \mid \vartheta\big) := \sum_{\sigma \in \mathrm{Gal}(L/K)} \vartheta(\sigma) x^\sigma$$

In other words, $\boldsymbol{w}(\sigma)$ acts on L as σ. The element $(\cdot \mid \vartheta)$ satisfies the following property: for any $\tau \in \mathrm{Gal}(L/K)$ and $x \in L$, we have

$$\tau\big(\big(x \mid \vartheta\big)\big) = \vartheta^{-1}(\tau)\big(x \mid \vartheta\big) \tag{3.3}$$

where ϑ^{-1} is the inverse character. As consequences we have

$$\tau\big(\big(x \mid \vartheta\big)^n\big) = \big(x \mid \vartheta\big)^n \quad \tau^n\big(\big(x \mid \vartheta\big)\big) = \big(x \mid \vartheta\big)$$

Gauss sums are the result of the above when $L/K = \mathbb{Q}(\underline{\boldsymbol{\mu}}_p)/\mathbb{Q}$, in which case $\mathrm{Gal}(\mathbb{Q}(\underline{\boldsymbol{\mu}}_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$. Particularly interesting is the case when ϑ is the unique order-two character, namely the Legendre symbol $(\cdot/p)$, or more generally of course, mth power residue symbols. We leave it to the reader to express the product of two resolvents in analogy with the Gauss sum above. Notice, however, that this is only possible for *abelian* extensions L/K.

For an idea of why Gauss sums (or resolvents) are of utmost importance in number theory, see [2] for instance.

These examples show that there is indeed interesting arithmetic for ordinary Lie algebras. Despite this we will up the stakes and give a hom-Lie algebra generalization of the above to show that we can capture significantly more arithmetic by (for instance) explicitly involving the Galois structure (where present). Actually, this case will in some sense be more natural than the Lie algebra case given above.

4 Arithmetic Witt-hom-Lie structures

Let as before A be an abelian group with a character $\chi^{\mathrm{a}} : \mathsf{A} \to \mathit{\Lambda}$ which will be (almost) constantly suppressed. Furthermore, let T be a $\mathit{\Lambda}$-domain, $G \subseteq \mathrm{Aut}_{\mathit{\Lambda}}(T)$ a subgroup together with a representation $\rho : G \to \mathrm{GL}(V)$, where V is a $\mathsf{Frac}(T)$-vector space (where $\mathsf{Frac}(T)$ denotes field of fractions of T). Let χ be the character of ρ. If the image of χ is not in T, make a base extension to $T \otimes_{\mathbb{Z}} \mathbb{Z}[\mathrm{im}\,\chi]$.

Consider $W_T(\mathsf{A}, \chi) = \mathbb{Z}[\mathsf{A}] \otimes_{\mathbb{Z}} T$ as the group algebra $T[\mathsf{A}]$, spanned by formal symbols $\boldsymbol{w}(g)$, $g \in \mathsf{A}$. Let $\sigma \in G$ be an algebra endomorphism on T and extend to $W_T(\mathsf{A}, \chi)$ as

$$\sigma\big(\boldsymbol{w}(g)\big) := \chi(\sigma)^{\chi^{\mathrm{a}}(g)}\boldsymbol{w}\big(g^\sigma\big) = \chi(\sigma)^g\boldsymbol{w}\big(g^\sigma\big) \quad \text{(Tate twist)}$$

and then linearly as

$$\sigma\big(a\boldsymbol{w}(g)+b\boldsymbol{w}(h)\big):=a^{\sigma}\sigma\big(\boldsymbol{w}(g)\big)+b^{\sigma}\big(\boldsymbol{w}(h)\big)$$

This defines an algebra endomorphism on $W_T(\mathsf{A},\chi)$; we define $(g+h)^{\sigma}:=g^{\sigma}+h^{\sigma}$, i.e., we demand that σ acts as a group endomorphism on A. Notice that we have yet to decide how to interpret $\boldsymbol{w}(g^{\sigma})$ and $\boldsymbol{w}(h^{\sigma})$. Define once again

$$\boldsymbol{w}(g)\cdot\boldsymbol{w}(h):=\alpha(g,h)\boldsymbol{w}(g+h)\quad\text{for }\alpha:\mathsf{A}\times\mathsf{A}\longrightarrow\Lambda$$

a symmetric 2-cocycle. We assume that $\alpha(g^{\sigma},h)=\alpha(g,h)$. Let E be a T-module and make the base extension $E(\mathsf{A}):=E\otimes_T T[\mathsf{A}]$. The T-module $W_T(\mathsf{A},\chi)=T[\mathsf{A}]$ acts on $E(\mathsf{A})$ as

$$(ag)(e\otimes h):=(ae)\otimes(gh)\quad\text{for }a\in T,\ g,h\in\mathsf{A},\ e\in E$$

Extend the action of G on T to a *semilinear* action on E:

$$(ae)^{\bar\sigma}:=\sigma(a)\bar\sigma(e)\quad\text{for }a\in T,e\in E\text{ and }\sigma\in G$$

Now we twist the action of G on E (and thus on T) as

$$(ae)^{\wedge\bar\sigma}:=\ell\big(\operatorname{id}-\bar\sigma\big)(ae)\quad\text{for }\ell\in T^{\sigma}\tag{4.1}$$

Then $\Delta_\sigma:=\ell(\operatorname{id}-\bar\sigma)$ (we suppress the dependence on ℓ in the notation) is a twisted derivation on E, i.e., a linear map $E\to E$ satisfying

$$\Delta_\sigma(ae)=\delta(a)e+a^{\sigma}\Delta_\sigma(e),\quad a\in T,\ e\in E,$$

and where δ is the induced twisted derivation $\delta:=\ell(\operatorname{id}-\sigma)$ on $T[\mathsf{A}]=W_T(\mathsf{A},\chi)$. We extend the action of $\bar\sigma$ to $E[\mathsf{A}]$ via the Tate twist. Explicitly,

$$\bar\sigma\big(e\otimes\boldsymbol{w}(g)\big):=\bar\sigma(e)\otimes\sigma\big(\boldsymbol{w}(g)\big)=\chi(\sigma)^{g}\bar\sigma(e)\otimes\boldsymbol{w}\big(g^{\sigma}\big)$$

This is a semilinear action of G on $E[\mathsf{A}]$. It follows that Δ_σ can be extended canonically to $E[\mathsf{A}]$. Assume that $(\operatorname{Ann}(\Delta_\sigma))^{\sigma}\subseteq\operatorname{Ann}(\Delta_\sigma)$, where

$$\operatorname{Ann}\big(\Delta_\sigma\big):=\big\{a\in T[\mathsf{A}]\mid a\Delta_\sigma(e)=0,\ \text{for all }e\in E[\mathsf{A}]\big\}$$

The left $T[\mathsf{A}]$-module $T[\mathsf{A}]\cdot\Delta_\sigma=T[\mathsf{A}]\Delta_\sigma$ is a hom-Lie algebra by [3, 4] under the product

$$\langle\!\langle a\boldsymbol{w}(g)\Delta_\sigma,b\boldsymbol{w}(h)\Delta_\sigma\rangle\!\rangle:=\big(a\boldsymbol{w}(g)\big)^{\sigma}\Delta_\sigma\big(b\boldsymbol{w}(h)\Delta_\sigma\big)-\big(b\boldsymbol{w}(h)\big)^{\sigma}\Delta_\sigma\big(a\boldsymbol{w}(g)\Delta_\sigma\big)$$

We denote this by $W_T^{\mathrm{hL}}(\mathsf{A},\alpha,\chi,\sigma)^{\Delta}$. Letting σ vary over G, we get the G-hom-Lie structure

$$\mathbf{W}_T^{\mathrm{hL}}(G)^{\Delta}:=\big\{W_T^{\mathrm{hL}}(\mathsf{A},\sigma)^{\Delta}\mid\sigma\in G\big\}$$

where we, as shown, often omit α and χ from the notation since these are fixed in the G-hom-Lie structure.

Using the twisted Leibniz rule we find the structure constants:

$$\begin{aligned}\langle\!\langle a\boldsymbol{w}(g)\Delta_\sigma,b\boldsymbol{w}(h)\Delta_\sigma\rangle\!\rangle&=\Big(\big(a\boldsymbol{w}(g)\big)^{\sigma}\Delta_\sigma\big(b\boldsymbol{w}(h)\big)-\big(b\boldsymbol{w}(h)\big)^{\sigma}\Delta_\sigma\big(a\boldsymbol{w}(g)\big)\Big)\Delta_\sigma\\&=\ell\alpha(g,h)\big(a^{\sigma}b\chi(\sigma)^{g}\boldsymbol{w}(g^{\sigma}+h)-b^{\sigma}a\chi(\sigma)^{h}\boldsymbol{w}(h^{\sigma}+g)\big)\Delta_\sigma\end{aligned}\tag{4.2}$$

Notice that, unless $g^{\sigma}=g$ for all $g\in\mathsf{A}$, this product is not graded. We refer to it as a "σ-twisted grading". In [3] there are explicit examples of this phenomenon.

Remark 4.1. The above constructions are all functorial on suitably defined categories, just as in Remark 3.2. However, the constructions involve a lot of notation so, since this will not be important for us, we omit it, but invite the interested reader to construct these possible categories for her- or himself.

4.1 Alternative construction

We keep the notation and conventions from before (but here T does not have to be a domain) and introduce the product

$$\langle\!\langle a\boldsymbol{w}(g), b\boldsymbol{w}(h)\rangle\!\rangle := \ell\big((a\boldsymbol{w}(g))^{\sigma}\cdot\big(b\boldsymbol{w}(h)\big)-\big(b\boldsymbol{w}(h)\big)^{\sigma}\cdot\big(a\boldsymbol{w}(g)\big)\big) \tag{4.3}$$

on the *algebra* $W_T(\mathsf{A},\chi)=T[\mathsf{A}]$. The G-hom-Lie structure thus constructed is denoted by

$$\mathbf{W}_T^{\mathrm{hL}}(G)=\big\{W_T^{\mathrm{hL}}(\mathsf{A},\sigma)\mid\sigma\in G\big\}$$

(compare with $\mathbf{W}_T^{\mathrm{hL}}(G)^{\Delta}$ from the previous section). Now we compute

$$\begin{aligned}\langle\!\langle a\boldsymbol{w}(g), b\boldsymbol{w}(h)\rangle\!\rangle &:= \ell\big(\big(a\boldsymbol{w}(g)\big)^{\sigma}b\boldsymbol{w}(h)-\big(b\boldsymbol{w}(h)\big)^{\sigma}a\boldsymbol{w}(g)\big)\\ &= \ell\big(a^{\sigma}\chi(\sigma)^{g}\boldsymbol{w}(g)^{\sigma}b\boldsymbol{w}(h)-b^{\sigma}\chi(\sigma)^{h}\boldsymbol{w}(h)^{\sigma}a\boldsymbol{w}(g)\big)\\ &= \ell\alpha(g,h)\big(a^{\sigma}\chi(\sigma)^{g}b\boldsymbol{w}\big(g^{\sigma}+h\big)-b^{\sigma}\chi(\sigma)^{h}a\boldsymbol{w}\big(g+h^{\sigma}\big)\big)\end{aligned}$$

There are two important points to make here: (1) Notice that

$$\langle\!\langle a\boldsymbol{w}(g), b\boldsymbol{w}(h)\rangle\!\rangle = a^{\sigma}\chi(\sigma)^{g}b\boldsymbol{w}\big(g^{\sigma}+h\big)-b^{\sigma}\chi(\sigma)^{h}a\boldsymbol{w}\big(g+h^{\sigma}\big) \tag{4.4}$$

from the above computation is the analogue of equation (3.2); (2) observe that (4.4) is *exactly* the "algebra factor" in the structure constant equation (4.2). This means that (4.2) and (4.4) define isomorphic hom-Lie algebras (under suitable conditions). That (4.4) indeed defines a hom-Lie algebra follows as a special case of [4, Theorem 3.1] (or can be proven directly with a straight-forward, albeit tedious, computation).

We will now use the above construction to generalize the Gauss sum construction from a previous section.

4.1.1 Gauss sums in Witt-hom-Lie algebras

Let L/K be an *abelian* Galois extension and put $\mathsf{A}:=\mathrm{Gal}(L/K)$. By $\vartheta,\vartheta^*:\mathrm{Gal}(L/K)\to L^{\times}$, we denote two multiplicative characters of order $n\le\#\mathsf{A}$. We will now consider the Gauss sums (resolvents)

$$\mathsf{G}(\vartheta):=\big(\cdot\mid\vartheta\big):=\sum_{g\in\mathsf{A}}\vartheta(g)\boldsymbol{w}(g),\quad \mathsf{G}\big(\vartheta^*\big):=\big(\cdot\mid\vartheta^*\big):=\sum_{g\in\mathsf{A}}\vartheta^*(g)\boldsymbol{w}(g)$$

and their products in $W_L^{\mathrm{hL}}(\mathsf{A},\chi,\sigma,\alpha)$, where $\sigma\in\mathrm{End}_K(L)$ (not necessarily in $\mathrm{Gal}(L/K)$), $\alpha:\mathsf{A}\times\mathsf{A}\to K$, a 2-cocycle. We define the action of A on $\boldsymbol{w}(g)$ as

$$\boldsymbol{w}(g)^{\tau}:=\chi(\tau)^{\chi^{\mathrm{a}}(g)}\boldsymbol{w}(\tau+g)=\chi(\tau)^{g}\boldsymbol{w}(\tau g)$$

To confuse things we will sometimes write the product in A as "+" and sometimes as composition "τg". Also, we define $g^{\tau}:=\tau g$. Just as for the previous case we can compute

$$\langle\!\langle\mathsf{G}(\vartheta),\mathsf{G}\big(\vartheta^*\big)\rangle\!\rangle=\sum_{g\in\mathsf{A}}\sum_{h\in\mathsf{A}}\vartheta(g)\vartheta^*(h)\langle\!\langle\boldsymbol{w}(g),\boldsymbol{w}(h)\rangle\!\rangle$$

Now,

$$\langle\!\langle\boldsymbol{w}(g),\boldsymbol{w}(h)\rangle\!\rangle=\boldsymbol{w}(g)^{\sigma}\cdot\boldsymbol{w}(h)-\boldsymbol{w}(h)^{\sigma}\cdot\boldsymbol{w}(g)$$

$$
\begin{aligned}
&= \chi(\sigma)^g \boldsymbol{w}(g^\sigma)\boldsymbol{w}(h) - \chi(\sigma)^h \boldsymbol{w}\big(h^\sigma\big)\boldsymbol{w}(g) \\
&= \chi(\sigma)^g \alpha(g,h)\boldsymbol{w}\big(g^\sigma + h\big) - \chi(\sigma)^h \alpha(h,g)\boldsymbol{w}\big(h^\sigma + g\big) \\
&= \alpha(g,h)\big(\chi(\sigma)^g - \chi(\sigma)^h\big)\boldsymbol{w}(\sigma g h)
\end{aligned}
$$

where we, in the last equality, used that A is abelian, α symmetric and that $g^\sigma = \sigma g$.

We now have the obvious generalization of Proposition 3.5 with essentially the same proof.

Proposition 4.2. *Given the above, we have*

$$\langle\!\langle \mathsf{G}(\vartheta), \mathsf{G}\big(\vartheta^*\big)\rangle\!\rangle = \sum_{k\in\mathsf{A}} \left(\sum_{g+h=k} \big(\chi(\sigma)^g - \chi(\sigma)^h\big)\alpha(g,h)(g\perp h) \right) \boldsymbol{w}(k)$$

4.1.2 CM-Elliptic curves and Witt-hom-Lie algebras

In this subsection we freely use concepts from complex multiplication and class field theory. Most (all?) of what is used here can be found in [9, Chapter 2].

Let K be an imaginary quadratic number field, i.e., $K = \mathbb{Q}(\sqrt{-d})$, $d > 0$ a square-free integer. Furthermore, let $\mathscr{E}$ be an elliptic curve over a field F with complex multiplication by the ring of integers $\mathfrak{o}_K$ in K, i.e., $\mathrm{End}(\mathscr{E}) \simeq \mathfrak{o}_K$.

Then the theory of complex multiplication tells us that $K(j(\mathscr{E}))$, where $j(\mathscr{E})$ is the j-invariant of $\mathscr{E}$, is the Hilbert class field of K. In addition, the field $L_{(N)} := K(j(\mathscr{E}), \mathscr{E}[N])$ is a finite abelian extension of $K(j(\mathscr{E}))$ for all N. The extension $L_{(N)}/K$ is *not* necessarily abelian. In fact, we have the following exact sequence:

$$1 \longrightarrow \mathrm{Gal}\big(L_{(N)}/K(j(\mathscr{E}))\big) \longrightarrow \mathrm{Gal}(L_{(N)}/K) \xrightarrow{\text{res}} \mathrm{Gal}\big(K\big(j(\mathscr{E})\big)/K\big) \longrightarrow 1$$

implying that $\mathrm{Gal}(L_{(N)}/K)$ is the semi-direct product

$$\mathrm{Gal}\big(L_{(N)}/K\big) = \mathrm{Gal}\big(K\big(j(\mathscr{E})\big)/K\big) \ltimes \mathrm{Gal}\big(L_{(N)}/K\big(j(\mathscr{E})\big)\big)$$

Now, we have

$$\big[\mathbb{Q}\big(j(\mathscr{E})\big)/\mathbb{Q}\big] = \big[K\big(j(\mathscr{E})\big)/K\big] = h(K)$$

where $h(K)$ is the class number of K and the Artin (reciprocity) map induces an isomorphism

$$\mathsf{Cl}\big(\mathfrak{o}_K\big) \xrightarrow{\simeq} \mathrm{Gal}\big(K\big(j(\mathscr{E})\big)/K\big)$$

with $\mathsf{Cl}(\mathfrak{o}_K)$ denoting the class group of K.

Obviously, with this setup we have several interesting possibilities for constructing Witt-hom-Lie structures. Consider, for instance,

$$T = L_{(N)}, \quad \mathsf{A} = \mathrm{Gal}\big(K\big(j(\mathscr{E})\big)/K\big)$$

Then $\mathrm{Gal}(L_{(N)}/K)$ acts on both $L_{(N)}$ and the grading group via the restriction morphism

$$\text{res}: \quad \mathrm{Gal}(L_{(N)}/K) \twoheadrightarrow \mathrm{Gal}\big(K\big(j(\mathscr{E})\big)/K\big)$$

In this way we get a $\mathrm{Gal}(L_{(N)}/K)$-Witt-hom-Lie structure $\mathbf{W}_T^{\mathrm{hL}}(\mathrm{Gal}(L_{(N)}/K))$, or, alternatively, a $\mathrm{Gal}(L_{(N)}/K)$-structure $\mathbf{W}_T^{\mathrm{hL}}(\mathrm{Gal}(L_{(N)}/K))^{\Delta}$ (as discussed before).

Remark 4.3. The actual structure of the hom-Lie algebras (structures) thus constructed remains to be investigated, but let me express some doubt as to whether such an investigation will have any deep implications for number theory.

4.1.3 Galois representations

We keep the assumptions from the previous subsection, except that $\mathscr{E}$ is not necessarily a CM-curve.

Consider now the case when $m = p$ a prime. Then

$$\varprojlim K\big[\mathscr{E}[p^n]\big] = \varprojlim K\Big[\big(\mathbb{Z}/p^n\mathbb{Z}\big)^2\Big] = K\Big[\big(\mathbb{Z}_p\big)^2\Big], \quad \text{(the “Tate group algebra over } K\text{”)}$$

where $\mathbb{Z}_p$ is the ring of p-adic integers. Given $\alpha : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \to K$ a 2-cocycle, we can lift this to a 2-cocycle $\alpha_p : \mathbb{Z}_p \times \mathbb{Z}_p \to K$ via the successive $\mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$.

Twisting the action of G_K on $(K\big[(\mathbb{Z}_p)^2\big], \alpha_p)$ to $\ell(\mathrm{id} - \sigma)$, for $\sigma \in G_K$ and $\ell \in K$, gives us a G_K-Witt-hom-Lie structure

$$\mathbf{W}_K^{\mathrm{hL}}(G_K) := \Big\{W_K^{\mathrm{hL}}\Big(\big(\mathbb{Z}_p\big)^2, \chi, \alpha_p, \sigma\Big) \mid \sigma \in G_K\Big\}$$

Of course, there is nothing to stop you from taking some K-algebra instead of K and some other 2-cocycle instead of the induced α_p.

Ideally, this construction would give us alternative ways to study Galois representations, i.e., representations of (absolute) Galois groups, in the form of hom-Lie structures. Thus, in a sense, we are in this way constructing “twisted Galois representations”.

We can sheafify $K[(\mathbb{Z}_p)^2]$ to a sheaf over $\mathrm{Spec}(\mathfrak{o}_K)$ and in this way we get a family of modular twisted Galois representations. (The details here is yet to be worked out.)

4.1.4 Rational points on abelian varieties

The study of rational points on abelian varieties is of fundamental importance in arithmetic and Diophantine geometry. Here we barely indicate how hom-Lie methods might aid in this study, leaving a more detailed exposition to a later treatise.

Let $\mathscr{A}$ be an abelian variety over a number field K. Clearly, $G_K := \mathrm{Gal}(K^{\mathrm{alg}}/K)$ acts on the L-rational points $\mathscr{A}(L)$ on $\mathscr{A}$, where $L \supseteq K$ is a field extension. The Mordell-Weil theorem says that, if $L \supseteq K$ is finite, then $\mathscr{A}(L) = \mathbb{Z}^r \oplus \mathscr{A}(L)_{\mathrm{tors}}$. It is well known that $\mathscr{A}(L)_{\mathrm{tors}}$ is finite for all finite extensions $L \supseteq K$. Equally well known is that the N-torsion points

$$\mathscr{A}[N] = \mathscr{A}(\mathbb{C})[N] \simeq (\mathbb{Z}/N\mathbb{Z})^{2d}, \quad \text{where } d = \dim_K \mathscr{A}$$

Since $\mathscr{A}(L)_{\mathrm{tors}}$ is finite, we have that $\mathscr{A}(L)[N]$ is finite. But $\mathscr{A}\big(K^{\mathrm{alg}}\big)[N] \subseteq \mathscr{A}[N]$, so $\mathscr{A}(K^{\mathrm{alg}})[N]$ is also finite.

By definition, $\mathscr{A}(L)$ is an abelian group, so $K[\mathscr{A}(L)]$ is a commutative group algebra and G_K acts on this in the obvious fashion. Therefore, we can form

$$\mathbf{W}_{\mathscr{A}(L)}^{\mathrm{hL}}\big(G_K\big) := \big\{W_K^{\mathrm{hL}}\big(\mathscr{A}(L), \chi, \alpha, \sigma\big) \mid \sigma \in G_K\big\}$$

for χ a character $\chi : G_K \to K$ and $\alpha : \mathscr{A}(L) \times \mathscr{A}(L) \to K$ a 2-cocycle.

The action of G_K on $\mathscr{A}(K)$ induces an action on the quotient

$$\mathscr{A}(K) \twoheadrightarrow \frac{\mathscr{A}(K)}{N\mathscr{A}(K)}$$

and so we get a surjective morphism of G_K-hom-Lie structures

$$\mathbf{W}_{\mathscr{A}(K)}^{\mathrm{hL}}\big(G_K\big) \twoheadrightarrow \mathbf{W}_{\mathscr{A}(K)/N\mathscr{A}(K)}^{\mathrm{hL}}\big(G_K\big)$$

Fitting this into the fundamental sequence

$$0 \longrightarrow \frac{\mathscr{A}(K)}{N\mathscr{A}(K)} \longrightarrow \mathsf{Sel}^{(N)}(\mathscr{A}/K) \longrightarrow \mathscr{A}(\mathscr{A}/K)[N] \longrightarrow 0$$

where $\mathsf{Sel}^{(N)}(\mathscr{A}/K)$ is the Nth *Selmer group* and $\mathscr{A}(\mathscr{A}/K)[N]$ the N-torsion part of the *Tate-Shafarevich group*, we get a sequence of group algebras

$$K\big[\mathscr{A}(K)\big] \longrightarrow K\left[\frac{\mathscr{A}(K)}{N\mathscr{A}(K)}\right] \longrightarrow K\big[\mathsf{Sel}^{(N)}(\mathscr{A}/K)\big] \longrightarrow K\big[\mathscr{A}(\mathscr{A}/K)[N]\big]$$

The question that arises is, can this be extended to a sequence of hom-Lie structures? The answer is yes, but in general not G_K-hom-Lie structures. The reason for this general "failure" is that the action of G_K does not in general lift to an action on $H^1(G_K, \mathscr{A})$, and hence, in general, not to $\mathsf{Sel}^{(N)}(\mathscr{A}/K)$ or $\mathscr{A}(\mathscr{A}/K)[N]$. Therefore, one needs to restrict to certain subgroups of G_K. Unfortunately, the details of this has to be postponed to another paper.

Remark 4.4. The above discussion gives us a way to see a hom-Lie structure as something that is canonically given by the abelian group structure of $\mathscr{A}$, much like the Lie algebra structure of algebraic groups (in this case this is obviously abelian). In this sense, the hom-Lie structure captures significantly more information than the Lie structure, since it involves the rational points and the Galois action on these in a very explicit manner.

References

[1] S. Caenepeel and I. Goyvaerts. Hom-Hopf algebras. Preprint arxiv:0907.0187, 2009.

[2] A. Fröhlich. Some remarks on wild extensions of number fields. *J. Reine Angew. Math.*, **495** (1998), 29–33.

[3] J.T. Hartwig, D. Larsson and S.D. Silvestrov. Deformations of Lie algebras using σ-derivations. *J. Algebra*, **295** (2006), 314–361.

[4] D. Larsson. Global and Arithmetic Hom-Lie algebras. Preprint, Uppsala University, U.U.D.M Report 2008:44; 2008.

[5] D. Larsson and S.D. Silvestrov. Quasi-deformations of $\mathfrak{sl}_2(\mathbb{F})$ using twisted derivations. *Comm. Algebra*, **35** (2007), 4303–4318.

[6] J. S. Milne. *Étale Cohomology.* Princeton Mathematical Series, **33**, Princeton University Press, Princeton, 1980.

[7] E. Nauwelaerts and F. Van Oystaeyen. Introducing crystalline graded algebras. *Algebr. Represent. Theory*, **11** (2008), 133–148.

[8] A. Schmidt. An arithmetic site for the rings of integers of algebraic number field. *Invent. Math.*, **123** (1996), 575–610.

[9] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves.* Grad. Texts in Math., **151**, Springer-Verlag, New York, 1994.

Received June 17, 2009
Revised September 20, 2009