Descent Theory
with an application to Infinite Dimensional Lie Algebras

Lectures by Arturo Pianzola
Notes by Zhihua Chang

March 18, 2013-March 22, 2013
Fields Institute for Research in Mathematical Sciences

Contents

1 Motivation 1
2 Flat and faithfully flat modules and rings 2
3 Faithfully flat descent: general case 6
4 Faithfully flat descent: the case of twisted forms 10
5 Galois descent 17
5.1 Generalities 17
5.2 Galois descent: general case 19
5.3 Galois descent: the case of twisted forms 23
6 Application to infinite dimensional Lie theory 28

1 Motivation

Let S/R be a ring extension, i.e., a ring homomorphism $R \to S$. Given an R–module N, there is a natural way to construct an S–module by extension of scalars $N \otimes_R S$. Roughly speaking, descent theory is the "converse" of this construction. The basic questions which are accounted by descent theory are the following:

- Given an S–module M, does there exist an R–module N' such that $N' \otimes_R S \cong M$?
- Can we classify all R–modules N' such that $N' \otimes_R S \cong M$?

It is hopeless to answer these questions in general. Nonetheless, in the situation where S/R is faithfully flat, there are very nice answers to these questions. More precisely, one can describe which S–module M is of the form $N \otimes_R S$ for some R–module N and if $M = N \otimes_R S$, one can classify all R–modules N' such that $N' \otimes_R S = M$.

The answers to these questions are significant in many areas in mathematics. Our primary motivation is the following situation. Let us consider the ring of Laurent polynomials $R = \mathbb{C}[t^{\pm 1}]$, and $\widehat{S} = \varinjlim \mathbb{C}[t^{\pm \frac{1}{m}}]$. Then $\widehat{S}/R$ is a faithfully flat extension. Let $\mathfrak{g}$ be a finite dimensional simple Lie algebra over $\mathbb{C}$. Then a Lie algebra $\mathcal{L}$ over R satisfies $\mathcal{L} \otimes_R \widehat{S} \cong \mathfrak{g} \otimes_{\mathbb{C}} \widehat{S}$ as Lie algebras over $\widehat{S}$ if and only if $\mathcal{L}$ is isomorphic to an affine Kac-Moody algebra (derived modulo its center). More generally, if one replace the ring R in this example by a Laurent polynomial ring in several variables $\mathbb{C}[t_1^{\pm 1}, \cdot, t_n^{\pm 1}]$, one can realize all Lie tori except those of type A in the same manner.

In this note, all rings are commutative with unit. We always assume R is a ring and $\otimes$ means the tensor product is taken over R.

2 Flat and faithfully flat modules and rings

Let R be a ring.

Definition 2.1. An R–module E is flat if whenever the sequence of R–modules

$$N' \xrightarrow{\alpha} N \xrightarrow{\beta} N''$$

is exact, the sequence of R–modules

$$N' \otimes_R E \xrightarrow{\alpha\otimes 1} N \otimes_R E \xrightarrow{\beta\otimes 1} N'' \otimes_R E$$

is exact.

Example 2.2.

(i) The $\mathbb{Z}$–module $\mathbb{Z}/2\mathbb{Z}$ is not flat. Indeed, we may consider the exact sequence of $\mathbb{Z}$–modules

$$0 \to \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z}.$$

Applying $- \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$, and identifying $\mathbb{Z} \otimes_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z})$ with $\mathbb{Z}/2\mathbb{Z}$, one gets

$$0 \to \mathbb{Z}/2\mathbb{Z} \xrightarrow{\cdot \bar{0}} \mathbb{Z}/2\mathbb{Z},$$

in which the zero map $\mathbb{Z}/2\mathbb{Z} \xrightarrow{\cdot \bar{0}} \mathbb{Z}/2\mathbb{Z}$ is obviously not injective.

(ii) For a multiplicative subset $U \subseteq R$, the module of fractions $U^{-1}R$ is a flat R–module. To prove this statement, we identify $N \otimes_R U^{-1}R$ with $U^{-1}N$ for every R–module N. From Remark 2.3 (i) below, it suffices to show that, for an injective homomorphism of R–modules $\alpha : N' \to N$, the homomorphism of $U^{-1}R$–modules $U^{-1}(\alpha) : U^{-1}N' \to U^{-1}N$ is injective. This can be done directly. Let $n/u \in \ker U^{-1}(\alpha)$, then $\alpha(n)/u = 0$ in $U^{-1}N$. i.e., there is $v \in U$ such that $v\alpha(n) = 0$. Now α is R–linear, $\alpha(vn) = v\alpha(n) = 0$. The injectivity of α implies that $vn = 0$. It follows $n/u = 0$ in $U^{-1}N'$. This completes the proof.

(iii) Every free or projective module is a flat module.

(iv) Any direct sum of flat modules is a flat module.

Remark 2.3.

(i) Since $- \otimes_R E$ is always right exact, E is a flat R–module if and only if whenever a homomorphism of R–modules $\alpha : N' \to N$ is injective, the homomorphism $\alpha \otimes 1 : N' \otimes E \to N \otimes E$ is injective.

(ii) If E is a flat R–module and $N' \subseteq N$ a submodule, we can identify $N' \otimes E$ with a submodule of $N \otimes E$. Moreover, there is a canonical isomorphism

$$(N \otimes E)/(N' \otimes E) \cong (N/N') \otimes E.$$

(iii) Given a homomorphism of R–modules $\alpha : N' \to N$, $\ker(\alpha) \subseteq N'$ is an R–submodule and $\mathrm{Im}(\alpha) \subseteq N$ is also an R–submodule. For a flat R–module E, we have

$$\ker(\alpha \otimes 1) = \ker(\alpha) \otimes E,$$
$$\mathrm{Im}(\alpha \otimes 1) = \mathrm{Im}(\alpha) \otimes E.$$

Proposition 2.4. *For an R–module E, the following are equivalent*

(FFa) $N' \xrightarrow{\alpha} N \xrightarrow{\beta} N''$ *is exact if and only if* $N' \otimes E \xrightarrow{\alpha\otimes 1} N \otimes E \xrightarrow{\beta\otimes 1} N'' \otimes E$ *is exact.*

(FFb) E *is flat and for any R–module N,* $N \otimes E = 0$ *implies* $N = 0$.

(FFc) E *is flat and if* $N' \xrightarrow{\alpha} N$ *such that* $\alpha \otimes 1$ *is injective, then* α *is injective.*

(FFd) E *is flat and if* $N' \xrightarrow{\alpha} N$ *such that* $\alpha \otimes 1 = 0$*, then* $\alpha = 0$.

(FFe) E *is flat and* $\mathfrak{m}E \neq E$ *for every maximal ideal* $\mathfrak{m}$ *of* R.

Proof. (FFa)⇒(FFb). Clearly E is a flat R–module. Consider the sequence of R–modules

$$0 \to N \to 0. \tag{2.1}$$

If $N \otimes_R E = 0$, the sequence (2.1) becomes exact after applying $- \otimes_R E$. Hence, (FFa) implies that (2.1) is exact, i.e., $N = 0$.

(FFb)⇒(FFc). Let $\alpha : N' \to N$ be a homomorphism of R–modules such that $\alpha \otimes 1$ is injective. We consider the exact sequence

$$0 \to \ker(\alpha) \to N' \xrightarrow{\alpha} N,$$

The flatness of E implies that the sequence

$$0 \to \ker(\alpha) \otimes E \to N' \otimes E \xrightarrow{\alpha\otimes 1} N \otimes E$$

is exact. Since $\alpha \otimes 1$ is injective, $\ker(\alpha) \otimes E = \ker(\alpha \otimes 1) = 0$. Hence, (FFb) ensures that $\ker(\alpha) = 0$, i.e., α is injective.

(FFc)⇒(FFd) Given $\alpha : N' \to N$, we consider the exact sequence

$$N' \xrightarrow{\alpha} N \xrightarrow{\beta} N/\alpha(N') \to 0$$

Since E is flat, the sequence

$$N' \otimes E \xrightarrow{\alpha\otimes 1} N \otimes E \xrightarrow{\beta\otimes 1} (N/\alpha(N')) \otimes E \to 0$$

is exact. If $\alpha \otimes 1 = 0$, then $\beta \otimes 1$ is injective. By (FFc), β is injective. It follows that $\alpha = 0$.

(FFd)⇒(FFa) Consider the following two sequences of R–modules

$$N' \xrightarrow{\alpha} N \xrightarrow{\beta} N'', \tag{2.2}$$

and

$$N' \otimes E \xrightarrow{\alpha\otimes 1} N \otimes E \xrightarrow{\beta\otimes 1} N'' \otimes E. \tag{2.3}$$

Since E is flat, (2.3) is exact if (2.2) is exact.

Conversely, assume (2.3) is exact. Then $(\beta\alpha) \otimes 1 = (\beta \otimes 1)(\alpha \otimes 1) = 0$. By (FFd), $\beta\alpha = 0$, i.e., $\mathrm{Im}(\alpha) \subseteq \ker(\beta)$. To prove it is an equality, we consider the canonical surjection $\pi : \ker(\beta) \twoheadrightarrow \ker(\beta)/\mathrm{Im}(\alpha)$. Since E is flat, by Remark 2.3 (ii) and (iii), we have

$$(\ker(\beta)/\mathrm{Im}(\alpha)) \otimes E \cong (\ker(\beta) \otimes E)/(\mathrm{Im}(\alpha) \otimes E) \cong \ker(\beta \otimes 1)/\mathrm{Im}(\alpha \otimes 1).$$

It follows from the exactness of (2.3) that $\ker(\beta\otimes 1)/\mathrm{Im}(\alpha\otimes 1) = 0$, i.e., $(\ker(\beta)/\mathrm{Im}(\alpha))\otimes E = 0$. Hence, $\pi \otimes 1 = 0$. By (FFd), $\pi = 0$, i.e., $\ker(\beta)/\mathrm{Im}(\alpha) = 0$. It follows that (2.2) is exact.

(FFb)⇒(FFe) Since E is flat, $E/\mathfrak{m}E \cong (R/\mathfrak{m}) \otimes E$. By (FFb), $R/\mathfrak{m} \neq 0$ implies that $E/\mathfrak{m}E \neq 0$, i.e., $E \neq \mathfrak{m}E$.

(FFe)⇒(FFb) Let $\mathfrak{a}$ be a nonzero proper ideal of R. Since $\mathfrak{a} \subset \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$, $\mathfrak{a}E \subseteq \mathfrak{m}E \neq E$. From Remark 2.3 (iii), $E/\mathfrak{a}E \cong (R/\mathfrak{a}) \otimes E$. Hence, $(R/\mathfrak{a}) \otimes E \neq 0$. It follows that $N' \otimes E \neq 0$ for every nonzero monogenic R–module N' (that is an R–module generated by one element). Now let N be a nonzero module, which contains a nonzero monogenic submodule N'. The flatness of E allows us to identify the nonzero R–module $N' \otimes E$ with an R–submodule of $N \otimes E$. Hence, $N \otimes E \neq 0$. □

Definition 2.5. E is *faithfully flat* if it satisfies the equivalent conditions in Proposition 2.4.

It is obvious from (FFa) that if E is a faithfully flat R–module, a homomorphism $\alpha : N' \to N$ is injective (resp. surjective, bijective) if and only if $\alpha \otimes 1$ is.

Example 2.6. $E = \bigoplus_{\mathfrak{p}\in \mathrm{Spec}(R)} R_{\mathfrak{p}}$ is faithfully flat.

Proof. First, E is flat because each $R_{\mathfrak{p}}$ is flat. To show E is faithfully flat, let $\mathfrak{m}$ be a maximal ideal of R. Then $\mathfrak{m}R_{\mathfrak{m}}$ is the maximal ideal of $R_{\mathfrak{m}}$. Thus $\mathfrak{m}R_{\mathfrak{m}} \neq R_{\mathfrak{m}}$. It follows that $\mathfrak{m}E \neq E$. By (FFe), E is faithfully flat. □

Proposition 2.7. *A homomorphism of R–modules $\alpha : N' \to N$ is injective (resp. surjective, or bijective) if and only if $\alpha_{\mathfrak{p}} : N'_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is injective (resp. surjective, or bijective) for all prime ideal $\mathfrak{p}$ of R, or equivalently, $\alpha_{\mathfrak{m}} : N'_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective (resp. surjective, or bijective) for all maximal ideal $\mathfrak{m}$ of R (cf. Chapter II, §3.3, Theorem 1 in [Bour]).*

Lemma 2.8. *Let E be faithfully flat (resp. flat) R–module and R'/R an arbitrary ring extension. Then $R' \otimes_R E$ is a faithfully flat (resp. flat) R'–module.*

Proof. This immediately follows from the fact that

$$N \otimes_{R'} (R' \otimes_R E) \cong N \otimes_R E,$$

for every R'–module N, which is also viewed as an R–module via the structure map $R \to R'$. □

Definition 2.9. A ring extension S/R is *faithfully flat* if S is a faithfully flat R–module.

Proposition 2.10. *Let S/R be a ring extension. The following are equivalent:*

(i) S/R is faithfully flat.

(ii) S/R is flat and for every R–module N the canonical map

$$\iota : N \to N \otimes S, \quad n \mapsto n \otimes 1,$$

is injective.

(iii) S/R is flat, and the map $\mathrm{Spec}(S) \to \mathrm{Spec}(R), \mathfrak{q} \mapsto \varepsilon^{-1}(\mathfrak{q})$ is surjective, where $\varepsilon : R \to S$ is the structure map.

Proof. (i)⇒(ii) To show ι is injective, by (FFc), it suffices to show $\iota \otimes 1$ is injective. Define

$$\beta : N \otimes S \otimes S \to N \otimes S, \quad n \otimes s \otimes t \mapsto n \otimes st.$$

Then one may check that

$$\beta(\iota \otimes 1)(n \otimes s) = \beta(n \otimes 1 \otimes s) = n \otimes s,$$

i.e., $\beta \circ (\alpha \otimes 1) = \mathrm{id}_{N \otimes S}$, and so $\iota \otimes 1$ is injective.

(ii)⇒(i) Let N be a nonzero R–module. From the injectivity of $\iota : N \to N \otimes S$, we know that $N \otimes S \neq 0$. By (FFb), S/R is faithfully flat.

(i)⇒(iii) Let $\mathfrak{p} \in \mathrm{Spec}(R)$. We claim that there is $\mathfrak{q} \in \mathrm{Spec}(S)$ such that $\varepsilon^{-1}(\mathfrak{q}) = \mathfrak{p}$. We consider the following commutative diagram

$$\begin{array}{ccc} R & \xrightarrow{\varepsilon} & S \\ {\scriptstyle \nu_1}\downarrow & & \downarrow{\scriptstyle \nu_2} \\ R_{\mathfrak{p}} & \xrightarrow[\varepsilon_{\mathfrak{p}}]{} & S_{\mathfrak{p}} \end{array}$$

where ν_1, ν_2 are the canonical homomorphism. Note that $\mathfrak{p}R_{\mathfrak{p}}$ is the maximal ideal of $R_{\mathfrak{p}}$ and $\mathfrak{p} = \nu_1^{-1}(\mathfrak{p}R_{\mathfrak{p}})$. Since S/R is faithfully flat, the ring extension $S_{\mathfrak{p}}/R_{\mathfrak{p}}$ is also faithfully flat since $S_{\mathfrak{p}} = R_{\mathfrak{p}} \otimes_R S$ (see Proposition 2.8). By (FFe), $\mathfrak{p}S_{\mathfrak{p}} \neq S_{\mathfrak{p}}$. Hence, there is a maximal ideal $\tilde{\mathfrak{q}}$ of $S_{\mathfrak{p}}$ such that $\tilde{\mathfrak{q}} \supseteq \mathfrak{p}S_{\mathfrak{p}}$. We thus know $\varepsilon_{\mathfrak{p}}^{-1}(\tilde{\mathfrak{q}})$ is a prime ideal of $R_{\mathfrak{p}}$, containing $\mathfrak{p}R_{\mathfrak{p}}$. It follows that $\varepsilon_{\mathfrak{p}}^{-1}(\tilde{\mathfrak{q}}) = \mathfrak{p}R_{\mathfrak{p}}$, and hence $(\varepsilon_{\mathfrak{p}}\nu_1)^{-1}(\tilde{\mathfrak{q}}) = \mathfrak{p}$. Let $\mathfrak{q} = \nu_2^{-1}(\tilde{\mathfrak{q}})$ which is a prime ideal of S. Then we conclude from the commutative diagram above that $\mathfrak{p} = (\varepsilon_{\mathfrak{p}}\nu_1)^{-1}(\tilde{\mathfrak{q}}) = \varepsilon^{-1}(\mathfrak{q})$.

(iii)⇒(i) Let $\mathfrak{m}$ be a maximal ideal of R. Since $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$ is surjective, there is $\mathfrak{q} \in \mathrm{Spec}(S)$ such that $\varepsilon^{-1}(\mathfrak{q}) = \mathfrak{m}$. It follows that $\mathfrak{m}S \subseteq \mathfrak{q}S \neq S$. By (FFe), S/R is faithfully flat. □

Given an extension S/R of rings, there are two maps

$$p_1 : S \to S \otimes S, \quad s \mapsto s \otimes 1, \tag{2.4}$$

and

$$p_2 : S \to S \otimes S, \quad s \mapsto 1 \otimes s. \tag{2.5}$$

For an R–module, we denote $p_i^N := \mathrm{id}_N \otimes p_i$ for $i = 1, 2$.

Proposition 2.11. *Assume that S/R is a faithfully flat ring extension and N is an R–module, then the sequence*

$$0 \longrightarrow N \xrightarrow{\iota} N \otimes S \underset{p_2^N}{\overset{p_1^N}{\rightrightarrows}} N \otimes S \otimes S$$

is exact, meaning that ι is injective and $\mathrm{Im}(\iota) = \ker(p_1^N - p_2^N)$.

Proof. The injectivity of ι has been proved in Proposition 2.10.

It is obvious that

$$p_1^N(n \otimes 1) = p_2^N(n \otimes 1),$$

for $n \in N$, which implies that $\mathrm{Im}(\iota) \subseteq \ker(p_1^N - p_2^N)$.

It remains to show $\ker(p_1^N - p_2^N)/\mathrm{Im}(\iota) = 0$. Since S/R is faithfully flat, by Remark 2.3 (ii) and (iii), it suffices to show

$$(\ker(p_1^N - p_2^N)/\mathrm{Im}(\iota)) \otimes S = \ker((p_1^N - p_2^N) \otimes 1)/\mathrm{Im}(\iota \otimes 1) = 0.$$

Consider the sequence

$$0 \longrightarrow N \otimes S \xrightarrow{\iota \otimes 1} N \otimes S \otimes S \underset{p_2^N \otimes 1}{\overset{p_1^N \otimes 1}{\rightrightarrows}} N \otimes S \otimes S \otimes S \ ,$$

and define

$$\beta : N \otimes S \otimes S \otimes S \to N \otimes S \otimes S, \quad n \otimes r \otimes s \otimes t \mapsto n \otimes r \otimes st.$$

If $x = \sum n_i \otimes s_i \otimes t_i \in \ker(p_1^N \otimes 1 - p_2^N \otimes 1)$, then

$$\sum n_i \otimes s_i \otimes 1 \otimes t_i = \sum n_i \otimes 1 \otimes s_i \otimes t_i.$$

Applying μ, we obtain

$$x = \beta\left(\sum n_i \otimes s_i \otimes 1 \otimes t_i\right) = \beta\left(\sum n_i \otimes 1 \otimes s_i \otimes t_i\right) = \sum n_i \otimes 1 \otimes s_i t_i.$$

Hence, $x = (\iota \otimes 1)(\sum n_i \otimes s_i t_i) \in \mathrm{Im}(\iota \otimes 1)$. This completes the proof. □

Proposition 2.12. *Let S/R be a faithfully flat ring extension and N an R–module. Then N is of finite type (resp. of finite presentation, or projective of finite type) if and only if the S–module $N \otimes S$ has the same property. (cf. Chapter I, §3.7, Proposition 11 and 12 in [Bour])*

3 Faithfully flat descent: general case

In this section, we fix a faithfully flat extension of rings, say S/R.

If M is an S–module, there are two $S \otimes S$–module structures on $M \otimes S$ given respectively by

$$(a \otimes b)(m \otimes s) = am \otimes bs,$$
$$(a \otimes b)(m \otimes s) = bm \otimes as,$$

for $m \in M$ and $a, b, s \in S$.

Definition 3.1. A *covering datum* on M is an $S \otimes S$–module isomorphism $\psi : M \otimes S \to M \otimes S$ between two $S \otimes S$–module structures on $M \otimes S$.

Example 3.2. Let N be an R–module and $M := N \otimes S$. Then

$$\theta : N \otimes S \otimes S \to N \otimes S \otimes S, \quad n \otimes s \otimes t \mapsto n \otimes t \otimes s \tag{3.1}$$

is a covering datum on M, called the *standard covering datum*.

In this situation, we can recover N from (M, θ). More precisely,

$$N \cong \{m \in M : \theta(m \otimes 1) = m \otimes 1\}.$$

Indeed, if $m = \sum n_i \otimes s_i \in M$ such that $\theta(m \otimes 1) = m \otimes 1$, then $\sum n_i \otimes s_i \otimes 1 = \sum n_i \otimes 1 \otimes s_i$. Then it follows from Proposition 2.11 that $m \in N$.

Given a covering datum ψ on an S–module M, it gives rise to three maps

$$\psi^i : M \otimes S \otimes S \to M \otimes S \otimes S, \quad i = 0, 1, 2$$

defined as follows: if $\psi(m \otimes a) = \sum m_i \otimes a_i$,

$$\psi^0(m \otimes u \otimes a) = \sum m_i \otimes u \otimes a_i, \tag{3.2}$$
$$\psi^1(m \otimes u \otimes a) = \sum m_i \otimes a_i \otimes u, \tag{3.3}$$
$$\psi^2(m \otimes a \otimes u) = \sum m_i \otimes a_i \otimes u, \tag{3.4}$$

for $m \in M$ and $a, u \in S$.

Remark 3.3. $\psi^2 = \psi \otimes 1$.

Definition 3.4. A covering datum ψ on M is called a *descent datum* if

$$\psi^1 = \psi^0 \psi^2. \tag{3.5}$$

Example 3.5. The standard covering datum θ on $M := N \otimes S$ is a descent datum. This can be easily verified directly. In fact, from the description of θ in (3.1), we deduce that

$$\theta^0(n \otimes a \otimes b \otimes c) = n \otimes c \otimes b \otimes a,$$
$$\theta^1(n \otimes a \otimes b \otimes c) = n \otimes c \otimes a \otimes b,$$
$$\theta^2(n \otimes a \otimes b \otimes c) = n \otimes b \otimes a \otimes c.$$

Hence, the equality $\theta^1 = \theta^0\theta^2$ holds obviously.

Let M be an S–module with a descent datum ψ, and

$$N := \{m \in M : \psi(m \otimes 1) = m \otimes 1\}. \tag{3.6}$$

Note that N is an R–module. Indeed, for $n \in N$, $r \in R$, we have $rn \in N$ since

$$\psi(rn \otimes 1) = \psi((r \otimes 1)(n \otimes 1)) = (1 \otimes r)\psi(n \otimes 1) = (1 \otimes r)(n \otimes 1) = n \otimes r = rn \otimes 1.$$

Moreover, N fits into the following exact sequence of R–modules

$$0 \longrightarrow N \longrightarrow M \underset{\psi\iota}{\overset{\iota}{\rightrightarrows}} M \otimes S \ ,$$

where $\iota : M \to M \otimes S, m \mapsto m \otimes 1$. Since S/R is flat, the sequence

$$0 \longrightarrow N \otimes S \longrightarrow M \otimes S \underset{\psi\iota\otimes 1}{\overset{\iota\otimes 1}{\rightrightarrows}} M \otimes S \otimes S \ . \tag{3.7}$$

is exact.

On the other hand, since S/R is faithfully flat, we have the exact sequence

$$0 \longrightarrow M \longrightarrow M \otimes S \underset{p_1^M}{\overset{p_2^M}{\rightrightarrows}} M \otimes S \otimes S \ . \tag{3.8}$$

Theorem 3.6. *The exact sequences (3.7) and (3.8) fit in the following commutative diagram*

$$\begin{array}{ccccccc} 0 & \longrightarrow & N\otimes S & \longrightarrow & M\otimes S & \overset{\iota\otimes 1}{\underset{\psi\iota\otimes 1}{\rightrightarrows}} & M\otimes S\otimes S \\ & & & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \psi^0} \\ 0 & \longrightarrow & M & \longrightarrow & M\otimes S & \overset{p_2^M}{\underset{p_1^M}{\rightrightarrows}} & M\otimes S\otimes S \end{array}$$

which induces an isomorphism of S–modules

$$\psi|_{N\otimes S} : N\otimes S \to M.$$

Proof. We first show the commutativity of the square with the two top arrows. For $m\in M, s\in S$, write $\psi(m\otimes s)=\sum m_i\otimes s_i$. Then

$$\begin{aligned} \psi^0(\iota\otimes 1)(m\otimes s) &= \psi^0(m\otimes 1\otimes s) = \textstyle\sum m_i\otimes 1\otimes s_i, \\ p_2^M\psi(m\otimes s) &= p_2^M(\textstyle\sum m_i\otimes s_i) = \sum m_i\otimes 1\otimes s_i, \end{aligned}$$

It follows the square with the two top arrows is commutative.

For the square with the two bottom arrows, we have

$$\begin{aligned} \psi^0(\psi\iota\otimes 1)(m\otimes s) &= \psi^0(\psi(m\otimes 1)\otimes s) = \psi^0\psi^2(m\otimes 1\otimes s) \\ &= \psi^1(m\otimes 1\otimes s) = \textstyle\sum m_i\otimes s_i\otimes 1 \\ p_1^M\psi(m\otimes s) &= p_1^M(\textstyle\sum m_i\otimes s_i) = \sum m_i\otimes s_i\otimes 1. \end{aligned}$$

This shows that the diagram is commutative. We put

$$\alpha := \iota\otimes 1-\psi\iota\otimes 1 \text{ and } \beta = p_2^M - p_1^M.$$

and identify $N\otimes S$ with S–submodule of $M\otimes S$. Then, for $n\in N, s\in S$,

$$\beta\psi(n\otimes s) = \psi^0\alpha(n\otimes s) = \psi^0(0) = 0.$$

Hence, $n\otimes s\in M$. It follows that ψ induces a map $\psi_{N\otimes S}: N\otimes S\to M$.

$\psi|_{N\otimes S}$ is injective since ψ is injective. To show $\psi|_{N\otimes S}$ is surjective, let $m\in M$. It follows from the bijectivity of ψ that $m\otimes 1=\psi(x)$ for some $x\in M\otimes S$. Then

$$\psi^0\alpha(x) = \beta\psi(x) = \beta(m\otimes 1) = 0,$$

and so $\alpha(x)=0$ since ψ^0 is bijective. Hence, $x\in N\otimes S$.

Finally, we verify that $\psi|_{N\otimes S}$ is S–linear. Indeed, for $n\in N, s\in S$,

$$\psi(n\otimes s) = (s\otimes 1)\psi(n\otimes 1) = (s\otimes 1)(n\otimes 1) = sn\otimes 1$$

Hence, $\psi|_{N\otimes S}(n\otimes s)=sn$, i.e., $\psi|_{N\otimes S}$ is S–linear. This completes the proof. □

Remark 3.7. Let M be an S–module and ψ a descent datum on M, and $\alpha: M\to M'$ an isomorphism of S–modules. We can define $\psi': M'\otimes S\to M'\otimes S$ such that the diagram

$$\begin{array}{ccc} M\otimes S & \xrightarrow{\psi} & M\otimes S \\ {\scriptstyle \alpha\otimes 1}\downarrow & & \downarrow{\scriptstyle \alpha\otimes 1} \\ M'\otimes S & \xrightarrow[\psi']{} & M'\otimes S \end{array}$$

is commutative. Then ψ' is a descent datum on M' and α induces an isomorphism of the descended modules.

A morphism $(M, \psi) \to (M', \psi')$ of covering data is a homomorphism of S–modules $\alpha : M \to M'$ such that the diagram

$$\begin{array}{ccc} M \otimes S & \xrightarrow{\psi} & M \otimes S \\ {\scriptstyle \alpha\otimes 1}\downarrow & & \downarrow{\scriptstyle \alpha\otimes 1} \\ M' \otimes S & \xrightarrow[\psi']{} & M' \otimes S \end{array}$$

is commutative. We thus have the category of S–modules with descent data, in which an object is a pair (M, ψ) consisting of an S–module M and a descent datum ψ on M, and a morphism $(M, \psi) \to (M', \psi')$ is a morphism of covering data.

Theorem 3.8. *There is an equivalence of categories from the category of R–modules to the category of S–modules with descent data.*

Proof. Let $\mathcal{F}$ be the functor from the category of R–modules to the category of S–modules with descent data given as follows: for each R–module N, define $\mathcal{F}(N) := (N \otimes S, \theta)$, where θ is the standard descent datum on $N \otimes S$; and for each homomorphism of R–modules $\alpha : N \to N'$, set $\mathcal{F}(\alpha) := \alpha \otimes 1$ is a morphism of S–modules with descent data.

Conversely, for each S–module with descent datum (M, ψ), we set

$$\mathcal{G}(M, \psi) = \{m \in M | \psi(m \otimes 1) = m \otimes 1\},$$

while for each morphism $\beta : (M, \psi) \to (M', \psi')$, we set $\mathcal{G}(\beta) := \beta|_{\mathcal{G}(M,\psi)}$. These define a functor $\mathcal{G}$ from the category of S–modules with descent data to the category of R–modules.

To show that the two categories are equivalent, it suffices to show $\mathcal{GF}(N)$ is naturally isomorphic to N for each R–module N and $\mathcal{FG}(M, \psi)$ is naturally isomorphic to (M, ψ) for each S–module with descent datum (M, ψ).

We know that

$$\mathcal{GF}(N) = \mathcal{G}(N \otimes S, \theta) = \{\textstyle\sum n_i \otimes s_i \in N \otimes S | \sum n_i \otimes s_i \otimes 1 = \sum n_i \otimes 1 \otimes s_i\},$$

which is isomorphic to N since S/R is faithfully flat (see Proposition 2.11). This isomorphism is functorial in N, namely, given a homomorphism of R–modules $\alpha : N \to N'$, the following diagram

$$\begin{array}{ccc} \mathcal{GF}(N) & \xrightarrow{\mathcal{GF}(\alpha)} & \mathcal{GF}(N') \\ {\scriptstyle \cong}\downarrow & & \downarrow{\scriptstyle \cong} \\ N & \xrightarrow[\alpha]{} & N' \end{array}$$

is commutative.

Now, given an S–module with descent datum (M, ψ). Let $N := \mathcal{G}(M, \psi)$ and θ be the standard descent datum on N. By Theorem 3.4, $\psi|_{N\otimes S} : N \otimes S \to M$ is an isomorphism of S–modules. Moreover, the following diagram is commutative:

$$\begin{array}{ccc} N \otimes S \otimes S & \xrightarrow{\theta} & N \otimes S \otimes S \\ {\scriptstyle (\psi|_{N\otimes S})\otimes 1}\downarrow & & \downarrow{\scriptstyle (\psi|_{N\otimes S})\otimes 1} \\ M \otimes S & \xrightarrow[\psi]{} & M \otimes S. \end{array}$$

Indeed, for $n \in N$ and $s, t \in S$,

$$\psi((\psi|_{N\otimes S}) \otimes 1)(n \otimes s \otimes t) = \psi(sn \otimes t) = tn \otimes s = ((\psi|_{N\otimes S}) \otimes 1)\theta(n \otimes s \otimes t).$$

Hence, $\psi|_{N\otimes S} : (N \otimes S, \theta) \to (M, \psi)$ is an isomorphism of S–modules with descent data, i.e., $\mathcal{FG}(M, \psi) \cong (M, \psi)$. This isomorphism is functorial in (M, ψ), i.e., for a morphism $\beta : (M, \psi) \to (M', \psi')$ of S–modules with descent data, the following diagram

$$\begin{array}{ccc} \mathcal{FG}(M,\psi) & \xrightarrow{\mathcal{FG}(\beta)} & \mathcal{FG}(M',\psi') \\ \cong\downarrow & & \downarrow\cong \\ (M,\psi) & \xrightarrow[\beta]{} & (M',\psi') \end{array}$$

is commutative, which follows from the fact that the following diagram

$$\begin{array}{ccc} \mathcal{G}(M,\psi)\otimes S & \xrightarrow{(\beta|_{\mathcal{G}(M,\psi)})\otimes 1} & \mathcal{G}(M',\psi')\otimes S \\ \psi|\downarrow & & \downarrow\psi'| \\ M & \xrightarrow[\beta]{} & M' \end{array}$$

is commutative. □

Remark 3.9. Let (M, ψ) be an S–module with descent datum. Assume in addition that M is an S–algebra and ψ is an $S \otimes S$–algebra isomorphism. Then the descended module

$$N = \{m \in M | \psi(m \otimes 1) = m \otimes 1\}$$

is actually an R–algebra.

In fact, if $M \times M \to M, (m_1, m_2) \mapsto m_1 \cdot m_2$ gives an S–algebra structure on M, which is preserved by ψ. Then one can verify that

$$\psi(n_1n_2 \otimes 1) = \psi((n_1 \otimes 1)(n_2 \otimes 1)) = \psi(n_1 \otimes 1)\psi(n_2 \otimes 1) = (n_1 \otimes 1)(n_2 \otimes 1),$$

for $n_1, n_2 \in N$. It follows that $n_1n_2 \in N$.

4 Faithfully flat descent: the case of twisted forms

In this section, we assume that S/R is a faithfully flat ring extension. Instead of considering descent data on an arbitrary S–module, we focus on an S–module M of the form

$$M = N \otimes S$$

for some R–module N. We know from Example 3.5 that the standard covering datum

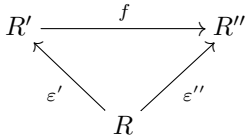
$$\theta : N \otimes S \otimes S \to N \otimes S \otimes S, \quad n \otimes s \otimes t \to n \otimes t \otimes s,$$

is a descent datum on M.

Let ψ be an arbitrary covering datum on M and $\varphi := \theta^{-1}\psi$. Since both θ and ψ switch the two $S \otimes S$–module structures on $M \otimes S$, φ preserves the $S \otimes S$–module structure on $M \otimes S$. Moreover, φ is bijective since both θ and ψ are bijective, it follows that $\varphi \in \mathrm{Aut}_{S\otimes S\text{-mod}}(N \otimes S \otimes S)$.

Before going into the discussion on descent data, we first introduce the group functor $\mathbf{GL}(N)$ for an R–module N. Let R-**alg** denote the category of ring extensions of R, i.e., an object in R-**alg**

is a homomorphism $\varepsilon : R \to R'$, and a morphism in R-**alg** is a commutative diagram of ring homomorphisms



Now, the functor $\mathbf{GL}(N)$ is the functor from the category R-**alg** to the category of groups given by

$$\mathbf{GL}(N) : R'/R \mapsto \mathrm{Aut}_{R'\text{-mod}}(N \otimes R').$$

Every morphism $f : R' \to R''$ in R-**alg** induces a group homomorphism

$$\mathbf{GL}(N)(f) : \mathrm{Aut}_{R'\text{-mod}}(N \otimes R') \to \mathrm{Aut}_{R''\text{-mod}}(N \otimes R''), \quad \phi \mapsto \phi_{R''},$$

where $\phi_{R''}$ is the R''–module automorphism of $N \otimes R''$ given by

$$\phi_{R''}(n \otimes r'') = \textstyle\sum n_i \otimes f(r'_i)r'',$$

if $\phi(n \otimes 1) = \sum n_i \otimes r'_i$, for $n \in N, r'' \in R''$. In this setting, $\varphi = \theta^{-1}\psi$ defined by the covering datum ψ is an element of $\mathbf{GL}(N)(S \otimes S)$.

In summary, ψ is a covering datum on $M := N \otimes S$ if and only if $\varphi = \theta^{-1}\psi \in \mathbf{GL}(N)(S \otimes S)$.

Now, let us find the condition on φ for $\psi := \theta\varphi$ to be a descent datum. Consider the following three morphisms in R-**alg**,

$$\begin{array}{rcl} & S \otimes S & \to S \otimes S \otimes S \\ p_{12} : & s \otimes t & \mapsto s \otimes t \otimes 1, \\ p_{13} : & s \otimes t & \mapsto s \otimes 1 \otimes t, \\ p_{23} : & s \otimes t & \mapsto 1 \otimes s \otimes t. \end{array}$$

By functoriality of $\mathbf{GL}(N)$, they induce three group homomorphism $\mathrm{d}^{jk} := \mathbf{GL}(N)(p_{jk}), 1 \leqslant i < j \leqslant 3$. Applying to φ, we get

$$\mathrm{d}^{jk}\varphi \in \mathbf{GL}(N)(S \otimes S \otimes S).$$

Explicitly, for $n \in N, a, b, u \in S$, if $\varphi(n \otimes a \otimes b) = \sum n_i \otimes a_i \otimes b_i$, then

$$\begin{aligned} (\mathrm{d}^{12}\varphi)(n \otimes a \otimes b \otimes u) &= \textstyle\sum n_i \otimes a_i \otimes b_i \otimes u, \\ (\mathrm{d}^{13}\varphi)(n \otimes a \otimes u \otimes b) &= \textstyle\sum n_i \otimes a_i \otimes u \otimes b_i, \\ (\mathrm{d}^{23}\varphi)(n \otimes u \otimes a \otimes b) &= \textstyle\sum n_i \otimes u \otimes a_i \otimes b_i. \end{aligned}$$

Lemma 4.1. *The following equalities hold*

$$\psi^1 = \theta^1(\mathrm{d}^{13}\varphi), \quad \psi^2 = \theta^2(\mathrm{d}^{12}\varphi), \quad \psi^0 = \theta^1(\mathrm{d}^{23}\varphi)\theta^2.$$

Proof. For $n \in N, a, b, u \in S$, we write $\varphi(n \otimes a \otimes b) = \sum n_i \otimes a_i \otimes b_i$. Then

$$\psi(n \otimes a \otimes b) = \theta\varphi(n \otimes a \otimes b) = \textstyle\sum n_i \otimes b_i \otimes a_i.$$

Hence,

$$\begin{aligned} \theta^1(\mathrm{d}^{23}\varphi)\theta^2(n \otimes a \otimes u \otimes b) &= \theta^1(\mathrm{d}^{23}\varphi)(n \otimes u \otimes a \otimes b) \\ &= \theta^1(\textstyle\sum n_i \otimes u \otimes a_i \otimes b_i) \\ &= \textstyle\sum n_i \otimes b_i \otimes u \otimes a_i \\ &= \psi^0(n \otimes a \otimes u \otimes b). \end{aligned}$$

Similarly,

$$\begin{aligned}\theta^2(\mathrm{d}^{12}\varphi)(n\otimes a\otimes b\otimes u) &= \theta^2(\textstyle\sum n_i\otimes a_i\otimes b_i\otimes u)\\ &= \textstyle\sum n_i\otimes b_i\otimes a_i\otimes u\\ &= \psi^2(n\otimes a\otimes b\otimes u),\\ \theta^1(\mathrm{d}^{13}\varphi)(n\otimes a\otimes u\otimes b) &= \theta^1(\textstyle\sum n_i\otimes a_i\otimes u\otimes b_i)\\ &= \textstyle\sum n_i\otimes b_i\otimes a_i\otimes u\\ &= \psi^1(n\otimes a\otimes u\otimes b).\end{aligned}$$

This competes the proof of the lemma. □

Recall from (3.5) that ψ is a descent datum if and only if

$$\psi^1 = \psi^0\psi^2.$$

By Lemma 4.1, it is equivalent to

$$\theta^1(\mathrm{d}^{13}\varphi) = \theta^1(\mathrm{d}^{23}\varphi)\theta^2\theta^2(\mathrm{d}^{12}\varphi).$$

i.e.,

$$\mathrm{d}^{13}\varphi = (\mathrm{d}^{23}\varphi)(\mathrm{d}^{12}\varphi). \tag{4.1}$$

Given $\varphi\in\mathbf{GL}(N)(S\otimes S)$, this is the necessary and sufficient condition for the covering datum $\psi := \theta\varphi$ to be a descent datum on $M = N\otimes S$. An element $\varphi\in\mathbf{GL}(N)(S\otimes S)$ satisfying (4.1) is called a 1–*cocycle*.

Recall from (3.6) that the descended module determined by the descent datum ψ is

$$N' = \{m\in M | \psi(m\otimes 1) = m\otimes 1\}.$$

In the situation where $\psi = \theta\varphi$ is given by a 1–cocycle $\varphi\in\mathbf{GL}(N)(S\otimes S)$, an element $m\in M$ satisfies $\psi(m\otimes 1) = m\otimes 1$ if and only if $\varphi(m\otimes 1) = \theta(m\otimes 1)$. Hence, the descended R–module given by the 1–cocycle φ is

$$N' = \{\textstyle\sum n_i\otimes s_i\in N\otimes S | \varphi(\sum n_i\otimes s_i\otimes 1) = \sum n_i\otimes 1\otimes s_i\}. \tag{4.2}$$

Now we consider two 1–cocycles φ and φ'. We know that the two descent data $\psi := \theta\varphi$ and $\psi' := \theta\varphi'$ are equivalent if there is an isomorphism $\lambda : N\otimes S\to N\otimes S$ such that

$$(\lambda\otimes 1)\psi = \psi'(\lambda\otimes 1), \tag{4.3}$$

which is equivalent to

$$(\lambda\otimes 1)\theta\varphi = \theta\varphi'(\lambda\otimes 1). \tag{4.4}$$

By the functoriality of $\mathbf{GL}(N)$, the two canonical morphisms $p_1, p_2 : S\to S\otimes S$ (see (2.4) and (2.5)) induces two group homomorphisms

$$\mathrm{d}^1 = \mathbf{GL}(N)(p_1),\quad \mathrm{d}^2 = \mathbf{GL}(N)(p_2).$$

Applying to λ, we get $\mathrm{d}^1\lambda, \mathrm{d}^2\lambda\in\mathbf{GL}(N)(S\otimes S)$. Explicitly, for $n\in N, a\in S$, if we write $\lambda(n\otimes a) = \sum n_i\otimes a_i$, then

$$\begin{aligned}(\mathrm{d}^1\lambda)(n\otimes a\otimes u) &= \textstyle\sum n_i\otimes a_i\otimes u,\\ (\mathrm{d}^2\lambda)(n\otimes u\otimes a) &= \textstyle\sum n_i\otimes u\otimes a_i.\end{aligned}$$

Lemma 4.2.

$$\theta(\mathrm{d}^2\lambda)\theta = \mathrm{d}^1\lambda = \lambda \otimes 1$$

Proof. For $n \in N, a, u \in S$, we have

$$\begin{aligned}\theta(\mathrm{d}^2\lambda)\theta(n \otimes a \otimes u) &= \theta(\mathrm{d}^2\lambda)(n \otimes u \otimes a) = \theta(\textstyle\sum n_i \otimes u \otimes a_i) \\ &= \textstyle\sum n_i \otimes a_i \otimes u = (\mathrm{d}^1\lambda)(n \otimes a \otimes u).\end{aligned}$$

□

Based on Lemma 4.2, the equality (4.4) is equivalent to

$$(\mathrm{d}^1\lambda)\theta\varphi = \theta\varphi'(\mathrm{d}^1\lambda),$$

i.e.,

$$\varphi' = \theta(\mathrm{d}^1\lambda)\theta\varphi(\mathrm{d}^1\lambda)^{-1} = (\mathrm{d}^2\lambda)\varphi(\mathrm{d}^1\lambda)^{-1}.$$

More generally, let $\mathbf{G}$ be a group functor from the category R-**alg** to the category of groups. Define the set of 1-cocycles to be

$$Z^1(S/R, \mathbf{G}) = \{\varphi \in \mathbf{G}(S \otimes S) | \mathrm{d}^{13}\varphi = (\mathrm{d}^{23}\varphi)(\mathrm{d}^{12}\varphi)\},$$

on which there is an equivalent relation $\sim$ given as follows: $\varphi \sim \varphi'$ if and only if there exists $\lambda \in \mathbf{G}(S)$ such that

$$(\mathrm{d}^2\lambda)\varphi(\mathrm{d}^1\lambda)^{-1} = \varphi'. \tag{4.5}$$

Then *the first cohomology set* $\mathrm{H}^1(S/R, \mathbf{G})$ is defined to be the set of equivalence classes, i.e.,

$$\mathrm{H}^1(S/R, \mathbf{G}) = Z^1(S/R, \mathbf{G})/\sim .$$

This is a set with a distinguished element, which is the identity element $e \in \mathbf{G}(S \otimes S)$.

Definition 4.3. An R–module N' is called an *S/R–form* of N if

$$N' \otimes S \cong N \otimes S$$

as S–modules.

Theorem 4.4. *Let S/R be a faithfully flat extension of rings and N an R–module. Then the set of isomorphism classes of S/R–forms of N bijectively corresponds to the first cohomology set* $\mathrm{H}^1(S/R, \mathbf{GL}(N))$. □

Let N' be an S/R–form of N. We determine a 1–cocycle associated to it directly. Suppose

$$\kappa : N' \otimes S \to N \otimes S$$

is an isomorphism of S–modules. Consider $p_i : S \to S^{\otimes 2} := S \otimes S$, $i = 1, 2$, the base change yields two $S^{\otimes 2}$–isomorphisms

$$\kappa_{p_i} : (N' \otimes S) \otimes_S S^{\otimes 2} \to (N \otimes S) \otimes_S S^{\otimes 2}, \quad i = 1, 2.$$

Applying the canonical $S^{\otimes 2}$–isomorphisms $(N' \otimes S) \otimes_S S^{\otimes 2} \cong N' \otimes_R S^{\otimes}$ and $(N \otimes S) \otimes_S S^{\otimes} \cong N \otimes_R S^{\otimes}$, we obtain additive isomorphism

$$\kappa_i : N' \otimes_R S^{\otimes 2} \to N \otimes_R S^{\otimes 2}, \quad i = 1, 2,$$

such that the following diagram

$$\begin{array}{ccc} (N' \otimes_R S) \otimes_S S^{\otimes 2} & \xrightarrow{\kappa_{p_i}} & (N \otimes_R S) \otimes_S S^{\otimes 2} \\ \cong \downarrow & & \downarrow \cong \\ N' \otimes_R S^{\otimes 2} & \xrightarrow[\kappa_i]{} & N \otimes_R S^{\otimes 2} \end{array}$$

is commutative for $i = 1, 2$. Hence, $\varphi := \kappa_2 \kappa_1^{-1} \in \mathbf{GL}(N)(S^{\otimes 2})$.

We next verify that φ is an 1–cocycle. For each $i = 1, 2$, we apply the base change

$$p_{jk} : S^{\otimes 2} \to S^{\otimes 3} := S \otimes S \otimes S$$

to the isomorphism $\kappa_i : N' \otimes_R S^{\otimes 2} \to N \otimes_R S^{\otimes 2}$, obtaining

$$\kappa_{i,p_{jk}} : (N' \otimes_R S^{\otimes 2}) \otimes_{S^{\otimes 2}} S^{\otimes 3} \to (N \otimes_R S^{\otimes 2}) \otimes_{S^{\otimes 2}} S^{\otimes 3},$$

for $i = 1, 2$ and $1 \leqslant j < k \leqslant 3$. Hence, we have an isomorphism of $S^{\otimes 3}$–modules

$$\kappa_{i,jk} : N' \otimes_R S^{\otimes 3} \to N \otimes_R S^{\otimes 3}$$

such that the following diagram

$$\begin{array}{ccc} (N' \otimes_R S^{\otimes 2}) \otimes_{S^{\otimes 2}} S^{\otimes 3} & \xrightarrow{\kappa_{i,p_{jk}}} & (N \otimes_R S^{\otimes 2}) \otimes_{S^{\otimes 2}} S^{\otimes 3} \\ \cong \downarrow & & \downarrow \cong \\ N' \otimes_R S^{\otimes 3} & \xrightarrow[\kappa_{i,jk}]{} & N \otimes_R S^{\otimes 3} \end{array}$$

is commutative, where the two vertical morphisms are the canonical isomorphisms of $S^{\otimes 3}$–modules. In summary, the isomorphism $\kappa_{i,jk}$ is obtained from the isomorphism κ by base change

$$S \xrightarrow{p_i} S^{\otimes 2} \xrightarrow{p_{jk}} S^{\otimes 3}.$$

On the other hand, we may consider the base change $q_i : S \to S^{\otimes 3}$ for $i = 1, 2, 3$ given respectively by

$$q_1(s) = s \otimes 1 \otimes 1, \quad q_2(s) = 1 \otimes s \otimes 1, \quad q_3(s) = 1 \otimes 1 \otimes s.$$

Then the base change of κ via q_i yields an isomorphism of $S^{\otimes 3}$–modules

$$\kappa_{q_i} : N' \otimes_R S^{\otimes 3} \to N \otimes_R S^{\otimes 3},$$

for $i = 1, 2, 3$. It is easy to verify that

$$\begin{array}{lll} p_{12} \circ p_1 = q_1, & p_{23} \circ p_1 = q_2, & p_{13} \circ p_1 = q_1, \\ p_{12} \circ p_2 = q_2, & p_{23} \circ p_2 = q_3, & p_{13} \circ p_2 = q_3. \end{array}$$

It follows that

$$\begin{array}{lll} \kappa_{1,12} = \kappa_{q_1}, & \kappa_{1,23} = \kappa_{q_2}, & \kappa_{1,13} = \kappa_{q_1}, \\ \kappa_{2,12} = \kappa_{q_2}, & \kappa_{2,23} = \kappa_{q_3}, & \kappa_{2,13} = \kappa_{q_3}. \end{array}$$

By definition, $\mathrm{d}^{jk}(\varphi) = \mathbf{GL}(N)(p_{jk})(\varphi)$ is the isomorphism of $S^{\otimes 2}$–modules obtained from φ via the base change $p_{jk} : S^{\otimes 2} \to S^{\otimes 3}$. Hence,

$$\mathrm{d}^{jk}\varphi = \kappa_{2,jk}\kappa_{1,jk}^{-1}.$$

Therefore,

$$(\mathrm{d}^{23}\varphi)(\mathrm{d}^{12}\varphi) = (\kappa_{2,23}\kappa_{1,23}^{-1})(\kappa_{2,12}\kappa_{1,12}^{-1}) = \kappa_{q_3}\kappa_{q_2}^{-1}\kappa_{q_2}\kappa_{q_1}^{-1} = \kappa_{2,13}\kappa_{1,13}^{-1} = \mathrm{d}^{13}\varphi,$$

i.e., φ is a 1–cocycle.

Let N' and N'' be two S/R–twisted form of N. Then the two isomorphisms of S–modules

$$\kappa : N' \otimes S \to N \otimes S, \text{ and } \kappa' : N'' \otimes S \to N \otimes S,$$

yield two 1–cocycles $\varphi = \kappa_2\kappa_1^{-1}$ and $\varphi' = \kappa'_2\kappa'^{-1}_1$. If $\alpha : N' \to N''$ is an isomorphism of R–modules, then $\lambda := \kappa'(\alpha \otimes \mathrm{id}_S)\kappa^{-1} \in \mathbf{GL}(N)(S)$. Hence,

$$\begin{aligned}
\varphi' &= \kappa'_2\kappa'^{-1}_1 \\
&= (\lambda\kappa(\alpha^{-1} \otimes \mathrm{id}_S))_2(\lambda\kappa(\alpha^{-1} \otimes \mathrm{id}_S))_1^{-1} \\
&= (\mathrm{d}^2\lambda)\kappa_2(\alpha^{-1} \otimes \mathrm{id}_{S''})(\alpha \otimes \mathrm{id}_{S''})\kappa_1^{-1}(\mathrm{d}^1\lambda)^{-1} \\
&= (\mathrm{d}^2\lambda)\kappa_2\kappa_1^{-1}(\mathrm{d}^1\lambda)^{-1} \\
&= (\mathrm{d}^2\lambda)\varphi(\mathrm{d}^1\lambda)^{-1},
\end{aligned}$$

i.e., φ' is equivalent to φ.

Next we will show that the S/R–form N' of N is isomorphic to the descended module determined by φ, i.e.,

$$N' \cong N_\varphi := \{\textstyle\sum n_i \otimes s_i \in N \otimes S | \varphi(\sum n_i \otimes s_i \otimes 1) = \sum n_i \otimes 1 \otimes s_i\}.$$

We consider the composition

$$\beta : N' \xrightarrow{\iota} N' \otimes S \xrightarrow{\kappa} N \otimes S,$$

which is an injective homomorphism of R–modules since S/R is faithfully flat. It suffices to verify that the image of β exactly coincide with $N_\varphi \subseteq N \otimes S$.

For $n' \in N'$, we write $\kappa(n' \otimes 1) = \sum n_i \otimes s_i$. Then $\beta(n') = \sum n_i \otimes s_i$, and

$$\begin{aligned}
\kappa_1(n' \otimes 1 \otimes 1) &= \textstyle\sum n_i \otimes s_i \otimes 1, \\
\kappa_2(n' \otimes 1 \otimes 1) &= \textstyle\sum n_i \otimes 1 \otimes s_i.
\end{aligned}$$

It follows that

$$\varphi(\textstyle\sum n_i \otimes s_i \otimes 1) = \kappa_2\kappa_1^{-1}(\sum n_i \otimes s_i \otimes 1) = \kappa_2(n' \otimes 1 \otimes 1) = \sum n_i \otimes 1 \otimes s_i,$$

i.e., $\beta(n') \in N_\varphi$.

Conversely, for $\sum n_i \otimes s_i \in N_\varphi$, we know that

$$\kappa_1^{-1}(\textstyle\sum n_i \otimes s_i \otimes 1) = \kappa_2^{-1}(\sum n_i \otimes 1 \otimes s_i),$$

which implies

$$p_1^{N'}(\kappa^{-1}(\textstyle\sum n_i \otimes s_i)) = p_2^{N'}(\kappa^{-1}(\sum n_i \otimes s_i)).$$

Since S/R is faithfully flat, it follows from Proposition 2.11 that $\kappa^{-1}(\sum n_i \otimes s_i) = n' \otimes 1$ for some $n' \in N'$. Hence, $\sum n_i \otimes s_i = \beta(n')$ for some $n' \in N'$.

Remark 4.5. As before, if N has additional structures, the descent formalism can be rewritten with respect to certain structures on N. For example, if N is a Lie algebra over R, we can define the group functor $\mathbf{Aut}(N)$ by

$$\mathbf{Aut}(N) : R' \to \mathrm{Aut}_{R'\text{-Lie}}(N \otimes R'),$$

where $\mathrm{Aut}_{R'\text{-Lie}}(N \otimes R')$ is the group of automorphisms of the R'–Lie algebra $N \otimes R'$. Then the set of isomorphism classes of R–Lie algebras N' such that

$$N' \otimes S \cong N \otimes S$$

as S–Lie algebras bijectively corresponds to the first cohomology set $\mathrm{H}^1(S/R, \mathbf{Aut}(N))$.

Example 4.6. Let $\mathbb{R}$ be the field of real numbers. The quaternion algebra $\mathbb{H}$ over $\mathbb{R}$ is the four dimensional associative $\mathbb{R}$–algebra $\mathbb{H} := \mathbb{R}1 \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$ defined by the relations

$$i^2 = j^2 = k^2 = -1, \quad k = ij = -ji.$$

Then $\mathbb{H}$ is a $\mathbb{C}/\mathbb{R}$–form (associative algebra) of the associative algebra $\mathrm{Mat}_2(\mathbb{R})$ of 2×2–matrices with entries in $\mathbb{R}$.

Corollary 4.7 (Hilbert's Theorem 90)**.** *Let R be a local ring, and $\mathbf{GL}_{n,R} := \mathbf{GL}(R^n)$ for $n \geqslant 1$. Then, for every faithfully flat ring extension S/R,*

$$\mathrm{H}^1(S/R, \mathbf{GL}_{n,R}) = 1.$$

Proof. Let $N = R^n$ be the free R–module of rank n. By Theorem 4.4, the first cohomology set $\mathrm{H}^1(S/R, \mathbf{GL}_{n,R})$ bijectively corresponds to the set of isomorphism classes of R–modules N' such that $N' \otimes S \cong N \otimes S$. Such an R–module N' is projective of finite type by Proposition 2.12. Since R is local, we know that N' is free. Moreover, N' is of rank n since

$$N' \otimes S \cong N \otimes S \cong S^n.$$

Hence, $N' \cong R^n$, i.e., there is only one N' (up to isomorphism) such that $N' \otimes S \cong N \otimes S$. This completes the proof. □

Remark 4.8. Let S_1/R and S_2/R be two faithfully flat extensions, and $f : S_1 \to S_2$ be a morphism in R-**alg**. By functoriality of $\mathbf{G}$, f induces a map

$$\mathrm{H}^1(S_1/R, \mathbf{G}) \to \mathrm{H}_1(S_2/R, \mathbf{G}).$$

Moreover, all faithfully flat extensions of R form an inductive system in R-**alg**, which yields an inductive system of pointed sets $\mathrm{H}^1(S/R, \mathbf{G})$. We define

$$\mathrm{H}^1(R, \mathbf{G}) = \varinjlim \mathrm{H}^1(S/R, \mathbf{G}),$$

where the limit is taken in the category of pointed sets with respect to the inductive system above.

For the twisted forms, the elements in $\mathrm{H}^1(R, \mathbf{GL}(N))$ bijectively correspond to isomorphism classes of R–modules N' such that $N' \otimes S \cong N \otimes S$ for some faithfully flat extension S/R.

Remark 4.9. If $f : \mathbf{G} \to \mathbf{H}$ be a morphism of group functors, then it induces a map of pointed set

$$\mathrm{H}^1(S/R, \mathbf{G}) \to \mathrm{H}^1(S/R, \mathbf{H})$$

for every faithfully flat extension S/R.

5 Galois descent

5.1 Generalities

Let Λ and X be non-empty sets. We use $\prod_\Lambda X$ to denote the direct product set of $|\Lambda|$ copies of X, and $(x_\lambda)_{\lambda\in\Lambda}$ to denote an element in $\prod_\Lambda X$.

For a ring extension S/R, we use $\mathrm{Aut}_R(S)$ to denote the group of automorphisms of S which fix R.

Definition 5.1. Let S/R be a ring extension, and Γ a finite subgroup of $\mathrm{Aut}_R(S)$. The ring extension S/R is called Galois with Galois group Γ if both of the following conditions are satisfied

(Gal1) S/R is faithfully flat.

(Gal2) The map

$$\varrho : S\otimes S \to \prod_\Gamma S, \quad a\otimes b \mapsto (\gamma(a)b)_{\gamma\in\Gamma}, \tag{5.1}$$

is an isomorphism of S–algebras.

It is obvious that if S/R is a Galois extension with Galois group Γ, then the map

$$\tilde{\varrho} : S\otimes S \to \prod_\Gamma S, \quad a\otimes b \mapsto (\gamma^{-1}(a)b), \tag{5.2}$$

is also an isomorphism of S–algebras.

Proposition 5.2. *Let S/R be a Galois extension with Galois group Γ. Then*

$$R = S^\Gamma = \{s\in S | \gamma(s) = s, \forall \gamma\in\Gamma\}.$$

Proof. Since S/R is faithfully flat, the sequence

$$0 \longrightarrow R \longrightarrow S \underset{p_2}{\overset{p_1}{\rightrightarrows}} S\otimes S$$

is exact. i.e.,

$$R = \{s\in S | s\otimes 1 = 1\otimes s\}.$$

Applying the isomorphism ϱ, we get

$$R = \{s\in S|\varrho(s\otimes 1) = \varrho(1\otimes s)\} = \{s\in S|\gamma(s) = s, \forall\gamma\in\Gamma\} = S^\Gamma.$$

This completes the proof. □

Example 5.3.

(i) A usual Galois extension of fields is a Galois extension with the Galois group (cf. P28 in [GS]).

(ii) Let $S = R\times R$ and $\Gamma = \{1,\sigma\}\cong \mathbb{Z}/2\mathbb{Z}$, where

$$\sigma : R\times R \to R\times R, \quad (a,b)\mapsto (b,a).$$

S is a ring extension of R via the diagonal map $\varepsilon : R\to R\times R, r\mapsto r\times r$. Then S/R is Galois with Galois group Γ. Indeed, we can explicitly write down ϱ and ϱ^{-1} as follows:

$$\begin{aligned} S\otimes_R S \to S\times S, &\quad (a,b)\otimes(c,d)\mapsto (ac,bd,bc,ad),\\ S\times S \to S\otimes_R S, &\quad (a,b,c,d)\mapsto (1,0)\otimes(a,d)+(0,1)\otimes(c,b).\end{aligned}$$

Example 5.4. Let $\zeta_m = e^{\frac{2\pi\mathbf{i}}{m}}$ be the standard m-th primitive root of unity in $\mathbb{C}$, $R = \mathbb{C}[t_1^{\pm 1}, \cdots, t_N^{\pm 1}]$ and $S = \mathbb{C}[t_1^{\pm\frac{1}{m_1}}, \cdots, t_N^{\pm\frac{1}{m_N}}]$. Let $\Gamma = \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_N\mathbb{Z}$, which acts on S as follows:

$$(\bar{i}_1, \cdots, \bar{i}_N).t_j^{\frac{1}{m_j}} = \zeta_{m_j}^{i_j} t^{\frac{1}{m_j}}.$$

Then S/R is Galois with Galois group Γ.

Proof. For simplicity, we write $\underline{i} := (i_1, \cdots, i_N) \in \mathbb{Z}^N$, and use $\pi(\underline{i}) = (\bar{i}_1, \cdots, \bar{i}_N)$ to denote the canonical image of $\underline{i}$ in Γ. Let $t^{\underline{i}} := t_1^{\frac{i_1}{m_1}} \cdots t_N^{\frac{i_N}{m_N}}$ and $\zeta^{\underline{i}} = \zeta_{m_1}^{i_1} \cdots \zeta_{m_N}^{i_N}$. Then

$$\pi(\underline{i}).t^{\underline{i}} = \zeta^{\underline{i}} t^{\underline{i}}.$$

For $\underline{i} = (i_1, \cdots, i_N)$ and $\underline{j} = (j_1, \cdots, j_N)$, $\underline{i} \leqslant \underline{j}$ if $i_1 \leqslant j_1, \cdots, i_N \leqslant j_N$, and

$$\underline{i} + \underline{j} = (i_1 + j_1, \cdots, i_N + j_N), \quad \underline{ij} = (i_1 j_1, \cdots, i_N j_N).$$

We first observe that S is a free R–module. In fact,

$$S = \bigoplus_{1 \leqslant \underline{i} \leqslant \underline{m}} t^{\underline{i}} R.$$

It remains to show $\varrho : S \otimes S \to \prod_\Gamma S$ is an isomorphism of S–algebras. To construct the inverse map of ϱ, it is suffices to prove that there are $a_\ell, b_\ell \in S$ such that

$$\sum_\ell \gamma(a_\ell) b_\ell = \delta_{1,\gamma} = \begin{cases} 1, & \text{if } \gamma = 1, \\ 0, & \text{if } \gamma \neq 1. \end{cases}$$

Indeed, if such a_ℓ, b_ℓ exist, one can define

$$\varrho^{-1} : \prod_\Gamma S \to S \otimes S, \quad (s_\gamma)_{\gamma\in\Gamma} \mapsto \sum_{\sigma\in\Gamma} \sum_\ell \sigma^{-1}(a_\ell) \otimes b_\ell s_\sigma,$$

which is the inverse of ϱ.

In our situation, we take $a_{\underline{\ell}} = t^{\underline{\ell}}$ and $b_{\underline{\ell}} = t^{-\underline{\ell}}$ for $0 \leqslant \underline{\ell} \leqslant \underline{m} - \underline{1}$, where $\underline{1} = (1, \cdots, 1)$. Then for $\gamma = \pi(\underline{i})$, we verify that

$$\sum_{0 \leqslant \underline{\ell} \leqslant \underline{m}-\underline{1}} \gamma(a_{\underline{\ell}}) b_{\underline{\ell}} = \sum_{0 \leqslant \underline{\ell} \leqslant \underline{m}-\underline{1}} \zeta^{\underline{i}\,\underline{\ell}} = \delta_{\gamma,1}.$$

This completes the proof. □

Lemma 5.5. *Let M be an S–module. The following maps*

$$\varrho_M : M \otimes S \to \prod_\Gamma M, \quad m \otimes s \mapsto (\gamma(s)m)_{\gamma\in\Gamma},$$
$$\widetilde{\varrho}_M : M \otimes S \to \prod_\Gamma M, \quad m \otimes s \mapsto (\gamma^{-1}(s)m)_{\gamma\in\Gamma},$$

are both bijective.

Proof. We show that ϱ_M is bijective. The proof for $\widetilde{\varrho}_M$ is similar.

Since M is an S–module, the canonical map $M \otimes_S S \to M, \quad m \otimes s \to sm$ is an isomorphism with inverse $M \to M \otimes_S S, m \mapsto m \otimes 1$. Note also that $p_2 : S \to S \otimes S, s \mapsto 1 \otimes s$ makes $S \otimes S$

an S–module. Then $M \otimes_S (S \otimes_R S) \to M \otimes_R S, m \otimes (s \otimes t) \mapsto tm \otimes s$ is an isomorphism with inverse map $M \otimes_R S \to M \otimes_S (S \otimes_R S), m \otimes s \mapsto m \otimes (s \otimes 1)$.

Now, we observe that ϱ_M is indeed the composition

$$\begin{array}{lll} M \otimes_R S & \to M \otimes_S S \otimes_R S & \xrightarrow{1\otimes\varrho} \prod_\Gamma (M \otimes_S S) \quad \to \prod_\Gamma M. \\ m \otimes s & \mapsto m \otimes (s \otimes 1) & \mapsto (m \otimes \gamma(s))_{s\in\Gamma} \quad \mapsto (\gamma(s)m)_{\gamma\in\Gamma}, \end{array}$$

in which each map is bijective. Hence, ϱ_M is bijective. □

Lemma 5.6. *The following maps are bijections*

$$\varrho' : S \otimes S \otimes S \to \prod_{\Gamma\times\Gamma} S, \quad a \otimes b \otimes c \mapsto (\gamma_1(a)\gamma_2(b)c)_{(\gamma_1,\gamma_2)\in\Gamma_1\times\Gamma_2}$$

$$\varrho'_M : M \otimes S \otimes S \to \prod_{\Gamma\times\Gamma} M, \quad m \otimes a \otimes b \mapsto (\gamma_1(a)\gamma_2(b)m)_{(\gamma_1,\gamma_2)\in\Gamma_1\times\Gamma_2}$$

Proof. Since Γ is finite, we may identify $S \otimes (\prod_\Gamma S)$ with $\prod_\Gamma (S \otimes S)$. Then ϱ' is indeed the composition

$$S \otimes S \otimes S \xrightarrow{1\otimes\varrho} S \otimes (\prod_\Gamma S) \to \prod_\Gamma (S \otimes S) \xrightarrow{\prod_\Gamma \varrho} \prod_{\Gamma\times\Gamma} S.$$

Each of the maps above is bijective, so is ϱ'.

Similarly, ϱ'_M is bijective. □

5.2 Galois descent: general case

Let S/R be a Galois extension with Galois group Γ and M an S–module with a covering datum

$$\psi : M \otimes S \to M \otimes S.$$

First, ψ uniquely determines a map $h : \prod_\Gamma M \to \prod_\Gamma M$ such that the following diagram

$$\begin{array}{ccc} M \otimes S & \xrightarrow{\tilde{\varrho}_M} & \prod_\Gamma M \\ {\scriptstyle\psi}\downarrow & & \downarrow{\scriptstyle h} \\ M \otimes S & \xrightarrow[\varrho_M]{} & \prod_\Gamma M \end{array} \tag{5.3}$$

commutes. Moreover, we have

Lemma 5.7. *h is a componentwise map. It determines a family of additive isomorphisms $h_\gamma : M \to M, \gamma \in \Gamma$ such that each h_γ is γ–semi-linear, i.e.,*

$$h_\gamma(sm) = \gamma(s)h_\gamma(m), \quad \forall s \in S, m \in M. \tag{5.4}$$

More explicitly, if $\psi(m \otimes 1) = \sum m_i \otimes s_i$, then $h_\gamma = \sum \gamma(s_i)m_i$.

Proof. Define $\delta_{\sigma,\tau} \in S$ by

$$\delta_{\sigma,\tau} = \begin{cases} 1, & \text{if } \sigma = \tau, \\ 0, & \text{otherwise.} \end{cases}$$

We show that h is componentwise, meaning for $\sigma \in \Gamma$ and $m \in M$, we have

$$h((\delta_{\sigma,\gamma}m)_{\gamma\in\Gamma}) = (\delta_{\sigma,\gamma}m')_{\gamma\in\Gamma}$$

for some $m' \in M$. Note that $(\delta_{\sigma,\gamma} m)_{\gamma\in\Gamma} \in \prod_\Gamma M$ is the element with m at the σ–component and 0 at all other components.

Fix $\sigma \in \Gamma$, $(\delta_{\sigma,\gamma})_{\gamma\in\Gamma} \in \prod_\Gamma S$. Recall from (5.1) that $\tilde{\varrho} : S \otimes S \to \prod_\Gamma S$ is an isomorphism. Hence, there is $\sum a_j \otimes b_j \in S \otimes S$ such that

$$\tilde{\varrho}(\textstyle\sum a_j \otimes b_j) = (\sum \gamma^{-1}(a_j) b_j)_{\gamma\in\Gamma} = (\delta_{\sigma,\gamma})_{\gamma\in\Gamma},$$

i.e., $\sum \gamma^{-1}(a_j) b_j = \delta_{\sigma,\gamma}$.

For $m \in M$, let $x = \sum b_j m \otimes a_j \in M \otimes S$. Then

$$\tilde{\varrho}_M(x) = (\textstyle\sum \gamma^{-1}(a_j) b_j m)_{\gamma\in\Gamma} = (\delta_{\sigma,\gamma} m)_{\gamma\in\Gamma}.$$

Write $\psi(m \otimes 1) = \sum m_i \otimes s_i$. Since h is determined by the commutative diagram (5.3) and ψ is a covering datum,

$$\begin{aligned} h((\delta_{\sigma,\gamma} m)_{\gamma\in\Gamma}) &= h\tilde{\varrho}_M(x) = \varrho_M \psi(\textstyle\sum b_j m \otimes a_j) \\ &= \varrho_M((a_j \otimes b_j)\sum(m_i \otimes s_i)) \\ &= \varrho_M(\textstyle\sum a_j m_i \otimes b_j s_i) \\ &= \textstyle\sum \gamma(b_j s_i) a_j m_i \\ &= (\gamma(\textstyle\sum \gamma^{-1}(a_j) b_j)\sum \gamma(s_i) m_i)_{\gamma\in\Gamma} \\ &= (\delta_{\sigma,\gamma} \textstyle\sum \gamma(s_i) m_i)_{\gamma\in\Gamma}. \end{aligned}$$

Hence, h is a componentwise map and it determines an additive map

$$h_\gamma : M \to M, \quad m \mapsto \textstyle\sum \gamma(s_i) m_i,$$

for each $\gamma \in \Gamma$, which is bijective since h is bijective and componentwise.

In addition, if $\psi(m \otimes 1) = \sum m_i \otimes s_i$, then $\psi(sm \otimes 1) = (1 \otimes s)\psi(m \otimes 1) = \sum m_i \otimes s s_i$. It follows that

$$h_\gamma(sm) = \textstyle\sum \gamma(s s_i) m_i = \gamma(s) \sum \gamma(s_i) m_i = \gamma(s) h_\gamma(m),$$

i.e., h_γ is γ–semi-linear. □

Conversely, given a family of additive isomorphisms $(h_\gamma : M \to M)_{\gamma\in\Gamma}$, there is obviously an additive bijection

$$h : \prod_\Gamma M \to \prod_\Gamma M, \quad (m_\gamma)_{\gamma\in\Gamma} \mapsto (h_\gamma(m_\gamma))_{\gamma\in\Gamma}.$$

It uniquely determines an additive isomorphism $\psi : M \otimes S \to M \otimes S$ such that the diagram (5.1) commutes. Moreover, if h_γ is γ–semi-linear for all $\gamma \in \Gamma$, then ψ is a covering datum. Indeed, it suffices to show, for $m \in M, a, b \in S$,

$$\psi(am \otimes bs) = (b \otimes a)\psi(m \otimes s),$$

which is equivalent to

$$\varrho_M \psi(am \otimes bs) = \varrho_M((b \otimes a)\psi(m \otimes s)).$$

We write $\psi(m \otimes s) = \sum m'_i \otimes s'_i$, then

$$(\textstyle\sum \gamma(s'_i) m'_i)_{\gamma\in\Gamma} = \varrho_M(\sum m'_i \otimes s'_i) = h\tilde{\varrho}_M(m \otimes s) = h((\gamma^{-1}(s)m)_{\gamma\in\Gamma}) = (s h_\gamma(m))_{\gamma\in\Gamma},$$

i.e.,

$$\textstyle\sum \gamma(s'_i) m'_i = s h_\gamma(m) \tag{5.5}$$

for all $\gamma \in \Gamma$. A direct computation shows that

$$\varrho_M\psi(am \otimes bs) = h\tilde{\varrho}_M(am \otimes bs) = (h_\gamma(\gamma^{-1}(bs)am))_{\gamma\in\Gamma} = (\gamma(a)bsh_\gamma(m))_{\gamma\in\Gamma}$$
$$\varrho_M((b \otimes a)\psi(m \otimes s)) = \varrho_M(\sum bm'_i \otimes as'_i) = (\gamma(a)b\sum\gamma(s'_i)m'_i)_{\gamma\in\Gamma}.$$

By (5.5), we conclude that $\varrho_M\psi(am \otimes bs) = \varrho_M((b \otimes a)\psi(m \otimes s))$. This proves ψ is a covering datum.

In summary, in the situation where S/R is a Galois ring extension with Galois group Γ, a covering datum on an S–module M is given by a family of additive isomorphisms $h_\gamma : M \to M, \gamma \in \Gamma$ such that each h_γ is γ–semi-linear.

In the rest of this subsection, we will rewrite the descent formulism using the Galois covering datum $(h_\gamma)_{\gamma\in\Gamma}$. We assume ψ is a covering datum on M and $\psi^i, i = 0, 1, 2$ are the maps determined by ψ as in (3.2), (3.3), and (3.4), respectively. For each $\gamma \in \Gamma$, h_γ denotes the γ–semi-linear map determined by ψ as above. For $i = 0, 1, 2$, the bijection ψ^i determines a bijection h^i such that the following diagram

$$\begin{array}{ccc} M \otimes S \otimes S & \xrightarrow{\varrho'_M} & \prod_{\Gamma\times\Gamma} M \\ \downarrow{\scriptstyle \psi^i} & & \downarrow{\scriptstyle h^i} \\ M \otimes S \otimes S & \xrightarrow[\varrho'_M]{} & \prod_{\Gamma\times\Gamma} M \end{array} \tag{5.6}$$

is commutative.

Lemma 5.8. *The three maps h^0, h^1, h^2 are determined by the $h_\gamma, \gamma \in \Gamma$. Explicitly, for $m \in M$, $(\sigma_1, \sigma_2) \in \Gamma \times \Gamma$,*

$$h^0\left((\delta_{\sigma_1,\gamma_1}\delta_{\sigma_2,\gamma_2}m)_{(\gamma_1,\gamma_2)\in\Gamma\times\Gamma}\right) = (\delta_{\sigma_2^{-1}\sigma_1,\gamma_1}\delta_{\sigma_2^{-1},\gamma_2}h_{\sigma_2^{-1}}(m))_{(\gamma_1,\gamma_2)\in\Gamma\times\Gamma}$$
$$h^1\left((\delta_{\sigma_1,\gamma_1}\delta_{\sigma_2,\gamma_2}m)_{(\gamma_1,\gamma_2)\in\Gamma\times\Gamma}\right) = (\delta_{\sigma_2^{-1},\gamma_1}\delta_{\sigma_2^{-1}\sigma_1,\gamma_2}h_{\sigma_2^{-1}}(m))_{(\gamma_1,\gamma_2)\in\Gamma\times\Gamma}$$
$$h^2\left((\delta_{\sigma_1,\gamma_1}\delta_{\sigma_2,\gamma_2}m)_{(\gamma_1,\gamma_2)\in\Gamma\times\Gamma}\right) = (\delta_{\sigma_1^{-1},\gamma_1}\delta_{\sigma_1^{-1}\sigma_2,\gamma_2}h_{\sigma_1^{-1}}(m))_{(\gamma_1,\gamma_2)\in\Gamma\times\Gamma}$$

Proof. Note that $(\delta_{\sigma_1,\gamma_1}\delta_{\sigma_2,\gamma_2}m)_{(\gamma_1,\gamma_2)\in\Gamma\times\Gamma}$ is the element in $\prod_{\Gamma\times\Gamma} M$ whose (σ_1, σ_2) component is m and other components are 0. Since every element of $\prod_{\Gamma\times\Gamma} M$ is a finite sum of such elements and h^i is additive, h^i is determined by $h^i\left((\delta_{\sigma_1,\gamma_1}\delta_{\sigma_2,\gamma_2}m)_{(\gamma_1,\gamma_2)\in\Gamma\times\Gamma}\right)$ with $m \in M, \sigma_1, \sigma_2 \in \Gamma$.

Let $x = \sum e_j \otimes e'_j \otimes e''_j \in S \otimes S \otimes S$ such that

$$\sum\gamma_1(e_j)\gamma_2(e'_j)e''_j = \delta_{1,\gamma_1}\delta_{1,\gamma_2}.$$

Such an element x always exists since we may take $x = \varrho'^{-1}((\delta_{1,\gamma_1}\delta_{1,\gamma_2})_{(\gamma_1,\gamma_2)\in\Gamma\times\Gamma})$.

Let $v = \sum e''_j m \otimes \sigma_1^{-1}(e_j) \otimes \sigma_2^{-1}(e'_j) \in M \otimes S \otimes S$. Then

$$\varrho'_M(v) = (\sum\gamma_1\sigma_1^{-1}(e_j)\gamma_2\sigma_2^{-1}(e'_j)e''_j m)_{(\gamma_1,\gamma_2)\in\Gamma\times\Gamma} = (\delta_{\sigma_1,\gamma_1}\delta_{\sigma_2,\gamma_2}m)_{(\gamma_1,\gamma_2)\in\Gamma\times\Gamma}.$$

We now compute $\psi^i(v)$. Write $\psi(m \otimes 1) = \sum m_i \otimes s_i$. Since ψ is a covering datum,

$$\psi(e''_j m \otimes \sigma_1^{-1}(e_j)) = \sum\sigma_1^{-1}(e_j)m_i \otimes e''_j s_i.$$

$$\psi(e''_j m \otimes \sigma_2^{-1}(e'_j)) = \sum\sigma_2^{-1}(e'_j)m_i \otimes e''_j s_i.$$

From the definition of ψ^0, ψ^1, ψ^2, we have

$$\begin{aligned}
\psi^0(v) &= \sum \psi^0(e''_j m \otimes \sigma_1^{-1}(e_j) \otimes \sigma_2^{-1}(e'_j)) \\
&= \sum \sigma_2^{-1}(e'_j) m_i \otimes \sigma_1^{-1}(e_j) \otimes e''_j s_i \\
\psi^1(v) &= \sum \psi^1(e''_j m \otimes \sigma_1^{-1}(e_j) \otimes \sigma_2^{-1}(e'_j)) \\
&= \sum \sigma_2^{-1}(e'_j) m_i \otimes e''_j s_i \otimes \sigma_1^{-1}(e_j) \\
\psi^2(v) &= \sum \psi^1(e''_j m \otimes \sigma_1^{-1}(e_j) \otimes \sigma_2^{-1}(e'_j)) \\
&= \sum \sigma_1^{-1}(e_j) m_i \otimes e''_j s_i \otimes \sigma_2^{-1}(e'_j)
\end{aligned}$$

Applying ϱ'_M, we obtain

$$\begin{aligned}
\varrho'_M \psi^0(v) &= \left(\sum \gamma_1 \sigma_1^{-1}(e_j) \gamma_2(e''_j s_i) \sigma_2^{-1}(e'_j) m_i\right)_{(\gamma_1,\gamma_2)\in\Gamma\times\Gamma} \\
&= \left(\gamma_2 \left(\sum_j \gamma_2^{-1} \gamma_1 \sigma_1^{-1}(e_j) \gamma_2^{-1} \sigma_2^{-1}(e'_j) e''_j\right) \sum_i \gamma_2(s_i) m_i\right)_{(\gamma_1,\gamma_2)\in\Gamma\times\Gamma} \\
&= \left(\delta_{1,\gamma_2^{-1}\gamma_1\sigma_1^{-1}} \delta_{1,\gamma_2^{-1}\sigma_2^{-1}} \sum \gamma_2(s_i) m_i\right)_{(\gamma_1,\gamma_2)\in\Gamma\times\Gamma} \\
&= \left(\delta_{\sigma_2^{-1}\sigma_1,\gamma_1} \delta_{\sigma_2^{-1},\gamma_2} h_{\sigma_2^{-1}}(m)\right)_{(\gamma_1,\gamma_2)\in\Gamma\times\Gamma}.
\end{aligned}$$

Similarly,

$$\begin{aligned}
\varrho'_M \psi^1(v) &= \left(\sum \gamma_1(e''_j s_i) \gamma_2 \sigma_1^{-1}(e_j) \sigma_2^{-1}(e'_j) m_i\right)_{(\gamma_1,\gamma_2)\in\Gamma\times\Gamma} \\
&= \left(\gamma_1 \left(\sum_j \gamma_1^{-1} \gamma_2 \sigma_1^{-1}(e_j) \gamma_1^{-1} \sigma_2^{-1}(e'_j) e''_j\right) \sum_i \gamma_1(s_i) m_i\right)_{(\gamma_1,\gamma_2)\in\Gamma\times\Gamma} \\
&= \left(\delta_{1,\gamma_1^{-1}\gamma_2\sigma_1^{-1}} \delta_{1,\gamma_1^{-1}\sigma_2^{-1}} \sum \gamma_1(s_i) m_i\right)_{(\gamma_1,\gamma_2)\in\Gamma\times\Gamma} \\
&= \left(\delta_{\sigma_2^{-1},\gamma_1} \delta_{\sigma_2^{-1}\sigma_1,\gamma_2} h_{\sigma_2^{-1}}(m)\right)_{(\gamma_1,\gamma_2)\in\Gamma\times\Gamma},
\end{aligned}$$

and

$$\begin{aligned}
\varrho'_M \psi^2(v) &= \left(\sum \gamma_1(e''_j s_i) \gamma_2 \sigma_2^{-1}(e'_j) \sigma_1^{-1}(e_j) m_i\right)_{(\gamma_1,\gamma_2)\in\Gamma\times\Gamma} \\
&= \left(\gamma_1 \left(\sum_j \gamma_1^{-1} \sigma_1^{-1}(e_j) \gamma_1^{-1} \gamma_2 \sigma_2^{-1}(e'_j) e''_j\right) \sum_i \gamma_1(s_i) m_i\right)_{(\gamma_1,\gamma_2)\in\Gamma\times\Gamma} \\
&= \left(\delta_{1,\gamma_1^{-1}\sigma_1^{-1}} \delta_{1,\gamma_1^{-1}\gamma_2\sigma_2^{-1}} \sum \gamma_1(s_i) m_i\right)_{(\gamma_1,\gamma_2)\in\Gamma\times\Gamma} \\
&= \left(\delta_{\sigma_1^{-1},\gamma_1} \delta_{\sigma_1^{-1}\sigma_2,\gamma_2} h_{\sigma_1^{-1}}(m)\right)_{(\gamma_1,\gamma_2)\in\Gamma\times\Gamma}.
\end{aligned}$$

This complete the proof of the lemma. □

Proposition 5.9. *Let ψ be a covering datum, and $h_\gamma : M \to M, \gamma \in \Gamma$ the additive automorphisms defined by ψ as in Lemma 5.7. Then ψ is a descent datum if and only if*

$$h_{\sigma_1\sigma_2} = h_{\sigma_1} h_{\sigma_2}, \tag{5.7}$$

for all $\sigma_1, \sigma_2 \in \Gamma$.

Proof. From (5.6), ψ is a descent datum if and only if $h^1 = h^0 h^2$. We deduce from Lemma 5.8 that

$$\begin{aligned}
&h^0 h^2((\delta_{\sigma_1,\gamma_1}\delta_{\sigma_2,\gamma_2} m)_{(\gamma_1,\gamma_2)\in\Gamma\times\Gamma}) \\
&= h^0((\delta_{\sigma_1^{-1},\gamma_1}\delta_{\sigma_1^{-1}\sigma_2,\gamma_2} h_{\sigma_1^{-1}}(m))_{(\gamma_1,\gamma_2)\in\Gamma\times\Gamma}) \\
&= (\delta_{(\sigma_1^{-1}\sigma_2)^{-1}\sigma_1^{-1},\gamma_1}\delta_{(\sigma_1^{-1}\sigma_2)^{-1},\gamma_2} h_{(\sigma_1^{-1}\sigma_2)^{-1}}(h_{\sigma_1^{-1}}(m)))_{(\gamma_1,\gamma_2)\in\Gamma\times\Gamma} \\
&= (\delta_{\sigma_2^{-1},\gamma_1}\delta_{\sigma_2^{-1}\sigma_1,\gamma_2} h_{\sigma_2^{-1}\sigma_1}(h_{\sigma_1^{-1}}(m)))_{(\gamma_1,\gamma_2)\in\Gamma\times\Gamma}
\end{aligned}$$

Recall that

$$h^1\left((\delta_{\sigma_1,\gamma_1}\delta_{\sigma_2,\gamma_2}m)_{(\gamma_1,\gamma_2)\in\Gamma\times\Gamma}\right)=(\delta_{\sigma_2^{-1},\gamma_1}\delta_{\sigma_2^{-1}\sigma_1,\gamma_2}h_{\sigma_2^{-1}}(m))_{(\gamma_1,\gamma_2)\in\Gamma\times\Gamma}$$

Hence, $h^1=h^0h^2$ is equivalent to

$$h_{\sigma_2^{-1}}=h_{\sigma_2^{-1}\sigma_1}h_{\sigma_1^{-1}},$$

for all $\sigma_1,\sigma_2\in\Gamma$, i.e., $h_{\sigma_1\sigma_2}=h_{\sigma_1}h_{\sigma_2}$ for all $\sigma_1,\sigma_2\in\Gamma$. □

Now, we consider the descended module associated to the descent datum given by $(h_\gamma)_{\gamma\in\Gamma}$. Recall that

$$N:=\{m\in M|\psi(m\otimes 1)=m\otimes 1\}$$

Hence, $\psi(m\otimes 1)=m\otimes 1$ if and only if $h\tilde{\varrho}_M(m\otimes 1)=\varrho_M\psi(m\otimes 1)=\varrho_M(m\otimes 1)$, i.e.,

$$h((m)_{\gamma\in\Gamma})=(m)_{\gamma\in\Gamma}.$$

which is equivalent to

$$h_\gamma(m)=m,\quad\forall\gamma\in\Gamma.$$

Hence, the descended module N can be rewritten as

$$N:=\{m\in M|h_\gamma(m)=m,\forall\gamma\in\Gamma\}. \tag{5.8}$$

Remark 5.10. Given a Galois descent datum $h_\gamma,\gamma\in\Gamma$, one defines

$$\Gamma\times M\to M,\quad(\gamma,m)\mapsto {}^{\gamma\cdot'}m:=h_\gamma(m),$$

which is an action of Γ on M (called the twisted action of Γ on M determined by ψ). This action is semi-linear, i.e.,

$${}^{\gamma\cdot'}(sm)=\gamma(s)^{\gamma\cdot'}m,\quad\forall s\in S,m\in M. \tag{5.9}$$

and $N=M^\Gamma:=\{m\in M|{}^{\gamma\cdot'}m=m,\forall\gamma\in\Gamma\}$.

Conversely, every semi-linear action of Γ on M defines a family $h_\gamma:M\to M$, $\gamma\in\Gamma$, which determines a descent datum.

5.3 Galois descent: the case of twisted forms

Recall that in the situation where $M=N\otimes S$, a descent datum on M is given by an 1-cocycle φ, which is an element $\varphi\in\mathbf{G}(S\otimes S)$ such that

$$\mathbf{G}(p_{13})(\varphi)=\mathbf{G}(p_{23})(\varphi)\mathbf{G}(p_{12})(\varphi). \tag{5.10}$$

In this section, we will reformulate the 1–cocylce condition (5.10) under the assumption that S/R is a Galois extension. Throughout this subsection, we assume that S/R is a Galois extension with Galois group Γ, N is an R–module and $M=N\otimes S$. We denote $\mathbf{GL}(N)$ by $\mathbf{G}$.

It is easy to observe that $\mathbf{G}(\prod_\Gamma S)=\prod_\Gamma\mathbf{G}(S)$[1]. By the functoriality of $\mathbf{G}$, the isomorphism $\varrho:S\otimes S\to\prod_\Gamma S$ induces an isomorphism

$$\mathbf{G}(\varrho):\mathbf{G}(S\otimes S)\to\prod_\Gamma\mathbf{G}(S),$$

[1]It is relevant to point out that this condition is always fulfilled if $\mathbf{G}$ is a local functor, e.g. an affine scheme.

under which an element $\varphi \in \mathbf{G}(S \otimes S)$ determines an element

$$\varphi_\gamma := \mathbf{G}(\mathrm{p}_\gamma \varrho)(\varphi) \in \mathbf{G}(S)$$

for each $\gamma \in \Gamma$, where $\mathrm{p}_\gamma : \prod_\Gamma S \to S$ is the standard projection to the γ–component.

Similarly, the isomorphism $\varrho' : S \otimes S \otimes S \to \prod_{\Gamma\times\Gamma} S$ yields the isomorphism of groups

$$\mathbf{G}(\varrho') : \mathbf{G}(S \otimes S \otimes S) \to \prod_{\Gamma\times\Gamma} \mathbf{G}(S)$$

Applying the isomorphism $\mathbf{G}(\varrho')$, the equality (5.10) is equivalent to

$$\mathbf{G}(\varrho' p_{13})(\varphi) = \mathbf{G}(\varrho' p_{23})(\varphi)\mathbf{G}(\varrho' p_{12})(\varphi) \tag{5.11}$$

in $\prod_{\Gamma\times\Gamma} \mathbf{G}(S)$. Consider the projection $\mathrm{p}_{\sigma,\tau} : \prod_{\Gamma\times\Gamma} S \to S$ to the (σ,τ)–component, (5.11) holds if and only if

$$\mathbf{G}(\mathrm{p}_{\sigma,\tau}\varrho' p_{13})(\varphi) = \mathbf{G}(\mathrm{p}_{\sigma,\tau}\varrho' p_{23})(\varphi)\mathbf{G}(\mathrm{p}_{\sigma,\tau}\varrho' p_{12})(\varphi), \quad \forall \sigma,\tau \in \Gamma. \tag{5.12}$$

Based on a direct computation, we know that

$$\begin{aligned}
&\mathrm{p}_{\sigma,\tau}\varrho' p_{12}(s\otimes t) = \mathrm{p}_{\sigma,\tau}\varrho'(s\otimes t\otimes 1) = \mathrm{p}_{\sigma,\tau}((\gamma_1(s)\gamma_2(t))_{(\gamma_1,\gamma_2)\in\Gamma\times\Gamma}) = \sigma(s)\tau(t),\\
&\mathrm{p}_{\sigma,\tau}\varrho' p_{13}(s\otimes t) = \mathrm{p}_{\sigma,\tau}\varrho'(s\otimes 1\otimes t) = \mathrm{p}_{\sigma,\tau}((\gamma_1(s)t)_{(\gamma_1,\gamma_2)\in\Gamma\times\Gamma}) = \sigma(s)t,\\
&\mathrm{p}_{\sigma,\tau}\varrho' p_{23}(s\otimes t) = \mathrm{p}_{\sigma,\tau}\varrho'(1\otimes s\otimes t) = \mathrm{p}_{\sigma,\tau}((\gamma_2(s)t)_{(\gamma_1,\gamma_2)\in\Gamma\times\Gamma}) = \tau(s)t,
\end{aligned}$$

and,

$$\mathrm{p}_\sigma\varrho(s\otimes t) = \mathrm{p}_\sigma((\gamma(s)t)_{\gamma\in\Gamma}) = \sigma(s)t.$$

Hence,

$$\mathrm{p}_{\sigma,\tau}\varrho' p_{12} = \tau\mathrm{p}_{\tau^{-1}\sigma}\circ\varrho, \quad \mathrm{p}_{\sigma,\tau}\varrho' p_{13} = \mathrm{p}_\sigma\varrho, \quad \mathrm{p}_{\sigma,\tau}\varrho' p_{23} = \mathrm{p}_\tau\varrho.$$

Therefore, the equality (5.12) holds if and only if

$$\varphi_\sigma = \varphi_\tau \cdot \mathbf{G}(\tau)(\varphi_{\tau^{-1}\sigma}), \quad \forall \sigma,\tau \in \Gamma. \tag{5.13}$$

For $\lambda \in \mathbf{G}(S)$, we define

$${}^\gamma\lambda := \mathbf{G}(\gamma)(\lambda) = (1\otimes\gamma)\lambda(1\otimes\gamma^{-1}), \quad \gamma \in \Gamma,$$

which indeed gives an action of Γ on $\mathbf{G}(S)$. The condition (5.13) can be rewritten as

$$\varphi_{\tau\sigma} = \varphi_\tau \cdot {}^\tau\varphi_\sigma, \quad \forall \sigma,\tau \in \Gamma.$$

In summary, under the automorphism $\mathbf{G}(\varrho)$, every element $\varphi \in \mathbf{G}(S\otimes S)$ yields a family of elements $\varphi_\gamma \in \mathbf{G}(S), \gamma \in \Gamma$, which can be viewed as a map

$$\Gamma \to \mathbf{G}(S), \quad \gamma \mapsto \varphi_\gamma.$$

In addition, φ is a 1–cocycle if and only if

$$\varphi_{\gamma_1\gamma_2} = \varphi_{\gamma_1} \cdot {}^{\gamma_1}\varphi_{\gamma_2}. \tag{5.14}$$

In other words, $(\varphi_\gamma)_{\gamma\in\Gamma}$ is a 1-cocycle in the sense of Galois cohomology (see Serre's book [Ser]).

Recall from (4.5) that two 1–cocycles $\varphi, \varphi' \in \mathbf{G}(S\otimes S)$ are equivalent if and only if there is an element $\lambda \in \mathbf{G}(S)$ such that

$$(\mathrm{d}^2\lambda)\varphi(\mathrm{d}^1\lambda)^{-1} = \varphi'$$

in $\mathbf{G}(S \otimes S)$, which is equivalent to

$$\mathbf{G}(\mathrm{p}_\sigma \varrho p_2)(\lambda) \cdot \mathbf{G}(\mathrm{p}_\sigma \varrho)(\varphi) \cdot \mathbf{G}(\mathrm{p}_\sigma \varrho p_1)(\lambda)^{-1} = \mathbf{G}(\mathrm{p}_\sigma \varrho)(\varphi'), \tag{5.15}$$

for all $\sigma \in \Gamma$.

As before, a direct computation yields that

$$\mathrm{p}_\sigma \varrho p_1(s) = \mathrm{p}_\sigma \varrho(s \otimes 1) = \mathrm{p}_\sigma((\gamma(s))_{\gamma\in\Gamma}) = \sigma(s), \mathrm{p}_\sigma \varrho p_2(s) \quad = \mathrm{p}_\sigma \varrho(1 \otimes s) = \mathrm{p}_\sigma((s)_{\gamma\in\Gamma}) = s.$$

Hence, the equality (5.15) is equivalent to

$$\lambda \cdot \varphi_\gamma \cdot {}^\gamma\lambda^{-1} = \varphi'_\gamma, \quad \forall \gamma \in \Gamma, \tag{5.16}$$

where $(\varphi_\gamma)_{\gamma\in\Gamma}$ and $(\varphi'_\gamma)_{\gamma\in\Gamma}$ are the Galois 1–cocycles associated to φ and φ', respectively.

The formula (5.16) defines an equivalent relation on the set of Galois 1–cocycles. The set of equivalence classes is denoted by $\mathrm{H}^1(\Gamma, \mathbf{G}(S))$. This definition can be generalized to an arbitrary group functor $\mathbf{G}$.

Given a Galois 1–cocyle $(\varphi_\gamma)_{\gamma\in\Gamma}$ associated to the 1–cocycle $\varphi \in \mathbf{G}(S \otimes S)$, let us write down the descended module associated to this Galois 1–cocyle. Recall from (4.2) that a descended module determined by φ is

$$N' = \{\textstyle\sum n_i \otimes s_i \in N \otimes S | \varphi(\sum n_i \otimes s_i \otimes 1) = \sum n_i \otimes 1 \otimes s_i\}.$$

Note that the following diagram is commutative:

$$\begin{array}{ccc}
N \otimes S \otimes S & \xrightarrow{\varphi} & N \otimes S \otimes S \\
\downarrow{\scriptstyle 1\otimes\varrho} & & \downarrow{\scriptstyle 1\otimes\varrho} \\
\prod_\Gamma N \otimes S & \xrightarrow{\mathbf{G}(\varrho)(\varphi)} & \prod_\Gamma N \otimes S \\
\downarrow{\scriptstyle \mathrm{p}_\gamma} & & \downarrow{\scriptstyle \mathrm{p}_\gamma} \\
N \otimes S & \xrightarrow[\varphi_\gamma := \mathbf{G}(\mathrm{p}_\gamma \varrho)(\varphi)]{} & N \otimes S
\end{array}$$

Hence, $\sum n_i \otimes s_i \in N'$ if and only if

$$\varphi_\gamma(\textstyle\sum n_i \otimes \gamma(s_i)) = \sum n_i \otimes s_i, \quad \forall \gamma \in \Gamma.$$

Note that Γ acts on $M = N \otimes S$ by ${}^\gamma(n \otimes s) = n \otimes \gamma(s)$, we obtain

$$N' = \{m \in M | \varphi_\gamma({}^\gamma m) = m, \forall \gamma \in \Gamma\}. \tag{5.17}$$

We can also explicitly write down the Galois descent datum corresponding to the Galois 1–cocycle $(\varphi_\gamma)_{\gamma\in\Gamma}$. In fact, one defines

$$h_\gamma : M \to M, \quad m \mapsto \varphi_\gamma({}^\gamma m),$$

for $\gamma \in \Gamma$. It is obvious that each h_γ is a γ–semi-linear additive automorphism for all $\gamma \in \Gamma$. To show $(h_\gamma)_{\gamma\in\Gamma}$ is a Galois descent datum, we verify that

$$\begin{aligned}
h_{\sigma\tau}(m) &= \varphi_{\sigma\tau}({}^{\sigma\tau}m) = \varphi_\sigma({}^\sigma\varphi_\tau)({}^{\sigma\tau}m) \\
&= \varphi_\sigma \, {}^\sigma(\varphi_\tau({}^{\sigma^{-1}\sigma\tau}m)) = \varphi_\sigma \, {}^\sigma(\varphi_\tau({}^\tau m)) \\
&= \varphi_\sigma \, {}^\sigma(h_\tau(m)) = h_\sigma h_\tau(m),
\end{aligned}$$

for all $\sigma, \tau \in \Gamma$ and $m \in M$, i.e., $h_{\sigma\tau} = h_\sigma h_\tau$. Hence, $(h_\gamma)_{\gamma\in\Gamma}$ is a Galois descent datum on M. In other words,

$$^{\gamma\cdot'}m = h_\gamma(m) = \varphi_\gamma(^\gamma m), \quad \gamma \in \Gamma, m \in M$$

defines a "twisted" action of Γ on M. The subset of elements of M which are fixed by this "twisted" action is equal to the descended module N' as described in (5.17).

Given an R–module N and a faithfully flat ring extension S/R, we know from Theorem 4.4 that the set of isomorphism classes of S/R–forms of N bijectively corresponds to the first cohomology set $\mathrm{H}^1(S/R, \mathbf{GL}(N))$, which is identified with $\mathrm{H}^1(\Gamma, \mathbf{GL}(N)(S))$ when S/R is a Galois extension. Alternatively, this can also be proved directly as follows:

Theorem 5.11. *Let S/R be a Galois extension of rings with finite Galois group Γ, N an R–module, and $\mathbf{G} := \mathbf{GL}(N)$. Then for a Galois 1–cocycle $\varphi : \Gamma \to \mathbf{G}(S), \gamma \mapsto \varphi_\gamma$, the R–module*

$$N_\varphi := \{m \in N \otimes S | \varphi_\gamma(^\gamma m) = m, \forall \gamma \in \Gamma\}$$

is an S/R–form of N. Moreover, the map which sends a cohomological class $[\varphi] \in \mathrm{H}^1(\Gamma, \mathbf{G}(S))$ to the R–module isomorphism class $[N_\varphi]$ containing N_φ is a bijection from $\mathrm{H}^1(\Gamma, \mathbf{G}(S))$ to the set of isomorphism classes of S/R–forms of N.

Proof. For convenience, we put $h_\gamma := \varphi_\gamma(1 \otimes \gamma) : N \otimes S \to N \otimes S$ for $\gamma \in \Gamma$. Then $h_{\sigma\tau} = h_\sigma h_\tau$ for $\sigma, \tau \in \Gamma$.

We first proof N_φ is an S/R–form of N. Define

$$f : N_\varphi \otimes S \to N \otimes S, \quad (\sum n_i \otimes s_i) \otimes s \mapsto \sum n_i \otimes s_i s. \tag{5.18}$$

It is obviously a homomorphism of S–modules. We claim that f is an isomorphism of S–modules.

We first show that f is surjective. Since $\varrho : S \otimes S \to \prod_\Gamma S$ is an isomorphism, there exist $s_i, t_i \in S$ such that $\sum_i \gamma(s_i)t_i = \delta_{1,\gamma}$ for all $\gamma \in \Gamma$. For $n \in N$, take $m_i = \sum_{\sigma\in\Gamma} h_\sigma(n \otimes s_i) \in N \otimes S$. Then

$$\varphi_\gamma(^\gamma m_i) = \textstyle\sum_{\sigma\in\Gamma} h_\gamma h_\sigma(n \otimes s_i) = \sum_{\sigma\in\Gamma} h_{\sigma\gamma}(n \otimes s_i) = \sum_{\sigma\in\Gamma} h_\sigma(n \otimes s_i) = m_i,$$

i.e., $m_i \in N_\varphi$. Let $x = \sum m_i \otimes t_i$. Then

$$\begin{aligned} f(\textstyle\sum_i m_i \otimes t_i) &= \displaystyle\sum_i m_i t_i = \sum_i \sum_{\sigma\in\Gamma} h_\sigma(n \otimes s_i)t_i = \sum_{\sigma\in\Gamma} \varphi_\sigma(n \otimes 1) \sum_i \sigma(s_i)t_i \\ &= \displaystyle\sum_{\sigma\in\Gamma} \delta_{1,\sigma}\varphi_\sigma(n \otimes 1) = \varphi_1(n \otimes 1) = n \otimes 1. \end{aligned}$$

Note that f is a homomorphism of S–module and $N \otimes S$ is an S–module generated by $n \otimes 1$ with $n \in N$. Hence, f is surjective.

To prove that f is injective. Let $\sum m_i \otimes a_i \in \ker f \subseteq N_\varphi \otimes S$, where $m_i \in N_\varphi$ and $s_i \in S$. Then

$$f(\textstyle\sum m_i \otimes a_i) = \sum m_i a_i = 0.$$

Since $m_i \in N_\varphi$, $h_\gamma(m_i) = m_i$ for all $\gamma \in \Gamma$. By the semi–linearity of h_γ, we have

$$0 = h_\gamma(\textstyle\sum m_i a_i) = \sum h_\gamma(m_i)\gamma(a_i) = \sum m_i \gamma(a_i), \quad \forall \gamma \in \Gamma. \tag{5.19}$$

Note that $N_\varphi \subseteq N \otimes S$ is an R–submodule and S/R is a faithfully flat extension, we may identify $N_\varphi \otimes S$ with an S–submodule of $N \otimes S \otimes S$. It is enough to show $\sum m_i \otimes a_i = 0$ in $N \otimes S \otimes S$. Since S/R is a Galois extension, the map

$$\beta : N \otimes S \otimes S \to \prod_\Gamma N \otimes S, \quad n \otimes s \otimes t \mapsto (n \otimes s\gamma(t))_{\gamma\in\Gamma}$$

is an isomorphism of R–modules. We deduce from (5.19) that

$$\beta(\sum m_i \otimes a_i) = (\sum m_i \gamma(a_i))_{\gamma\in\Gamma} = 0,$$

Hence, $\sum m_i \otimes a_i = 0$, i.e., f is injective.

Now we claim that $N_\varphi \cong N_{\varphi'}$ (as R–modules) if and only if $\varphi \sim \varphi'$. If $\phi : N_\varphi \to N_{\varphi'}$ is an isomorphism of R–module, we consider

$$\lambda := f_{\varphi'}(\phi \otimes \mathrm{id}) f_\varphi^{-1},$$

where $f_\varphi : N_\varphi \otimes S \to N \otimes S$ and $f_{\varphi'} : N_{\varphi'} \otimes S \to N \otimes S$ are the isomorphisms described in (5.18). Then $\lambda \in \mathbf{G}(S)$. Let $h_\gamma = \varphi_\gamma(\mathrm{id} \otimes \gamma)$ and $h'_\gamma = \varphi'_\gamma(\mathrm{id} \otimes \gamma)$ for $\gamma \in \Gamma$. Then we verify that, for $m \in N_\varphi \subseteq N \otimes S$ and $\gamma \in \Gamma$,

$$\lambda h_\gamma(m) = \lambda(m) = \phi(m) = h'_\gamma(\phi(m)) = h'_\gamma \lambda(m).$$

Note that f_φ is an isomorphism of S–modules, $N \otimes S$ is generated by $m, m \in N_\varphi$ as an S–module. We thus obtain

$$\lambda h_\gamma = h'_\gamma \lambda, \quad \forall \gamma \in \Gamma.$$

It follows that

$$\begin{aligned}
\varphi'_\gamma &= h'_\gamma(\mathrm{id} \otimes \gamma^{-1}) \\
&= \lambda h_\gamma \lambda^{-1}(\mathrm{id} \otimes \gamma^{-1}) \\
&= \lambda \varphi_\gamma(\mathrm{id} \otimes \gamma)\lambda^{-1}(\mathrm{id} \otimes \gamma^{-1}) \\
&= \lambda \varphi_\gamma {}^\gamma \lambda^{-1},
\end{aligned}$$

i.e., $\varphi \sim \varphi'$.

Conversely, if $\varphi \sim \varphi'$, then there is $\lambda \in \mathbf{G}(S)$ such that

$$\varphi'_\gamma = \lambda \cdot \varphi_\gamma \cdot {}^\gamma \lambda^{-1}.$$

Hence, for $m \in N \otimes S$ and $\gamma \in \Gamma$, we have

$$\varphi'_\gamma({}^\gamma(\lambda(m))) = \lambda \cdot \varphi_\gamma \cdot ({}^\gamma\lambda^{-1})({}^\gamma(\lambda(m))) = \lambda \varphi_\gamma({}^\gamma m).$$

From the definition of N_φ and $N_{\varphi'}$, we deduce that $m \in N_\varphi$ if and only $\lambda(m) \in N_{\varphi'}$. Hence, $\lambda|_{N_\varphi} : N_\varphi \to N_{\varphi'}$ is an isomorphism of R–modules.

To conclude the proof, we show that every S/R–form of N is isomorphic to N_φ for some Galois 1–cocycle $\varphi = (\varphi_\gamma)_{\gamma\in\Gamma}$. Let N' be an S/R–form of N, then there is an isomorphism of S–module

$$\kappa : N' \otimes_R S \to N \otimes_R S.$$

We define $\varphi_\gamma = \kappa(1 \otimes \gamma)\kappa^{-1}(1 \otimes \gamma^{-1})$ for $\gamma \in \Gamma$. It is easy to verify that $\varphi_\gamma \in \mathbf{G}(S)$ for each $\gamma \in \Gamma$ and

$$\varphi_{\sigma\tau} = \varphi_\sigma \cdot {}^\sigma \varphi_\tau, \quad \forall \sigma, \tau \in \Gamma,$$

i.e., $\varphi = (\varphi_\gamma)_{\gamma\in\Gamma}$ is a Galois 1–cocyle. Finally, one easily verifies that $\kappa|_{N' \otimes 1}$ is an isomorphism onto N_φ. □

6 Application to infinite dimensional Lie theory

Let k be a ring, and A an k–algebra. The *centroid* of A is defined to be

$$\mathrm{Ctd}_k(A) = \{\chi \in \mathrm{End}_k(A) | \chi(ab) = \chi(a)b = a\chi(b), \forall a, b \in A\}.$$

It is easy to observe that $\mathrm{Ctd}_k(A)$ is an associative algebra with unit over k, and A is naturally a (left) $\mathrm{Ctd}_k(A)$–algebra.

Further more, each $r \in k$ yields an element of $\mathrm{Ctd}_k(A)$, namely $\chi_r : A \to A, x \mapsto rx$ $\chi_r \in \mathrm{Ctd}_k(A)$. Hence, there is a canonical map

$$\chi_{A,k} : k \to \mathrm{Ctd}_k(A), \quad r \mapsto \chi_r.$$

We say that A is *central* if $\chi_{A,k}$ is an isomorphism.

We say A is *perfect* if $A = AA = \{\sum a_i b_i : a_i, b_i \in A\}$.

Lemma 6.1. *Let R/k be a ring extension, and A an R–algebra. If A is perfect, then $\mathrm{Ctd}_R(A)$ is commutative and $\mathrm{Ctd}_R(A) = \mathrm{Ctd}_k(A)$.*

Proof. Let $\chi_1, \chi_2 \in \mathrm{Ctd}_R(A)$. Then

$$\chi_1\chi_2(ab) = \chi_1(\chi_2(ab)) = \chi_1(\chi_2(a)b) = \chi_2(a)\chi_1(b) = \chi_2(a\chi_1(b)) = \chi_2(\chi_1(ab)) = \chi_2\chi_1(ab),$$

for $a, b \in A$. Since A is perfect, $\chi_1\chi_2 = \chi_2\chi_1$.

Also, if $r \in R$, $\chi \in \mathrm{Ctd}_k(A)$

$$\chi(rab) = ra\chi(b) = r(a\chi(b)) = r\chi(ab),$$

for $a, b \in A$. Since A is perfect, $\chi \in \mathrm{Ctd}_R(A)$. □

Lemma 6.2. *Let A be a k–algebra which is of finite presentation as a k–module. Assume R/k is a flat ring extension. Then the canonical isomorphism*

$$\mathrm{End}_k(A) \otimes_k R \to \mathrm{End}_R(A \otimes_k R)$$

induces an isomorphism

$$\mathrm{Ctd}_k(A) \otimes_k R \cong \mathrm{Ctd}_R(A \otimes_k R).$$

Proof. Define

$$\begin{aligned} \beta_{A,k} : \mathrm{End}_k(A) &\to \mathrm{Hom}_k(A \otimes A, A \oplus A) \\ f &\mapsto \beta_{A,k} : a \otimes b \mapsto (f(ab) - f(a)b, f(ab) - af(b)) \end{aligned}$$

By definition, we have

$$\mathrm{Ctd}_k(A) = \ker(\beta_{A,k}).$$

Since R/k is flat and A is of finite presentation as a k–module, the following diagram is commutative

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Ctd}_k(A) \otimes_k R & \longrightarrow & \mathrm{End}_k(A) \otimes_k R & \longrightarrow & \mathrm{Hom}_k(A \otimes A, A \oplus A) \otimes_k R \\ & & & & \cong \downarrow & & \downarrow \cong \\ 0 & \longrightarrow & \mathrm{Ctd}_R(A \otimes_k R) & \longrightarrow & \mathrm{End}_R(A \otimes_k R) & \longrightarrow & \mathrm{Hom}_R(A_R \otimes_R A_R, A_R \oplus A_R) \end{array}$$

It follows that $\mathrm{Ctd}_k(A) \otimes_k R \cong \mathrm{Ctd}_R(A \otimes_k R)$. □

From now on, we assume $k = \mathbb{C}$ is the field of complex numbers, and $\zeta_m = e^{\frac{2\pi i}{m}}$ is the standard m-th primitive root of unity. We also fix the notations

$$\begin{aligned} R &= k[t_1^{\pm 1}, \cdots, t_N^{\pm 1}], \\ S &= k[t_1^{\pm \frac{1}{m_1}}, \cdots, t_N^{\pm \frac{1}{m_N}}], \\ \Gamma &= (\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_N\mathbb{Z}). \end{aligned}$$

Recall from Example 5.4 that S/R is a Galois extension with Galois group Γ.

Let A be a finite dimensional k–algebra and $\sigma_1, \cdots, \sigma_N \in \mathrm{Aut}_k(A)$ mutually commutative and of finite order $\sigma_i^{m_i} = 1$, $i = 1, \cdots, N$. Then A is decomposed as a direct sum

$$A = \bigoplus_{(\bar{i}_1, \cdots, \bar{i}_N) \in \Gamma} A_{\bar{i}_1, \cdots, \bar{i}_N},$$

where $A_{\bar{i}_1, \cdots, \bar{i}_N} = \{a \in A | \sigma_j(a) = \zeta_{m_j}^{i_j} a, j = 1, 2, \cdots, N\}$ for $(i_1, \cdots, i_N) \in \mathbb{Z}^N$.

Now, we define

$$\mathcal{L} = \mathcal{L}(A, \sigma_1, \cdots, \sigma_N) = \bigoplus_{(i_1, \cdots, i_N) \in \mathbb{Z}^N} A_{i_1, \cdots, i_N} \otimes k t_1^{\frac{i_1}{m_1}} \cdots t_N^{\frac{i_N}{m_N}}.$$

Remark 6.3. Every affine Kac-Moody algebra (derived modulo center) is isomorphic to a twisted loop Lie algebra $L(\mathfrak{g}, \pi)$, where $\mathfrak{g}$ is a finite dimensional simple Lie algebra over k and π is an automorphism of $\mathfrak{g}$ determined by an automorphism of the Dykin diagram of $\mathfrak{g}$.

Remark 6.4. The centreless core of an extended affine Lie algebra is a Lie torus. Except for the Lie tori of type A, which is well understood, every Lie torus is a multiloop algebra $\mathcal{L}(\mathfrak{g}, \sigma_1, \cdots, \sigma_N)$, where $\mathfrak{g}$ is a finite dimensional Lie algebra, and $\sigma_1, \cdots, \sigma_N$ are a family of mutually commutative diagram automorphisms of $\mathfrak{g}$. [2] (cf. [ABFP09]).

For a twisted multiloop algebra $\mathcal{L} = \mathcal{L}(A, \sigma_1, \cdots, \sigma_N)$, we know the following facts:

(i) $\mathcal{L}$ is an R–algebra

(ii) $\mathcal{L} \otimes_R S \cong A \otimes_k S$ as an S–algebra. In fact, $\mathcal{L}$ is isomorphic to the S/R–form determined by the Galois 1–cocylce

$$u : \Gamma \to \mathbf{Aut}(A)(S), \quad (\bar{i}_1, \cdots, \bar{i}_N) \mapsto (\sigma_1^{-i_1} \otimes 1) \cdots (\sigma_N^{-i_N} \otimes 1).$$

Lemma 6.5. *Assume A is central and perfect. Then $\mathcal{L}$ is perfect and $\chi_{\mathcal{L},R} : R \to \mathrm{Ctd}(\mathcal{L})$ is an isomorphism, where $\mathrm{Ctd}(\mathcal{L}) = \mathrm{Ctd}_k(\mathcal{L}) = \mathrm{Ctd}_R(\mathcal{L})$.*

Proof. Clearly $\mathcal{L}\mathcal{L} \otimes_R S = (\mathcal{L} \otimes_R S)(\mathcal{L} \otimes_R S)$,

$$(\mathcal{L}/\mathcal{L}\mathcal{L}) \otimes_R S \cong \frac{\mathcal{L} \otimes_R S}{(\mathcal{L} \otimes_R S)(\mathcal{L} \otimes_R S)} \cong \frac{A \otimes_k S}{(A \otimes_k S)(A \otimes_k S)} = 0$$

Since S/R is faithfully flat, $\mathcal{L}/\mathcal{L}\mathcal{L} = 0$, i.e., $\mathcal{L} = \mathcal{L}\mathcal{L}$.

Consider

$$R \otimes_R S \to \mathrm{Ctd}(\mathcal{L}) \otimes_R S \cong \mathrm{Ctd}(\mathcal{L} \otimes_R S) = \mathrm{Ctd}(A \otimes_k S) \cong \mathrm{Ctd}_k(A) \otimes_k S \cong S$$

Hence, $R \otimes_R S \to \mathrm{Ctd}(\mathcal{L}) \otimes_R S$ is an isomorphism. Since S/R is faithfully flat, $\chi_{\mathcal{L},R}$ is an isomorphism. □

[2] The converse result is not true. i.e., a multiloop Lie algebra is not necessarily a Lie torus.

Next, we will describe $\mathrm{Der}_k(\mathcal{L})$. Define a map

$$\eta_{\mathcal{L}} : \mathrm{Der}_k(\mathcal{L}) \to \mathrm{Der}_k(\mathrm{Ctd}(\mathcal{L})) = \mathrm{Der}_k(R), \quad \delta \mapsto \eta_{\mathcal{L}}(\delta),$$

where

$$\eta_{\mathcal{L}}(\delta) : \mathrm{Ctd}(\mathcal{L}) \to \mathrm{Ctd}(\mathcal{L}), \quad \chi \mapsto [\delta, \chi] = \delta\chi - \chi\delta.$$

It can be verified that $\eta_{\mathcal{L}}$ is a homomorphism of Lie algebras over k. Moreover, it fits in the exact sequence of Lie algebras

$$0 \to \mathrm{Der}_R(\mathcal{L}) \to \mathrm{Der}_k(\mathcal{L}) \xrightarrow{\eta_{\mathcal{L}}} \mathrm{Der}_k(R), \tag{6.1}$$

In the case where $\mathcal{L} = A \otimes_k R$, the homomorphism $\eta_{\mathcal{L}}$ has a section

$$\rho : \mathrm{Der}_k(R) \to \mathrm{Der}_k(A \otimes_k R), \quad d' \mapsto 1 \otimes d'.$$

This shows that the sequence (6.1) is split for $\mathcal{L} = A \otimes_k R$.

In general, we observe that the extension S/R indeed is étale (flat and unramified), in which case any $d \in \mathrm{Der}_k(R)$ can be extended uniquely to a derivation $d' \in \mathrm{Der}_k(S)$. Further, note that for $\gamma \in \Gamma$, $\gamma d' \gamma^{-1}$ is also a derivation extending d, thus $\gamma d' = d'\gamma$.

Now $\mathcal{L} \subseteq A \otimes_k S$ is a twisted form of $A \otimes_k R$, which is given by a 1-cocycle $(\varphi_\gamma)_{\gamma\in\Gamma}$, i.e.,

$$\mathcal{L} = \{x \in A \otimes_k S | \varphi_\gamma({}^\gamma x) = x, \forall \gamma \in \Gamma\}.$$

If $x = \sum a_i \otimes s_i \in \mathcal{L}$, then

$$\begin{aligned}
\varphi_\gamma({}^\gamma((1 \otimes d')x)) &= \varphi_\gamma({}^\gamma(\textstyle\sum a_i \otimes d'(s_i))) \\
&= \varphi_\gamma(\textstyle\sum a_i \otimes \gamma d'(s_i)) \\
&= \varphi_\gamma(\textstyle\sum a_i \otimes d'\gamma(s_i)) \\
&= (1 \otimes d')\varphi_\gamma(\textstyle\sum a_i \otimes \gamma(s_i)) \\
&= (1 \otimes d')\textstyle\sum a_i \otimes s_i.
\end{aligned}$$

Hence $\varphi_\gamma({}^\gamma((1 \otimes d')x)) = (1 \otimes d')x$, i.e., $(1 \otimes d')x \in \mathcal{L}$.

Hence, we obtain a map $\rho : \mathrm{Der}_k(R) \to \mathrm{Der}_k(\mathcal{L})$, which is a a section of $\eta_{\mathcal{L}}$. The exactness of the sequence (6.1) implies that

$$\mathrm{Der}_k(\mathcal{L}) = \mathrm{Der}_R(\mathcal{L}) \rtimes \rho(\mathrm{Der}_k(R)). \tag{6.2}$$

In the case where $A = \mathfrak{g}$ is a finite dimensional simple Lie algebra over k, the $\mathrm{Der}_R(\mathcal{L})$ is also understood by descent. Using Whitehead's first lemma,

$$\mathrm{Der}_S(\mathfrak{g} \otimes_k S) = \mathrm{IDer}(\mathfrak{g} \otimes_k S) = \{\mathrm{ad}x | x \in \mathfrak{g} \otimes_k S\}.$$

Since $\mathcal{L} \otimes_R S \cong \mathfrak{g} \otimes_k S$, it is clear that

$$\mathrm{IDer}(\mathcal{L}) \otimes_R S \cong \mathrm{IDer}(\mathcal{L} \otimes_R S) = \mathrm{IDer}(\mathfrak{g} \otimes_k S).$$

It follows that

$$\frac{\mathrm{Der}_R(\mathcal{L})}{\mathrm{IDer}(\mathcal{L})} \otimes_R S \cong \frac{\mathrm{Der}_S(A \otimes_k S)}{\mathrm{IDer}(A \otimes_k S)} = 0.$$

Hence, the faithful flatness of S/R yields that

$$\mathrm{Der}_R(\mathcal{L}) = \mathrm{IDer}(\mathcal{L}). \tag{6.3}$$

Summarizing (6.2) and (6.3), we know that

$$\mathrm{Der}_k(\mathcal{L}) = \mathrm{IDer}(\mathcal{L}) \rtimes \rho(\mathrm{Der}_k(R)).$$

References

[ABFP09] B. Allison, S. Berman, J. Faulkner, and A. Pianzola, *Multiloop realization of extended affine Lie algebras and Lie tori*. Transactions of the American Mathematical Society, 361(9):4807-4842, 2009.

[Bour] N. Bourbaki, *Algèbre Commutative, Chapitres 1 à 4*, Springer, 1985.

[GS] P. Gille and T. Szamuely, *Central Simple Algebras and Galois Cohomology*, Cambridge University Press, 2006.

[P05] A. Pianzola, *Vanishing of H^1 for Dedekind rings and applications to loop algebras*, Comptes Rendus Mathematique, 340(9):633-638, 2005.

[P10] A. Pianzola, *Derivations of certain algebras defined by étale descent*, Mathematische Zeitschrift, 264(3):485-495, 2010.

[Ser] J. P. Serre, *Galois Cohomology*. Springer Verlag, 2002.