GALOIS DESCENT

KEITH CONRAD

1. Introduction

Let L/K be a field extension. A K-vector space W can be extended to an L-vector space $L \otimes_K W$, and W embeds into $L \otimes_K W$ by $w \mapsto 1 \otimes w$. Under this embedding, when $W \neq 0$ a K-basis $\{e_i\}$ of W turns into an L-basis $\{1 \otimes e_i\}$ of $L \otimes_K W$. Passing from W to $L \otimes_K W$ is called *ascent*. In the other direction, if we are given an L-vector space $V \neq 0$, we may ask how to describe the K-subspaces $W \subset V$ such that a K-basis of W is an L-basis of V.

Definition 1.1. For an L-vector space V, a K-subspace W such that a K-basis of W is an L-basis of V is called a K-*form* of V.

For completeness, when $V = 0$ (so there is no basis), we regard $W = 0$ as a K-form of V. The passage from an L-vector space V to a K-form of V is called *descent*. Whether we can descend is the question of filling in the question mark in the figure below.

$$\begin{array}{ccccc} L & & L \otimes_K W & & V \\ | & & \uparrow & & \uparrow \\ K & & W & & ? \end{array}$$

Example 1.2. A K-form of L^n is K^n since the standard K-basis of K^n is an L-basis of L^n.

Example 1.3. A K-form of $\mathrm{M}_n(L)$ is $\mathrm{M}_n(K)$ since the standard K-basis of $\mathrm{M}_n(K)$ is an L-basis of $\mathrm{M}_n(L)$.

Example 1.4. A K-form of $L[X]$ is $K[X]$ since the K-basis $\{1, X, X^2, \dots\}$ of $K[X]$ is an L-basis of $L[X]$.

Example 1.5. Every L-vector space V has a K-form: when $V \neq 0$, pick any L-basis $\{e_i\}$ of V and its K-span is a K-form of V since the e_i's are linearly independent over K and thus are a basis of their K-span.

When $K = \mathbf{R}$ and $L = \mathbf{C}$, ascent (passing from W to $\mathbf{C} \otimes_{\mathbf{R}} W$) is the process of complexification and descent is related to conjugations on complex vector spaces: an $\mathbf{R}$-form of a complex vector space is the fixed set of a conjugation.

Our definition of a K-form involves a choice of basis. Let's check this choice doesn't really matter:

Theorem 1.6. *Let V be a nonzero L-vector space and W be a nonzero K-subspace of V. The following conditions are equivalent:*

1. *any K-basis of W is an L-basis of V,*
2. *some K-basis of W is an L-basis of V.*

(3) *the L-linear map $L \otimes_K W \to V$ given by $a \otimes w \mapsto aw$ is an isomorphism of L-vector spaces.*

Proof. (1) $\Rightarrow$ (2): Obvious.

(2) $\Rightarrow$ (3): Suppose the K-basis $\{e_i\}$ of W is an L-basis of V. Then the L-linear map $L \otimes_K W \to V$ given by $a \otimes w \mapsto aw$ sends $1 \otimes e_i$ to e_i so it identifies L-bases of two L-vector spaces. Therefore this map is an isomorphism.

(3) $\Rightarrow$ (1): Suppose $L \otimes_K W \cong V$ as L-vector spaces by $a \otimes w \mapsto aw$. For any K-basis $\{e_i\}$ of W, $\{1 \otimes e_i\}$ is an L-basis of $L \otimes_K W$ and therefore under the indicated isomorphism the vectors $1 \cdot e_i = e_i$ are an L-basis of V. □

The second property of Theorem 1.6 is how we defined a K-form. The first property shows the concept of a K-form is independent of the choice of basis. The third property is the "right" definition of a K-form,[1] although the other properties are arguably a better way to understand what the concept is all about (or even to recognize it in concrete cases like Examples 1.2, 1.3, and 1.4.)

In the $\mathbf{C}/\mathbf{R}$-case, $\mathbf{R}$-forms of a complex vector space are parametrized by the conjugations on V. Generalizing this, we will see that when L/K is a finite Galois extension, we can parametrize the K-forms of an L-vector space V by keeping track of how $\mathrm{Gal}(L/K)$ can act in a "semilinear" way on V.[2] We will find that for any semilinear action of $\mathrm{Gal}(L/K)$ on a nonzero L-vector space V, there is an L-basis of $\mathrm{Gal}(L/K)$-invariant vectors: that means $\sigma(v) = v$ for all $\sigma \in \mathrm{Gal}(L/K)$.

References on this material are [1, pp. 295–296], [3, Chap. 17], and [5, pp. 66–68].

2. Galois descent on vector spaces

From now on we suppose L/K is a finite Galois extension and write $G = \mathrm{Gal}(L/K)$. We will introduce an organized way for G to act on an L-vector space (which we will call a G-structure), where G interacts in a reasonable way with scalar multiplication by L.

Definition 2.1. For an L-vector space V and $\sigma \in G$, a *σ-linear* map $r\colon V \to V$ is an additive function on V such that

$$r(av) = \sigma(a)r(v) \tag{2.1}$$

for all a in L and v in V.

When σ is the identity automorphism of L, r is L-linear. For general σ in G, r is K-linear (take $a \in K$ in (2.1)), but it is not quite L-linear; the effect of scaling by L on V is "twisted" by σ when r is applied. When the reference to σ in (2.1) is not needed, the label *semilinear* is used, but it should be kept in mind that a semilinear map is always relative to a choice of field automorphism σ of L.

Example 2.2. If V is a complex vector space and $\sigma\colon \mathbf{C} \to \mathbf{C}$ is complex conjugation, a σ-linear map on V is a conjugate-linear map.

Example 2.3. On L^n, $r_\sigma(a_1, \ldots, a_n) = (\sigma(a_1), \ldots, \sigma(a_n))$ is σ-linear.

Example 2.4. On $\mathrm{M}_n(L)$, $r_\sigma(a_{ij}) = (\sigma(a_{ij}))$ is σ-linear.

[1] Among other things, the third property makes sense for the zero vector space without needing a separate definition in that case.

[2] The concept of a K-form does not require L/K to be Galois, but in the Galois case we can say a lot about all the K-forms.

Example 2.5. On $L[X]$, $r_\sigma(\sum_{i=0}^d a_i X^i) = \sum_{i=0}^d \sigma(a_i)X^i$ is σ-linear.

Example 2.6. When W is a K-vector space, we can apply σ to the "first component" in $L \otimes_K W$: the function $r_\sigma = \sigma \otimes \mathrm{id}_W$ mapping $L \otimes_K W$ to itself by

$$r_\sigma(a \otimes w) = \sigma(a) \otimes w$$

on simple tensors is σ-linear, since $r_\sigma(a'(a\otimes w)) = r_\sigma(a'a\otimes w) = \sigma(a'a)\otimes w = \sigma(a')\sigma(a)\otimes w = \sigma(a')(\sigma(a)\otimes w)$, so $r_\sigma(a't) = a'r_\sigma(t)$ for all t in $L \otimes_K W$ by additivity.

Since $r_\sigma(1 \otimes w) = 1 \otimes w$ and the condition $r_\sigma(a \otimes w) = \sigma(a) \otimes w$ is equivalent to $r_\sigma(a(1 \otimes w)) = \sigma(a)r_\sigma(1 \otimes w)$, this semilinear action of G on $L \otimes_K W$ is the unique one that fixes $1 \otimes W$ pointwise.

Definition 2.7. A *G-structure* on an L-vector space V is a set of functions $r_\sigma \colon V \to V$, one for each σ in G, such that r_σ is σ-linear, $r_1 = \mathrm{id}_V$, and $r_\sigma \circ r_{\sigma'} = r_{\sigma\sigma'}$. When V is given a G-structure, we say G acts *semilinearly* on V.

Example 2.8. When $K = \mathbf{R}$ and $L = \mathbf{C}$, so $G = \mathrm{Gal}(\mathbf{C}/\mathbf{R})$ is the identity and complex conjugation, to describe a G-structure on a complex vector space V we only need to describe the map $r \colon V \to V$ associated to complex conjugation, since by Definition 2.1 the map associated to the identity of G has to be the identity. The conditions r must satisfy are: r is additive, $r(zv) = \overline{z}r(v)$, and $r^2 = \mathrm{id}_V$. This is nothing other than a conjugation on V, so a choice of $\mathrm{Gal}(\mathbf{C}/\mathbf{R})$-structure on a complex vector space is the same as a choice of conjugation on it.

Example 2.9. The maps r_σ in Examples 2.3, 2.4, 2.5, and 2.6, as σ runs over G, are a G-structure on L^n, $\mathrm{M}_n(L)$, $L[X]$, and $L \otimes_K W$. The G-structure in Example 2.6 is called the *standard G-structure* on $L \otimes_K W$.

Example 2.10. If $\varphi \colon V \to V'$ is an L-vector space isomorphism and V has a G-structure $\{r_\sigma\}$, there is a unique G-structure $\{r'_\sigma\}$ on V' compatible with φ: $r'_\sigma(v') = \varphi(r_\sigma\varphi^{-1}(v'))$:

$$\begin{array}{ccc} V & \xrightarrow{\varphi} & V' \\ {\scriptstyle r_\sigma}\downarrow & & \downarrow{\scriptstyle r'_\sigma} \\ V & \xrightarrow[\varphi]{} & V' \end{array}$$

Just as it is simpler to write group actions on sets as gx instead of $\pi_g(x)$ (where π_g is the permutation on X associated to g), it is simpler to write $r_\sigma(v)$ as just $\sigma(v)$. In this notation, the equation $r_\sigma(av) = \sigma(a)r_\sigma(v)$ becomes $\sigma(av) = \sigma(a)\sigma(v)$. So a G-structure on an L-vector space V is a way of making the group G act semilinearly on V: each $\sigma \in G$ is σ-linear on V, $\mathrm{id}_L \in G$ acts as id_V, and $\sigma(\sigma'(v)) = (\sigma\sigma')(v)$ for all σ and σ' in G and $v \in V$.

On a complex vector space V there is a one-to-one correspondence between $\mathbf{R}$-forms of V and conjugations on V. We will generalize this correspondence to one between K-forms of an L-vector space and G-structures on the vector space. (This is a generalization since Example 2.8 says conjugations on a complex vector space are basically the same thing as $\mathrm{Gal}(\mathbf{C}/\mathbf{R})$-structures on the vector space.)

First we need several lemmas.

Lemma 2.11. *Let V be an L-vector space with a G-structure and let V' be an L-subspace that is preserved by G: for all $\sigma \in G$, $\sigma(V') \subset V'$. Then the quotient vector space V/V' has a G-structure defined by $\sigma(v + V') = \sigma(v) + V'$.*

Proof. We check that the action of G on V/V' is well-defined: if $v_1 \equiv v_2 \bmod V'$ then $v_1 - v_2 \in V'$, so for any $\sigma \in G$ we have $\sigma(v_1 - v_2) \in \sigma(V') \subset V'$. Thus $\sigma(v_1) - \sigma(v_2) \in V'$, so $\sigma(v_1) \equiv \sigma(v_2) \bmod V'$. That each σ acts σ-linearly on V/V' is clear, because the relevant conditions are already satisfied on V and thus work out on coset representatives. Further details are left to the reader. □

Lemma 2.12. *Let A be an abelian group and $\chi_1, \ldots, \chi_n \colon A \to L^\times$ be distinct homomorphisms. For an L-vector space V and $v_1, \ldots, v_n \in V$, if $\chi_1(a)v_1 + \cdots + \chi_n(a)v_n = 0$ for all $a \in A$ then all v_i are 0.*

Proof. The special case $V = L$ is the linear independence of characters. It is left as an exercise to reread the proof of that special case and generalize the argument. □

When V is an L-vector space with a G-structure, the fixed set of G in V is

$$V^G = \{v \in V : \sigma(v) = v \text{ for all } \sigma \in G\}.$$

This is a K-subspace. When $K = \mathbf{R}$ and $L = \mathbf{C}$, so a G-structure on V is a choice of conjugation c on V, $V^G = \{v \in V : c(v) = v\}$.

Lemma 2.13. *Let V be an L-vector space with a G-structure. Define a corresponding trace map $\mathrm{Tr}_G \colon V \to V$ by*

$$\mathrm{Tr}_G(v) = \sum_{\sigma \in G} \sigma(v).$$

Then $\mathrm{Tr}_G(V) \subset V^G$, and when $v \neq 0$ in V there is $a \in L$ such that $\mathrm{Tr}_G(av) \neq 0$. In particular, if $V \neq 0$ then $V^G \neq 0$.

Proof. To show the values of Tr_G are in V^G, for any $\sigma' \in G$

$$\sigma'(\mathrm{Tr}_G(v)) = \sum_{\sigma \in G} \sigma'(\sigma(v)) = \sum_{\sigma \in G} (\sigma'\sigma)(v) = \sum_{\sigma \in G} \sigma(v) = \mathrm{Tr}_G(v).$$

To show if $v \neq 0$ that $\mathrm{Tr}_G(av) \neq 0$ for some $a \in L$, we prove the contrapositive. Assume for a fixed $v \in V$ that $\mathrm{Tr}_G(av) = 0$ for all $a \in L$. Then

$$0 = \sum_{\sigma \in G} \sigma(av) = \sum_{\sigma \in G} \sigma(a)\sigma(v)$$

for all $a \in L$. By Lemma 2.12 with $A = L^\times$, every $\sigma(v)$ is 0. In particular, at $\sigma = \mathrm{id}_L$ we get $v = 0$. □

Next is our main result linking K-forms and G-structures. We will use the tensor product description of a K-form (from Theorem 1.6): a K-subspace W of an L-vector space V is a K-form exactly when the natural L-linear map $L \otimes_K W \to V$ is an isomorphism of L-vector spaces.

Theorem 2.14. *Let V be an L-vector space. There is a bijection between the following data on V:*

(1) *K-forms of V,*
(2) *G-structures on V.*

In brief, the correspondence from (1) to (2) is $W \rightsquigarrow L \otimes_K W$ with its standard G-structure and the correspondence from (2) to (1) is $V \rightsquigarrow V^G$.

Proof. This is clear if $V = 0$ since $\{0\}$ is the only K-form (even the only K-subspace) and there is only one G-structure. So from now on take $V \neq 0$. If we start with a K-form W of V, so $\varphi\colon L \otimes_K W \to V$ by $a \otimes w \mapsto aw$ is an L-linear isomorphism, we get a G-structure on V by using φ to transport the standard G-structure $\{r_\sigma\}$ on $L \otimes_K W$ (Example 2.6) to a G-structure $\{\sigma_W\}_{\sigma \in G}$ on V (Example 2.10). We simply insist the diagrams

$$\begin{array}{ccc} L \otimes_K W & \xrightarrow{\varphi} & V \\ {\scriptstyle r_\sigma}\downarrow & & \vdots\,{\scriptstyle \sigma_W} \\ L \otimes_K W & \xrightarrow[\varphi]{} & V \end{array}$$

commute for all $\sigma \in G$. Explicitly, set

$$\sigma_W\left(\sum_i a_i w_i\right) = \sum_i \sigma(a_i) w_i,$$

where $a_i \in L$ and $w_i \in W$. (The well-definedness of this formula, where the w_i's are any elements of W, depends on φ being an isomorphism of L-vector spaces.)

Conversely, if V has a G-structure then the K-subspace V^G turns out to be a K-form on V: the L-linear map $f\colon L \otimes_K V^G \to V$ by $a \otimes w \mapsto aw$ is an isomorphism.

To show f is one-to-one, suppose $f(t) = 0$ for some $t \in L \otimes_K V^G$. Write t as a sum of simple tensors, say $t = \sum a_i \otimes w_i$. This finite sum can be arranged to have w_i's that are linearly independent over K: here we need to know $V^G \neq 0$ (Lemma 2.13). Then $0 = f(t) = \sum a_i w_i$. We will show K-linearly independent vectors in V^G are L-linearly independent in V, hence all a_i are 0 and this would mean $t = 0$ so f is injective. To prove every K-linearly independent set in V^G is L-linearly independent, assume otherwise: there is a K-linearly independent set in V^G that is L-linearly dependent: such a dependence relation looks like

$$a_1 w_1 + \cdots + a_n w_n = 0, \tag{2.2}$$

where $w_1, \ldots, w_n \in V^G$ and the a_i's in L are not all 0. Take (2.2) to be a nontrivial L-linear relation among K-linearly independent vectors in V^G of least length (least number of terms). Then every a_i is nonzero and $n \geq 2$. By scaling, we may suppose $a_n = 1$. Applying $\sigma \in G$ to (2.2), we get

$$\sigma(a_1) w_1 + \cdots + \sigma(a_n) w_n = 0. \tag{2.3}$$

Subtract (2.3) from (2.2):

$$(a_1 - \sigma(a_1)) w_1 + \cdots + (a_n - \sigma(a_n)) w_n = 0.$$

The last term is 0 since $a_n = 1$, so this L-linear relation has $n-1$ terms. By the minimality of n, such an L-linear relation among K-linearly independent vectors $w_1, \ldots, w_{n-1}$ has to be the trivial relation: $a_i - \sigma(a_i) = 0$ for $i = 1, 2, \ldots, n-1$. So each a_i is fixed by all σ in G, hence $a_i \in K$ for $i = 1, 2, \ldots, n-1$. Also $a_n = 1 \in K$. But that means (2.2) is a nontrivial linear dependence relation among the w_i's over K, that is impossible (the w_i's are linearly independent over K). So we have a contradiction, which proves f is one-to-one.

To show f is onto, we look at the image $f(L \otimes_K V^G)$, which is an L-subspace of V. This image is stable under the action of G: on simple tensors $a \otimes w$ in $L \otimes_K V^G$,

$$\sigma(f(a \otimes w)) = \sigma(aw) = \sigma(a)\sigma(w) = \sigma(a)w = f(\sigma(a) \otimes w),$$

so by additivity of σ on V we have $\sigma(f(L \otimes_K V^G)) \subset f(L \otimes_K V^G)$. Therefore the quotient space $\overline{V} := V/f(L \otimes_K V^G)$ inherits a G-structure from V by $\sigma(\overline{v}) = \overline{\sigma(v)}$ (Lemma 2.11). For $v \in V$, $\mathrm{Tr}_G(v) \in V^G \subset f(L \otimes_K V^G)$, so on $\overline{V}$ we have $\mathrm{Tr}_G(\overline{v}) = \overline{\mathrm{Tr}_G(v)} = \overline{0}$. Since all elements of $\overline{V}$ have trace $\overline{0}$, $\overline{V}$ has to be $\overline{0}$ by Lemma 2.13. (A nonzero element of $\overline{V}$ would have a nonzero L-multiple with nonzero trace.) Since $\overline{V} = \overline{0}$, $V = f(L \otimes_K V^G)$, so f is onto.

In the $\mathbf{C}/\mathbf{R}$-case, the surjectivity of $f\colon \mathbf{C} \otimes_{\mathbf{R}} V_c \to V$ for any complex vector space V with a conjugation c is based on the equation

$$v = \frac{v + c(v)}{2} + i\frac{v - c(v)}{2i}, \tag{2.4}$$

where the vectors $\frac{1}{2}(v + c(v))$ and $\frac{1}{2i}(v - c(v))$ are fixed by c. The formula (2.4) can be generalized to the L/K-case using Tr_G: if $\{\alpha_1, \ldots, \alpha_d\}$ is a K-basis of L then there are $\{\beta_1, \ldots, \beta_d\}$ in L such that $v = \sum_j \alpha_j \mathrm{Tr}_G(\beta_j v)$ for all $v \in V$. That would give a second proof of surjectivity of f.

It remains to check that our correspondences between K-forms of V and G-structures on V are inverses of one another.

K-form to G-structure and back: Pick a K-form W of V. The corresponding G-structure $\{\sigma_W : \sigma \in G\}$ on V is given by $\sigma_W(\sum_i a_i w_i) := \sum_i \sigma(a_i) w_i$ for $a_i \in L$ and $w_i \in W$. We need to check the subspace $V^G = \{v \in V : \sigma_W(v) = v \text{ for all } \sigma \in G\}$ associated to this G-structure is W. Certainly $W \subset V^G$.

To show $V^G \subset W$, pick a K-basis $\{e_i\}$ of W. Since W is a K-form of V, any $v \in V$ has the form $v = \sum a_i e_i$ with $a_i \in L$ (all but finitely many coefficients a_i are 0). Then $\sigma_W(v) = \sum_i \sigma(a_i) e_i$. If $\sigma_W(v) = v$ for all $\sigma \in G$ then

$$\sum_i (\sigma(a_i) - a_i) e_i = 0$$

for all $\sigma \in G$. The e_i's are linearly independent over L (because they are the basis of a K-form of V), so $\sigma(a_i) - a_i = 0$ for all a_i and all $\sigma \in G$. Thus all a_i are in K, so $v \in W$. Thus $V^G \subset W$.[3]

G-structure to K-form and back: Given a G-structure on V, which we write simply as $v \rightsquigarrow \sigma(v)$, the corresponding K-form is V^G. We have to check that the isomorphism $L \otimes_K V^G \to V$ given by $a \otimes w \mapsto aw$ transports the standard G-structure on $L \otimes_K V^G$ to the original G-structure we started with on V (rather than to some other G-structure on V). Under the isomorphism $L \otimes_K V^G \to V$, a tensor $\sum_i a_i \otimes w_i$ in $L \otimes_K V^G$ is identified with $\sum_i a_i w_i$ in V, and the standard G-structure on the tensor product is given by $\sigma(\sum_i a_i \otimes w_i) = \sum_i \sigma(a_i) \otimes w_i$ (for all $\sigma \in G$), which goes over to $\sum_i \sigma(a_i) w_i$ in V by the isomorphism. Since the w_i's are in V^G, $\sum_i \sigma(a_i) w_i = \sigma(\sum_i a_i w_i)$, so the isomorphism from $L \otimes_K V^G$ to V does identify the standard G-structure on $L \otimes_K V^G$ with the original G-structure on V. □

The down-to-earth content of Theorem 2.14 is that when G acts semilinearly on V, there is a spanning set of V over L consisting of G-invariant vectors. Using this is called *Galois descent*.

Remark 2.15. Theorem 2.14 is true when L/K is an infinite Galois extension and the semilinear action $G \times V \to V$ is continuous, where G has its profinite topology and V has the discrete topology. See [2, Lemma 5.8.1].

[3]That $V^G \subset W$ can also be proved using the normal basis theorem.

Corollary 2.16. *If V has a G-structure, K-independent vectors in V^G are L-independent.*

Proof. A K-independent subset of V^G can be extended to a K-basis of V^G, which is an L-basis of V (since V^G is a K-form of V), so it is linearly independent over L. □

Corollary 2.17. *For any K-vector space W, with $L \otimes_K W$ given its standard G-structure, $(L \otimes_K W)^G = 1 \otimes W$.*

Proof. Exercise. □

Example 2.18. Let X be a finite set on which the Galois group $G = \mathrm{Gal}(L/K)$ acts (by permutations). Then the space $V = \mathrm{Map}(X, L)$ of all functions $X \to L$ is an L-vector space under pointwise operations. A basis of V over L is $\{\delta_x : x \in X\}$. The group G acts semilinearly on V: for any function $f\colon X \to L$ in V and $\sigma \in G$, define $\sigma(f)\colon X \to L$ so the diagram

$$\begin{array}{ccc} X & \xrightarrow{f} & L \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\sigma} \\ X & \xrightarrow[\sigma(f)]{} & L \end{array}$$

commutes. This means $\sigma(f)(\sigma(x)) = \sigma(f(x))$ for all $x \in X$, so

$$\sigma(f)(x) = \sigma(f(\sigma^{-1}(x))).$$

This equation defines $\sigma(f)$ as a function $X \to L$. Let's check $\sigma\colon V \to V$ is σ-linear. For $a \in L$, we want to check that $\sigma(af) = \sigma(a)\sigma(f)$. Well, at each $x \in X$,

$$\begin{aligned} (\sigma(af))(x) &= \sigma((af)(\sigma^{-1}(x))) \\ &= \sigma(af(\sigma^{-1}(x))) \\ &= \sigma(a)\sigma(f(\sigma^{-1}(x))) \\ &= \sigma(a)(\sigma(f)(x)), \end{aligned}$$

so $\sigma(af) = \sigma(a)\sigma(f)$ as functions in $\mathrm{Map}(X, L)$. Check $\sigma(\delta_x) = \delta_{\sigma(x)}$.

What is V^G? It is natural to guess that V^G equals $\mathrm{Map}(X, K)$, which is the K-span of $\{\delta_x : x \in X\}$. As a small piece of evidence, $\mathrm{Map}(X, K)$ is a K-subspace of V with K-dimension $\#X$ and $\dim_K(V^G) = \dim_L(V) = \#X$ too. However, the delta-functions δ_x lie in $\mathrm{Map}(X, K)$ and $\sigma(\delta_x) = \delta_x$ only when $\sigma(x) = x$. Therefore all the δ_x's are in V^G only when G acts trivially on X. So V^G is *not* $\mathrm{Map}(X, K)$ if G acts nontrivially on X. In fact,

$$\begin{aligned} V^G &= \{f : \sigma(f) = f\} \\ &= \{f : \sigma(f(\sigma^{-1}(x))) = f(x) \text{ for all } \sigma, x\} \\ &= \{f : \sigma(f(x)) = f(\sigma(x)) \text{ for all } \sigma, x\}, \end{aligned}$$

so V^G consists of the functions $X \to L$ that commute with the G-actions on X and L. Functions satisfying $\sigma(f(x)) = f(\sigma(x))$ for all $\sigma \in G$ and $x \in X$ are called G-maps (they respect the G-actions). Because V^G spans V over L, every function $X \to L$ is an L-linear combination of G-maps $X \to L$.

If G acts trivially on X then $V^G = \{f : \sigma(f(x)) = f(x) \text{ for all } \sigma, x\} = \mathrm{Map}(X, K)$, so a G-map $X \to L$ in this case is just a function $X \to K$.

We conclude this section by showing how to interpret Theorem 2.14 in terms of representations. (If you don't know representations of finite groups, you may want to skip the rest of this section.) First let's recall how you could discover that the ring $\mathbf{C}[G]$ should be relevant to representations of G on complex vector spaces. Let's stare at the formulas

$$\rho(\sigma)(cv) = c\rho(\sigma)(v) \quad \text{and} \quad \rho(\sigma)(\rho(\tau)v) = \rho(\sigma\tau)(v) \tag{2.5}$$

for a representation ρ of G on a complex vector space V (here $c \in \mathbf{C}$ and $v \in V$). Now abstract these formulas by writing some neutral symbol e_σ for $\rho(\sigma)$ and taking away v: introduce the $\mathbf{C}$-vector space $\mathbf{C}[G] = \bigoplus_{\sigma \in G} \mathbf{C}e_\sigma$ with multiplication rules

$$e_\sigma c = ce_\sigma \quad \text{and} \quad e_\sigma e_\tau = e_{\sigma\tau} \tag{2.6}$$

inspired by (2.5). Now $\mathbf{C}[G]$ is an associative ring with identity, and even a $\mathbf{C}$-algebra since $\mathbf{C}$ commutes with all the basis vectors e_σ. We can consider any representation ρ of G on V as a way of letting the basis vectors e_σ act as $\mathbf{C}$-linear maps $V \to V$, by $e_\sigma v = \rho(\sigma)(v)$, and the conditions (2.5) and (2.6) say precisely that this makes V into a (left) $\mathbf{C}[G]$-module. Conversely, any left $\mathbf{C}[G]$-module structure on V provides a representation of G on V by focusing attention on how the e_σ's inside $\mathbf{C}[G]$ act on V (which doesn't lose any information since the e_σ's span V).

Now let's look at G-structures on an L-vector space V, where $G = \mathrm{Gal}(L/K)$, with the goal of finding an abstract ring whose module structures on any L-vector space V are the same thing as G-structures on V. Any G-structure on V provides us with σ-linear maps $r_\sigma \colon V \to V$ for all $\sigma \in G$, which means the r_σ's are additive and

$$r_1(v) = v, \quad r_\sigma(cv) = \sigma(c)r_\sigma(v), \quad \text{and} \quad r_\sigma(r_\tau(v)) = r_{\sigma\tau}(v) \tag{2.7}$$

for all $c \in L$ and $v \in V$. Now let's wipe v out of these equations and turn the maps r_σ into basis vectors e_σ. Define the L-vector space $C(G) = \bigoplus_{\sigma \in G} Le_\sigma$ and declare multiplication in $C(G)$ to be given by the rules

$$e_1 = 1, \quad e_\sigma c = \sigma(c)e_\sigma, \quad \text{and} \quad e_\sigma e_\tau = e_{\sigma\tau} \tag{2.8}$$

for σ and τ in G and $c \in L$.[4] This makes $C(G)$ an associative ring with identity e_1 (check!) and $C(G)$ is a K-algebra (since $e_\sigma c = ce_\sigma$ when $c \in K$). If G is not trivial (that is, $L \neq K$), $e_\sigma c$ is not ce_σ for $c \in L - K$, so $C(G)$ is not an L-algebra (in the same way the quaternions $\mathbf{H}$ are an $\mathbf{R}$-algebra but not a $\mathbf{C}$-algebra even though $\mathbf{C} \subset \mathbf{H}$).

The multiplication rules (2.8) in $C(G)$ are an abstract form of the way a G-structure behaves, as described in (2.7): a G-structure on V is the same thing as a left $C(G)$-module structure on V, where e_σ acts on V as the σ-linear map r_σ. Explicitly, if we have a G-structure $\{r_\sigma\}$ on V then make V into a $C(G)$-module by the formula

$$\left(\sum_{\sigma \in G} a_\sigma e_\sigma\right)(v) = \sum_{\sigma \in G} a_\sigma r_\sigma(v)$$

and, conversely, if V has a $C(G)$-module structure then focusing on how the basis vectors e_σ act on V gives us a G-structure (check specifically why each e_σ is a σ-linear map on V from the definition of a $C(G)$-module structure on V). Theorem 2.14 therefore says, in terms of $C(G)$, that the K-forms of V are essentially the same thing as the $C(G)$-module structures on V.

[4]Unlike the group ring $\mathbf{C}[G]$, the construction of $C(G)$ depends essentially on G being a Galois group since we use its action on L in the definition of the multiplication in (2.8).

The most basic example of a $C(G)$-module is L, on which $G = \mathrm{Gal}(L/K)$ acts by its very nature as a Galois group and this extends to a $C(G)$-module structure via the formula $(\sum_{\sigma\in G} a_\sigma e_\sigma)(x) = \sum_{\sigma\in G} a_\sigma\sigma(x)$ for all $x \in L$. That every G-structure has an associated K-form tells us something about $C(G)$-submodules of a $C(G)$-module. Let V be a nonzero $C(G)$-module (which is a concise way of saying V is a nonzero L-vector space with a G-structure). The existence of a K-form means V has an L-basis $\{v_i\}$ of G-invariant vectors: $V = \bigoplus_{i\in I} Lv_i$ and $\sigma(v_i) = v_i$ for all $\sigma \in G$. The line Lv_i is preserved under the action of G and L, hence under the action of $C(G) = \bigoplus_{\sigma\in G} Le_\sigma$. Therefore each Lv_i is a $C(G)$-submodule, and v_i being G-invariant makes Lv_i isomorphic to L as $C(G)$-modules by the natural map $xv_i \mapsto x$. (Warning: a $C(G)$-linear map is not L-linear since the e_σ's don't commute with L, unless G is trivial.) Thus all nonzero $C(G)$-modules are direct sums of copies of L as a $C(G)$-module. This in fact is another way of thinking about the existence of K-forms.

Indeed, suppose we knew (by some other method) that every nonzero $C(G)$-module is a direct sum of $C(G)$-submodules that are each isomorphic to L as a $C(G)$-module. Then for any nonzero L-vector space V with a G-structure, view V as a $C(G)$-module and break it up as $\bigoplus_{i\in I} V_i$ where $V_i \cong L$ as $C(G)$-modules. Let $f_i\colon L \to V_i$ be a $C(G)$-module isomorphism and set $v_i = f_i(1)$. Then for any $\sigma \in G$, $\sigma(v_i) = \sigma(f_i(1)) = f_i(\sigma(1)) = f_i(1) = v_i$, so v_i is a G-invariant vector. Since $Lv_i \subset V_i$ and both are L-vector spaces of the same finite K-dimension (because f_i is a K-linear isomorphism, forgetting a little structure in the process), $Lv_i = V_i$. Now the direct sum decomposition $V = \bigoplus_{i\in I} Lv_i$ reveals a K-form for V, namely $W = \bigoplus_{i\in I} Kv_i$.

3. Applications to Vector Spaces

Our first application of Galois descent is to systems of linear equations. If the equations have coefficients in K and there is a nonzero solution over L then there is also one over K.

Theorem 3.1. *For any homogeneous system of linear equations in n unknowns with coefficients in K, the solutions in L^n are L-linear combinations of the solutions in K^n. In particular, if there is a nonzero L-solution then there is a nonzero K-solution.*

Proof. Write the system of linear equations in the form $A\mathbf{x} = \mathbf{0}$, where A is an $m \times n$ matrix with entries in K (m being the number of equations). Let $V \subset L^n$ be the L-solutions of the system: $V = \{\mathbf{v} \in L^n : A\mathbf{v} = \mathbf{0}\}$. There is a standard semilinear (coordinatewise) action of G on L^n, and because A has entries in K the G-action preserves V: if $\mathbf{v} \in V$ then $\sigma(\mathbf{v}) \in V$ because $\sigma(A\mathbf{v}) = A(\sigma(\mathbf{v}))$ and $\sigma(\mathbf{0}) = \mathbf{0}$. So we get a coordinatewise G-structure on V, and by Theorem 2.14 V is spanned over L by its G-fixed set $V^G = V \cap (L^n)^G = V \cap K^n$, which are the solutions to $A\mathbf{x} = \mathbf{0}$ in K^n. □

Theorem 3.1 is true without L/K being Galois: for a K-linear map $A\colon K^n \to K^m$, the map $1 \otimes A\colon L^n \to L^m$ satisfies $\mathrm{im}(1 \otimes A) = L \cdot \mathrm{im}(A)$.

Next we describe how descent behaves on subspaces: if $V' \subset V$ and we have a G-structure on V, when does V' have a K-form in V^G? The answer is connected to the preservation of V' by the G-structure on V.

Theorem 3.2. *Let V be an L-vector space with a G-structure. For an L-subspace $V' \subset V$, the following conditions are equivalent:*

(1) *V' has an L-spanning set in V^G,*
(2) *$\sigma(V') \subset V'$ for all $\sigma \in G$,*

(3) $\sigma(V') = V'$ *for all* $\sigma \in G$,
(4) V' *has a* K*-form in* V^G.

When these hold, the only K*-form of* V' *in* V^G *is* $V' \cap V^G$. *If* $\dim_L(V') < \infty$, *these conditions are the same as* $\dim_K(V' \cap V^G) = \dim_L(V')$.

Proof. Everything is obvious if $V' = 0$, so we may take $V' \neq 0$.

(1) $\Rightarrow$ (2): Suppose $V' = \sum Lv_i$ where $v_i \in V^G$. Then for $\sigma \in G$, $\sigma(V') \subset \sum \sigma(L)v_i = \sum Lv_i = V'$.

(2) $\Rightarrow$ (1): Suppose $\sigma(V') \subset V'$ for all $\sigma \in G$. Then the given G-structure on V is a G-structure on V', so by Theorem 2.14 V' has an L-spanning set in $(V')^G \subset V^G$.

(2) $\Rightarrow$ (3): Using σ^{-1} in place of σ, we have $\sigma^{-1}(V') \subset V'$ so $V' \subset \sigma(V')$. Thus $\sigma(V') = V'$ for all $\sigma \in G$.

(3) $\Rightarrow$ (2): Obvious.

(3) $\Rightarrow$ (4): The G-structure on V is a G-structure on V', so $(V')^G$ is a K-form of V' and $(V')^G \subset V^G$.

(4) $\Rightarrow$ (2): For a K-form W' of V' in V^G, $V' = LW'$, so $\sigma(V') \subset L\sigma(W') = LW' = V'$.

When these conditions hold, $(V')^G$ is a K-form of V', and $(V')^G = V' \cap V^G$. Suppose W' is any K-form of V' in V^G. We want to show $W' = (V')^G$. The natural map $L \otimes_K W' \to V'$ given by $a \otimes w' \mapsto aw'$ is an L-vector space isomorphism, and the transported G-structure on V' from the standard G-structure on $L \otimes_K W'$ through this isomorphism is

$$\sigma_{W'}(aw') = \sigma(a)w'$$

for $a \in L$ and $w' \in W'$. Since $W' \subset V^G$, in terms of the original G-structure on V we have $\sigma(a)w' = \sigma(a)\sigma(w') = \sigma(aw') = \sigma_{V^G}(aw') = \sigma_{(V')^G}(aw')$, so $\sigma_{W'} = \sigma_{(V')^G}$. By the one-to-one correspondence between K-forms and G-structures on V', $W' = (V')^G$.

Now assume $\dim_L(V')$ is finite. We want to show the four conditions are equivalent to $\dim_K(V' \cap V^G) = \dim_L(V')$. We will show this dimension constraint is equivalent to (1). Let $d = \dim_L(V')$.

Suppose (1) holds. If V' has an L-spanning set in V^G it has an L-basis in V^G, say $v_1, \ldots, v_d$. Then for $v' \in V'$, write $v' = \sum_{i=1}^d a_i v_i$ with $a_i \in L$. If $v' \in V^G$ too, then for any $\sigma \in G$,

$$v' = \sigma(v') = \sum_{i=1}^d \sigma(a_i)v_i,$$

so linear independence of the v_i's over L implies $a_i = \sigma(a_i)$ for all i (and σ), so $a_i \in K$ for all i. Thus $v' \in \sum_{i=1}^d Kv_i$, so $V' \cap V^G \subset \sum_{i=1}^d Kv_i$. The reverse inclusion is clear, so $\dim_K(V' \cap V^G) = d = \dim_L(V')$.

Conversely, assume $\dim_K(V' \cap V^G) = \dim_L(V')$ and let $\{v_1, \ldots, v_d\}$ be a K-basis of $V' \cap V^G$. This basis has size d because of the dimension constraint. The v_i's are a K-linearly independent set, so they are L-linearly independent since V^G is a K-form of V. Then $\sum_i Lv_i$ has L-dimension d and lies in V', whose L-dimension is d, so $\sum_i Lv_i = V'$, which is condition (1). □

Remark 3.3. Since K-independent vectors in V^G are L-independent, for all V' we have $\dim_K(V' \cap V^G) \leq \dim_L(V')$. Thus the dimension condition in Theorem 3.2 says $V' \cap V^G$ has its biggest possible K-dimension.

Any two conjugations on a complex vector space are related to each other by an automorphism of the vector space. More generally, any two G-structures on an L-vector space are linked to one another by an automorphism of the vector space:

Theorem 3.4. *Let $\{r_\sigma\}$ and $\{r'_\sigma\}$ be two G-structures on an L-vector space $V \neq 0$. There is a $\varphi \in \mathrm{GL}(V)$ such that $r'_\sigma = \varphi r_\sigma \varphi^{-1}$ for all $\sigma \in G$: the diagram*

$$\begin{array}{ccc} V & \xrightarrow{\varphi} & V \\ {\scriptstyle r_\sigma}\downarrow & & \downarrow{\scriptstyle r'_\sigma} \\ V & \xrightarrow[\varphi]{} & V \end{array} \tag{3.1}$$

commutes for all $\sigma \in G$.

Here and later, $\mathrm{GL}(V)$ means automorphisms of V as an L-vector space.

Proof. Let $W = \{v \in V : r_\sigma(v) = v \text{ for all } \sigma \in G\}$ be the K-form of V for $\{r_\sigma\}$. (It would be bad to write this as V^G since there are two G-structures we are dealing with on V and thus the notation V^G would be ambiguous.) Let $W' = \{v \in V : r'_\sigma(v) = v \text{ for all } \sigma \in G\}$ be the K-form of V for $\{r'_\sigma\}$. The two diagrams

$$\begin{array}{ccc} L \otimes_K W & \xrightarrow{f} & V \\ {\scriptstyle \sigma_W}\downarrow & & \downarrow{\scriptstyle r_\sigma} \\ L \otimes_K W & \xrightarrow[f]{} & V \end{array} \qquad \begin{array}{ccc} L \otimes_K W' & \xrightarrow{f'} & V \\ {\scriptstyle \sigma_{W'}}\downarrow & & \downarrow{\scriptstyle r'_\sigma} \\ L \otimes_K W' & \xrightarrow[f']{} & V \end{array}$$

commute for all $\sigma \in G$, where f and f' are the natural L-linear maps (isomorphisms).

Since f and f' are isomorphisms, $\dim_K(W) = \dim_L(V) = \dim_K(W')$ (these might be infinite cardinal numbers). Therefore there is a K-linear isomorphism $\psi\colon W \to W'$, its base extension $1 \otimes \psi\colon L \otimes_K W \to L \otimes_K W'$ is an L-linear isomorphism, and the diagram

$$\begin{array}{ccc} L \otimes_K W & \xrightarrow{1\otimes\psi} & L \otimes_K W' \\ {\scriptstyle \sigma_W}\downarrow & & \downarrow{\scriptstyle \sigma_{W'}} \\ L \otimes_K W & \xrightarrow[1\otimes\psi]{} & L \otimes_K W' \end{array}$$

commutes for all $\sigma \in G$: on any simple tensor $a \otimes w$, going along the top and right or along the left and bottom sends this simple tensor to $\sigma(a) \otimes \psi(w)$. Now combine the three commutative diagrams to get the commutative diagram

$$\begin{array}{ccccccc} V & \xrightarrow{f^{-1}} & L \otimes_K W & \xrightarrow{1\otimes\psi} & L \otimes_K W' & \xrightarrow{f'} & V \\ {\scriptstyle r_\sigma}\downarrow & & {\scriptstyle \sigma_W}\downarrow & & {\scriptstyle \sigma_{W'}}\downarrow & & \downarrow{\scriptstyle r'_\sigma} \\ V & \xrightarrow[f^{-1}]{} & L \otimes_K W & \xrightarrow[1\otimes\psi]{} & L \otimes_K W' & \xrightarrow[f']{} & V \end{array}$$

for every $\sigma \in G$. The maps along the top and bottom don't involve σ, and are all L-linear isomorphisms. Call the (common) composite map along the top and bottom φ, so $\varphi \in \mathrm{GL}(V)$, and remove the middle vertical maps to be left with a commutative diagram of the form (3.1). □

Corollary 3.5. *Let V be an L-vector space with two K-forms W and W'. Let $\{\sigma_W\}$ and $\{\sigma_{W'}\}$ be the corresponding G-structures on V. There is $\varphi \in \mathrm{GL}(V)$ such that $\varphi(W) = W'$ and the diagram*

$$\begin{array}{ccc} V & \xrightarrow{\varphi} & V \\ {\scriptstyle \sigma_W}\downarrow & & \downarrow{\scriptstyle \sigma_{W'}} \\ V & \xrightarrow{\varphi} & V \end{array}$$

commutes for all $\sigma \in G$.

Proof. By Theorem 3.4, there is $\varphi \in \mathrm{GL}(V)$ such that

$$\begin{array}{ccc} V & \xrightarrow{\varphi} & V \\ {\scriptstyle \sigma_W}\downarrow & & \downarrow{\scriptstyle \sigma_{W'}} \\ V & \xrightarrow{\varphi} & V \end{array}$$

commutes for all $\sigma \in G$.

It remains to check $\varphi(W) = W'$. We have $W = \{v \in V : \sigma_W(v) = v \text{ for all } \sigma \in G\}$ and $W' = \{v \in V : \sigma_{W'}(v) = v \text{ for all } \sigma \in G\}$. So for $w \in W$ and $\sigma \in G$, $\sigma_{W'}(\varphi(w)) = \varphi(\sigma_W(w)) = \varphi(w)$. Thus $\varphi(w) \in W'$, so $\varphi(W) \subset W'$. For $w' \in W'$, write $w' = \varphi(v)$ with $v \in V$. From $\sigma_{W'}(w') = w'$, $\sigma_{W'}(\varphi(v)) = \varphi(v)$, so $\varphi(\sigma_W(v)) = \varphi(v)$. Since φ is injective, $\sigma_W(v) = v$ for all σ, so $v \in W$. Thus $W' \subset \varphi(W)$. □

Theorem 3.6. *Let V_1 and V_2 be L-vector spaces equipped with G-structures. Let W_1 and W_2 be the corresponding K-forms of V_1 and V_2. An L-linear map $\Phi\colon V_1 \to V_2$ is the L-linear base extension of a K-linear map $\varphi\colon W_1 \to W_2$ if and only if the diagram*

$$\begin{array}{ccc} V_1 & \xrightarrow{\Phi} & V_2 \\ {\scriptstyle \sigma_{W_1}}\downarrow & & \downarrow{\scriptstyle \sigma_{W_2}} \\ V_1 & \xrightarrow{\Phi} & V_2 \end{array}$$

commutes for all $\sigma \in G$. Equivalently, the L-vector space $\mathrm{Hom}_L(V_1, V_2)$ has a G-structure given by

$$\sigma(\Phi) := \sigma_{W_2} \circ \Phi \circ \sigma_{W_1}^{-1}$$

with corresponding K-form $\mathrm{Hom}_K(W_1, W_2)$.

Proof. Exercise. □

We conclude this section with a reinterpretation of Theorem 3.4 in terms of modules, using the ring $C(G) = \bigoplus_{\sigma \in G} Le_\sigma$ introduced at the end of Section 2. We saw there that any nonzero $C(G)$-module is a direct sum of copies of L as a $C(G)$-module. By the invariance of dimension of vector spaces, this means a $C(G)$-module is completely determined up to isomorphism by its L-dimension. In other words, the end of Section 2 shows that any two $C(G)$-module structures on a nonzero L-vector space V are isomorphic: there is a $C(G)$-linear map $\varphi\colon V \to V$ that turns one $C(G)$-module structure into the other. This is the same as saying φ is a L-linear automorphism of V such that $\varphi(e_\sigma v) = e_\sigma \varphi(v)$ (be careful only to view V as a *left* L-vector space, considering how multiplication of it with G inside of $C(G)$ is twisted), and that equation for all σ is precisely the conclusion of Theorem 3.4 except it is given in the terminology of G-structures rather than $C(G)$-modules. So we

already had a proof of Theorem 3.4 at the end of Section 2 and it's a lot more conceptual than the proof we wrote out for Theorem 3.4. This illustrates how useful it can be to interpret G-structures as $C(G)$-module structures.

4. Applications to Ideals

Our next set of applications of Galois descent concern ideals in $L[X_1, \ldots, X_n]$, which we will abbreviate to $L[\underline{X}]$. A basic question is whether an ideal in this ring is generated by polynomials in $K[\underline{X}]$. Let $V = L[\underline{X}]$ and let G act on V by acting on coefficients. This action is a G-structure on V with corresponding K-form $W := V^G = K[\underline{X}]$. For any ideal I of $L[\underline{X}]$, $I^G = I \cap K[\underline{X}]$ is an ideal in $K[\underline{X}]$. Say an ideal $I \subset L[\underline{X}]$ is *defined over* K if it has a generating set (as an ideal!) in $K[\underline{X}]$.

Example 4.1. In $\mathbf{C}[X, Y]$, $I = (X + iY^2, X - iY^2)$ is defined over $\mathbf{R}$ since $I = (X, Y^2)$.

Theorem 4.2. *For an ideal $I \subset L[\underline{X}]$, the following conditions are equivalent:*

(1) *I is defined over K,*
(2) *$\sigma(I) \subset I$ for all $\sigma \in G$,*
(3) *$\sigma(I) = I$ for all $\sigma \in G$.*

Proof. It is trivial that (1) implies (2) since a generating set of I in $K[\underline{X}]$ is not changed by σ. Since (2) is stated over all σ, from $\sigma^{-1}(I) \subset I$ for all σ we get $I \subset \sigma(I)$ for all σ, so $\sigma(I) = I$ for all σ, which is (3). Finally, assuming (3), since $\sigma(I) = I$ the Galois group G acts semilinearly on I as an L-vector space, so by Galois descent on I, I has a spanning set as an L-vector space in $I^G = I \cap K[\underline{X}] \subset K[\underline{X}]$. Since I is an ideal in $L[\underline{X}]$, an L-vector space spanning set of I is also a generating set of I as an ideal. □

Here is an example where L/K is non-Galois and Theorem 4.2 breaks down. Let $K = \mathbf{F}_p(T)$, $L = \mathbf{F}_p(\sqrt[p]{T})$, and $I = (X - \sqrt[p]{T})$ in $L[X]$. Then $\sigma(I) = I$ for all $\sigma \in \mathrm{Aut}_K(L)$ (which is a trivial group), but I has no generator in $K[X]$. In fact, $I \cap K[X] = (X^p - T)$, so the ideal in $L[X]$ generated by $I \cap K[X]$ is smaller than I.

Remark 4.3. By Hilbert's basis theorem,

$$I \cap K[\underline{X}] = (f_1, \ldots, f_r) = \sum_{i=1}^{r} K[\underline{X}] f_i$$

for some f_i's in $K[\underline{X}]$. If I is defined over K then by the proof of Theorem 4.2, I is spanned as an L-vector space by polynomials in $I \cap K[\underline{X}]$: $I = \sum_j L h_j$ where $h_j \in I \cap K[\underline{X}]$. Each h_j is a $K[\underline{X}]$-linear combination of the f_i's, so $I \subset \sum_{i=1}^r L[\underline{X}] f_i$ and the reverse inclusion holds since I is an ideal, so $I = \sum_{i=1}^r L[\underline{X}] f_i$. That is, an ideal in $L[\underline{X}]$ defined over K is finitely generated over $L[\underline{X}]$ by any finite set of ideal generators of $I \cap K[\underline{X}]$.

The special case of (3) $\Rightarrow$ (1) in Theorem 4.2 in one variable can be proved using Hilbert's Theorem 90 instead of Galois descent. Let I be an ideal in $L[X]$. Since $L[X]$ is a PID, $I = (f)$ for some $f \in L[X]$. Then $\tau(I) = (\tau(f))$ for all $\tau \in G$. Saying $\tau(I) = I$ for all $\tau \in G$ is equivalent to $\tau(f) = \lambda_\tau f$ for some $\lambda_\tau \in L^\times$. Then apply any $\sigma \in G$ to get $\sigma(\tau(f)) = \sigma(\lambda_\tau)\sigma(f)$, so $(\sigma\tau)(f) = \sigma(\lambda_\tau)\lambda_\sigma f$. Also $(\sigma\tau)(f) = \lambda_{\sigma\tau} f$, so $\lambda_{\sigma\tau} f = \sigma(\lambda_\tau)\lambda_\sigma f$, so $\lambda_{\sigma\tau} = \sigma(\lambda_\tau)\lambda_\sigma$ since $f \neq 0$. Hence the numbers $\{\lambda_\sigma : \sigma \in G\}$ are a 1-cocycle $G \to L^\times$. By the multiplicative form of Theorem 90, $\lambda_\sigma = \sigma(\alpha)/\alpha$ for some $\alpha \in L^\times$ and all $\sigma \in G$, so $\sigma(f) = (\sigma(\alpha)/\alpha)f$, so $\sigma(f/\alpha) = f/\alpha$ for all $\sigma \in G$. Thus $f/\alpha \in K[X]$ and $(f/\alpha) = (f)$ as ideals in $L[X]$. So (f) is defined over K.

The relations between Galois descent and cohomology go further. Let V be an L-vector space with a G-structure. A 1-cocycle on V is a function $c\colon G \to V$ such that $c(\sigma\tau) = c(\sigma) + \sigma(c(\tau))$.

Example 4.4. Fixing $v \in V$, $c(\sigma) = \sigma(v) - v$ is a 1-cocycle since

$$c(\sigma) + \sigma(c(\tau)) = (\sigma(v) - v) + \sigma(\tau(v) - v) = (\sigma\tau)(v) - v = c(\sigma\tau).$$

The additive form of Theorem 90 says all 1-cocycles $c\colon G \to L$ look like the example: $c(\sigma) = \sigma(\alpha) - \alpha$ for some $\alpha \in L$. Let's recall a proof. For $x \in L$, set $y = \sum_{\tau \in G} c(\tau)\tau(x)$. For any $\sigma \in G$, $\sigma(y) = \sum_\tau \sigma(c(\tau))(\sigma\tau)(x) = \sum_\tau (c(\sigma\tau) - c(\sigma))(\sigma\tau)(x) = \sum_\tau (c(\tau) - c(\sigma))\tau(x) = y - c(\sigma)\mathrm{Tr}_{L/K}(x)$. Choose x so $\mathrm{Tr}_{L/K}(x) \neq 0$. Then $c(\sigma) = z - \sigma(z)$ for $z = y/\mathrm{Tr}_{L/K}(x)$. Set $\alpha = -z$, so $c(\sigma) = \sigma(\alpha) - \alpha$.

Using Galois descent we can extend this from cocycles in L to cocycles in L-vector spaces with a G-structure.

Theorem 4.5. *For any L-vector space V with a G-structure, every 1-cocycle on V has the form $c(\sigma) = \sigma(v) - v$ for some $v \in V$.*

Proof. We may suppose $V \neq 0$. Let $\{v_i\}$ be a K-basis of V^G, so by Galois descent

$$V = \bigoplus_i Lv_i.$$

For any 1-cocycle $c\colon G \to V$, write $c(\sigma) = \sum_i a_{\sigma,i} v_i$, where $a_{\sigma,i} \in L$. Then the cocycle condition $c(\sigma\tau) = c(\sigma) + \sigma(c(\tau))$ means

$$\begin{aligned} \sum_i a_{\sigma\tau,i} v_i &= \sum_i a_{\sigma,i} v_i + \sigma\left(\sum_i a_{\tau,i} v_i\right) \\ &= \sum_i a_{\sigma,i} v_i + \sum_i \sigma(a_{\tau,i}) v_i \\ &= \sum_i \left(a_{\sigma,i} + \sigma(a_{\tau,i})\right) v_i, \end{aligned}$$

so for each i, $a_{\sigma\tau,i} = a_{\sigma,i} + \sigma(a_{\tau,i})$. Thus for each i, $\sigma \mapsto a_{\sigma,i}$ is a 1-cocycle in L. By Theorem 90, for each i there is $b_i \in L$ such that $a_{\sigma,i} = \sigma(b_i) - b_i$ for all σ. Since $a_{\sigma,i} = 0$ for all but finitely many i, we can use $b_i = 0$ for all but finitely many i. Then

$$c(\sigma) = \sum_i (\sigma(b_i) - b_i) v_i = \sum_i \sigma(b_i) v_i - \sum_i b_i v_i = \sigma(v) - v,$$

where $v = \sum_i b_i v_i$. □

Here is an important application of Theorem 4.5 to the Galois action on quotient rings of $L[\underline{X}]$.

Theorem 4.6. *Let $I \subset L[\underline{X}]$ be an ideal defined over K, so $L[\underline{X}]/I$ has a G-structure by $\sigma(f + I) = \sigma(f) + I$ (Lemma 2.11). For each $f \in L[\underline{X}]$, the following are equivalent:*

1. *$\sigma(f) \equiv f \bmod I$ for all $\sigma \in G$,*
2. *$f \equiv g \bmod I$ for some $g \in K[\underline{X}]$.*

Proof. It is trivial that the second condition implies the first. For the more interesting reverse direction, assume $\sigma(f) \equiv f \bmod I$ for all $\sigma \in G$. Define $c\colon G \to I$ by $c(\sigma) = \sigma(f) - f$.

By a computation, $c(\sigma) + \sigma(c(\tau)) = c(\sigma\tau)$ for all σ and τ in G, so c is a 1-cocycle in the L-vector space I. By Theorem 4.5, $c(\sigma) = \sigma(h) - h$ for some $h \in I$, so

$$\sigma(f) - f = \sigma(h) - h$$

for all $\sigma \in G$. Therefore $f - h$ is fixed by all $\sigma \in G$, so $f - h \in K[\underline{X}]$. Set $g = f - h$, so $f \equiv g \bmod I$ and $g \in K[\underline{X}]$. □

Even though ideals in $L[\underline{X}]$ are finitely generated as ideals, they are infinite-dimensional as L-vector spaces (except for the zero ideal), so it is crucial that Theorem 4.5 applies to general vector spaces, not just finite-dimensional vector spaces.

These Galois descent features on ideals lead to applications in algebraic geometry. We present two of them.

Theorem 4.7. *Let $V \subset L^d$ be the zero set of $f_1, \ldots, f_r \in K[\underline{X}]$. The ideal of all polynomials in $L[\underline{X}]$ that vanish in L^d where the f_i's vanish has a generating set in $K[\underline{X}]$. Equivalently, the ideal $I(V) = \{g \in L[\underline{X}] : g(P) = 0$ for all $P \in V\}$ is defined over K.*

Note that before Theorem 4.7 we've written V for a vector space. Now V is denoting an algebraic variety, so it is definitely not a vector space in general!

There is nontrivial content to Theorem 4.7 because the ideal $I(V)$ need not be generated by the f_i's themselves. For instance, in $\mathbf{C}^2$ let V be the zero set of $f_1 = X_1^3$ and $f_2 = X_1^2 - X_1X_2$. Then $I(V) = (X_1)$ whereas the ideal (f_1, f_2) is strictly contained in X_1 (any polynomial in the ideal (f_1, f_2) has no X_1-term, but X_1 of course does).

Proof. For $P \in V$, $f_i(P) = 0$ for all i, so $f_i(\sigma(P)) = 0$ for all $\sigma \in G$. Thus $\sigma(P) \in V$, so $\sigma(V) \subset V$ for all $\sigma \in G$, hence $\sigma(V) = V$ for all $\sigma \in G$.

To show $I(V)$ is defined over K, we show $\sigma(I(V)) \subset I(V)$ for all $\sigma \in G$. Pick $f \in I(V) \subset L[\underline{X}]$. For $\sigma \in G$ and $P \in V$, set $Q = \sigma^{-1}(P) \in V$. Then $f(Q) = 0$, and applying σ to this gives $(\sigma f)(\sigma(Q)) = 0$, so $(\sigma f)(P) = 0$. Thus $\sigma(f) \in I(V)$, so $\sigma(I(V)) \subset I(V)$ for all $\sigma \in I(V)$. Therefore $I(V)$ is defined over K. □

Example 4.8. If $V \subset \mathbf{C}^d$ is the zero set of some real polynomials $f_1, \ldots, f_r$, then the ideal $I(V)$ of complex polynomials vanishing on V is generated by real polynomials.

The proof of Theorem 4.7 is not constructive, so we don't get a method to write down generators of $I(V)$ in $K[\underline{X}]$ from the original polynomials f_i in $K[\underline{X}]$ that define V.

Theorem 4.9. *Let $I \subset L[\underline{X}]$ be a homogeneous prime ideal defined over K. Then $L(I)^G = \{g/h : g, h \in K[\underline{X}], h \notin I, g$ and h are homogeneous of equal degree$\}$.*

Proof. The inclusion $\supset$ is obvious. We work out the inclusion $\subset$. Suppose $g, h \in L[\underline{X}]$ are homogeneous of equal degree, $h \notin I$, and $g/h \in L(I)^G$, which means $\sigma(g/h) = g/h$ for all σ in G. We can write $g/h = gk/hk$ for any nonzero $k \in L[\underline{X}]$. For $\sigma \in G$, since $h \notin I$ and $\sigma(I) = I$, $\sigma(h) \notin I$. Then $\prod_{\sigma \in G} \sigma(h) \notin I$ and the product is in $K[\underline{X}]$. So without loss of generality, $h \in K[\underline{X}]$. Then $\sigma(g/h) = \sigma(g)/h$, so $\sigma(g) = g$ in $L(I)$. Both $\sigma(g)$ and g are in $L[I] = L[\underline{X}]/I$, so

$$\sigma(g) \equiv g \bmod I$$

for all $\sigma \in G$. Therefore Theorem 4.6 tells us $g \equiv \widetilde{g} \bmod I$ for some $\widetilde{g} \in K[\underline{X}]$. Since $g - \widetilde{g} \in I$, I is a homogeneous ideal, and g is a homogeneous polynomial, the homogeneous parts of $\widetilde{g}$ not of degree $\deg g$ are in I. Therefore without loss of generality $\widetilde{g}$ is homogeneous of the same degree as g. So $g/h = \widetilde{g}/h$ in $L(I)$, and $\widetilde{g}$ and h are in $K[I]$. □

5. Applications to Algebras

Our final set of applications of Galois descent is to L-algebras. We understand L-algebra to be used in the sense of any L-vector space equipped with an L-bilinear multiplication law. We will not assume the algebra is associative. Examples of L-algebras include $\mathrm{M}_n(L)$, $L[\underline{X}]$, and a Lie algebra over L (which is not associative) such as $\mathfrak{gl}_n(L)$. For any K-algebra A, $L \otimes_K A$ is an L-algebra.

Definition 5.1. A *K-form* of an L-algebra $\mathcal{A}$ is a K-subalgebra A of $\mathcal{A}$ such that the natural map $L \otimes_K A \to \mathcal{A}$ given by $x \otimes a \mapsto xa$ is an isomorphism of L-algebras.

A K-form of an L-algebra is a K-form as an L-vector space, but it's more than that: the algebra structure needs to be respected.

If $\mathcal{A}$ is an L-algebra and A is a K-form of $\mathcal{A}$ then $\mathcal{A}$ is associative if and only if A is associative and $\mathcal{A}$ is a Lie algebra over L if and only if A is a Lie algebra over K. The reason is that the relevant properties (associativity or the Jacobi identity) are true on an L-algebra if and only if they are true on an L-basis, and we can use a K-basis of A as an L-basis of $\mathcal{A}$.

Example 5.2. Two $\mathbf{R}$-forms of the $\mathbf{C}$-algebra $\mathrm{M}_2(\mathbf{C})$ are $\mathrm{M}_2(\mathbf{R})$ and the quaternions $\mathbf{H}$, viewed inside $\mathrm{M}_2(\mathbf{C})$ by $a+bi+cj+dk \mapsto \left(\begin{smallmatrix} a+bi & -c-di \\ c-di & a-bi \end{smallmatrix}\right)$. Both are 4-dimensional $\mathbf{R}$-algebras whose standard $\mathbf{R}$-basis is a $\mathbf{C}$-basis of $\mathrm{M}_2(\mathbf{C})$.

Since $\mathrm{M}_2(\mathbf{R})$ and $\mathbf{H}$ are not isomorphic $\mathbf{R}$-algebras ($\mathbf{H}$ is a division ring and $\mathrm{M}_2(\mathbf{R})$ is not), different K-forms of an L-algebra *need not* be isomorphic K-algebras. This is an important contrast with the linear theory (Theorem 3.4), where all K-forms of an L-vector space are isomorphic as K-vector spaces. When working with algebras we have to keep tabs on the multiplicative structure too, and that creates new possibilities.

As with K-forms of an L-vector space, K-forms of an L-algebra correspond to an appropriate system of semilinear G-actions on the algebra. A *G-structure* on an L-algebra $\mathcal{A}$ is a collection of maps $r_\sigma \colon \mathcal{A} \to \mathcal{A}$ for all $\sigma \in G$ such that r_σ is a σ-linear K-algebra automorphism (not L-algebra automorphism!), $r_{\mathrm{id}_L} = \mathrm{id}_{\mathcal{A}}$, and $r_\sigma \circ r_{\sigma'} = r_{\sigma\sigma'}$.

Example 5.3. The entrywise or coefficientwise G-actions on $\mathrm{M}_n(L)$, $\mathfrak{gl}_n(L)$, and $L[\underline{X}]$ as L-vector spaces are also G-structures as L-algebras.

Example 5.4. If A is a K-algebra then the L-algebra $L \otimes_K A$ gets a standard G-structure by

$$\sigma_A\left(\sum_i c_i \otimes a_i\right) := \sum \sigma(c_i) \otimes a_i.$$

This is σ-linear (σ_A is additive and $\sigma_A(ct) = \sigma(c)\sigma_A(t)$ for all $c \in L$ and $t \in L \otimes_K A$) and also σ_A is multiplicative ($\sigma_A(tt') = \sigma_A(t)\sigma_A(t')$), so σ_A is a K-algebra automorphism of $L \otimes_K A$. Thinking of A just as a K-vector space, by the proof of Theorem 2.14 we have $(L \otimes_K A)^G = 1 \otimes A$.

If $\mathcal{A}$ is an L-algebra with a G-structure, the fixed set $\mathcal{A}^G$ is a K-form of $\mathcal{A}$ as vector spaces by Theorem 2.14. The space $\mathcal{A}^G$ is also a K-algebra and the L-linear isomorphism $L \otimes_K \mathcal{A}^G \to \mathcal{A}$ is an isomorphism of L-algebras, not just of L-vector spaces. So $\mathcal{A}^G$ is a K-form of $\mathcal{A}$ as an L-algebra. Thus G-structures leads to K-forms.

Conversely, if $\mathcal{A}$ is an L-algebra with a K-form A, the natural map $L \otimes_K A \to \mathcal{A}$ is an L-algebra isomorphism and the standard G-structure on $L \otimes_K A$ in Example 5.4 can be

transported to a G-structure on $\mathcal{A}$ whose fixed set is A. (This is an algebra analogue of Example 2.10.) So K-forms on an L-algebra $\mathcal{A}$ leads to G-structures on $\mathcal{A}$.

It can be no surprise at this point that Theorem 2.14 has an analogue for algebras: the K-forms of $\mathcal{A}$ (as an algebra) are in one-to-one correspondence with the G-structures on $\mathcal{A}$ (as an algebra). One just reads through the proof of Theorem 2.14 and checks the maps constructed there between algebras are not just semilinear but also multiplicative.

Example 5.5. With respect to their standard G-structures, the K-forms of the L-algebras $\mathrm{M}_n(L)$, $\mathfrak{gl}_n(L)$, and $L[\underline{X}]$ are $\mathrm{M}_n(K)$, $\mathfrak{gl}_n(K)$, and $K[\underline{X}]$.

For a $\mathbf{C}$-algebra $\mathcal{A}$, a $\mathrm{Gal}(\mathbf{C}/\mathbf{R})$-structure is determined by a conjugation on the algebra. This is a function $c\colon \mathcal{A} \to \mathcal{A}$ such that c is semilinear with respect to complex conjugation on $\mathbf{C}$, is an $\mathbf{R}$-algebra automorphism of $\mathcal{A}$, and $c^2 = \mathrm{id}_{\mathcal{A}}$.

Example 5.6. The $\mathbf{C}$-algebra $\mathrm{M}_2(\mathbf{C})$ has $\mathbf{R}$-forms $\mathrm{M}_2(\mathbf{R})$ and $\mathbf{H}$ (embedded in $\mathrm{M}_2(\mathbf{C})$ as in Example 5.2). These are each the fixed points of one of the following two conjugations on $\mathrm{M}_2(\mathbf{C})$:

$$c\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \overline{\alpha} & \overline{\beta} \\ \overline{\gamma} & \overline{\delta} \end{pmatrix}, \quad c'\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \overline{\delta} & -\overline{\gamma} \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix}.$$

Note c', whose fixed set is $\mathbf{H}$, is *not* an extension of the usual conjugation on quaternions, as that doesn't fix all of $\mathbf{H}$ (also, the usual quaternionic conjugation reverses the order of multiplication).

Let $\mathcal{A}$ be an L-algebra and A and A' be two K-forms of $\mathcal{A}$ (as an L-algebra). Each K-form provides $\mathcal{A}$ with a G-structure, say $\{r_\sigma\}$ and $\{r'_\sigma\}$ for A and A'. Call A and A' *equivalent* K-forms of $\mathcal{A}$ if there is a K-algebra isomorphism $\psi\colon A \to A'$ commuting with the G-actions: $\psi(r_\sigma(a)) = r'_\sigma(\psi(a))$ for all $a \in A$ and $\sigma \in G$. Because of examples like $\mathrm{M}_2(\mathbf{R})$ and $\mathbf{H}$ inside $\mathrm{M}_2(\mathbf{C})$, not all K-forms of an L-algebra are equivalent, as the K-forms may not be isomorphic K-algebras. The equivalence of K-forms of an L-algebra can be described by the algebra analogue of Theorem 3.4 (where all K-forms are equivalent, using an obvious notion of equivalence for vector spaces with G-structure):

Theorem 5.7. *Let $\mathcal{A}$ be an L-algebra with K-forms A and A'. Write the corresponding G-structures on $\mathcal{A}$ as $\{r_\sigma\}$ and $\{r'_\sigma\}$. Then A and A' are equivalent K-forms of $\mathcal{A}$ if and only if there is an L-algebra automorphism φ of $\mathcal{A}$ such that $r'_\sigma = \varphi r_\sigma \varphi^{-1}$ for all $\sigma \in G$: the diagram*

$$\begin{array}{ccc} \mathcal{A} & \xrightarrow{\varphi} & \mathcal{A} \\ {\scriptstyle r_\sigma}\downarrow & & \downarrow{\scriptstyle r'_\sigma} \\ \mathcal{A} & \xrightarrow[\varphi]{} & \mathcal{A} \end{array}$$

commutes for all $\sigma \in G$.

Proof. ($\Leftarrow$) If there is such a φ then φ is a K-algebra automorphism of $\mathcal{A}$, and for $a \in A$, $\varphi(a) = r'_\sigma(\varphi(a))$ for all σ, so $\varphi(a) \in A'$. If $\varphi(a) \in A'$ with $a \in \mathcal{A}$, then $\varphi(r_\sigma(a)) = \varphi(a)$, so $r_\sigma(a) = a$ for all σ, so $a \in A$. Thus $\varphi(A) = A'$, so φ restricts to a K-algebra isomorphism from A to A'.

($\Rightarrow$) Suppose there is a K-algebra isomorphism $\psi\colon A \to A'$ such that $\psi(r_\sigma(a)) = r'_\sigma(\psi(a))$ for all $a \in A$. Base extend ψ to $1 \otimes \psi$, an L-algebra isomorphism from $L \otimes_K A$ to $L \otimes_K A'$. These base extensions are both L-algebra isomorphic to $\mathcal{A}$ in a natural way, so $1 \otimes \psi$ can

be regarded as an L-algebra automorphism φ of $\mathcal{A}$. It is left to the reader to check with this φ that the diagram commutes. □

For our last application of Galois descent, we work out the structure of the L-algebra $L\otimes_K L$, where scaling by L comes in the first component: $c(x\otimes y) = cx\otimes y$ on simple tensors. For $\sigma \in G$, let L_σ be L as a ring with L-scaling given by the twisted rule $c \cdot x = \sigma(c)x$. Then L_σ is an L-algebra. Set

$$\mathcal{A} = \prod_{\sigma\in G} L_\sigma,$$

whose elements are written in tuple notation as $(x_\sigma)_\sigma$. This is an L-algebra using componentwise operations. In particular, scaling by L on $\mathcal{A}$ is given by

$$c \cdot (x_\sigma)_\sigma = (c \cdot x_\sigma)_\sigma = (\sigma(c)x_\sigma)_\sigma.$$

Let $\tau \in G$ act on $\mathcal{A}$ by

$$\tau((x_\sigma)_\sigma) = (x_{\sigma\tau})_\sigma = (y_\sigma)_\sigma,$$

where $y_\sigma = x_{\sigma\tau}$. To show this is a G-structure on $\mathcal{A}$, it is easy to see that τ acts additively and multiplicatively on $\mathcal{A}$, and the identity of G acts on $\mathcal{A}$ as the identity map. For τ_1 and τ_2 in G,

$$\begin{aligned} \tau_1(\tau_2((x_\sigma)_\sigma)) &= \tau_1((y_\sigma)_\sigma) \text{ where } y_\sigma = x_{\sigma\tau_2} \\ &= (z_\sigma), \end{aligned}$$

where $z_\sigma = y_{\sigma\tau_1} = x_{\sigma\tau_1\tau_2}$. So

$$\begin{aligned} \tau_1(\tau_2((x_\sigma)_\sigma)) &= (x_{\sigma\tau_1\tau_2}) \\ &= (\tau_1\tau_2)((x_\sigma)_\sigma). \end{aligned}$$

Thus composing the actions of τ_1 and τ_2 on $\mathcal{A}$ gives the action of $\tau_1\tau_2$. Also

$$\begin{aligned} \tau(c \cdot (x_\sigma)_\sigma) &= \tau((\sigma(c)x_\sigma)_\sigma) \\ &= (y_\sigma)_\sigma, \end{aligned}$$

where $y_\sigma = (\sigma\tau)(c)x_{\sigma\tau} = \sigma(\tau(c))x_{\sigma\tau}$ and

$$\begin{aligned} \tau(c)(\tau((x_\sigma)_\sigma)) &= \tau(c)((x_{\sigma\tau})_\sigma) \\ &= (\tau(c) \cdot x_{\sigma\tau})_\sigma \\ &= (\sigma(\tau(c))x_{\sigma\tau})_\sigma \\ &= (y_\sigma)_\sigma, \end{aligned}$$

so τ acts τ-linearly on $\mathcal{A}$.

The fixed set $\mathcal{A}^G$ for this G-structure on $\mathcal{A}$ is $\{(x_\sigma)_\sigma : \tau((x_\sigma)_\sigma) = (x_\sigma)_\sigma \text{ for all } \tau \in G\}$, which amounts to $x_{\sigma\tau} = x_\sigma$ for all σ and τ, so all the coordinates are the same element, say x, of L: $\mathcal{A}^G = \{(x)_\sigma : x \in L\}$. Thus $L \cong \mathcal{A}^G$ as K-algebras by $x \mapsto (x)_\sigma$. (This map is K-linear but *not* L-linear if $\#G > 1$.)

Since $L \cong \mathcal{A}^G$ as K-algebras, $L \otimes_K L \cong L \otimes_K \mathcal{A}^G$ as L-algebras by $\alpha \otimes \beta \mapsto \alpha \otimes (\beta)_\sigma$. By Galois descent, $L \otimes_K \mathcal{A}^G \cong \mathcal{A}$ as L-algebras by $\alpha \otimes (\beta)_\sigma \mapsto \alpha \cdot (\beta)_\sigma = (\alpha \cdot \beta)_\sigma = (\sigma(\alpha)\beta)_\sigma$, so

$$L \otimes_K L \cong \mathcal{A} = \prod_{\sigma\in G} L_\sigma \tag{5.1}$$

by $\alpha \otimes \beta \mapsto (\sigma(\alpha)\beta)_\sigma$.

For an application of (5.1) to a proof of the normal basis theorem, see [4].

References

[1] N. Jacobson, "Lie Algebras," Dover, New York, 1979.
[2] J. H. Silverman, "The Arithmetic of Elliptic Curves," Springer-Verlag, New York, 1986.
[3] W. Waterhouse, "Introduction to Affine Group Schemes," Springer-Verlag, New York, 1979.
[4] W. Waterhouse, *The Normal Basis Theorem*, Amer. Math. Monthly **86** (1979), 212.
[5] D. J. Winter, "The Structure of Fields," Springer-Verlag, New York, 1974.