Essays on the structure of reductive groups

Bill Casselman
University of British Columbia
cass@math.ubc.ca

Algebraic structures and fields of definition

I have written this essay in order to summarize in one place what one needs eventually to classify algebraic groups over local fields. Since this essay is partly directed to those who work mostly with groups defined over $\mathbb{R}$, who might not be familiar with algebraic geometry, I include a very short introduction to affine algebraic varieties. There are a few novel points in my treatment of Galois descent, notably the use of the extension $E$ in.

I wish to thank Christophe Cornut for correcting an error in my original explanation of restriction of scalars.

Contents

1. Introduction
2. Galois conjugation on vector spaces
3. Non-abelian cohomology
4. Tensor structures
5. Central simple algebras
6. Affine varieties
7. Descending fields of definition
8. Classification of splittings
9. References

Following a common convention, I take the action of a Galois group to be on the right: $x \mapsto x^\sigma$.

1. Introduction

I explain the basic problem by an example. The equation $xy - 1 = 0$ determines an algebraic variety defined over $\mathbb{R}$, and its set of $\mathbb{R}$-rational points may be identified with the non-zero elements of $\mathbb{R}$ through projection onto either the $x$-axis or the $y$-axis. This algebraic variety is an algebraic group, with multiplication defined coordinate-wise:

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2, y_1 y_2).$$

The unit group of $z$ in $\mathbb{C}$ with $|z| = 1$ may be identified with the points $(x, y)$ in $\mathbb{R}^2$ such that $x^2 + y^2 = 1$. This also is an algebraic group defined over $\mathbb{R}$, where the group operation is defined by complex multiplication as described in terms of real and imaginary components:

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1).$$

As algebraic varieties over $\mathbb{R}$ these two are certainly distinct, since the set of real points on one is compact, while on the other it is not.

But now consider the set of points $(x, y)$ in $\mathbb{C}^2$ such that $x^2 + y^2 = 1$. Since we can write this as

$$(x + iy)(x - iy) = 1,$$

...
there is a map from this set to the complex hyperbola \( xy = 1 \), taking \( (x, y) \) to \( (x + iy, x - iy) \). The map is invertible, since given \( (u, v) \) with \( uv = 1 \) we can solve for \( x, y \):

\[
\begin{align*}
    u &= x + iy \\
    v &= x - iy \\
    x &= \frac{(u + v)}{2} \\
    y &= \frac{(u - v)}{2i}.
\end{align*}
\]

Thus the two varieties \( x^2 + y^2 = 1 \) and \( xy = 1 \) are isomorphic over \( \mathbb{C} \), although not over \( \mathbb{R} \). This demonstrates a common and important phenomenon.

What I want to do in this essay is explain very generally how to classify algebraic varieties and other algebraic structures defined over a field \( F \) that become isomorphic to a given one over a Galois extension \( E/F \). This general theory will be useful in classifying algebraic tori over arbitrary fields, reductive groups over finite fields, and reductive groups over \( \mathbb{R} \), although I shall not do that here.

The algebraic varieties above are all affine algebraic varieties—those defined by a set of polynomials in some vector space—and in fact I am going to work only with affine varieties. Since I am writing for those who are not necessarily experts in algebraic geometry, I include a short explanation of what’s important here.

The origin of results about descending fields of definition is [Weil:1956], but this used Weil’s own, now completely obsolete, terminology in algebraic geometry. The current standard reference is §IV.4 of [Serre:1959], which I follow closely. I have also used [Serre:1965].

2. Galois conjugation on vector spaces

Suppose \( V \) to be a vector space over a field \( E \), and \( \sigma \) an automorphism of \( E \). A \( \sigma \)-conjugation of \( V \) is an additive map \( v \mapsto v^{[\sigma]} \) from \( V \) to itself such that

\[
(cv)^{[\sigma]} = c^{\sigma}v^{[\sigma]}.
\]

If \( V \) is defined over the field \( F \) and \( E/F \) is Galois, then we have for each \( \sigma \) in \( G(E/F) \) the \( \sigma \)-linear map

\[
x \otimes v \mapsto e^x \otimes v
\]

frm \( E \otimes_F V \) to itself. The subspace of fixed points of all these is \( V \) itself. Conversely:

**2.1. Theorem.** Suppose \( E \) to be a finite Galois extension over \( F \). Suppose \( V \) and that we are given a homomorphism from \( G = \text{Gal}(E/F) \) to the \( G \)-conjugations of \( V \). Then the canonical map from \( E \otimes_F V^\sigma \) to \( V \) is an isomorphism.

The hypothesis means that we are given for each \( \sigma \) in \( G \) a \( \sigma \)-conjugation \( v \to v^{[\sigma]} \), and that \( v^{[\sigma \tau]} = (v^{[\sigma]})^{[\tau]} \).

There is another way to see this. The conjugate vector space \( V^\sigma \) is the same additive group as \( V \), but with the new scalar multiplication

\[
c \cdot v = e^{c^{-1}} v.
\]

With my conventions, \( V^{\sigma \tau} = (V^\sigma)^\tau \). The hypothesis is that we are given a compatible family of isomorphisms of \( V \) with all its conjugates.

The Theorem will follow from a sequence of rather elementary results in linear algebra. In following the argument, it might be useful to keep in mind that if \( V = E \) we are recovering the basic theorem of Galois theory.

**2.2. Lemma.** The Galois transformations of \( E \) are linearly independent over \( E \).
This is a basic result from Galois theory, but I’ll sketch the proof here. Suppose
\[ \sum_{\sigma \in \mathcal{G}} c_{\sigma}\sigma = 0. \]
For each \( \sigma \) in \( \mathcal{G} \) the map taking \( e \) to \( \sigma(e) \) is multiplicative. So the result follows from this well known proposition:

**2.3. Lemma.** If \( G \) is a group and \( E \) a field, any set of distinct homomorphisms
\[ \chi: G \longrightarrow E^\times \]
are linearly independent over \( E \).

*Proof.* I’ll prove this induction on \( n \) that if
\[ \sum_{\chi} c_{\chi} = 0 \]
with \( n \) coefficients \( c_{\chi} \) then all the \( c_{\chi} \) vanish. For \( n = 1 \) this is immediate, since the values of the characters are non-zero.

Suppose this is true for \( m < n \) and suppose such a relation
\[ \sum_{i=1}^{n} c_{i} \chi_{i} = 0 \]
where we may assume \( c_{n} = 1 \). Substituting \( xg \) for \( x \) in
\[ \sum_{i=1}^{n-1} c_{i} \chi_{i}(x) + \chi_{n}(x) = 0 \]
we get
\[ 0 = \sum_{i=1}^{n-1} c_{i} \chi_{i}(x) \chi_{i}(g) + \chi_{n}(x) \chi_{n}(g) \]
\[ = \sum_{i=1}^{n-1} \chi_{n}(g)^{-1} \chi_{i}(g) c_{i} \chi_{i}(x) + \chi_{n}(x) \]
and subtracting this from the original equation we get
\[ \sum_{i=1}^{n-1} c_{i} (\chi_{n}(g)^{-1} \chi_{i}(g) - 1) \chi_{i}(x) \]
for each \( x \). By induction, each coefficient vanishes. Choose \( g \) such that \( \chi_{n}(g) \neq \chi_{1}(g) \). But then by induction each \( c_{i} = 0 \) for \( i \leq n-1 \), hence also \( c_{n} = 0 \).

For every \( e \) in \( E \) let \( \mu(e) \) be the map from \( E \) to itself, taking \( x \) to \( ex \). This gives an embedding of \( E \) into \( \text{End}_F(E) \). Recall that \( F[\mathcal{G}] \) is the group algebra of \( \mathcal{G} \) with coefficients in \( F \). The map taking \( \sigma \) to the \( \sigma \)-conjugation of \( V \) induces a ring homomorphism from \( F[\mathcal{G}] \) to \( \text{End}_E(V) \). The following is a straightforward consequence of the Lemma just proved.

**2.5. Lemma.** The map \( E \otimes_{F} F[\mathcal{G}] \rightarrow \text{End}_F(E) \) is an isomorphism of algebras.

*Proof.* Linear independence implies that it is an injection, and dimensions match. Furthermore, in this case the unique irreducible \( M \)-module may be identified with \( E \).
Say \([E: \mathbb{F}] = n\). The vector space \(V\) is a module over \(E \otimes_F \mathbb{F}[G]\), hence by over \(M = M_n(\mathbb{F})\), and with this isomorphism goes one of \(E\) with \(F^n\). The result we want, that \(V = E \otimes_F V^G\), follows from:

2.6. Lemma. Suppose \(V\) to be any module over \(M = \text{End}(U)\) with \(U\) a vector space of finite dimension over \(F\). The canonical map from \(V\) to \(U \otimes_F \text{Hom}_M(U, V)\) is an isomorphism.

**Proof.** The map from \(\hat{U} \otimes_F U\) to \(M\) is a bijection, and therefore

\[
V = \text{Hom}_M(M, V) = \text{Hom}_M(\hat{U} \otimes_F U, V) = U \otimes_F \text{Hom}_M(U, V)
\]

for trivial reasons.

In our case \(U = E\) as a module over \(E[\mathbb{F}] = E \otimes_F F[\mathbb{F}] \cong \text{End}_F(E)\). And furthermore

\[
\text{Hom}_{E[\mathbb{F}]}(E, V) = \text{Hom}_F(F, V) = V^G
\]

through \(f \mapsto f(1)\). This concludes the proof of .

**Remark.** is a special case of a more general construction of central simple algebras over \(F\), as we shall see in a later section.

3. Non-abelian cohomology

In this section I’ll recall what we’ll need to know later about cohomology groups \(H^1(G, A)\), where \(G\) is a group and the group \(A\)—possibly non-abelian—is one on which \(G\) acts through a homomorphism to \(\text{Aut}(A)\).

**ONE-COHOMOLOGY.** Let me first explain the problem for which \(H^1\) is a solution. Suppose we consider a short exact sequence

\[
1 \longrightarrow A \longrightarrow A \longrightarrow G \longrightarrow 1.
\]

At first I do not make any further assumption on it. Suppose given \(g\) in \(G\). Choose \(\overline{g}\) in \(A\) projecting onto \(g\).

The map

\[
x \longmapsto \overline{xg}\overline{x}^{-1}
\]

is an automorphism of \(A\). Any other choice projecting onto \(g\) will be of the form \(x\overline{g}\), and conjugation by \(g\) will differ from the original one by an inner automorphism of \(A\). We therefore get a homomorphism from \(G\) to the group \(\text{Out}(A) = \text{Aut}(A)/\text{Int}(A)\) of outer automorphisms of \(A\). These are not necessarily in fact automorphisms of \(A\), unless we make some further assumption. One possible assumption is that \(A\) be abelian.

Another good assumption is that the extension split. In that case, the splitting defines an action of \(G\) on \(A\), and we may identify \(A\) with the semidirect product \(A \rtimes G\), with elements \((g, a)\) and multiplication

\[
(g, a)(h, b) = (gh, h^{-1}ah \cdot b).
\]

In the future I shall write \(g^{-1}ag\) as \(a^g\), so the second factor above is \(a^h\).

There will in general be many other splittings. They may give rise to different actions of \(G\) on \(A\). If we are given one splitting, we can get another by composing the first with conjugation by an element of \(A\), in which case the two are said to be equivalent. The problem that \(H^1\) solves is to a classify equivalence classes of splittings.

Fix one splitting, hence an identification of the extension with a semi-direct product. We get also a fixed action of \(G\) on \(A\). Any section of the projection from \(A \rtimes G\) to \(G\) takes \(g\) to some \((g, a_g)\). The following is straightforward:

3.1. Lemma. The section \(g \mapsto (g, a_g)\) is a splitting if and only if

\[
a_{gh} = a_g^h a_h
\]
for all \( g, h \) in \( G \).

Let \( Z^1(G, A) \) be the set of maps \( G \to A \) satisfying this \textbf{cocycle condition.}

If we choose \( a \in A \) and replace this splitting \( a_g \) by composition with conjugation by \( b \), the new splitting takes \( g \) to \( b(g, a_g)b^{-1} = (g, b^g a_g b^{-1}) \). So the cocycles equivalent to \( g \mapsto a_g \) are those of the form

\[
g \mapsto b^g a_g b^{-1},
\]

which are said to be \textbf{cohomologous} to the original cocycle. The group \( H^1(G, A) \) is defined to be the set of cocycles \( Z^1(G, A) \) modulo this equivalence. It is a set, not necessarily a group, but it does have a distinguished element—the cocycles equivalent to the trivial one, those of the form \( b^g b^{-1} \).

In summary:

\textbf{3.3. Proposition.} The map taking \( a_g \in Z^1(G, A) \) to the corresponding splitting of \( G \rtimes A \) induces a bijection of \( H^1(G, A) \) with the classes of splittings modulo conjugation by elements of \( A \).

So far, all I have done is to make a more or less tautologous translation from one language to another. What are the advantages of this translation? One is that if \( A \) is abelian groups \( H^q(G, A) \) may be defined for all \( q \).

Another is the existence of long exact sequences.

\textbf{TWO-COHOMOLOGY.} Suppose now \( A \) to be abelian, and again consider a short exact sequence

\[
1 \to A \to A \to G \to 1.
\]

As we have seen, this gives rise to an action of \( G \) on \( A \). Suppose we choose a section \( g \mapsto \overline{g} \) from \( G \) to \( A \). If \( g \) and \( h \) lie in \( G \) then

\[
\overline{gh} = g h a_{g,h}
\]

for some unique \( a_{g,h} \) in \( A \). Since

\[
(\overline{gh})^k = \overline{gh a_{g,h}^k} = g h a_{g,h}^k = g h k a_{g,h} a_{g,h}^k,
\]

\[
\overline{g} \overline{h} = \overline{g} a_{g,h} \overline{h} = g h a_{g,h} a_{g,h}^k
\]

Associativity in \( A \) is therefore equivalent to the identity

\[
a_{gh,k} a_{g,h}^k = a_{g,h,k} a_{gh,k}.
\]

Define \( Z^2(G, A) \) to be the set of maps from \( G \times G \) to \( A \) satisfying this condition.

Suppose we replace the given section by \( \overline{g} h \). Then

\[
\overline{g} h b_g \overline{h} = \overline{g} h b_g b h = \overline{g} h b_g \cdot b_{gh}^{-1} a_{gh} b_{gh} b h.
\]

The cocycles \( a_{g,h} \) and \( b_{gh}^{-1} a_{gh} b_{gh} b h \) are said to be cohomologous, and \( H^2(G, A) \) is defined to be the set of equivalence classes of two-cocycles. It contains the cocycles

\[
b_{gh}^{-1} b_{gh} b h
\]

equivalent to the trivial two-cocycle.

Two extensions of \( G \) by \( A \) are said to be equivalent if there exists an isomorphism between them that induces the identity on both \( G \) and \( A \).
3.5. **Proposition.** The map from extensions to $\mathbb{Z}^2(G, A)$ induces a bijection of equivalence classes of extensions of $G$ by $A$ with $H^2(G, A)$.

**THE CONNECTING MAP.** Suppose we are given a short exact sequence of $G$-modules

$$1 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 1,$$

with $A$ contained in the centre of $B$. The projection from $B$ to $C$ gives us a map

$$H^1(G, B) \longrightarrow H^1(G, C).$$

Suppose we are given a cocycle $c_g$ representing a cohomology class in $H^1(G, C)$. Let $b_g$ be any element of $B$ projecting onto $c_g$. Define

$$a_{g,h} = b_g^{-1}b_{gh}b_h.$$

It defines a two-cocycle in $Z^2(G, A)$, and we get in this way a map

$$H^1(G, C) \longrightarrow H^2(G, A).$$

3.6. **Proposition.** Suppose given the short exact sequence of $G$-modules

$$1 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 1,$$

with $A$ in the centre of $B$. The corresponding sequence

$$H^1(G, A) \longrightarrow H^1(G, B) \longrightarrow H^1(G, C) \longrightarrow H^1(G, A)$$

is an exact sequence of pointed sets.

It is instructive to interpret this in terms of extensions of $G$ by $A$.

**PROFINITE GROUPS.** If $G$ is the projective limit of finite quotients $G/H$, then by definition

$$H^q(G, A) = \lim_{\longrightarrow} H^q(G/H, A^H).$$

4. Tensor structures

In this section I’ll explain some simple examples relating Galois cohomology and isomorphism classes of certain structures on a vector space.

**VARIATIONS ON THEOREM 90.** The following is a basic result in the cohomology of Galois groups. We’ll see later why one could have predicted it.

4.1. **Proposition.** Suppose $E/F$ to be a Galois extension with group $G$, $V$ a vector space defined over $F$. Then $H^1(G, GL_E(V)) = \{1\}$.

**Proof.** Suppose $f_\sigma$ to be a one-cocycle of $G$ with values in $GL_n(E)$. Then

$$v \mapsto v^{[\sigma]} = f_{\sigma^{-1}}(v)\sigma$$

is a $\sigma$-linear map from $E^n$ to itself: $(cv)^{[\sigma]} = c^{[\sigma]}v^{[\sigma]}$. The cocycle condition on $f_\sigma$ tells us that $v^{[\sigma\tau]} = (v^{[\sigma]})^{[\tau]}$, so this gives a right $G$-action on $V$. We may therefore apply to deduce that if $U$ is the space of all $v$ in $V$ such that $\varphi_\sigma(v) = v$ then $U$ is an $F$-vector space such that $V = U \otimes_F E$. Let $E = (e_i)$ be an $F$-basis of $U$. By definition, these are fixed under the map $\varphi_\sigma$, so

$$\varphi_\sigma \left( \sum x_i e_i \right) = \sum x_i^\sigma e_i$$
If a ring structure on \( \text{Symplectic structures on a vector space} \) are unique, so this tells us that

\[ f_{\sigma^{-1}}(Ex)^\sigma = Ex^\sigma, \quad f_\sigma = E^\sigma E^{-1}. \]

**Tensor Structures.** If \( V \) is a finite-dimensional vector space over \( F \), let \( \hat{V} \) be the space of \( F \)-linear functions on it. A **tensor structure** \( T \) on \( V \) is a finite set of tensors in \( \bigotimes^* V \otimes_F \bigotimes^* \hat{V} \). An isomorphism of tensor structures is one of vector spaces taking one tensor structure into the other. The group \( \text{Aut}_F(T) \) of \( F \)-rational automorphisms of \( (V,T) \) is a subgroup of \( GL_F(V) \). If \( V \) is assigned a basis, it becomes a group of matrices with entries in \( F \).

**Example.** Suppose the characteristic of \( F \) not to be 2. A quadratic form on \( V \) may be identified with a linear function on the symmetric tensors \( S^2 V \).

**Example.** Again suppose the characteristic of \( F \) not equal to 2. An alternating form \( A \) is a linear function on \( \bigwedge^2 V \).

**Example.** A ring structure on \( V \) is a product \( V \otimes V \to V \) satisfying certain properties. A unit in the ring is an element of \( V \).

**Example.** If \( V \) is a vector space over \( F \) and \( E/F \) a finite extension, a structure on \( V \) of vector space over \( E \) is a tensor structure.

Suppose given \((V,T)\) defined over \( F \). If \( E/F \) is any field extension, this structure gives rise in the obvious way to a tensor structure on \( E \otimes_F V \).

The following problem is very natural:

*Suppose \((V,T)\) to be defined over \( F \) and \( E/F \) Galois. Classify all the \( F \)-rational tensor structures on \( V \) that become isomorphic to \( T \) over \( E \).*

The group \( GL_n \) is the automorphism group of vector spaces. Therefore \( H^1(\mathcal{G}, GL_n(E)) \) should parametrize isomorphism classes of vector spaces over \( F \) that become isomorphic to \( E^n \) over \( E \). Of course all vector spaces over \( F \) of the same dimension are isomorphic, which leads us to expect .

**Example.** Suppose \( V \) to be \( F^2 \) (assumed not to be of characteristic 2) and \( T \) to be the quadratic form \( xy \). Those tensor structures isomorphic to this one over \( E \) are those nondegenerate quadratic forms \( Q(v) \) which possess an isotropic vector in \( \hat{V}_E = E \otimes_F V \) (i.e. a \( v \neq 0 \) with \( Q(v) = 0 \)). In particular, if \( E \) is separably closed then these are all the non-degenerate quadratic forms on \( V \).

There is a very useful, if somewhat tautological, way to solve the problem I posed above. Suppose \( S \) and \( T \) given on \( V \). They will be isomorphic over \( E \) if and only if there exists an element \( \alpha \) of \( GL(V_E) \) such that \( \alpha(S) = T \). But since \( S \) and \( T \) are both \( F \)-rational, this implies that \( \alpha^\sigma \) will also take \( S \) to \( T \), and then \( f_\sigma = \alpha^\sigma \alpha^{-1} \) will lie in \( \text{Aut}_E(T) \). The map \( \sigma \mapsto f_\sigma \) will be a cocycle. The map taking \( S \) to this cocycle is a map from structures \( S \) to \( Z^1(\mathcal{G}, \text{Aut}_E) \).

**4.2. Theorem.** The map defined above from \( S \) to \( Z^1(\mathcal{G}, \text{Aut}_E(T)) \) induces a bijection of isomorphism classes of tensor structures \((V,S)\) that become isomorphic to \( T \) over \( E \) with \( H^1(\mathcal{G}, \text{Aut}_E(T)) \).

**Proof.** The only slightly tricky point is surjectivity. If given a cocycle \( f_\sigma \) in \( \text{Aut}_E(T) \), according to there exists \( \alpha \) in \( GL_E(V) \) with \( \alpha^\sigma \alpha^{-1} = f_\sigma \). Then \( S = \alpha^{-1}T \) is fixed by the Galois action, hence \( F \)-rational.

**Example.** Symplectic structures on a vector space are unique, so this tells us that \( H^1(\mathcal{G}, \text{Sp}(V)) = \{1\} \).
5. Central simple algebras

There is a particularly important category of tensor structures. Suppose $R$ to be an algebra over the field $F$, of finite dimension.

5.1. Theorem. The following are equivalent:

(a) the ring $R$ has no two-sided ideals, and its centre is $F$;
(b) if $\bar{F}$ is an algebraically closed extension of $F$, then $\bar{F} \otimes_F R$ is isomorphic to some $M_n(\bar{F})$;
(c) the ring $R$ is isomorphic to some $M_n(D)$, with $D$ a division algebra whose centre is $F$;
(d) there exists some Galois extension $E/F$ such that $E \otimes_F R$ is isomorphic to some $M_n(E)$.

This is proved in §IX.1 of [Weil:1995].

The field $E$ in (d) is said to split $R$. It is also proved there that the division algebra $D$ in (c) is uniquely determined by $R$ (it is the endomorphism ring of the unique irreducible module over $R$), and that every automorphism of $R$ amounts to conjugation by an invertible element of $R$.

In particular, $\text{Aut}_E(M_n)$ is isomorphic to $\text{PGL}_n(E)$.

The following is also proved in [Weil:1995]:

5.2. Proposition. If $A$ is a central simple algebra over $F$, there exist unique functions $\text{TR}$ and $\text{NM}$ on $A$ agreeing with the trace and determinant on $M_n(E)$ whenever $E \otimes_F R$ is isomorphic to $M_n(E)$.

5.3. Proposition. Suppose $D$ to be a division algebra of degree $r^2$ over $F$. A field $E$ splits $M_n(D)$ if and only if it contains a subfield of degree $r$ over $F$ contained in $D$.

The following is a special case of the basic descent theorem:

5.4. Proposition. The isomorphism classes of central simple algebras $R$ such that $E \otimes_F R$ is isomorphic to $M_n(E)$ are in bijection with $H^1(\text{Gal}(E/F), \text{PGL}_n(E))$.

From the short exact sequence

$$1 \longrightarrow E^\times \longrightarrow \text{GL}_n(E) \longrightarrow \text{PGL}_n(E) \longrightarrow 1$$

we derive the exact segment

$$\cdots \longrightarrow H^1(\mathcal{G}, \text{GL}_n(E)) \longrightarrow H^1(\mathcal{G}, \text{PGL}_n(E)) \longrightarrow H^2(\mathcal{G}, E^\times)$$

and in particular a map

$$H^1(\mathcal{G}, \text{PGL}_n(E)) \hookrightarrow H^2(\mathcal{G}, E^\times)$$

whose inverse image of the trivial class is also trivial. It is somewhat awkward to consider this map all by itself, but this awkwardness can be eliminated by introducing a new structure.

The Brauer group. Two algebras are said to be equivalent when one is some $M_n(D)$ and the other is $M_m(D)$, for the same division algebra $D$. If $R$ and $S$ are central simple algebras over $F$, so is $R \otimes_F S$. This product induces a product on the set of equivalence classes, since $M_n(C) \otimes M_n(D)$ is isomorphic to $M_{nm}(C \otimes_D D)$. If $R$ is a central simple algebra over $F$, its opposite $R^{opp}$ is the same vector space over $F$, but with multiplication reversed in order. The product $R \otimes R^{opp}$ is isomorphic to the ring $\text{End}_F(R)$, so $R^{opp}$ is an inverse with respect to this product. In other words, the set of equivalence classes of central simple algebras over $F$ together with the product induced by tensoring is a group—the Brauer group $\text{BR}(F)$.

Let $F_\text{s}$ be a separable closure of $F$. The connecting maps defined earlier determine a connecting map

$$\text{BR}(F) \longrightarrow H^2(\text{Gal}(F_\text{s}/F), F_\text{s}^\times).$$

It is an isomorphism of abelian groups (Proposition 9 of X.5 in [Serre:1968]).
I’ll not prove this, but I can give some idea of why it works. Suppose \( E/F \) to be a Galois extension of degree \( n, a_{\sigma, \tau} \) in \( Z^2(G(E/F), E^\times) \). Let \( \varepsilon_\sigma \) be a basis of some vector space \( U \) over \( F \) parametrized by \( G(E/F) \). Define on \( U \otimes_F E \) a product by formulas

\[
x \varepsilon_\sigma = \varepsilon \sigma^\sigma, \quad \varepsilon_\sigma \varepsilon_\tau = \varepsilon_{\sigma \tau} a_{\sigma, \tau}.
\]

It is an associative product because of the definition of two-cocycles, so we have defined in this way an algebra over \( F \). It turns out to be a central simple algebra.

**The Brauer Group of the Real Numbers.** Let \( G = \{1, \sigma\} \) be the Galois group of \( \mathbb{C}/\mathbb{R} \). The cohomology group \( H^2(G, \mathbb{C}^\times) \) is isomorphic to \( \mathbb{R}^\times / \mathbb{R}_{>0}^\times = \{\pm 1\} \). What is the algebra corresponding to the non-trivial class?

Hamilton’s quaternion algebra \( \mathbb{H} \) is the algebra of dimension 2 over \( \mathbb{C} \) spanned by 1 and \( \sigma \) with relations

\[
z \sigma = \sigma z, \quad \sigma^2 = -1.
\]

The multiplicative group \( \mathbb{H}^\times \) contains an extension of \( \mathbb{C}^\times \) by \( \{\sigma, 1\} \) which does not split. Because \( \sigma^2 \) does not lie in \( N \mathbb{C}^\times \), this construction defines a division algebra.

In general, when \( F \) is a local field, the Brauer group is a fundamental object in class field theory.

**General Remarks.** There are many reasons why central simple algebras are important. One of them is that the unit groups of central simple algebras are among the simplest reductive groups, and often help to analyze others. For example, suppose \( D \) over a field \( F \). If \( D \) is a division algebra of degree \( r^2 \), the maximal tori of \( D^\times \) are the groups \( E^\times \) with \( E/F \) of degree \( n \), and semi-simple conjugacy classes are classified easily in terms of the non-zero elements of such field. It is not easy to classify all field extensions \( E/F \) of a given degree, but that rarely important. What counts is how the semi-simple classes of \( D^\times \) and \( \text{GL}_r(F) \), which are inner forms of each other) are related. For \( p \)-adic fields these groups are particularly significant since the groups isogenous to \( D^\times / F^\times \) are the only anisotropic semi-simple groups.

Another reason for importance is that central simple algebras can be used to prove the basic facts of class field theory.

### 6. Affine varieties

From a naive point of view, an algebraic variety defined over a field \( F \) is the set of points in some \( F^n \) satisfying a set of polynomial equations \( P_i(x) = 0 \). But this is certainly not the right definition. For example, the variety \( x^2 + y^2 + 1 = 0 \) has no points at all with real coordinates, but it would not be wise to think that it is trivial as an algebraic variety. The same equation specifies points also in \( \mathbb{C}^2 \) satisfying it. Very generally, a collection of polynomials \( P_i \) with coefficients in a field \( F \) is also a collection of polynomials with coefficients in any extension field \( E/F \). An algebraic variety defined over \( F \) also determines an algebraic variety defined over every field extension \( E/F \), and this should be considered as part of its nature. **Base field extension** is one feature of algebraic varieties that must be taken into account.

Another thing to be aware of is that an algebraic variety can have several incarnations. For example, projection onto the \( x \)-axis allows us to identify the real line \( x = y \) with the \( x \)-axis. An **algebraic variety must not be identified with a particular set of points or with an explicit realization in a vector space.**

So I ask:

**What is the proper definition of an (affine) algebraic variety defined over a field \( F \)?**

The answer is, its **coordinate or affine ring** \( A_F[V] \). Let \( \overline{F} \) be an algebraically closed extension of \( F \).

If \( V \) is defined by polynomial equations \( P_i(x) = 0 \) (where \( x = (x_1, \ldots, x_n) \)) with coefficients in the field \( F \) then \( A_F[V] \) is the ring made up of the restrictions of all polynomial functions \( P(x_1, \ldots, x_n) \) to the points in \( \overline{F}^n \) satisfying these equations.
Algebraic structures and fields of definition

There are a couple of things to keep in mind when considering this definition, which is slightly subtle.

The first is that the condition of algebraic closure is important. As I have already said, one feature of an algebraic variety defined over a field $F$ is that it determines also an algebraic variety over any field extension of $F$. If two varieties are to be considered the same, a minimal condition is that there must be a bijection between the points on each of them with coordinates in every field extension of $F$, and in particular in an algebraic closure $\overline{F}$. This is a fairly straightforward requirement. What is not quite so obvious is to what extent looking only at $\overline{F}$ is sufficient. This is what the Nullstellensatz asserts, as I’ll recall in a moment.

There is another problem. Let $I$ be the ideal of $F[x]$ generated by the $P_i$. The set of points where all the $P_i$ vanish is the same as the set where all $P$ in $I$ vanish. There is hence a canonical map from the quotient ring $F[x]/I$ to the ring of functions on the zero set of the polynomials $P_i$ in $\overline{F}$. Why don’t I define the affine ring of the variety defined by the $P_i$ to be $F[x]/I$? Because the map from $F[x]/I$ to the ring of functions on the zero set is not necessarily an injection. The ring $A_F(V)$ that I have defined is the quotient of $F[x]$ by the ideal of all polynomials that vanish on the points on the variety with coordinates in $\overline{F}$. It includes the original $P_i$ as well as all of the ideal $I$ in $F[X]$ that they generate, but it might include other polynomials as well. To see a simple example, let $P_1(x, y) = x^2$ and $P_2(x, y) = y^2$. The set of common zeroes for this pair is just the origin, but the polynomials $x$ and $y$ also vanish there, and are not in the ideal generated by $x^2$ and $y^2$.

Hilbert’s Nullstellensatz clears up these matters. This was formulated originally in §II.3 of [Hilbert:1893]. (Violating the usual convention of naming theorems, this result is both non-trivial and due to Hilbert.) The traditional approach to it, which is somewhat abstract, is presented succinctly in [Grayson:2000]. The theorem has been taken up more recently in [Tao:2007], in which is formulated and proven a constructive version. Another recent exposition can be found in [Arrondo:2006].

The Nullstellensatz asserts roughly (even in Hilbert’s version) that if $I$ is a polynomial ideal of $F[x]$ the set of points in $\overline{F}$ in the zero set of $I$ is sufficiently large. If $P(x) = 0$ for all $P$ in $I$ and $Q^n \in I$, then we also have $Q(x) = 0$. So certainly every polynomial in the radical $\sqrt{I}$ of $I$, the ideal generated by all such $Q$, vanishes on the zero set of $I$. If the zero set were small, there might well be other polynomials that vanish on this set. This is exactly what happens if $F$ is not necessarily algebraically closed. But the Nullstellensatz tells us that this does not happen if $F$ is algebraically closed:

6.1. Proposition. (Nullstellensatz) If $F$ is algebraically closed and $Q(x) = 0$ for all points $x$ in the zero set of $I$ then $Q$ lies in the radical of $I$.

The projection from $F[x]/I$ to $A_F[V]$ factors through $F[x]/\sqrt{I}$. Therefore the definition above says that the affine ring $A_F[V]$ determined by the ideal $I$ in $F[x]$ is the ring $F[x]/\sqrt{I}$. As one consequence, the ring $A_F[V]$ possesses no nilpotent elements other than 0—it is said to be reduced. (Grothendieck has generalized the notion of variety to that of scheme, in which he allows non-reduced affine rings. This is in many circumstances exactly the right thing to do, but schemes will not play a role here.)

The affine ring alone does not determine the structure of an affine algebraic variety. There is an extra ingredient only implicit in what we have been discussing. Suppose $V$ to be an affine variety in $F^n$ determined by the ideal $I$ in $F[x]$. For $\sigma$ an automorphism of $F$ the conjugate $V^\sigma$ will be the affine variety determined by the ideal $I^\sigma$. It will contain, for example, all the points $x^\sigma$ as $x$ ranges over the zero set of $I$ in $F^n$. The affine ring of $V^\sigma$ is the quotient $F[x]/I^\sigma$. It is isomorphic to $F[x]/I$, since $P \mapsto P^\sigma$ is an isomorphism. But the two varieties $V$ and $V^\sigma$ are distinct. What goes wrong is that isomorphism of affine rings conjugates elements in copy of $F$ in $F[x]/I$. It is necessary to take into account not only the isomorphism class of $A_F[V]$, but also the embedding of $F$ into $A_F[V]$ that makes it into an $F$-algebra. Different embeddings in fact may correspond to different algebraic varieties.

In this essay, therefore:

**Definition.** An affine algebraic variety defined over the field $F$ is a pair $(A, \iota)$ where $A$ is a ring and $\iota: F \hookrightarrow A$ an embedding, such that (a) $A$ is finitely generated over the image of $F$ and (b) $A$ is reduced.
Two algebraic varieties \((A_1, \iota_1)\) and \((A_2, \iota_2)\) are isomorphic if there exists an isomorphism \(\varphi: A_1 \to A_2\) such that \(\varphi(\iota_1(x)) = \iota_2(x)\) for all \(x\) in \(F\).

I’ll often write \(A\) as \(A_F\) to emphasize succinctly the role of the embedding of \(F\).

The simplest examples of affine varieties are the affine spaces \(V = A_n\) over \(F\), with \(A_F[V] = F[x] = F[x_1, \ldots, x_n]\).

I believe that this definition is ultimately due to Chevalley, although it became much more versatile in the hands of Serre and Grothendieck. It has many virtues, although they are not all immediately manifest. It is not obviously geometric in nature, but it still somehow manages to encapsulate the geometry in algebraic geometry without losing an algebraic flavour. But in order to understand this, certain natural questions must be answered. We would like geometric properties of an algebraic variety to be determined by its affine ring.

• **What does this definition have to do with the usual one in terms of zero sets?** This question has several different components. One is, how does the zero set of a collection of polynomials determine its affine ring?

I have already answered this—if \(I\) is an ideal in the polynomial algebra \(F[x]\) then the affine ring defining the variety where \(P = 0\) for all \(P\) in \(I\) is the quotient ring \(F[x]/I\). If \(F\) is algebraically closed, the affine ring may be identified with the restrictions of polynomials to the zero set of \(I\).

• A second component of the same question is, if the variety is to be dissociated from any particular incarnation in some affine space, **what are the points of the variety?** That is to say, we would like to identify these points independently of a representation of \(A\) as a quotient of some \(F[x]\). How can we do this? If \(A = F[x]/I\), a point \(x = (x_i)\) in the variety with coordinates in any field \(E\) containing \(F\) is one for which \(P(x) = 0\) for \(P\) in \(I\). Every such point \(x\) determines by evaluation at \(x\) a ring homomorphism \(\varphi_x\) from \(A_F[V]\) to \(E\), taking \(P\) to \(P(x)\), compatible with the embedding of \(F\) into \(E\). Conversely, any such homomorphism \(\varphi\) determines the point \((\varphi(x_i))\) in \(E^n\). This identifies the \(E\)-rational points of the variety with such homomorphisms. The natural answer to the question is therefore:

A point of the variety \(V\) determined by the affine ring \((A, \iota)\), rational over the field \(E\) containing \(F\), is a homomorphism from \(A\) to \(E\) compatible with the embeddings of \(F\) into both.

This definition does have peculiarities—it allows \(E\) to be the quotient field of \(A\) itself if it exists. This is called a **generic point** of the variety. Such points are a major part of Weil’s approach to algebraic geometry, which was the precursor of Grothendieck’s.

The truly geometric points of the variety are those whose coordinates are algebraic over \(F\). Since \(A_F[V]\) is finitely generated over \(F\), its image will be a finite algebraic extension of \(F\), hence a field. Its kernel \(\ker(\varphi)\) will therefore be a maximal ideal of \(A_F[V]\). Hence, a second answer to the question is this:

A point of the variety \(V\) determined by the affine ring \((A, \iota)\), rational over the field extension \(E/F\), is a maximal ideal \(m\) of \(A\), together with a homomorphism from \(A/m\) to \(E\) compatible with embeddings of \(F\).

There is something to be proven, namely that if \(m\) is a maximal ideal of \(A_F[V]\) then \(A_F[V]/m\) is an algebraic extension of \(F\). This is in fact another version of Hilbert’s Nullstellensatz. In many expositions, for example [Grayson:2000], this is its principal formulation.

• **What are maps from one variety to another?** If \(\Phi: U \to V\) is an algebraic map of algebraic varieties and \(f\) is in the affine ring of \(V\), then the pull-back \(f \circ \Phi\) is an affine function on \(U\). This induces a ring homomorphism \(\Phi^*\) from \(A_F[V]\) to \(A_F[U]\) compatible with the embeddings of \(F\). Indeed, as a matter of definition an algebraic map \(\Phi\) from \(U\) to \(V\) is neither more nor less than such a homomorphism:

\[
\begin{array}{ccc}
A_F[V] & \xrightarrow{\Phi^*} & A_F[U] \\
\downarrow & & \downarrow \\
F & & F
\end{array}
\]
Such a homomorphism determines, for example, an associated map from points of $U$ to points of $V$, since if we are given $\varphi: A_F[U] \to E$ then $\varphi \circ \Phi^*$ is an $E$-rational point of $V$.

- **What are the irreducible components of the variety?** A variety can be the union of several subvarieties. For example, the variety $xy = 0$ is the union of $x$ and $y$ axes. The characteristic feature of a reducible variety is the existence of zero-divisors in its affine ring—here, $x$ and $y$. The product $xy$ vanishes on the variety, but neither of its factors vanishes identically on it. A variety is **irreducible** if $A_F[V]$ is an integral domain, and **absolutely irreducible** if $A \otimes_F \overline{F}$ is irreducible. The variety defined by $x^2 + y^2 = 0$ is irreducible over $\mathbb{R}$ but not over $\mathbb{C}$, where it breaks into the lines $x + iy = 0$ and $x - iy = 0$. In general, a variety is the union of a finite number of irreducible components. An affine variety is said to be **Zariski-connected** if its affine ring is not the direct sum of two subrings.

- **What is the Galois action on points?** If $E/F$ is a Galois extension with Galois group $G$, $V$ is embedded in affine space, and $x = (x_i)$ is a point on $V$ with coordinates in $E$, then the conjugate $x^\sigma$ by $\sigma$ in $G$ is the point $(x_i^\sigma)$. How do we translate this operation in terms of the intrinsic definition of points? Given a homomorphism $\varphi$ from $A_F[V]$ to $E$, the conjugate point $\varphi^\sigma$ is $P \mapsto \varphi(P)^\sigma$.

- **What is the conjugate of a variety?** Suppose $V$ to be defined by equations $P_i = 0$ where the $P_i$ have coefficients in $F$. If $A, i: U \to \mathbb{A}^n$ are functions in $A$ then $1 \in U$ is a point of $V$, where it breaks into the lines $x + iy = 0$ and $x - iy = 0$. In general, a variety is the union of a finite number of irreducible components. An affine variety is said to be **Zariski-connected** if its affine ring is not the direct sum of two subrings.

The map taking $P$ to $P^\sigma$ depends on a particular realization of $V$, so the characterization above of the affine ring of $V^\sigma$ seems to depend on a particular embedding of $V$ into a vector space. **Is there a characterization depending only on the ring of $V$?** There is a very simple answer:

**6.2. Proposition.** If $\sigma$ is an automorphism of $F$ then the $\sigma$-conjugate of $(A, i)$ may be identified with $(A, i \circ \sigma^{-1})$.

Or, in other words, the vector space structure on $A_F[V^\sigma]$ is the $\sigma$-conjugate of that on $A_F[V^\sigma]$.

**Proof.** Because the following diagram is commutative:

$$
\begin{array}{ccc}
F[x]/I & \xrightarrow{\sigma} & F[x]/I^g \\
\uparrow{_{\iota^{-1}}} & & \uparrow{_{\iota^{-1}}} \\
F & \xrightarrow{1} & F \\
\end{array}
$$

If $x$ is a point of $V$ and $\varphi_x$ is the corresponding homomorphism from $A[V]$ to $F$, then the homomorphism corresponding to $x^\sigma$ is $\sigma \circ \varphi$.

- **What is the direct product of two varieties?** If $f$ and $g$ are functions in $A[U]$ and $A[V]$, then $f(u)g(v)$ is an affine function on $U \times V$. This map induces an isomorphism of $A[U] \otimes A[V]$ with $A[U \times V]$.

An algebraic map from one variety to another is defined by its graph, or equivalently by a ring homomorphism in the inverse direction. This corresponds to the observation that if $f: U \to V$ is an algebraic map between two algebraic $F$-varieties, composition with $f$ is an $F$-map and a ring homomorphism from $A[V]$ to $A[U]$. The map is uniquely determined by this homomorphism. If $\Phi^*: A[U] \to A[V]$ corresponds to an algebraic map of varieties, then $\Phi^{*, \sigma}$ is in these terms the same map, but with the twisted embedding of $F$. Equivalently, it is the map determined by the graph conjugate. Explicitly:

$$
f^\sigma(x) = \sigma^{-1}(f(\sigma(x))) = f(x^\sigma)^{\sigma^{-1}}.
$$
• **Restriction of scalars.** If $E/F$ is a finite field extension of degree $d$ then a variety defined over $E$ of dimension $n$ determines one of dimension $nd$ defined over $F$. This construction is called **restriction of scalars.** The non-canonical way to construct it is to assign a basis to $E$ as a vector space over $F$, and write out the equations defining $E$ in terms of the coordinates of elements of $E$. I’ll present a coordinate-free definition later on. For example, the multiplicative group of $\mathbb{C}$ is a one-dimensional group over $\mathbb{C}$, but by assigning it real and imaginary coordinates it becomes a two-dimensional group over $\mathbb{R}$. More specifically, the complex points of $\mathbb{C} \times$ may be identified with the pairs $(w, z)$ in $\mathbb{C}^2$ with $wz - 1 = 0$. If we set $w = u + iv, z = x + iy$ this becomes a pair of equations with coefficients in $\mathbb{R}$:

$$ux - vy = 1$$
$$vx + uy = 0 .$$

Therefore the complex points of the variety $wz - 1 = 0$ may be identified with the real points of the two-dimensional variety in $\mathbb{R}^4$ defined by this pair of equations.

### 7. Descending fields of definition

An affine variety defined over $F$ determines one over any extension field $E$ of $F$:

$$A_E[V] = E \otimes_F A[V] ,$$

together with the canonical embedding of $E$. This is called **extending** the base field. **Under what circumstances does a variety defined over $E$ arise in this way?** In other words, **when can we descend the field of definition?** In how many different ways?

In the most important case, $E$ is a finite Galois extension of $F$, say with Galois group $\mathcal{G}$. If $V$ is an affine variety defined over $F$, then since the defining polynomials of $V$ have coefficients in $F$, they are not affected by conjugation. In other words, the conjugate of $V$ is the same as $V$. Thus a necessary condition for $V$ to possess $F$ as field of definition is that $V^\sigma \cong V$ for all $\sigma \in \mathcal{G}$. However, something stronger is required as well.

Let me explain. A map $\varphi_\sigma$ from $V$ to $V^\sigma$ is the same thing as a ring homomorphism from $A_F[V^\sigma]$ to $A_F[V]$ or, according to , a ring homomorphism $\varphi_\sigma^*$ fitting into this commutative diagram:

$$\begin{array}{ccc}
A_E[V] & \xrightarrow{\varphi_\sigma^*} & A_E[V] \\
\downarrow & & \downarrow \\
E & \xrightarrow{\sigma^{-1}} & E
\end{array}$$

But if $V$ is defined over $F$ then $A_E[V] = E \otimes_F A_F[V]$, and we may take

$$\varphi_\sigma^*: e \otimes P \mapsto e^\sigma \otimes P .$$

In summary:

**7.1. Proposition.** If $V$ is defined over $F$, the ring isomorphism

$$A_E[V^\sigma] \to A_E[V]: e \otimes P \mapsto e^\sigma \otimes P$$

defines a canonical isomorphism of $V$ with $V^\sigma$ over the Galois extension $E/F$.

The following questions now arise naturally:
Suppose conversely $V$ to be an affine algebraic variety defined over $E$ and suppose that for every $\sigma$ in $G$ the variety $V$ is isomorphic to $V^{\sigma}$. Can we find an affine algebraic variety defined over $F$ over $E$?

Suppose $V$ to be an affine variety defined over $F$. How can we classify all affine varieties defined over $F$ that are isomorphic to $V$ over $E$? All those with some additional structure possessed by $V$? For example, if $G$ is an affine algebraic group defined over $F$, how to classify all affine algebraic groups defined over $F$ that are isomorphic as algebraic groups to $G$ over $E$?

The answer to the first question is, in brief, “not necessarily.” There can be an obstruction to making the descent, which can be characterized very explicitly in more familiar terms. For any variety $V$ defined over $E$ let

$$E = \{ (\sigma, f_\sigma) \mid \sigma \in G, f_\sigma : V \to V^{\sigma} \text{ an isomorphism} \}.$$ 

A map $f_\sigma$ may be considered as an algebraic variety, since it is determined by its graph $\{ (v, f(v)) \}$. Here $P(v) = 0$ and $P^{\sigma}(f_\sigma(v)) = 0$ for all defining $P$. Each conjugate $f^{\tau}$ is then defined. It is made up of points $(v^{\tau}, f(v)^{\tau})$, and is hence an isomorphism of $V^{\tau}$ with $V^{\sigma \tau}$.

This allows us to make a group out of $E$—given $(\sigma, f_\sigma)$ and $(\tau, f_\tau)$ we compose to get $(\sigma \tau, f_{\sigma \tau})$:

$$f_{\sigma \tau} = f_\sigma^{\tau} f_\tau : V \to V^{\sigma \tau}.$$ 

This is consistent with the calculation

$$(\sigma, f_\sigma)(\tau, f_\tau) = (\sigma \tau, f_{\sigma \tau}).$$

The assumption that $V \cong V^{\sigma}$ for each $\sigma$ in $G$ means that we have a short exact sequence

$$(7.2) \quad 1 \to \text{Aut}_E(V) \to E \to G \to 1.$$ 

Here $\text{Aut}_E(V)$ is the group of $E$-automorphisms of $V$, that is to the group of isomorphisms of $V$ with itself that are defined over $E$ or, equivalently, the group of $E$-linear automorphisms of $A_E[V]$. This extension $E$ of $\text{Aut}_E(V)$ by the Galois group $G$ measures precisely how difficult it is to define $V$ over $F$. If one is interested in descending to $F$ some structure in addition to just that of an algebraic variety, one uses only automorphisms preserving the structure.

According to, every model of $V$ over $F$ that gives rise to $V$ over $E$ determines a splitting of this exact sequence.

**Theorem.** (André Weil) Every splitting of the short exact sequence gives rise to a model of $V$ defined over $F$.

In particular, if the sequence does not split then there are no models over $F$. The mechanism by which splittings give rise to a descent will be explained in the prelude to the next result.

Suppose we are given a splitting. This means we are given for each $\sigma$ a map $f_\sigma : V \to V^{\sigma}$, such that $f_\sigma^{\tau} f_\tau = f_{\sigma \tau}$ for each pair $\sigma, \tau$. The map $f_\sigma$ corresponds to a ring homomorphism $f_\sigma^* : A_E[V]$ to itself fitting into the diagram on the left:

$\begin{array}{ccc}
A_E[V] & \xrightarrow{f_\sigma^*} & A_E[V] \\
\downarrow_{\sigma^{-1}} & & \downarrow_{\sigma^{-1}} \\
E & \xrightarrow{\iota} & E
\end{array}$

But the diagram on the left is equivalent to that on the right, so the map $f_\sigma^*$ is one that induces $\sigma$ on the copy of $E$ in $A_E[V]$. Now I apply the following observation, which I leave as an exercise.

**Lemma.** If we identify the affine ring of $V^{\sigma}$ with that of $V$, but assigned a different $E$-structure, then $f^{\sigma}$ is just $f$ itself.
The assumption \( f_{\sigma^r} = f_r^* f_r \) therefore translates to the conditions (a) \( f_{\sigma^r}^* = f_r^* f_r^* \) and (b) \( f_r^* = \sigma \) on \( iE \). In other words we are given a homomorphism from \( G \) to the automorphisms of \( A_E[V] \) inducing Galois automorphisms on \( E \). I define the proposed affine ring of the variety defined over \( F \) to be the subring \( A^G \) of elements of \( A \) fixed by elements of \( G \). It certainly contains \( F \). The proof of the Theorem will be concluded if we prove this more precise formulation:

**7.5. Theorem.** Suppose we are given a homomorphism \( \sigma \mapsto \varphi_\sigma \) from the Galois group \( G(E/F) \) to \( \text{Aut}_E(V) \) such that \( \varphi_\sigma = \sigma \) on the image of \( E \). Then \( A^G \) is finitely generated, and the canonical map from \( E \otimes_F A^G \to A \) is an isomorphism.

The last claim follows immediately from . So it remains only to prove that \( A^G \) is a finitely generated ring.

Suppose \( x_i \) to be one of the generators of \( A \) and let \( N = |G| \). Then

\[
P(x) = \prod_{\sigma \in G} (x - x_i^{\sigma}) = \sum_{m=0}^N a_{i,m} x^m
\]

is a polynomial with coefficients in \( A^G \) such that \( P(x_i) = 0 \). If \( B \) is the ring generated by all the \( a_{i,m} \) then it is a Noetherian ring such that \( A \) is finitely generated as a module over \( B \). Hence \( A^G \), which contains \( B \), is also finitely generated over \( B \), and is also finitely generated as a ring.

Assuming that the Theorem has been proved, there remains one important question: In case of a splitting, how do we describe the \( F \)-rational points of \( V \)? The answer is relatively simple, but even so I want to say something that will motivate that answer. If \( V \) is defined over \( F \), then there exists an action of \( G \) on the \( E \)-rational points of \( V \). In terms of geometric points the Galois automorphism \( \sigma \) takes \( (x_i) \) to \( (x_i^\sigma) \). The \( E \)-rational points of \( V \) are the homomorphisms from \( A_F[V] \) to \( E \), and the Galois action is through its action on \( E \). Describing \( F \)-rational points of \( V \) therefore reduces to specifying the Galois action on the \( E \)-rational points corresponding to the descent.

**7.6. Proposition.** If \( (f_\sigma) \) is a set of descent data, then the corresponding Galois action of \( G \) on \( V \) takes \( x \) to \( f_{\sigma^{-1}}(x)^\sigma \).

If \( f \) is trivial this is just the old conjugation \( x \mapsto x^\sigma \). The point \( f_{\sigma^{-1}}(x) \) lies in \( V^{\sigma^{-1}} \), and if \( x \) lies in \( V^{\sigma^{-1}} \) then \( x^\sigma \) is in \( V \). Thus \( f_{\sigma^{-1}}(x)^\sigma \) lies in \( V \).

Another way of putting it is that the \( F \)-rational points on the descended variety are the \( E \)-rational points \( x \) of \( V \) such that \( f_\sigma(x) = x^\sigma \).

**Example.** Restriction of scalars. Suppose \( V \) to be a variety defined over the Galois extension \( E/F \). Let \( U = \prod G V^\sigma \). There is a canonical isomorphism of \( U \) with \( U^\sigma \), giving rise to the structure of a variety \( R_{E/F}U \) defined over \( F \). This is the same as what I called before the variety obtained by restriction of scalars from \( E \) to \( F \). I leave as an exercise to verify that there is a canonical bijection of the \( F \)-rational points of \( R_{E/F}U \) with the \( E \)-rational points of \( U \).

8. Classification of splittings

I now take up the second question asked above. Suppose we are given a variety \( V \) defined over \( F \) and a Galois extension \( E/F \). How to classify, up to isomorphism, all the varieties defined over \( F \) that become isomorphic to \( V \) over \( E \)?

The answer is very simple.

**8.1. Theorem.** Suppose \( E/F \) to be a finite Galois extension. If \( V \) is an affine variety defined over \( E \), then two descents defined by splittings of the short exact sequence \( \frac{\text{if} \text{and only if}}{\text{if} \text{and only if}} \) they are conjugate by an element of \( \text{Aut}_E(V) \).
Proof. One way is entirely straightforward. On the other hand, suppose we are given two homomorphisms \( \varphi, \psi \) from \( \text{Gal}(E/F) \) to the group of automorphisms of \( A_E[V] \) compatible with the Galois action on \( E \), and an automorphism \( \alpha \) of \( A_E[V] \) such that

\[
\alpha \varphi \sigma \alpha^{-1} = \psi \sigma
\]

for all \( \sigma \) in \( \text{Gal}(E/F) \). Then \( \alpha \) also takes one corresponding subring of invariants to the other, and is hence an isomorphism of the two varieties over \( F \).

This is usually phrased in terms of Galois cohomology. Suppose \( U \) to be a variety defined over \( F \), isomorphic to \( V \) over \( E \). Let

\[
\varphi: U \rightarrow V
\]

be an isomorphism defined over \( E \). Set

\[
f_\sigma = \varphi^\sigma \varphi^{-1},
\]

which lies in \( \text{Aut}_E(V) \). It satisfies the condition

\[
(8.2) f_{\sigma \tau} = f_\sigma f_\tau.
\]

Conversely, suppose that we are given a map \( \sigma \mapsto f_\sigma \) satisfying \( f_\sigma f_\tau = f_{\sigma \tau} \). It tells us we can define by these data a variety \( U \) defined over \( F \) and isomorphic to \( V \) over \( E \).

They will be isomorphic over \( F \) only if we can change \( \varphi \) to \( \alpha^{-1} \varphi \) with \( \alpha \) in \( \text{Aut}_E(V) \) such that \( \psi^{-1} \alpha^{-1} \varphi \) is defined over \( F \), or equivalently

\[
(\psi^{-1} \alpha^{-1} \varphi)^\sigma = \psi^{-1} \alpha^{-1} \varphi
\]

for all \( \sigma \). This condition translates to

\[
\varphi^\sigma \varphi^{-1} = \alpha^\sigma \psi^\sigma \psi^{-1} \alpha^{-1}.
\]

I have therefore proved:

8.3. Theorem. Suppose \( V \) to be an affine variety defined over \( F \), \( E/F \) finite and Galois. Isomorphism classes of affine varieties defined over \( F \) that become isomorphic to \( V \) over the Galois extension \( E/F \) are in bijection with \( H^1(\text{Gal}(E/F), \text{Aut}_E(V)) \).

The difference between this and the previous formulation is that \( V/F \) determines a base-point.

Given the cocycle \( f_\sigma \), it tells us that the new Galois action on points is

\[
x \mapsto f_\sigma^{-1}(x) \sigma.
\]

where \( x \mapsto x^\sigma \) is the conjugation on points of the original \( F \)-variety \( V \). For example, suppose \( V \) to be the algebraic group \( \mathbb{G}_m \) defined over \( \mathbb{R} \). Let \( \sigma \) be complex conjugation, and \( f_\sigma(x) = 1/x \). Then the \( \mathbb{R} \)-rational points on the variety defined by \( f_\sigma \) are the points of \( \mathbb{C}^\times \) such that \( \overline{z} = 1/z \).

One advantage of identifying descents with a cohomology set is that one then has conveniently at hand the long exact sequence of cohomology arising from short exact sequences of (possibly non-commutative) Galois modules.

9. References


   http://www.jmilne.org/math/CourseNotes/ag.html


