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, mainly reductive 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.

Although my original motivation for this essay was to understand the classification and structure of reductive groups, I deal with this topic elsewhere.

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

Contents

NOTATION. Following [Springer:1966], I take the action of a Galois group to be on the left, and in a superscript: $x \mapsto {}^{\sigma}x$. Thus ${}^{\sigma\tau}x = {}^{\sigma}({}^{\tau}x)$.

If g and h are in the same group, then

$$ {}^{g}h = ghg^{-1}, \quad h^{g} = g^{-1}hg\,. $$

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 axis. This algebraic variety is an algebraic group, with multiplication defined coordinate-wise:

$$ (x_1, y_1) \cdot (x_2, y_2) = (x_1x_2, y_1y_2)\ . $$

On the other hand, 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:

$$ (x_1, y_1) \cdot (x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1)\ . $$

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:

$$\begin{aligned} u &= x + iy \\ v &= x - iy \\ x &= (u + v)/2 \\ y &= (u - v)/2i \ . \end{aligned}$$

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, which is what I hope to explain in this note and a sequel specifically about algebraic groups.

More precisely, 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 and describing reductive groups over arbitrary fields although, as I have already mentioned, in the present version I do not say much about these problems.

The algebraic varieties above are *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 terminology in algebraic geometry, now obsolete. The current standard reference is §V.4 of [Serre:1959]. [Milne:2009] is a somewhat different account of much of the same material.

2. Galois conjugation on vector spaces

If U is a vector space over the field F and E/F is a finite Galois extension, define for each σ in $\mathcal{G} = \mathcal{G}(E/F)$ the F-linear automorphism of the space $E \otimes_F U$:

$$\sigma \otimes I\colon\ e \otimes u \longmapsto {}^{\sigma}e \otimes u \tag{2.1}$$

Using a basis of U, and knowing that $E^{\mathcal{G}} = F$, one sees that the subspace of fixed points of all these is U itself. This section is concerned with the converse problem: *given a vector space V over E, how to classify all F-subspaces U of V such that $E \otimes_F U = V$?*

If V is a vector space over E, and σ in $\mathcal{G}$, a σ-linear automorphism of V is an F-linear automorphism φ such that

$$\varphi(ev) = {}^{\sigma}e\,\varphi(v)\,.$$

for all e in E, v in V. A **$\mathcal{G}$-conjugation** is a homomorphism $\sigma \mapsto \varphi_\sigma$ from $\mathcal{G}$ to $\mathrm{Aut}_F(V)$ for which each φ_σ is σ-linear. The maps in (2.1) define such a homomorphism.

Given a $\mathcal{G}$-conjugation φ on V, let

$$V^{\varphi} = \{v \in V \mid \varphi_\sigma(v) = v \text{ for all } \sigma \in \mathcal{G}\}\,.$$

For example, a basis of V over E gives rise to a splitting φ with V^{φ} equal to the F-space spanned by the basis. Here is the basic result of Galois descent:

2.2. Theorem. *Let E be a finite Galois extension of F, and suppose V to be a vector space over E. The map taking φ to V^{φ} is a bijection between $\mathcal{G}$-conjugations of V and subspaces U such that the canonical map from $E \otimes_F U$ to V is an isomorphism.*

In this case, the conjugation $\sigma \otimes I$ on $E \otimes U$ is identified with φ_σ.

Proof. The only troublesome point is to show that $E \otimes_F V^{\varphi} = V$. The proof of this will occupy the much of the rest of this section, and will involve 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 a basic theorem of Galois theory.

LINEAR INDEPENDENCE. The following is one of the basic tools in Galois theory.

2.3. Lemma. *The Galois transformations of E are linearly independent over E.*

This is a well known result from Galois theory, but I'll sketch a proof here. Suppose

$$\sum\nolimits_{\sigma\in\mathcal{G}} c_\sigma \sigma = 0\,.$$

For each σ in $\mathcal{G}$ the map taking e to $\sigma(e)$ is multiplicative. So the result follows from this well known proposition:

2.4. Lemma. *If G is a group and E a field, any set of distinct homomorphisms*

$$\chi\colon\ G \longrightarrow E^\times$$

are linearly independent over E.

Proof. I'll prove by induction on n that if

$$\sum_{\chi} c_i\chi_i = 0$$

with n coefficients c_i then all the c_i vanish. For $n = 1$ this is immediate, since the values of the characters are non-zero.

Suppose this to be true for $m < n$ and suppose such a relation

$$\sum_{i=1}^{n} c_i\chi_i = 0 \tag{2.5}$$

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

$$\begin{aligned} 0 &= \sum_{i=1}^{n-1} c_i\chi_i(x)\chi_i(g) + \chi_n(x)\chi_n(g) \\ &= \sum_{i=1}^{n-1} \chi_n(g)^{-1}\chi_i(g)c_i\chi_i(x) + \chi_n(x) \end{aligned}$$

and subtracting this from the original equation (2.5) we get

$$\sum_{i=1}^{n-1} c_i\big(\chi_n(g)^{-1}\chi_i(g) - 1\big)\chi_i(x)$$

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 $c_n = 0$. ∎

CROSS PRODUCTS. The **cross product** $E \odot_F \mathcal{G}$ is the vector space $E \otimes_F F[\mathcal{G}]$, made into a ring with product

$$(e \otimes \sigma)\cdot(f \otimes \tau) = e\,{}^\sigma f \otimes \sigma\tau\,.$$

Its multiplicative identity is $1 \otimes I$.

The following explains the reason for introducing cross products. The proofis immediate:

2.6. Lemma. *Suppose $\sigma \mapsto \varphi_\sigma$ to be a homomorphism from $\mathcal{G}$ to $\mathrm{Aut}_F(V)$. It is conjugation-compatible if and only if*

$$(e \otimes \sigma)\colon v \longmapsto e\varphi_\sigma(v)$$

defines V as a module over $E \odot_F \mathcal{G}$.

As a particular case of Lemma 2.6, the Galois action on E makes E into a module over $E \odot_F \mathcal{G}$. We obtain therefore a ring homomorphism

$$E \odot_F \mathcal{G} \longrightarrow \mathrm{End}_F(E)\,.$$

2.7. Lemma. *This map is an isomorphism.*

Proof. Lemma 2.3 implies that the associated ring homomorphism into $\mathrm{End}_F(E)$ is injective. Since dimensions agree, it is an isomorphism. ∎

Remarks. The isomorphism of $E \odot_F \mathcal{G}$ with $\mathrm{End}_F(E)$ is a special case of a more general construction of central simple algebras over F, as we shall see in a later section.

∘ ———— ∘

Now for a last step. Say $[E\colon F] = n$. The vector space V is a module over $E \odot_F \mathcal{G}$, hence by the previous remark over $M = M_n(F)$, and with this isomorphism goes one of E with F^n.

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

Proof. There is a canonical map from $U \otimes_F \widehat{U}$ to M, taking $u \otimes \widehat{u}$ to the linear transformation

$$v \longmapsto \langle \widehat{u}, v\rangle u\,.$$

It is a bijection, and therefore

$$V = \mathrm{Hom}_M(M, V) = \mathrm{Hom}_M(U \otimes_F \widehat{U}, V) = U \otimes_F \mathrm{Hom}_M(U, V)$$

for trivial reasons. ∎

Now to conclude the proof of the Theorem. In our case $U = E$ as a module over $E \odot_F \mathcal{G} \cong \mathrm{End}_F(E)$. If f is in $\mathrm{Hom}_F(E, V)$ then it is in $\mathrm{Hom}_{E\odot_F\mathcal{G}}(E, V)$ if and only if

$$f(e^\sigma x) = e\varphi_\sigma(f(x))$$

for all e, x in E. This happens if and only if $\varphi_\sigma(f(1)) = f(1)$ and therefore

$$\mathrm{Hom}_{E\times\mathcal{G}}(E, V) = V^\varphi\,.$$

This concludes the proof of Theorem 2.2. ∎

Later on, we shall be interested in applying Theorem 2.2 to vector spaces with added structure. In that case, $\mathrm{GL}_E(V)$ will be replaced by a group $\mathrm{Aut}_E(V)$ of automorphisms preserving structure.

DESCENT AND EXTENSIONS. There is one way to characterize Galois conjugations that will be useful later on. Let $\mathcal{E}$ be the set of all g in $\mathrm{Aut}_F(V)$ that are σ-linear for some $\sigma = \sigma(g)$ in $\mathcal{G}$. It is a group with a canonical projection to $\mathcal{G}$. If (v_i) is a basis of V over E, then the map

$$\sum x_i v_i \longmapsto \sum {}^\sigma x_i v_i$$

is in $\mathcal{E}$, so this projection is surjective, and the sequence

$$1 \longrightarrow \mathrm{GL}_E(V) \longrightarrow \mathcal{E} \longrightarrow \mathcal{G} \longrightarrow 1$$

is exact. The following is just a matter of definition.

2.9. Lemma. *A $\mathcal{G}$-conjugation on V is equivalent to a splitting of this exact sequence.*

3. Extensions and cohomology

In this section I'll recall what we'll need to know later about cohomology groups $H^\bullet(G, A)$ in low degree, where G is a group and the group A—possibly non-abelian—is one on which G acts through a homomorphism to $\mathrm{Aut}(A)$. My principal reference has been [Maclane:1963].

ZERO-COHOMOLOGY. If A is any group on which G acts, the group $H^0(G, A)$ is the subgroup of a in A such that $a = a^\sigma$ for all σ in G. A G-equivariant map from A to B gives rise to a canonical map from $H^0(G, A)$ to $H^0(G, B)$. A short exact sequence

$$1 \longmapsto A \longmapsto B \longmapsto C \longmapsto 1$$

thus gives rise to an exact sequence

(3.1)
$$1 \longmapsto H^0(G, A) \longmapsto H^0(G, B) \longmapsto H^0(G, C)$$

of groups. The last map is not necessarily surjective, but the disparity can be measured., as we shall see shortly.

ONE-COHOMOLOGY. Suppose given a short exact sequence

$$1 \longrightarrow A \longrightarrow \mathcal{E} \longrightarrow G \longrightarrow 1$$

in which G is a finite group. At first I do not make any further assumption on the extension. Given g in G, choose s_g in $\mathcal{E}$ projecting onto it. The map

$$x \longmapsto s_g x s_g^{-1}$$

is an automorphism of A, which in general will depend on the particular lift s_g. Any other choice projecting onto g will be of the form as_g, and conjugation by it will differ from the original one by an inner automorphism of A. We therefore get a canonical homomorphism from G to the group $\mathrm{Out}(A) = \mathrm{Aut}(A)/\mathrm{Int}(A)$ of outer automorphisms of A, which is called the **kernel** of the extension. These do not necessarily lift to automorphisms of A, unless we make some further assumption. One possible assumption is that A be abelian. We shall look at this case in a later section.

Another interesting assumption is that the extension splits, which means that there is a homomorphism from $\mathcal{G}$ back to $\mathcal{E}$. Any choice of splitting s gives rise to a conjugation action of G on A, $a \mapsto {}^g a$, where ${}^g a = s_g a s_g^{-1}$. It is important to realize that this may well vary with the particular splitting. A splitting gives a bijection from $A \times G$ to $\mathcal{E}$, $(a, g) \mapsto as_g$. This is an isomorphism of $\mathcal{E}$ with the semidirect product $A \rtimes G$, made up of pairs (a, g) and multiplication

$$(a, g)(b, h) = (a\,{}^g b, gh)\,.$$

There will in general be many splittings. If we are given one, 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 $H^1(G, A)$ solves is to a classify equivalence classes of splittings.*

Fix one splitting, so we may identify $\mathcal{E}$ with $A \rtimes G$, in which $s_g = (1, g)$. 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 (a_g, g). The following is straightforward:

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

$$a_{gh} = a_g\,{}^g a_h$$

for all g, h in G.

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

Suppose we are given splitting defined by the cocycle (a_g). Since

$$(b, 1)(a_g, g)(b^{-1}, 1) = (b a_g\,{}^g b^{-1}, g)\,,$$

the conjugated splitting is defined by the cocycle

(3.3) $$b a_g {}^g b^{-1} .$$

which is said to be **cohomologous** to the original one. I define $H^1(G, A)$ 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 $b\,{}^g b^{-1}$.

Remark. In one common convention, the sections are of the form σb_σ rather $a_\sigma \sigma$. The functions b_σ satisfy the condition

$$b_{\sigma\tau} = b_\sigma^\tau b_\tau .$$

The formula $b_\sigma = a_\sigma^\sigma$ translates between the two conventions.

∘ ———— ∘

In partial summary:

3.4. Proposition. *The map taking a_g in $Z^1(G, A)$ to the corresponding splitting of $A \rtimes G$ 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 the existence of long exact sequences. Suppose given

$$1 \longmapsto A \longmapsto B \longmapsto C \longmapsto 1 .$$

A G-equivariant map from X to Y gives to one from $H^1(G, X)$ to $H^1(G, Y)$. In addition, suppose given c in $H^0(G, C)$. Choose b in B with image c. Then for each g in G, $a_g = b^g b^{-1}$ lies in A, and (a_g) defines a cocycle in $Z^1(G, A)$. In this way we get a connecting map from $H^0(G, C)$ to $H^1(G, A)$.

3.5. Proposition. *A short exact sequence*

$$1 \longmapsto A \longmapsto B \longmapsto C \longmapsto 1$$

of groups on which G acts compatibly gives rise to an exact sequence

$$H^0(G, B) \longmapsto H^0(G, C) \longmapsto H^1(G, A) \longmapsto H^1(G, B) \longmapsto H^1(G, C)$$

of pointed sets.

Proof. Left as exercise. ∎

This means, for example, that the subset of $H^0(G, C)$ that maps to the distinguished element of $H^1(G, A)$ is the image of $H^0(G, B)$. It answers a question raised by (3.1) , but raises a new one: can we measure how far the right hand map is from being surjective?

Example. I'll give here a variant of the well known Hilbert's Theorem 90. The following is a basic result in the cohomology of Galois groups. We'll see later why one could have predicted it.

3.6. Proposition. *Suppose E/F to be a Galois extension with group $\mathcal{G}$. Then $H^1(\mathcal{G}, \mathrm{GL}_n(E)) = \{1\}$.*

Proof. Every element $\gamma = (g, \sigma)$ in the semi-direct product corresponds to a linear transformation in $\mathrm{Aut}_F(V)$:

$$\pi_\gamma \colon\ x \longmapsto g \cdot {}^\sigma x ,$$

is a σ-linear map from E^n to itself. Here v is expressed as a column vector. A 1-cocycle (g_σ), which amounts a splitting of the semi-direct product, therefore gives rise to a Galois-compatible homomorphism π from $\mathcal{G}$ to $\mathrm{Aut}_F(V)$. We may therefore apply Theorem 2.2 to deduce that if U is the space of all v in E^n such that $\pi_\sigma(v) = v$ for all σ in $\mathcal{G}$, then U is an F-vector space such that $E^n = U \otimes_F E$.

Let (u_i) be an F-basis of U, expressed as a matrix u of column vectors with coordinates in E. Then u is fixed by each (g_σ, σ), so

$$g_\sigma \cdot {}^\sigma u = u, \quad g_\sigma = u \cdot {}^\sigma u^{-1} .$$ ∎

This is all really just a rephrasing of the of elementary fact that if U and W are any two F-subspaces of V such that $E \otimes_F U = E \otimes_F W = V$, then there exists g in $\mathrm{GL}_E(V)$ taking U to W.

∘ ———— ∘

TWO-COHOMOLOGY. Suppose now A to be abelian, and again consider a short exact sequence

$$1 \longrightarrow A \longrightarrow \mathcal{E} \longrightarrow G \longrightarrow 1\,.$$

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

$$s_g s_h = a_{g,h} s_{gh}$$

for some unique $a_{g,h}$ in A. Associativity imposes a condition on the factors $a_{g,h}$. Since

$$\begin{aligned}
(s_g\, s_h) s_k &= a_{g,h}\, s_{gh} s_k \\
&= a_{g,h} a_{gh,k}\, s_{ghk} \\
s_g (\, s_h\, s_k) &= s_g a_{h,k} s_{hk} \\
&= s_g a_{h,k} s_g^{-1} \cdot s_g s_{hk} \\
&= s_g a_{h,k} s_g^{-1}\, a_{g,hk} \cdot s_{ghk} \\
&= {}^g a_{h,k}\, a_{g,hk} \cdot s_{ghk}\,,
\end{aligned}$$

we deduce the identity

(3.7) $$a_{g,h} a_{gh,k} = {}^g a_{h,k}\, a_{g,hk}\,.$$

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 $b_g\, s_g$. Then

$$\begin{aligned}
b_g s_g \cdot b_h s_h &= b_g {}^g b_h s_g s_h \\
&= b_g {}^g b_h a g, h s_{gh} \\
&= b_g {}^g b_h a g, h b_{gh}^{-1} \cdot b_{gh} s_{gh}\,.
\end{aligned}$$

The cocycles $a_{g,h}$ and 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

$$b_g {}^g b_h b_{gh}^{-1}$$

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.

3.8. Proposition. *The map from extensions to $Z^2(G,A)$ 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

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

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

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

3.9. Proposition. *Suppose given the short exact sequence of G-groups*

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

with A in the centre of B. The corresponding sequence

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

is an exact sequence of pointed sets.

It would be instructive to see this interpreted in terms of extensions of A by G.

Remark. We'll see later how H^2 classifies central simple algebras over F.

[Maclane:1963] and [Springer:1966] define sets $H^2(G,A)$ when A is not necessarily abelian, in terms of the kernel $G \to \mathrm{Out}(A)$. [Borovoi:1993] shows how useful this construction is.

THREE-COHOMOLOGY. MacLane applies H^3 in certain cases as an obstruction to the existence of an extension with a given kernel.

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.

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

Here are some examples:

$\diamond$ 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^2V.

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

$\diamond$ 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.

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.*

$\diamond$ 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 $V_E = E \otimes_F V$ (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 α of $\mathrm{GL}(V_E)$ such that $\alpha(S) = T$. But since S and T are both F-rational, this implies that ${}^\sigma\alpha$ will also take S to T, and then

$f_\sigma = \alpha^\sigma \alpha^{-1}$ will lie in $\mathrm{Aut}_E(T)$. The map $\sigma \mapsto f_\sigma$ will be a cocycle. The map taking S to this cocycle is a map from structures S to $Z^1(\mathcal{G}, \mathrm{Aut}_E)$.

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

Proof. The only slightly tricky point is surjectivity. If given a cocycle f_σ in $\mathrm{Aut}_E(T)$, according to Proposition 3.6 there exists α in $\mathrm{GL}_E(V)$ with $\alpha^\sigma \alpha^{-1} = f_\sigma$. Then $S = \alpha^{-1}T$ is fixed by the Galois action, hence F-rational.

⋄ The group GL_n is the automorphism group of vector spaces. Therefore $H^1(\mathcal{G}, \mathrm{GL}_n(E))$ 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 Proposition 3.6.

⋄ Symplectic structures on a vector space are unique, so this tells us that $H^1(\mathcal{G}, \mathrm{Sp}(V)) = \{1\}$.

⋄ But if Q is a non-degenerate quadratic form on E^n, then $H^1(\mathcal{G}, O(Q))$ classifies quadratic forms on F^n that become isomorphic to Q over E. It is not generally trivial.

⋄ As I have already remarked, if A is abelian then any extension of A by a group G gives rise to a unique action of G on A. How can we classify extensions like this

$$1 \longrightarrow \mathbb{C}^\times \longrightarrow \mathcal{E} \longrightarrow \mathcal{G}(\mathbb{C}/\mathbb{R}) \longrightarrow 1 \tag{4.2}$$

in which $\mathcal{G}$ acts by conjugation? The extension is completely determined by a single element σ whose image is conjugation $z \mapsto \overline{z}$. Its square $\alpha = \sigma^2$ will lie in $\mathbb{C}^\times$. Since

$$\begin{aligned} \sigma(\sigma\sigma) &= \sigma\alpha \\ &= \overline{\alpha}\sigma \\ &= (\sigma\sigma)\sigma \\ &= \alpha\sigma\,, \end{aligned}$$

we deduce that α lies in $\mathbb{R}^\times$. Conversely, any choice of α in $\mathbb{R}^\times$ will determine an extension.

4.3. Lemma. *Up to isomorphism, there are two extensions like (4.2) , depending on whether α^2 is positive or negative.*

In other words, $H^2(\mathcal{G}, \mathbb{C}^\times)$ hs two elements.

Proof. Conjugation of σ by z changes α to $z\overline{z}\alpha$.

The extension determines an algebra over $\mathbb{R}$ of dimension 4 whose center is $\mathbb{R}$. It contains a copy of $\mathbb{C}$ and an $\mathbb{C}$-basis $1, \varepsilon$ such that

$$\varepsilon z = \overline{z}\varepsilon,\ \varepsilon^2 = \alpha\,.$$

If $\alpha = 1$, we recover the algebra $\mathbb{C} \odot_F \mathcal{G}$ which, as we have seen, is isomorphic to $M_2(\mathbb{R})$. Otherwise, we recover the Hamiltonian quaternions $\mathbb{H}$.

In general, a central simple algebra over F is one that becomes $M_n(E)$ over some Galois extension E/F. They are classified by $H^1(\mathcal{G}(E/F), \mathrm{PGL}_n(E))$, and also constructed explicitly by using cocycles in $Z^2(\mathcal{G}(E/F), E^\times)$ derived from the connecting map $H^1 \to H^2$.

5. 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 coordinates in $\mathbb{R}$, but it would not be wise to think that it is trivial as an algebraic variety. The same equation specifies points also in $\mathbb{C}$, and there are lots of (x, y) 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 $P(x_1, \ldots, x_n)$ in $F[x]$ to the points in $\overline{F}^n$ satisfying these equations.*

There are a number 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 $\overline{F}^n$. 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 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 a constructive version is formulated. 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 $\overline{F}^n$ 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 Nullstellenatz tells us that this does *not* happen if F is algebraically closed:

5.1. 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 σ an automorphism of F the conjugate ${}^\sigma V$ will be the affine variety determined by the ideal ${}^\sigma I$. It will contain, for example, all the points ${}^\sigma x$ as x ranges over the zero set of I in F^n. The affine ring of ${}^\sigma V$ is the quotient $F[x]/{}^\sigma I$. It is isomorphic to $F[x]/I$, since $P \mapsto {}^\sigma P$ is an isomorphism. But the two varieties V and ${}^\sigma V$ are generally distinct. What goes wrong is that an embedding of a variety into F^n embeds F into the ring of functions on the variety. The isomorphism $P \mapsto {}^\sigma P$ is not compatible with that embedding. *It is necessary to take into account not only the isomorphism class of the ring $A_F[V]$, but also the embedding $\iota = \iota_V$ of F into $A_F[V]$ that makes it into an F-algebra.* Different embeddings may in fact correspond to non-isomorphic algebraic varieties.

In this essay, therefore:

> **Definition.** *An* **affine algebraic variety** *defined over the field F is a pair (A, ι) where A is a ring and $\iota\colon F \hookrightarrow A$ an embedding, such that (a) A is finitely generated over the image of F and (b) A is reduced.*
>
> *Two algebraic varieties (A_1, ι_1) and (A_2, ι_2) are isomorphic when there exists an isomorphism $\varphi\colon A_1 \to A_2$ 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 A_n over F, with affine rings $F[x] = F[x_1, \ldots, x_n]$. If $A_F[V]$ is generated by n variables, then V may be embedded into A_n.

This definition is due to Chevalley, although it was extended greatly by 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 see this, certain natural questions must be answered.

• *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, in two statements—(1) 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 $F[x]/\sqrt{I}$; (2) 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_F 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 ε_x from $A_F[V]$ to E, taking P to $P(x)$, compatible with the embedding of F into E. Conversely, any such homomorphism ε determines the point $\big(\varepsilon(x_i)\big)$ 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_F, ι), rational over the field E containing F, is a homomorphism from A_F 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, 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, the image of the corresponding homomorphism ε will be a finite algebraic

extension of F. Its kernel $\mathrm{Ker}(\varepsilon)$ will be a maximal ideal of $A_F[V]$. This suggests a second answer to the question:

> *A point of the variety V determined by the affine ring (A_F, ι), rational over the field extension E/F, is a maximal ideal $\mathfrak{m}$ of A_F.*

There is something to be proven, namely that if $\mathfrak{m}$ is a maximal ideal of $A_F[V]$ then $A_F[V]/\mathfrak{m}$ 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 $\varphi\colon U \to V$ is an algebraic map of algebraic varieties and f is in the affine ring of V, then the pull-back $f\circ\varphi$ is an affine function on U. This induces a ring homomorphism φ^* from $A_F[V]$ to $A_F[U]$ compatible with the embeddings of F. Indeed, as a matter of definition an algebraic map φ from U to V is neither more nor less than such a homomorphism:

$$\begin{array}{ccc} A_F[V] & \xrightarrow{\varphi^*} & A_F[U] \\ & {\scriptstyle\iota_V}\nwarrow \quad \nearrow{\scriptstyle\iota_U} & \\ & F & \end{array}$$

Such a homomorphism determines, for example, an associated map from points of U to points of V, since if we are given $\varepsilon\colon A_F[U] \to E$ then $\varepsilon\circ\varphi^*$ is an E-rational point of V. *It is important to realize that an 'algebraic map' from one variety to another is defined by its formula, not its action on E-valued points. There might be none!*

Of course

$$(\varphi\psi)^* = \psi^*\varphi^* .$$

• *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. If $F = \mathbb{C}$, this means that the variety is topologically connected.

• *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 $A[U \times V]$.

• *Tangent vectors.* If φ is a ring homomorphism from $A_F[V]$ to the 'dual ring' $F[\varepsilon]/(\varepsilon^2)$, the coefficient of ε is a derivation. Such homomorphisms parametrize points x of V together with a tangent vector at x.

• *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 $\mathbb{R}$:

$$\begin{aligned} ux - vy &= 1 \\ vx + uy &= 0 . \end{aligned}$$

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.

• *What is the conjugate of a variety?* Suppose E/F to be a finite Galois extension with group $\mathcal{G}$. Suppose V to be defined by equations $P_i = 0$, where the P_i have coefficients in E. If $\sigma\colon x \longmapsto {}^\sigma x$ is the automorphism of E^n induced by one of E/F, the **σ-conjugate** ${}^\sigma V$ is that defined by the polynomials ${}^\sigma P_i$ whose coefficients are the σ-conjugates of the coefficients of the P_i. The Galois group also acts on points in E^n by conjugating coordinates. Since ${}^\sigma P({}^\sigma x) = {}^\sigma(P(x))$, the E-rational points on ${}^\sigma V$ are the ${}^\sigma x$ with x an E-rational point of V.

If the coordinate ring of V is $A_E[V] = E[x]/I$ then the coordinate ring $A_E[{}^\sigma V]$ of its conjugate is $E[x]/{}^\sigma I$. For both, the embedding ι of E is the restriction of the canonical one into $E[x]$. The map taking P to ${}^\sigma P$ from $A_E[V]$ to $A_E[{}^\sigma V]$ is an isomorphism of the two rings, but *the two varieties may very well be distinct, because the isomorphism is not compatible with the corresponding embeddings of E.* Instead:

5.2. Proposition. *If σ is an automorphism of E then the map taking P to ${}^\sigma P$ is an isomorphism of $(A_E[V], \iota\circ\sigma^{-1})$ with $(A_E[{}^\sigma V], \iota)$.*

Proof. Because the following diagram is commutative:

$$\begin{array}{ccc} E[x]/I & \xrightarrow{\sigma} & E[x]/I^\sigma \\ \uparrow{\scriptstyle \iota\cdot\sigma^{-1}} & & \uparrow{\scriptstyle \iota} \\ E & \xrightarrow{I} & E \end{array}$$

We therefore have a definition of the conjugate variety independent of an embedding into some E^n.

• *What is the Galois action on points?* If E/F is a Galois extension with Galois group $\mathcal{G}$, V is embedded in affine space, and $x = (x_i)$ is a point on V with coordinates in E, then the conjugate ${}^\sigma x$ by σ in $\mathcal{G}$ is the point $({}^\sigma x_i)$, which is a point of ${}^\sigma V$. How do we translate this operation in terms of the intrinsic definition of points? An E-rational point of V is a homomorphism ε from A_E making the left hand diagram below commutative.

$$\begin{array}{ccc} A_E[V] & \xrightarrow{\varepsilon} & E \\ & {\scriptstyle\iota}\nwarrow \quad \nearrow & \\ & E & \end{array} \qquad\qquad \begin{array}{ccc} A_E[V] & \xrightarrow{\sigma\cdot\varepsilon} & E \\ & {\scriptstyle\iota\cdot\sigma^{-1}}\nwarrow \quad \nearrow & \\ & E & \end{array}$$

The right hand one is an E-rational point of ${}^\sigma V$. So if ε is an E-rational point of V, its conjugate is $\sigma\circ\varepsilon$. If x corresponds to the maximal ideal $\mathfrak{m}$, ${}^\sigma x$ corresponds to the same maximal ideal, but the embedding of F is different.

• *What is the conjugate of a map?* 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 $f\colon U \to V$ is an algebraic map between two algebraic E-varieties, composition with f is an E-map and a ring homomorphism from $A[V]$ to $A[U]$. The map is uniquely determined by this homomorphism.

5.3. Proposition. *If φ is an algebraic map from U to V, then $({}^\sigma\varphi)^* = \varphi^*$.*

In other words, the map of affine rings is the same, but with twisted embeddings of E:

$$\begin{array}{ccc} A_E[V] & \xrightarrow{\varphi^*} & A_E[U] \\ \uparrow{\scriptstyle \iota\cdot\sigma^{-1}} & & \uparrow{\scriptstyle \iota\cdot\sigma^{-1}} \\ E & \xrightarrow{I} & E \end{array}$$

Equivalently, it is the map determined by the graph conjugate. Explicitly:

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

6. Descending fields of definition

An affine variety defined over F, say with affine ring A_F, determines one over any extension field E of F. Its affine ring is

$$A_E = E \otimes_F A_F\,,$$

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? When can one* **descend** *the field of definition? In how many different ways? What can we say about the structure of a descent?*

DESCENT AND EXTENSIONS. Suppose E/F to be a finite Galois extension with group $\mathcal{G}$. If V is defined over F by the ideal I then ${}^\sigma I = I$, and V is may be identified with any of its $\mathcal{G}$-conjugates. Thus in order for a variety V over E to arise from one over F, it is necessary that it be isomorphic to each of its conjugates ${}^\sigma V$. But—as shown by counterexamples in [Mestre:1991]—this is not a sufficient condition. What is required is some coherence of the isomorphisms.

Suppose V to be defined over F with $A_F = A_F[V]$. Then $A_E = A_E[V] = E \otimes_F A_F$ is its affine ring over E, with canonical embedding of E. For each σ in $\mathcal{G}$, $\Phi_\sigma = \sigma \otimes I$ is a ring automorphism of A_E such that $\Phi_\sigma(e) = {}^\sigma e$. Furthermore, A_F is the subring A_E^Φ of A_E whose elements are fixed by all Φ_σ.

Conversely, suppose V to be an arbitrary variety defined over E. For each σ in $\mathcal{G}$, let $\mathcal{E}_\sigma$ be the set of all ring automorphisms Φ of $A_E[V]$ such that $\Phi = \sigma$ on E. As I might have observed earlier, the map $f \mapsto (f^*)^{-1}$ is an isomorphism of $\mathrm{Aut}_E(V)$ with $\mathcal{E}_I$.

It might happen that $\mathcal{E}_\sigma$ is empty, but there is a simple criterion that this does not happen. Reformulating Proposition 5.2 slightly, we see that an isomorphism $\varphi\colon V \to {}^\sigma V$ is equivalent to a ring automorphism φ^* making the following diagram commutative, and hence lying in $\mathcal{E}_\sigma$:

$$\begin{array}{ccc} A_E[V] & \xrightarrow{\varphi^*} & A_E[V] \\ {\scriptstyle\iota}\uparrow & & \uparrow{\scriptstyle\iota} \\ E & \xrightarrow{\sigma} & E \end{array}$$

In fact, elements of $\mathcal{E}_\sigma$ are in bijection with isomorphisms of V with ${}^\sigma V$. If I assume that V be isomorphic to ${}^\sigma V$ for all σ, the sequence

$$1 \longrightarrow \mathrm{Aut}_E(V) \longrightarrow \mathcal{E} \longrightarrow \mathcal{G} \longrightarrow 1\,. \tag{6.1}$$

is exact.

A splitting of this sequence amounts to a map $\sigma \mapsto \Phi_\sigma$ from $\mathcal{G}$ to $\mathrm{Aut}_F(A_E(V))$ such that
(a) $\Phi_\sigma(e) = {}^\sigma e$;
(b) $\Phi_{\sigma\tau} = \Phi_\sigma \Phi_\tau$.

I'll call such a map a **descent datum** for V. Given a descent datum Φ, the subring $A_E[V]^\Phi$ is that of all elements in $A_E[V]$ fixed by each Φ_σ. Theorem 2.2 tells us that such subrings are precisely those subrings A_F such that $A_E[V] = E \otimes_F A_F$.

6.2. Lemma. *Given a descent datum Φ, the subring $A_E[V]^\Phi$ is finitely generated over F.*

Proof. Suppose x_i to be one of the generators of $A_E(V)$ and let $N = |\mathcal{G}|$. Then

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

is a polynomial with coefficients in $A^\mathcal{G}$ 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 $A^\mathcal{G}$, which contains B, is also finitely generated over B, and is also finitely generated as a ring.

The ring $A_E[V]^\Phi$ is therefore the affine ring of an algebraic variety defined over F. This proves half of the following, and the remaining half is straightforward:

6.3. Proposition. *The map taking a descent datum Φ to the subring $A_E[V]^\Phi$ is a bijection between descent data and affine varieties over F isomorphic to V over E. Two descent data give rise to isomorphic varieties over F if and only if they are conjugate by an automorphism in $\mathrm{Aut}_E(V)$.*

DESCENT AND COHOMOLOGY. Suppose now that we are given a Galois extension E/F and a variety V defined over E, as well as descent data (Φ_σ) of the variety V to F. The space $A_E[V]^\Phi$ is the same as $A_F[V]$. Conjugation by the automorphisms Φ_σ defines an action of $\mathcal{G}$ on $\mathrm{Aut}_E(V)$.

How can we classify all of the varieties defined over F that are isomorphic to V over E?

Each one will be defined by a descent datum $(g_\sigma\Phi_\sigma)$ with g_σ in $\mathrm{Aut}_E(V)$. The equivariance condition means that (g_σ) is a 1-cocycle in $Z^1(\mathcal{G}, \mathrm{Aut}_E(V))$: $g_{\sigma\tau} = g_\sigma {}^\sigma g_\tau$. Proposition 6.3 implies that two such cocycles give rise to isomorphic varieties over F if and only if they are cohomologous.

In other words:

6.4. Proposition. *In these circumstances, equivalence classes of descents of V from E to F are parametrized by the cohomology set $H^1(\mathcal{G}, \mathrm{Aut}_E(V))$.*

CONJUGATION OF POINTS. In practice, the following question often arises: *Given descent data (Φ_σ), how do we characterize the F-rational points of V among the E-rational ones?*

If V is embedded in E^n and $A_E[V] = E[x]/I$ with $I \subset F[x]$, then conjugation $x \mapsto \sigma_\Phi(x) = ({}^\sigma x_i)$ takes E-rational points of V to other E-rational points of V.

In fact, this conjugation of points can be characterized independently of an embedding into E^n. A point is determined by its evaluation of polynomials. If $P(x) = \sum p_i x^i$ then

$$P(\sigma_\Phi(x)) = \sum p_i {}^\sigma x_i = {}^\sigma\left(\sum {}^{\sigma^{-1}} p_i x^i\right),$$

which can be rephrased as

$$P(\sigma_\Phi(x)) = {}^\sigma([\Phi_{\sigma^{-1}}(P)])(x)). \tag{6.5}$$

This formula defines the conjugate point $\sigma_\Phi(x)$ purely in terms of descent data.

If the point x is in $V(E)$, then it is in $V(F)$ if and only if ${}^\sigma(P(x)) = [\Phi_{\sigma^{-1}}P](x)$ for all P in A_E. Hence, with this definition:

6.6. Proposition. *An E-rational point of V is F-rational if and only if $\sigma_\Phi(x) = x$ for all σ.*

Suppose we are given the conjugation associated with one descent datum Φ. What is the conjugation for the datum $\Psi_\sigma = g_\sigma\Phi_\sigma$? It is

$$\sigma_\Psi(x) = g_\sigma {}^\sigma x\,. \tag{6.7}$$

You can easily check that with this definition $(\sigma\tau)_\Psi = \sigma_\Psi\tau_\Psi$.

RESTRICTION OF SCALARS. Suppose V to be a variety defined over the Galois extension E/F. Let $U = \prod_{\mathcal{G}} V^\tau$. There is a canonical isomorphism of U with U^σ that just permutes the factors. This defines the structure of a variety $R_{E/F}U$ defined over F. It is the same as what I called before the variety obtained by restriction of scalars from E to F.

6.8. Proposition. *There is a canonical bijection of the F-rational points of $R_{E/F}U$ with the E-rational points of U.*

Proof. The conjugation on points (x_τ) takes x_σ to ${}^\tau x_\sigma$. So the fixed points are the points with $x_\sigma = {}^\sigma x$ for some x a point of V.

Remark. Mestre's examples of varieties for which $\mathcal{E}$ does not split are not easy to explain, but there is a related phenomenon that is rather simple. Consider the multiplicative group of Hamiltonian quaternions $\mathbb{H}$, acting

by left multiplication on $\mathbb{H}$. This representation is irreducible, since its commuting algebra is the ring of right multiplications, which may be identified with $\mathbb{H}$. It is also defined over $\mathbb{R}$. But over $\mathbb{C}$ the commuting algebra becomes $M_2(\mathbb{C})$, and the representation decomposes into two copies of the spin representation of dimension 2. This irreducible representation is therefore isomorphic to its conjugate, but is not definable over $\mathbb{R}$.

Remark. Grothendieck made a generalization of the theory of descent into a major component of algebraic geometry. For this see [Grothendieck:1958–60]. For a short account, look at Chapter 16 of [Milne:2009].

7. Real varieties

The case $E/F = \mathbb{C}/\mathbb{R}$ is special, since the algebraic closure of $\mathbb{R}$ has finite degree over it, and a descent can be characterized entirely in terms of point conjugation. This is because the equation (6.5) can be rewritten now, with σ a complex conjugation, as

$$^{\sigma}\big(P(\sigma_\Phi(x)\big) = [\Phi_\sigma(P)])(x)\,,$$

since because $\mathbb{C}$ is algebraic an affine function is determined by its values on complex points.

I'll look now at some examples. Suppose G to be a split reductive group defined over $\mathbb{R}$. There exists on $G(\mathbb{C})$ a well defined conjugation $g \mapsto \overline{g}$ such that $G(\mathbb{R})$ is the subgroup of g with $\overline{g} = g$. Real forms of G are parametrized by certain equivalence classes of algebraic automorphisms σ of $G(\mathbb{C})$ such that $\overline{\sigma}\sigma = I$—to σ corresponds the conjugation $g \mapsto \sigma(g)\overline{g}$.

Every reductive group posses at least one non-trivial automorphism, the canonical involution θ, which is rational over $\mathbb{R}$. For classical groups in a suitable coordinate system, this takes a matrix X to ${}^tX^{-1}$. It is defined over $\mathbb{R}$ by its action on a maximal torus and root spaces in the Lie algebra. The real form corresponding to this is always a compact connected group.

Example. The conjugation defining $\mathrm{GL}_n(\mathbb{R})$ in $\mathrm{GL}_n(\mathbb{C})$ takes X to $\overline{X}$. That defining the compact unitary group $\mathbb{U}(n)$ is

$$X \longmapsto {}^t\overline{X}^{-1}\,.$$

Example. Let $H = H_n$ be the skew-diagonal $n \times n$ matrix with

$$h_{i,j} = \begin{cases} 1 & \text{if } j = n+1-i \\ 0 & \text{otherwise.} \end{cases}$$

for $n = 2m+1$. For example

$$H_3 = \begin{bmatrix} \circ & \circ & 1 \\ \circ & 1 & \circ \\ 1 & \circ & \circ \end{bmatrix}.$$

Note that $-H$ lies in $\mathrm{SO}(H)$. The real group $G = \mathrm{SO}(H_n)$ is the split form of the orthogonal group of dimension n. Under the assumption that n be odd, there are no outer automorphisms of G and the center of G is trivial, and the real forms of G are parametrized by $H^1(\mathcal{G}(\mathbb{C}/\mathbb{R}, \mathrm{SO}(\mathbb{C}))$, which also parametrizes real quadratic forms of dimension n. There is one of these for every $k \leq m$, with matrix $H_{2k} \oplus I_{n-2k}$. For example, if $n = 3$ are just two, the hyperbolic form H_3 and the positive definite one. The conditions that a matrix X belong to $\mathrm{SO}(H)$ are that

$$\det(X) = 1, \quad {}^tXHX = H$$

or

$${}^tX^{-1} = HXH^{-1}\,.$$

For many groups the canonical involution is an outer automorphism, but that is not the case here. The compact form of G is the group of matrices X in $G(\mathbb{C})$ such that ${}^t\overline{X}^{-1} = X$. It is clearly compact since it is a closed subgroup of $\mathrm{SU}(n)$. Of course it must be isomorphic to the compact SO_n, but how does that work out explicitly?

I start with an observation in dimension 2. Suppose e, f an orthonormal basis of $\mathbb{R}^2$. Then

$$\langle if, if\rangle = -1\,.$$

If we choose the complex basis

$$\frac{e-if}{\sqrt{2}},\quad \frac{e+if}{\sqrt{2}}$$

then

$$\langle e-if, e+if\rangle = 2\,.$$

so that if

$$S = \frac{1}{\sqrt{2}}\cdot\begin{bmatrix} 1 & 1\\ -i & i\end{bmatrix}$$

then

$${}^tS\cdot S = \begin{bmatrix}\circ & 1\\ 1 & \circ\end{bmatrix} = H_2\,.$$

7.1. Lemma. *If*

$${}^tFRX = Q$$

then

$$X \mapsto Y = FXF^{-1}$$

is an isomorphism $\mathrm{SO}(R)\to\mathrm{SO}(Q)$.

Proof. Because ${}^tXRX = R$ if and only if

$${}^tX\,{}^tFQFX = {}^tFQF\,.$$

In our case $R = I$, so then $X \longmapsto SXS^{-1}$ is an isomorphism of $\mathrm{SO}(H_2)$ with the orthogonal group $\vee(2)$. Sure enough

$$\begin{bmatrix} 1 & 1\\ -i & i\end{bmatrix}\begin{bmatrix} z & \circ\\ \circ & 1/z\end{bmatrix}\begin{bmatrix} 1 & 1\\ -i & i\end{bmatrix}^{-1} = \frac{1}{2i}\begin{bmatrix} i(z+1/z) & 1/z-z\\ z-1/z & i(z+1/z)\end{bmatrix} = \begin{bmatrix}\cos(\theta) & -\sin(\theta)\\ \sin(\theta) & \cos(\theta)\end{bmatrix}$$

if $z = e^{i\theta}$.

Similarly, if

$$S = \begin{bmatrix} 1/\sqrt{2} & \circ & 1/\sqrt{2}\\ \circ & 1 & \circ\\ -i/\sqrt{2} & \circ & i/\sqrt{2}\end{bmatrix}$$

then

$${}^tS\,S = H_3\,.$$

Therefore $X \mapsto SXS^{-1}$ is an isomorphism of $\mathrm{SO}(H_3)$ with $\mathrm{SO}(3)$. But $\overline{S} = SH$. This implies that if ${}^t\overline{X}^{-1} = X$ then SXS^{-1} is real. This in turn gives an explicit isomorphism of the compact form of $\mathrm{SO}(H_3)$ with $\mathrm{SO}(3)$. The same argument works for all n.

8. References

1. Enrique Arrondo, 'Another elementary proof of the Nullstellensatz', *American Mathematical Monthly* **113** (2006), 169–171.

2. Armand Borel and Dan Mostow (editors), **Algebraic groups and discontinuous subgroups**, *Proceedings of Symposia in Pure Mathematics* **IX**, American Mathematical Society, 1966.

3. Mikhail Borovoi, 'Abelianization of the second non-abelian cohomology', *Duke Mathematical Journal* **72** (1993), 217–239.

4. Claude Chevalley, 'Schemas I et II', exposées 5 and 6 in volume 8 of the *Séminaire Henri Cartan*, 1955–56.

5. Dan Grayson, 'The Hilbert Nullstellensatz', at `http://www.math.uiuc.edu/~dan/ShortProofs/`.

6. Alexandre Grothendieck, 'Techniques de descentes et théorèmes d'existence en géometrie algébrique I.', *Séminaire Bourbaki* exposé 190 (1958–60), 299-327.

7. David Hilbert, 'Über die Theorie der algebraischen Formen', *Mathematische Annalen* **36** (1890), 473–534.

8. ——, 'Über die vollen Invariantensysteme', *Mathematische Annalen* **42** (1893), 313–373.

9. Saunders Maclane, **Homology**, Springer, 1963.

10. Jean François Mestre, 'Construction de courbes de genre 2 à partir de leurs modules', pp. 313–334 in [Mora-Traverso:1991].

11. James Milne, **Topics in algebraic geometry**, preprint dated 2009, available at
`http://www.jmilne.org/math/CourseNotes/ag.html`

12. Teo Mora and Carlo Traverso, **Effective methods in algebraic geometry**, Birkhäuser, 1991

13. Jean-Pierre Serre, **Groupes algébriques et corps de classes**, Hermann, 1959.

14. ——, **Cohomologie Galoisienne**, *Lecture Notes in Mathematics* **5**, Springer-Verlag, 1964.

15. ——, **Corps locaux**, Hermann, 1968.

16. Tonny Springer, 'Nonabelian H^2 in Galois cohomology', pp. 164–182 in Borel-Mostow1966.

17. Terence Tao, 'Hilbert's Nullstellensatz', posted in 2007 at
`http://terrytao.wordpress.com/2007/11/26/hilberts-nullstellensatz/`

18. André Weil, 'The field of definition of a variety', *American Journal of Mathematics* **78** (1956), 509–524.

19. ——, **Basic number theory** (second edition), Springer, 1995.