EXISTENCE OF INVARIANT BASES

ELLIS KOLCHIN AND SERGE LANG[1]

Let K be a field, G a group of automorphisms of K, and M a vector space over K on which G acts in such a way that $\sigma(aD) = \sigma a \cdot \sigma D$ for $\sigma \in G$, $a \in K$, and $D \in M$. The problem arises to find whether M has a basis consisting of invariant elements under G. In other words, letting K_0 be the fixed field under G, and M_0 the set of fixed elements of M under G so that M_0 is a vector space over K_0, to find out whether M is isomorphic to the tensor product

$$M \approx K \otimes_{K_0} M_0$$

under the natural map. We shall see that this is so if and only if a certain cocycle of G in the full linear group is trivial.

In some applications, a rational structure is added to K and G, namely K is the function field of a principal homogeneous space over a group variety G. We shall show that the cocycle involved is then determined rationally. This leads us into a discussion of rational cocycles in §3, and of their comparison with the ordinary cocycles of Galois theory, i.e. where G is a finite Galois group. All cocycles involved with coefficients in the full linear group split, and in fact the Galois cohomology (in dimension 1) of the group variety of units in an algebra is trivial (Propositions 2 and 5).

1. The invariant subspace.

Let K be a field, and G a group of automorphisms of K. By a (G, K)-*space* M we shall mean a vector space over K which is also a unitary G-module, such that

$$\sigma(aD) = \sigma a \cdot \sigma D$$

for $a \in K$, $D \in M$ and $\sigma \in G$. An element D of M is said to be invariant under G if $\sigma D = D$ for all $\sigma \in G$. A basis $(D) = (D_i)$ of M over K will be called *invariant* if $\sigma D_i = D_i$ for every $\sigma \in G$ and every i.

PROPOSITION 1. *Let M be a finite dimensional (G, K)-space. If $(D) = (D_1, \cdots, D_m)$ is any basis of M, and if*

$$A(\sigma) = (a_{ij}(\sigma)) \qquad (i, j = 1, \cdots, m)$$

is the matrix defined by

$$\sigma D_j = \sum_{\nu} a_{\nu j}(\sigma) D_\nu \qquad (1 \leqq j \leqq m),$$

Received by the editors April 1, 1959.

[1] This paper was prepared in connection with contract NONR 266(57).

then $A(\sigma)\cdot\sigma A(\tau)=A(\sigma\tau)$. A necessary and sufficient condition that M have an invariant basis is that there exist an invertible matrix B with coordinates in K such that $A(\sigma)=B^{-1}\sigma B$.

PROOF. That $A(\sigma)$ satisfies the cocycle relation is easy to see. Suppose $A(\sigma)=B^{-1}\sigma B$. Using matrix notation, we may write $\sigma(D)={}^tA(\sigma)(D)$, where for any matrix X, we denote by ${}^tX$ the transpose of X. Let a new basis (D') be defined by $(D')={}^tB^{-1}(D)$. Then

$$\sigma(D') = \sigma{}^tB^{-1}\sigma(D) = {}^t\sigma(B)^{-1}\cdot{}^tA(\sigma)\cdot(D) = {}^tB^{-1}(D) = (D')$$

and thus (D') is invariant. Conversely, if (D') is an invariant basis, define the matrix B by the relation $(D)={}^tB(D')$. Then

$${}^tA(\sigma)(D) = \sigma(D) = {}^t\sigma B\cdot\sigma(D') = {}^t\sigma B\cdot(D') = {}^t\sigma B\cdot{}^tB^{-1}(D)$$

and $A(\sigma)=B^{-1}\sigma B$. This proves our proposition.

If we denote by M_0 the set of G-invariant elements of M and by K_0 the fixed field of K under G, then M_0 is a vector space over K_0. If M admits an invariant basis, then one sees immediately that M is isomorphic to the tensor product

$$K\otimes_{K_0} M_0 \approx M$$

under the natural map $a\otimes D\rightarrow aD$, $a\in K$, $D\in M_0$.

We observe that the set of K_0-linear transformations of K, denoted by $\mathrm{End}_{K_0}(K)$, forms a (G, K)-space in a natural fashion: If $D\in\mathrm{End}_{K_0}(K)$, and $\sigma\in G$, then one defines

$$(\sigma D)(a) = \sigma(D(\sigma^{-1}a)),$$

and verifies trivially that $\sigma(aD)=\sigma a\cdot\sigma D$.

In the applications, one frequently takes the subspace of $\mathrm{End}_{K_0}(K)$ consisting of the derivations of K over K_0, or a finite dimensional space of linear transformations over a subfield of K.

REMARK. Proposition 1 and its proof generalizes so that K can be a ring (with unity, not necessarily commutative) and M can be a unitary K-module with finite basis. In this situation, a matrix B over K with m rows and n columns is *invertible* if there exists a matrix C over K with n rows and m columns such that BC is the unity matrix of degree m and CB is the unity matrix of degree n. C is then unique and is denoted by B^{-1}. The generalized proposition states that if (D) is a basis of m elements, and $A(\sigma)$ is defined as above, then $A(\sigma)\cdot\sigma A(\tau)=A(\sigma\tau)$, and a necessary and sufficient condition that there exist an invariant basis of n elements is that there exist an invertible matrix B over K with n rows and m columns such that $A(\sigma)=B^{-1}\sigma B$.

2. Galois cohomology in dimension 1.

As we have seen in the last section, it is useful to have a criterion to split a 1-cocycle. We shall give one in this section.

Let G be a group variety (i.e. a connected algebraic group) defined over a field k. Let K be a finite Galois extension of k with Galois group $\mathfrak{g}$. Then $\mathfrak{g}$ operates as a group of automorphisms of the subgroup of G consisting of the points of G which are rational over K. We denote this subgroup by G_K. Suppose we are given a family $(x_\sigma)_{\sigma\in\mathfrak{g}}$ of points of G_K satisfying

$$x_\sigma\cdot\sigma x_\tau = x_{\sigma\tau}, \qquad \sigma, \tau \in \mathfrak{g}.$$

Such a family is called a cocycle of $\mathfrak{g}$ in G_K. The set of these cocycles is denoted by $Z^1(\mathfrak{g}, G_K)$. We say that (x_σ) is *cohomologous* to (y_σ) and write $(x_\sigma)\sim(y_\sigma)$ if there exists an element $z\in G_K$ such that

$$y_\sigma = z^{-1}x_\sigma\sigma z$$

for each $\sigma\in\mathfrak{g}$. This is obviously an equivalence relation between cocycles. The set of equivalence classes is called the *first cohomology set* of $\mathfrak{g}$ in G_K and is denoted by $H^1(\mathfrak{g}, G_K)$. If $z\in G_K$ then $(z^{-1}\sigma z)$ is a cocycle, and such a cocycle is called a coboundary of $\mathfrak{g}$ in G_K. The set of all such coboundaries is denoted by $B^1(\mathfrak{g}, G_K)$ and is itself an equivalence class, i.e. an element of $H^1(\mathfrak{g}, G_K)$. (Of course, if G is commutative, these sets are groups, and $H^1(\mathfrak{g}, G_K)$ is a commutative group.)

If $L\supset K$ is another Galois extension of k, then there is a natural map of $H^1(\mathfrak{g}_{K/k}, G_K)$ into $H^1(\mathfrak{g}_{L/k}, G_L)$ obtained by inflation: A cocycle for $\mathfrak{g}_{K/k}$ determines one for $\mathfrak{g}_{L/k}$ simply by extending the function to cosets of the subgroup of $\mathfrak{g}_{L/k}$ of which $\mathfrak{g}_{K/k}$ is a factor group. It is trivially seen that this natural map is actually *injective* and we may take the injective limit of these cohomology sets as L becomes larger and larger. The limiting set, union of all $H^1(\mathfrak{g}_{L/k}, G_L)$, will be denoted by $H^1(k, G)$.

We are interested in a noncommutative group, namely the full linear group. More generally, let A_0 be a finite dimensional associative algebra with unity element over the field k, let Ω be a universal domain containing k, and let A be the algebra over Ω which is the tensor product of A_0 with Ω. Let $e_1, \cdots, e_m$ be a linear basis of A_0 over k, and therefore of A over Ω. Expressing elements of A in terms of this basis, $x=\sum\xi_ie_i$, one sees that there exists a polynomial $P(X_1, \cdots, X_m)\in k[X_1, \cdots, X_m]$ such that x is invertible if and only if $P(\xi_1, \cdots, \xi_m)\neq 0$, or as we shall abbreviate, $P(x)\neq 0$. These invertible elements therefore form a group variety defined over k (it is a k-open subset of affine m-space in the Zariski topology), and we shall denote it by $\Gamma(A)$ or simply Γ. The general linear group $GL(m)$ is an example of such a group variety defined over the prime field.

PROPOSITION 2. *Let* $\Gamma=\Gamma(A)$ *be as above the group variety of units in an algebra defined over* k, *and let* K *be a Galois extension of* k *of finite degree, with Galois group* $\mathfrak{g}$. *Then* $H^1(\mathfrak{g}, \Gamma_K)$ *is trivial, that is, every cocycle is a coboundary.*

PROOF. The case in which k is finite is a special case of the fact that $H^1(\mathfrak{g}, G_K)$ is trivial for any group variety defined over a finite field k (see [2]). In the infinite case, the theorem is proved in [1]. We reproduce the proof here for the convenience of the reader. Let (x_τ) be in $Z^1(\mathfrak{g}, \Gamma_K)$. If $(t_\tau)_{\tau\in\mathfrak{g}}$ is a family of elements of Ω, algebraically independent over K, then $P(\sum_\tau t_\tau x_\tau)\neq 0$ because this polynomial does not vanish when one t_τ is replaced by 1 and all the others by 0. It is well known (see, for instance, Bourbaki, *Algèbre*, Chapter V, §10, Theorem 4, p. 57) that this implies the existence of an element $\alpha\in K$ such that $P(\sum(\tau\alpha)x_\tau)\neq 0$. Writing $y=\sum(\tau\alpha)x_\tau$ we see that $y\in\Gamma_K$ and $\sigma y=\sum(\sigma\tau\alpha)\sigma x_\tau=\sum(\sigma\tau\alpha)x_\sigma^{-1}x_{\sigma\tau}=x_\sigma^{-1}y$, so that $(x_\sigma)=(y\sigma y^{-1})$ is in $B^1(\mathfrak{g}, \Gamma_K)$. This concludes the proof.

3. **Rational cohomology.** We recall the notion of a homogeneous space and use the terminology of Weil [4]. Let V be a variety and G a group variety. Suppose we are given a rational map

$$f\colon V\times G\rightarrow V$$

which is everywhere defined. Given $v\in V$ and $x\in G$, we write vx instead of $f(v, x)$. We say that V is a *transformation space* for G if

$$v(xy) = (vx)y \qquad \text{and} \qquad ve = v$$

for $x, y\in G$ and $v\in V$. Here, as usual, e denotes the unity element of G. We say that the transformation space V is defined over k if G, V and the rational map f are defined over k.

We observe that if Ω is the universal domain, then G can be viewed as a group of automorphisms of the function field $\Omega(V)$. Indeed, for each $x\in G$, we have the automorphism σ_x such that

$$(\sigma_x f)(v) = f(vx)$$

whenever f is a function in $\Omega(V)$, and v is a generic point of V over a field of definition for f over which x is rational. In the same manner, if the transformation space V is defined over k, then G_k is a group of automorphisms of $k(V)$.

A transformation space is said to be a *homogeneous space* if given two points $v, w\in V$, there exists $x\in G$ such that $vx=w$. We say that

V is a *principal* homogeneous space if the element x is uniquely and rationally determined. By this we mean that there exists an everywhere defined rational map μ: $V\times V\rightarrow G$ such that $x=\mu(v, w)$. One may write symbolically $x=v^{-1}w$. The principal space V is said to be defined over k if, as a transformation space it is defined over k, and the rational map μ is defined over k.

Let now G, G' be group varieties, let V be a transformation space of G, all these being defined over k. A rational map

$$f\colon V\times G\rightarrow G'$$

of $V\times G$ into G', defined over k, is said to be a 1-*cocycle* if it satisfies the relation

$$f(v, x)f(vx, y) = f(v, xy)$$

whenever v, x, y are independent generic points of V, G, and G' over k. *It then follows that* $f(v, x)$ *is defined whenever* x *is any point and* v *is a generic point of* V *over* $k(x)$, because we can write

$$f(v, x) = f(v, xy)f(vx, y)^{-1}$$

with y generic over $k(v, x)$. The 1-cocycles form a set denoted by $Z^1_k(G, V, G')$. We say that two cocycles are *cohomologous* and write $f\sim g$, if there exists a rational map ϕ: $V\rightarrow G'$ defined over k such that $f(v, x)=\phi(v)^{-1}g(v, x)\phi(vx)$. This establishes an equivalence relation among the cocycles, and the equivalence classes form the first cohomology set $H^1_k(G, V, G')$. The cocycles in the identity class, i.e. those of type $\phi(v)^{-1}\phi(vx)$ are called *coboundaries*, and form a set $B^1_k(G, V, G')$.

(If G' is commutative, and written additively, we can define cocycles in higher dimension, an r-cocycle being by definition a rational map

$$f\colon V\times G\times\cdots\times G\rightarrow G'$$

defined over k satisfying the coboundary formula

$$\begin{aligned} 0 = (\delta f)(v, x_1, \cdots, x_{r+1}) &= f(vx_1, x_2, \cdots, x_{r+1}) \\ &+ \sum (-1)^{\nu} f(v, x_1, \cdots, x_\nu x_{\nu+1}, \cdots, x_{r+1}) \\ &+ (-1)^{r+1}f(v, x_1, \cdots, x_r). \end{aligned}$$

One then has an rth cohomology group for $r\geqq 0$.)

We return to the noncommutative case, and assume that V is a principal homogeneous space for the group variety G, all defined over k. Let $f\in Z^1_k(G, V, G')$. If $w_0\in V$ has the property that f is defined at $(u, u^{-1}w_0)$ for u generic on V over $k(w_0)$ and if we define

$\phi(v)=f(v, v^{-1}w_0)^{-1}$, so that ϕ is a rational map of V into G' defined over $k(w_0)$, then $f(v, x)=\phi(v)^{-1}\phi(vx)$. Thus f is trivial as an element of $Z^1_{k(w_0)}(G, V, G')$. It follows that if the points of V which are rational over k are dense in the Zariski topology, then every element of $Z^1_k(G, V, G')$ is a coboundary. (This is the case for instance if k is separably closed.)

Now we transform the above cocycles into a homogeneous form. Let λ: $V\times V\rightarrow V\times G$ be the canonical map such that $\lambda(u, v)=(u, u^{-1}v)$. Then the inverse of λ is a rational map sending (v, x) onto (v, vx). Given a cocycle $f\in Z^1_k(G, V, G')$, there exists therefore a rational map F: $V\times V\rightarrow G'$ which makes the following diagram commutative:

$$\begin{tikzcd}
V\times G \arrow[rr, "f"] & & G' \\
& V\times V \arrow[ul, "\lambda"] \arrow[ur, "F"'] &
\end{tikzcd}$$

and the mapping F satisfies the relation

$$F(u, v)F(v, w) = F(u, w)$$

whenever u, v, w are independent generic points of V over k. We may of course start with an arbitrary variety V defined over k and a group variety G' with such a mapping. We may thus define homogeneous cocycles $Z^1_k(V, G')$, and coboundaries $B^1_k(V, G')$, these being rational maps of type $F(u, v)=\phi(u)^{-1}\phi(v)$ where ϕ: $V\rightarrow G'$ is a rational map defined over k. This allows us to define $H^1_k(V, G')$ for any variety V defined over k.

PROPOSITION 3. *Let V be a principal homogeneous space for G, and let G' be another group variety defined over k. Then there is a bijective mapping between $H^1_k(G, V, G')$ and $H^1_k(V, G')$ given by*

$$f(v, x) = F(v, vx).$$

The proof is trivial.

As Serre has pointed out to us, we can inject $H^1_k(V, G')$ into the Galois cohomology set $H^1(k, G')$ as defined in §2. The way this is done is described in the following proposition.

PROPOSITION 4. *Let V be a principal homogeneous space for G, and let G' be another group variety, defined over k. For each $\overline{F}\in H^1_k(V, G')$ choose a representative cocycle F in $Z^1_k(V, G')$, and choose a finite Galois extension K of k with group denoted by $\mathfrak{g}$ such that V has a point v_0 rational over K for which $F(u, v_0)$ is defined when u is generic over K.*

For each $\sigma \in \mathfrak{g}$, let $x_\sigma = F(u, v_0)^{-1}F(u, \sigma v_0)$, where u, v_0 are chosen as above. Then $(x_\sigma)_{\sigma\in\mathfrak{g}}$ is a cocycle in $Z^1(\mathfrak{g}, G'_K)$, the corresponding element $\bar{x}$ of $H^1(k, G')$ is independent of the choice of F, K, v_0, u and the mapping $\overline{F} \to \bar{x}$ is an injection

$$H_k^1(V, G') \to H^1(k, G').$$

PROOF. From the coboundary relation one verifies immediately that for independent generic points u, v of V over K, we have

$$F(u, v_0)^{-1}F(u, \sigma v_0) = F(v, v_0)^{-1}F(v, \sigma v_0),$$

so that each x_σ is rational over K, and (x_σ) is a cocycle. The rest of the proof is straightforward and is left to the reader.

In particular, we get

COROLLARY. *Let V be a principal homogeneous space for G and let G' be another group variety, defined over k. If $H^1(k, G')$ is trivial, then so is $H_k^1(V, G')$.*

Examples of group varieties G' for which $H^1(k, G')$ is trivial are:

The group variety of units in a finite dimensional algebra as we showed in Proposition 2, and in particular the full linear groups $GL(m)$;

The additive and multiplicative groups of the universal domain, this being Hilbert's Theorem 90 in its multiplicative and additive forms;

The group varieties G' having a normal sequence $G' = G_0 \supset G_1 \supset \cdots \supset G_r = 1$ defined over k, with each G_{i-1}/G_i either the additive or multiplicative group as above.

One may ask how it is possible to characterize those elements of $H^1(k, G')$ which come from an element of $H_k^1(V, G')$. It is known [3, Proposition 4] that $H^1(k, G')$ is in bijective correspondence with the set of isomorphism classes of principal homogeneous spaces of G' over k, and the reader may easily verify that the image of $H_k^1(V, G')$ in $H^1(k, G')$ corresponds to those principal homogeneous spaces of G', defined over k, which have a rational point in a field $k(v)$ where v is a generic point of V over k. The reader will also note that a cocycle $F: V \times V \to G'$ determines a principal homogeneous space of G' through which it can be factored [4, Proposition 4] and that this space corresponds precisely to the one determined by the cocycle described in Proposition 4 (Serre).

4. Rational determination of the invariant subspace. Let V be a principal homogeneous space for the group variety G. For each point

x of G, there is a unique automorphism σ_x of the function field $\Omega(V)$ over the universal domain Ω, such that, if $f \in \Omega(V)$ then $\sigma_x f$ is defined at a point v of V whenever f is defined at vx, and $(\sigma_x f)(v) = f(vx)$. The mapping $x \rightarrow \sigma_x$ is a group isomorphism permitting us to identify G with a group of automorphisms of $\Omega(V)$ over Ω. If k is a field of definition of V, and if we make the assumption that x is rational over k, then σ_x maps $k(V)$ onto itself. Therefore without this assumption, σ_x maps $k(V)$ into $k(x)(V)$.

Let f: $V \times G \rightarrow W$ be a rational map of $V \times G$ into some variety W, and let x be a point of G. Assume that the following condition is satisfied. For some field of definition k for f (i.e. for V, G, W and the graph of f), and for some generic point v of V over $k(x)$, f is defined at (v, x). Then there exists a unique rational map f_x: $V \rightarrow W$ defined over $k(x)$, such that $f_x(v) = f(v, x)$. When the above condition is satisfied, we shall say that f_x is *meaningful.* Of course, if x is generic on G over k, then f_x must be meaningful.

Let M be a vector space over $\Omega(V)$, of finite dimension m, which is a $(G, \Omega(V))$-space. If $(D) = (D_1, \cdots, D_m)$ is a basis of M, then for each point x of G, every $\sigma_x D_j$ is a linear combination of the basis vectors D_i with coefficients in $\Omega(V)$. We shall call the basis *rational* if there exist rational functions f_{ij} on $V \times G$ such that, for some common field of definition k of V and the f_{ij}, and for every generic point x of G over k, we have

$$\sigma_x D_j = \sum_i f_{ijx} D_i, \qquad (1 \leqq j \leqq m). \tag{1}$$

A simple computation shows that when this is the case then, for independent generic points x, y of G over k, we have

$$f(v, xy) = f(v, x) f(vx, y)$$

where we denote by f the matrix (f_{ij}). In other words, f is a 1-cocycle in $Z_k^1(G, V, GL(m))$. It follows (§3) that f_x (i.e. each f_{ijx}) is meaningful for every point x of G, and also, that Equation (1) holds for every point x of G since each point of G can be expressed as a product of generic points $(x = xy \cdot y^{-1})$. In particular, any common field of definition of V and the f_{ij} must enjoy the same properties that have been attributed to k above. Such a common field of definition will be called a *field of rationality* of the rational basis (D). It is obvious that every invariant basis of M is rational, and admits as field of rationality any field of definition of the principal homogeneous space V.

It is almost immediate that if one basis of a $(G, \Omega(V))$-space is rational, then so are all its bases. By a *rational* $(G, \Omega(V))$*-space* we shall mean a $(G, \Omega(V))$-space with rational bases. The nature of such spaces is completely described by the following theorem, the proof of which follows that of Proposition 1, making use of the results of §2 and §3.

THEOREM. *Let M be a finite dimensional $(G, \Omega(V))$-space. A necessary and sufficient condition that M be rational is that M have an invariant basis. If (D) is any rational basis of M, and k is a field of rationality of (D), then there exists an invertible matrix over $k(V)$ transforming (D) into an invariant basis of M.*

PROOF. Since invariant bases are rational, the sufficiency is clear. To prove the necessity and the final part of the theorem, let (D) be a rational basis of M with field of definition k. Denoting the corresponding cocycle in $Z_k^1(G, V, GL(m))$ by $f=(f_{ij})$, we conclude from §§2, 3 that there exist rational functions $\phi_{ij} \in k(V)$ such that the matrix $\phi=(\phi_{ij})$ is invertible and $f(v, x)=\phi(v)^{-1}\phi(vx)$ for $x \in G$ and v generic on V over $k(x)$. Setting $E_j=\sum_i \psi_{ij} D_i$ $(1 \leqq j \leqq m)$, where $(\psi_{ij})=(\phi)^{-1}$, we conclude that (E) is an invariant basis of M.

In the applications of the above theorem, one is usually given a subset $M_{k(V)}$ of M which is a vector space over $k(V)$ such that we have an isomorphism

$$M \approx \Omega(V) \otimes_{k(V)} M_{k(V)}$$

under the natural map $f \otimes D \rightarrow fD$, and such that a basis of $M_{k(V)}$ over $k(V)$ is a rational basis of M, having k as field of rationality. One may then say that M is *rationally $k(V)$-extended*. In that case one may say that an element D of M is *defined* over a field $k' \supset k$ if D lies in $k'(V)M_{k(V)}$. If M_k^0 is the set of elements of M which are invariant and defined over k, then M_k^0 is a vector space over k, and our theorem shows that we have an isomorphism

$$k(V) \otimes_k M_k^0 \approx M_{k(V)}$$

again under the map $f \otimes D \rightarrow fD$.

BIBLIOGRAPHY

1. E. Kolchin, *On the Galois theory of differential fields*, Amer. J. Math. vol. 77 (1955) pp. 868–894.

2. S. Lang, *Algebraic groups over finite fields*, Amer. J. Math. vol. 78 (1956) pp. 555–563.

3. S. Lang and J. Tate, *Principal homogeneous spaces over abelian varieties*, ibid. vol. 80 (1958) pp. 659–684.

4. A. Weil, *Algebraic groups and homogeneous spaces*, ibid. vol. 77 (1955) pp. 493–512.

COLUMBIA UNIVERSITY