Galois theory and the normal basis theorem

Arthur Ogus

December 3, 2010

Recall the following key result:

Theorem 1 (Independence of characters) *Let M be a monoid and let K be a field. Then the set of monoid homomorphisms from M to the multiplicative monoid of K is a linearly independent subset of the K-vector space K^M.*

Proof: It is enough to prove that if $\chi_1, \ldots, \chi_n$ is a sequence of distinct homorphisms $M \to K$ and $c_1, \ldots, c_n$ is a sequence in K such that $\sum c_i \chi_i = 0$, then each $c_i = 0$. We do this by induction on n. If $n = 1$, we have have $c_1 = c_1\chi_1(1) = 0$, so $c_1 = 0$. For the induction step, observe that for any $g, h \in M$, we have

$$\begin{aligned} c_1\chi_1(g) + \cdots + c_n\chi_n(g) &= 0 \\ c_1\chi_1(gh) + \cdots + c_n\chi_n(gh) &= 0 \end{aligned}$$

Multiply the first equation by $\chi_n(h)$ and subtract from the second equation to obtain

$$c_1\chi_1(g)(\chi_1(h) - \chi_n(h)) + \cdots + c_{n-1}\chi_{n-1}(g)(\chi_{n-1}(h) - \chi_n(h)) = 0$$

Fixing h and letting g vary, we see that

$$c_1(\chi_1(h) - \chi_n(h))\chi_1 + \cdots + c_{n-1}(\chi_{n-1}(h) - \chi_n(h))\chi_{n-1} = 0.$$

By the induction assumption, $c_i(x_i(h) - \chi_n(h)) = 0$ for all h and $1 \le i < n$. Since $\chi_i \neq \chi_n$ if $i < n$, this implies that $c_i = 0$ if $i < n$. Then $c_n\chi_n = 0$ and it follows also that $c_n = 0$. □

Now let k be a field and let $\mathcal{A}_k$ denote the category of k-algebras.

Corollary 2 *If k is a field, if A and K are objects of $\mathcal{A}_k$ and K is a field, then the set*

$$\mathcal{X}_K(A) := \mathrm{Mor}_{\mathcal{A}_k}(A, K)$$

is a linearly independent subset of the K-vector space $\mathrm{Hom}_k(A, K)$. In particular, if A is finite dimensional, then $|\mathcal{X}_K(A)| \leq \dim_k(A)$.

Proof: The set of algebra homomorphisms $\mathcal{X}_K(A)$ is contained in the set of monoid homomorhisms $A \to K$, and hence is a linearly independent subset of the K-vector space K^A. It is evidently contained in the set $\mathrm{Hom}_k(A, K)$ of k-linear vector space homomorphisms $A \to K$. But the K-dimension of this is equal to the k-dimension of A. □

Theorem 3 *Let A be a finite dimesnsional k-algebra, let k^a (resp. k^s) be an algebraic (resp. seperable) closure of k. Then the following conditions are equivalent.*

1. $|\mathcal{X}_{k^a}(A)| = \dim_k(A)$.
2. $|\mathcal{X}_{k^s}(A)| = \dim_k(A)$.
3. $|\mathcal{X}_K(A)| = \dim_k(A)$ *for some finite separable extension K of k.*
4. $|\mathcal{X}_K(A)| = \dim_k(A)$ *for some finite Galois extension K of k.*
5. *The nilradical of A is zero and for each maximal ideal m of A, A/m is a separable field extensionk.*

□

A finite dimensional k-algebra satisfying the above conditions is said to be *separable* over k. Our aim is to classify the category of all the finite separable k-algebras. For example, if k is algebraically or even just separably closed, the above theorem tells us that any such algebra is just a finite product of copies of k.

The result above shows that if A/k is finite and separable, there is a finite Galois extension K/k such that $|\mathcal{X}_K(A)| = \dim_k(A)$. We shall simplify our problem by fixing a finite Galois extension K/k and just studying those A for which this equality holds.

Definition 4 *Let K/k be a field extension. Then a finite dimensional k-algebra A is K-split if $|\mathcal{X}_K(A)| = \dim_k(A)$.*

In particular K itself is K-split iff $G(K/k) := \mathrm{Mor}_{\mathcal{A}_k}(K, K)$ has cardinality equal to the degree of K over k. Note that this set is a group under composition, and we denote it by $G(K/k)$. Thus a finite field extension K/k is Galois iff it is K-split. If K/k is Galois, Grothendieck's version of Galois theory establishes an anti-equivalence between the category $\mathcal{A}_{K/k}$ of K-split k-algebras and the category Σ_G of finite G-sets.

If A is an object of $\mathcal{A}_k$, let $\mathcal{X}_K(A) := \mathrm{Mor}_{\mathcal{A}_k}(A, K)$. Note that if $s \colon A \to K$ and $g \in G(K/k)$, then $g \circ s \in \mathcal{X}_K(A)$. Thus $G(K/k)$ operates naturally on the left on $\mathcal{X}_K(A)$. Furthermore, if $\theta \colon A \to B$ is a homomophism in $\mathcal{A}_{K/k}$, then the induces morphism

$$\mathcal{X}_K(\theta) \colon \mathcal{X}_K(B) \to \mathcal{X}_K(A)$$

is compatible with the G-actions. Thus we can (and shall) regard $\mathcal{X}_K$ as a contravariant functor from the category $\mathcal{A}_k$ to the category $\mathbf{\Sigma}_G$ of finite G-sets.

On the other hand, if S is a finite G-set, let

$$\mathcal{A}(S) := \mathrm{Mor}_G(S, K) \subseteq K^S$$

that is, the set of morphisms of G-sets $S \to K$. Note that $\mathcal{A}(S)$ is naturally a k-subalgebra of the k-algebra K^S, and that a morphism of G-sets $S \to T$ induces a homomorphismi of k-algebras: $cA(T) \to \mathcal{A}(S)$. Thus we can (and shall) regard $\mathcal{A}$ as a contravariant functor from the category Σ_G to the category $\mathcal{A}_k$.

There are natural transformations:

1. For each $S \in \Sigma_G$, a morphism of G-sets:

$$\epsilon_S \colon S \to \mathcal{X}(\mathcal{A}(S)) : \epsilon_S(s)(a) := a(s)$$

2. For each $A \in \mathcal{A}_k$, a homomorphism of k-algebras:

$$\alpha_A \colon A \to \mathcal{A}(\mathcal{X}(A)) : \alpha_A(a)(x) := x(a)$$

Theorem 5 *Let the notations be as above.*

1. *If S is any finite G-set, $\mathcal{A}(S)$ is a K=split k-algebra of dimension $|S|$, and the map ϵ_S is an isomorphism.*

2. *If A is an object of $\mathcal{A}_{K/k}$, then $\mathcal{X}(A)$ has cardinality $\dim_k A$, and α_A is an isomorphism.*

Thus the contravariant functors

$$\mathcal{A}\colon \mathbf{\Sigma}_G \to \mathcal{A}_{K/k} \quad \text{and} \quad \mathcal{X}\colon \mathcal{A}_{K/k} \to \mathbf{\Sigma}_G$$

are mutually inverse equivalences of categories.

For example, if $K = k$, the theorem asserts that the category of k-split algebras is antiequivalent to the category of finite sets. Let us check this as a warmup.

Lemma 6 *If S is finite set, the map $\epsilon_S\colon \to \mathrm{Mor}(k^S, k)$ is bijective and k^S has dimension $|S|$.*

Proof: For each $s \in S$, we have an element $a_s \in \mathcal{A}(S)$, defined by

$$a_s(s') := \begin{cases} 1 & \text{if } s' = s \\ 0 & \text{otherwise.} \end{cases}$$

Furthermore, $\{a_s : s \in S\}$ forms a k-basis of k^S, and $\epsilon_S(s)(a_s) \neq \epsilon_S(s')(a_s)$ if $s \neq s'$. This shows that ϵ is injective. On the other hand, the dimension of $\mathrm{Hom}_k(\mathcal{A}(S), k)$ is the dimension of $\mathcal{A}(S)$, which is the cardinality of S, and by Corollary 2, the dimension of $\mathcal{X}(\mathcal{A}(S))$ is at most the dimension of $\mathcal{A}(S)$, *i.e.*, the cardinality of S. So ϵ is bijective. □

Lemma 7 *If A is a K-split k-algebra, the map $\alpha_A\colon A \to \mathcal{A}(\mathcal{X}_K(A))$ is injective.*

Proof: It suffices to prove that the map $A \to K^{\mathcal{X}(A)}$ is injective. Let I be the kernel. Then every $x \in \mathcal{X}(A)$ factors through A/I, and hence $\mathcal{X}(A) = \mathcal{X}(A/I)$. But $\dim A = |X| = |\mathcal{X}(A/I)| \leq \dim(A/I)$ so $I = 0$. □

We can now easily prove Theorem 5 when $K = k$. Statement (1) follows from Lemma 6. On the other hand, if $A \in \mathcal{A}_{k/k}$, Lemma 7 implies that $\alpha_A\colon A \to \mathcal{A}(\mathcal{X}(A))$ is injective. But $\mathcal{X}(A)$ has cardinality $\dim(A)$, and $\mathcal{A}(\mathcal{X}(A))$ has the same dimension, so α_A is also surjective.

Now let us look at the category of G-sets. If S is a G-set, we denote by $\Gamma_G(S)$ the set of fixed points of S. Observe next that the category of G-sets has products: the product of two sets X and Y is the usual set theoretic product with the action $g(x, y) := (gx, gy)$. It also has an "internal Hom" construction: If S and T are G-sets, we have a natural action of G on the set

$$H(S, T) := T^S$$

of functions $T \to S$, by letting

$$(g\phi)(s) := g(\phi(g^{-1}s).$$

With this definition, the usual isomorphism

$$T^{X \times Y} \cong (T^Y)^X$$

is compatible with the G-actions. Furthermore,

$$\Gamma_G(T^S) = \mathrm{Mor}_G(S, T),$$

and hence

$$\mathrm{Mor}_G(S \times X, T) \cong \mathrm{Mor}_G(S, T^X).$$

Finally, observe that if S and T are G-sets and $\phi \in \mathrm{Mor}_G(S \times G, T)$, then

$$\phi(s, g) = g\phi(g^{-1}s, e).$$

and if ψ is any function $S \to T$, then

$$\tilde{\psi}(s, g) := g\psi(g^{-1}s)$$

defines a morphism of G-sets $S \times G \to T$. This gives a bijection

$$\beta\colon \mathrm{Mor}_G(S \times G, T) \cong T^S$$

For example, if S is a singleton set, evaluation at the identity of G defines a bijection:

$$\beta\colon \Gamma_G(T^G) \cong \mathrm{Mor}_G(G, T) \cong T.$$

The inverse of β takes an element t of T to the function $g \mapsto gt$.

The key to our proof is the so-called "Normal basis theorem." It gives an explicit description of K viewed as a left G-set. Endow k^G with its standard action as a left G-set. This has a basis $\{e_h : h \in G\}$, where $e_h(g) = \delta_{g,h}$. Observe that $ge_h = e_{gh}$, since $ge_h(h') = e_h(g^{-1}h') = \delta_{h',gh}$. Thus we can also view k^G as a the group algebra $k[G]$ with its standard left action of G. The left G action of G on K, together with its k-vector space structure, make K a left $k[G]$-module.

Theorem 8 *Let K/k be a finite Galois extension. Then K, viewed as a left $k[G]$-module, is free of rank one. Explciitly, there exists an element w of K such that the map*

$$F_w\colon G \to K : g \mapsto g(w)$$

is a k-basis of K. In particular, the corresponding linear map induces an an isomorphism of $k[G]$-modules

$$\tilde{F}_w \colon \colon k^G \to K.$$

We defer the proof, proceeding instead to a proof of the main theorem.

Lemma 9 *main.l If S is a finite G-set, the map the dimension of $\mathcal{A}(S)$ is $|S|$, and the map $\epsilon_S \colon S \to \mathcal{X}(\mathcal{A}(S))$ is an isomorphism.*

Proof: We use the normal basis theorem to find an isomorphism of k-vector spaces

$$\mathcal{A}(S) = \mathrm{Mor}_G(S, K) = \mathrm{Mor}_G(S, k^G)$$

But as we have seen,

$$\mathrm{Mor}_G(S, k^G) = \mathrm{Mor}_G(S \times G, k) = k^S.$$

Thus the dimension of $\mathcal{A}(S)$ is indeed $|S|$. To prove that ϵ_S is injective, it suffices to show that the map

$$\epsilon \colon S \to \mathcal{X}(\mathcal{A}(S)) \to \mathrm{Hom}_k(\mathcal{A}(S), K)$$

is injective. Now if we use the isomorphism provided by the normal basis theorem to repalce K by k^G, the map above becomes identified with the evaluation map

$$\tilde{\epsilon} \colon S \to \mathrm{Hom}_k(\mathrm{Mor}_G(S, k^G), k^G).$$

The map $k^S \to \mathrm{Mor}_G(S, k^G)$ defines a map

$$\mathrm{Hom}_k(\mathrm{Mor}_G(S, k^G), k^G) \to \mathrm{Hom}_k(k^S, k^G).$$

We find a commuatative diagram:

$$\begin{array}{ccccc}
S & \xrightarrow{\tilde{\epsilon}} & \mathrm{Hom}_k(\mathrm{Mor}_G(S, k^G), k^G)) & & \\
\downarrow & & \downarrow & & \\
S & \longrightarrow & \mathrm{Hom}_k(k^S, k^G) & \xrightarrow{\delta_e} & \mathrm{Hom}_k(k^S, k)
\end{array}$$

where δ_e is the map induced from the map $k^G \to k$ "evaluation at e." Thus the composed horizontal map along the bottom is the usual evaluation map appearing in Lemma 6 and in particular is injective. It follows that $\tilde{\epsilon}$ is also injective, as claimed. □

Lemma **??** proves statement (1) of the theorem. Statement (2) follows immediately. Indeed, if A is K-split, let $X := \mathcal{X}(A)$. Then by the lemma $\mathcal{A}(X)$ has dimesion equal to the cardinality of X, which is the dimension of A. But the map $A \to \mathcal{A}(X)$ is injective, hence bijective, and we are done.

Corollary 10 *Let K/k be a finite Galois extension and let A be a finite K-split k-algebra. Then the natural map*

$$K \otimes A \to K^{\mathcal{X}(A)}$$

is an isomorphism of K-algebras and is compatible with the G-actions, where G acts trivially on A.

Proof: Then $K \otimes A$ is a K-algebra, and $\dim_K(K \otimes A) = \dim_k(A)$. Furthermore, $\mathcal{X}(K \otimes A) = \mathcal{X}(A)$. It follows that $K \otimes A$ is K-split. Furthermore the map of K-split K-algebras because it induces an isomorphism after applying $\mathcal{X}$.

□

Proof of the Normal basis theorem: It is clear that the map F_w is k-linear. To check that it is compatible with the G-actions, it is enough to check on the generators. Then

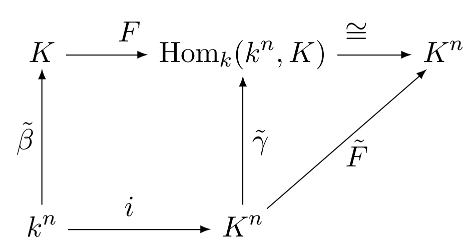
$$F_w(ge_h) = F_w(e_{gh}) = gh(w) = gF_w(e_h),$$

as required.

We prove the existence of w under the assumption that k is infinite. The map $w \to F_w$ is a k-linear map

$$F: K \to \mathrm{Hom}(k^G, K)$$

We claim that for some $w \in K$, $F(w)$ is an isomorphism. Let n be the cardinality of G, and choose an indexing $(g_1, \ldots, g_n)$ of G and a k-basis $(b_1, \ldots, b_n)$ of K. Using the index of G, we identify k^G with k^n. Consider the following diagram:



Here the map $\tilde{\beta}$ is induced by the basis $(b_1, \ldots, b_n)$ of K and i is the inclusion. Let us compute $F \circ \tilde{\beta}$. If e_i is the i^{th} standard basis vector for k^n, $F(\tilde{\beta}(e_i)) = F(b_i)$, which is the map taking g_j to $g_j(b_i)$. Thus the clockwise map from k^n to K^n sends e_i to $(g_1(b_i), \ldots, g_n(b_i))$. We can use the same formula to define $\tilde{F}$ to get the commutative diagram.

Now we claim that $\tilde{F}$ is an isomorphism. It suffices to check that the sequence of vectors $\tilde{F}(e_1), \cdots, \tilde{F}(e_n)$ is linearly independent over K, *i.e.*, that the columns of the matrix $A_{ij} := g_j(b_i)$ are linearly independent. Equivalently, we can check that the rows are linearly independent. Suppose we are given a sequence $(c_1, \ldots c_n)$ in K such that $\sum_j c_j g_j(b_i) = 0$ for all i. Then $\sum_j c_j g_j = 0$ in $\mathrm{End}(K)$, and by the linear independence of the characters, all $c_j = 0$, as required.

It follows that the map $\tilde{\gamma}\colon K^n \to \mathrm{Hom}_k(k^n, K)$ is an isomorphism, and in particular is surjective. But then there is some element $\tilde{w} \in K^n$ such that $\tilde{\gamma}(\tilde{w})$ is an isomorphism $k^n \to K$. Now if we identify K with k^n again we can view $\tilde{\gamma}$ as a linear map from K^n to the set of $n \times n$ matrices with coefficients in k. Then $\det \circ \tilde{\gamma}$ is a polynomial function of the coordinates in K^n, and we have shown that for some $\tilde{w} \in K^n$, $\det(\tilde{\gamma}(\tilde{w})) \neq 0$. This means that the polynomial $\det \circ \tilde{\gamma}$ polynomial is not zero. Since k^n is infinite, there is a point x in k^n at which it does not vanish. Then $F\tilde{\beta}(x)$ is an isomorphism also, and $w := \beta(x)$ is the desired element of K.

Here is a proof when k and K are finite. In this case we know that $\mathrm{Gal}(K/k)$ is cyclic, generated by the Frobenius automorphism ϕ and has order n, where n is the dimension of K over k. View Thus the group algebra $k[G]$ is just $k[t]/(t^n - 1)$, which we view as a quotient of $k[t]$. Then K becomes a $k[t]$-module. Since $k[t]$ is a PID, K is a direct sum of cyclic modules of the form $k[t]/(g_i)$, where $g_1 | g_2 | g_3 \ldots$. Since the minimal polynomial of ϕ is t^{n-1}, $g_1 = (t^n - 1)$. But then $k[t]/(g_1)$ has dimension n, and there can be no other factors. $\square$

Remark 1 It is easily seen that, under the equivalence of categories provided by Theorem 5, a G-set S corresponds to a field if and only if the action of G on S is transitive. More generally, if $A \in \mathcal{A}_{K/k}$ and $s \in \mathcal{X}(A)$, $\mathrm{Ker}(s)$ is a prime ideal of A, so there is a natural map $\mathcal{X}(A) \to \mathrm{Spec}\, A$. Furthermore, if $g \in G$, $\mathrm{Ker}(gs) = \mathrm{Ker}(s)$, and it is easy to check that the induced map from the orbit space $\mathcal{X}(A)/G$ to $\mathrm{Spec}\, A$ is a bijection.

We can easily deduce a strong form of Hilbert's theorem 90 from the above approach. It is most standard to state this in terms of tensor products.

Theorem 11 *Let K/k be a finite Galois extension with group G and let V be a K-vector space equipped with a semi-linear left action of G. (This means a G-action such that $g(av) = g(a)g(v)$ for $a \in K$ and $v \in V$). Then $\Gamma_G(V)$ is a k-vector subspace of V, and the natural map*

$$K \otimes_k \Gamma_G(V) \to V$$

is an isomorphism.

Proof: Observe that as a consequence of Corollary **??**, we get:

Corollary 12 *The natural map*

$$K \otimes_k K \to K^G$$

is an isomorphism of K-algebras, and is compatible with the G-actions, where G acts trivially on one of the two factors of $K \otimes_k K$.

Now it is clear that the natural map

$$K_{triv} \otimes_k \Gamma_G(V) \to \Gamma_G(K_{triv} \otimes_k V)$$

is an isomorphism. On the other hand, multipication defines an isomorphism of K-vector spaces $K_{triv} \otimes_K V \to K_{triv} \otimes_k V$, compatible with the G-actions. Now using the corollary, we get

$$K_{triv} \otimes_k V \cong K^G \otimes_K V \cong V^G.$$

Assembling thse we end up with an isomorphism

$$K_{triv} \otimes_k \Gamma_G(V) \cong \Gamma_G(V^G)$$

sending $a \otimes v$ to the function $g \mapsto g(a)v$. As we saw above, evaluation at the identity element of v defines an isomorphism

$$\Gamma_G(V^G) \to V.$$

Thus we have a commutative diagram:

$$\begin{array}{ccc} K_{triv} \otimes_k \Gamma_G(V) & \xrightarrow{\cong} & \Gamma_G(V^G) \\ & \searrow & \downarrow \cong \\ & & V \end{array}$$

in which the slanted arrow is multiplication. The diagram proves that it is an isomorphism. □