THE ALGEBRA-GEOMETRY DICTIONARY VIA ABSTRACT GALOIS CORRESPONDENCES

STEVEN GLENN JACKSON

1. The correspondence between sets of polynomials and subsets of affine space

Let k be an algebraically closed field. Affine algebraic geometry (over k) begins with the study of a certain correspondence between subsets of n-dimensional affine space k^n and subsets of the polynomial ring $\mathsf{k}[x_1, \ldots, x_n]$, which we now define:

Definition 1.1. Let S be any subset of the n-dimensional affine space k^n. We associate with S the set of polynomials

$$\mathbb{I}(S) = \{f \in \mathsf{k}[x_1, \ldots, x_n] \mid f(\mathbf{a}) = 0 \ \forall \mathbf{a} \in S\}.$$

Similarly, if F is any subset of the polynomial ring $\mathsf{k}[x_1, \ldots, x_n]$ we associate with F the set of points

$$\mathbb{V}(F) = \{\mathbf{a} \in \mathsf{k}^n \mid f(\mathbf{a}) = 0 \ \forall f \in F\}.$$

In other words, we have a map $\mathbb{I}$ from the power set of k^n to the power set of $\mathsf{k}[x_1, \ldots, x_n]$, and a map $\mathbb{V}$ from the power set of $\mathsf{k}[x_1, \ldots, x_n]$ to the power set of k^n:

$$\{\text{Subsets of } \mathsf{k}^n\} \underset{\mathbb{V}}{\overset{\mathbb{I}}{\rightleftarrows}} \{\text{Subsets of } \mathsf{k}[x_1, \ldots, x_n]\}$$

The theory would be most pleasing if $\mathbb{I}$ and $\mathbb{V}$ were inverses of each other; that is, if $\mathbb{I} \circ \mathbb{V}$ and $\mathbb{V} \circ \mathbb{I}$ were both identity maps. However, *neither* composition is the identity map, as the following examples show:

Example 1.2. Take $n = 1$ and $F = \{x^2\}$. Then $\mathbb{V}(F) = \{0\}$ so that $\mathbb{I}(\mathbb{V}(F))$ is the set of all polynomials vanishing at the origin. This coincides with the ideal $\langle x \rangle$ generated by x, which obviously contains many polynomials other than x^2. Thus

$$\mathbb{I}\left(\mathbb{V}\left(\{x^2\}\right)\right) = \mathbb{I}(\{0\}) = \langle x \rangle \neq \{x^2\}.$$

Example 1.3. Take $n = 1$ and $S = \mathsf{k} - \{0\}$. Since k is infinite, any polynomial vanishing on S has infinitely many roots, so it is the zero polynomial. Thus $\mathbb{I}(S) = \{0\}$ and we have

$$\mathbb{V}(\mathbb{I}(\mathsf{k} - \{0\})) = \mathbb{V}(\{0\}) = \mathsf{k} \neq (\mathsf{k} - \{0\}).$$

Notice that in the first example, $\mathbb{I}(\mathbb{V}(F))$ was larger than F itself, and in the second example $\mathbb{V}(\mathbb{I}(S))$ was larger than S itself. In fact we have the following:

Theorem 1.4. *The pair of maps $\{\mathbb{I}, \mathbb{V}\}$ has the following three properties:*

(1) $F \subseteq \mathbb{I}(\mathbb{V}(F))$ *for any* $F \subseteq \mathsf{k}[x_1, \ldots, x_n]$,

---

Date: October 8, 2007.

(2) *$S \subseteq \mathbb{V}(\mathbb{I}(S))$ for any $S \subseteq \mathsf{k}^n$, and*
(3) *the maps $\mathbb{I}$ and $\mathbb{V}$ are both inclusion-reversing.*

(The third condition means that $F_1 \subseteq F_2$ implies $\mathbb{V}(F_1) \supseteq \mathbb{V}(F_2)$ and $S_1 \subseteq S_2$ implies $\mathbb{I}(S_1) \supseteq \mathbb{I}(S_2)$.)

Proof. For (1), choose $f \in F$. It follows from the definition of $\mathbb{V}$ that f annihilates every point of $\mathbb{V}(F)$. Thus $f \in \mathbb{I}(\mathbb{V}(F))$.

For (2), choose $\mathbf{a} \in S$. It follows from the definition of $\mathbb{I}$ that $\mathbf{a}$ is annihilated by every $f \in \mathbb{I}(S)$, so in fact $\mathbf{a} \in \mathbb{V}(\mathbb{I}(S))$.

To see that $\mathbb{I}$ is inclusion-reversing, suppose $S_1 \subseteq S_2$ and choose $f \in \mathbb{I}(S_2)$. Then f annihilates every point of S_2. In particular, it annihilates every point of S_1, so in fact $f \in \mathbb{I}(S_1)$.

Finally, to see that $\mathbb{V}$ is inclusion-reversing, suppose $F_1 \subseteq F_2$ and choose $\mathbf{a} \in \mathbb{V}(F_2)$. Then $\mathbf{a}$ is annihilated by every polynomial in F_2. In particular, it is annihilated by every polynomial in F_1, so it is in $\mathbb{V}(F_1)$. □

The situation described by the theorem arises so frequently in mathematics that it is the subject of a definition. In the next section we will see that the pair $\{\mathbb{I}, \mathbb{V}\}$ is an example of an *abstract Galois correspondence*.

2. Poset isomorphisms and abstract Galois correspondences

Definition 2.1. Let A be a set. A *partial order* on A is a relation on A which is reflexive, antisymmetric, and transitive. A *partially ordered set* (or *poset* for short) is a pair $(A, \leq)$ where A is a set and $\leq$ is a partial order on A.

Example 2.2. If S is any set, then the power set $\mathcal{P}(S)$ is a poset with respect to set inclusion. In particular, the power sets of k^n and $\mathsf{k}[x_1, \ldots, x_n]$ are both posets with respect to set inclusion.

Definition 2.3. Let $(A, \leq)$ and $(B, \leq)$ be posets. An *isomorphism* between A and B is a pair of maps

$$A \underset{g}{\overset{f}{\rightleftarrows}} B$$

such that

(1) $f(g(b)) = b$ for every $b \in B$,
(2) $g(f(a)) = a$ for every $a \in A$, and
(3) f and g are both order-preserving.

(The last condition means that $a_1 \leq a_2$ implies $f(a_1) \leq f(a_2)$ and $b_1 \leq b_2$ implies $g(b_1) \leq g(b_2)$.)

This definition is analogous to that of isomorphism of groups or rings: the first two conditions ensure that f and g are bijective and inverses of one another, while the last condition ensures that they "preserve the structure," in this case the order relation. So we can think of B as a "copy" of A in which the names of elements might be different but the (order) structure is the same.

The situation here is similar to that in Theorem 1.4, but differs from it in two important respects: first, the maps in the theorem do not quite satisfy conditions (1) and (2), and second, the maps in the theorem do not preserve order but reverse it. We consider the latter difference first:

Definition 2.4. Let $(A, \leq)$ and $(B, \leq)$ be posets. An *anti-isomorphism* between A and B is a pair of maps

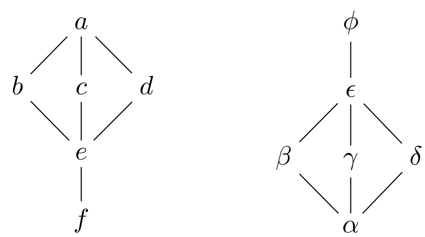
$$A \underset{g}{\overset{f}{\rightleftarrows}} B$$

such that

(1) $f(g(b)) = b$ for every $b \in B$,
(2) $g(f(a)) = a$ for every $a \in A$, and
(3) f and g are both order-reversing.

(The last condition means that $a_1 \leq a_2$ implies $f(a_1) \geq f(a_2)$ and $b_1 \leq b_2$ implies $g(b_1) \geq g(b_2)$.)

Here we can think of B as a copy of A in which the order has been turned upside-down. For example, the posets



are anti-isomorphic. Finally, we define:

Definition 2.5. Let $(A, \leq)$ and $(B, \leq)$ be posets. An *abstract Galois correspondence* between A and B is a pair of maps

$$A \underset{g}{\overset{f}{\rightleftarrows}} B$$

such that

(1) $f(g(b)) \geq b$ for every $b \in B$,
(2) $g(f(a)) \geq a$ for every $a \in A$, and
(3) f and g are both order-reversing.

Example 2.6. The pair $\{\mathbb{I}, \mathbb{V}\}$ is an abstract Galois correspondence between the power set of k^n and the power set of $\mathsf{k}[x_1, \ldots, x_n]$.

An abstract Galois correspondence is not quite an anti-isomorphism since in general f and g are neither injective nor surjective. Consequently, although the order structure is respected, some "collapsing" and "expanding" of the set-theoretic structure may be taking place. However, this happens in a fairly controlled way, as the next few results show:

Lemma 2.7. *Suppose $\{f, g\}$ is an abstract Galois correspondence between A and B. Then*

(1) $g \circ f \circ g = g$, *and*
(2) $f \circ g \circ f = f$.

Proof. For (1), choose $b \in B$. From the definition of an abstract Galois correspondence we have

$$f(g(b)) \geq b.$$

Applying g to both sides and bearing in mind that g is order-reversing we obtain

$$g(f(g(b))) \leq g(b).$$

On the other hand, taking $a = g(b)$ in the definition of an abstract Galois correspondence we obtain

$$g(f(g(b))) \geq g(b).$$

Since $\leq$ is an antisymmetric relation, we conclude that

$$g(f(g(b))) = g(b).$$

The proof of (2) is similar. □

This leads immediately to the following:

Theorem 2.8. *Suppose that*

$$A \underset{g}{\overset{f}{\rightleftarrows}} B$$

is an abstract Galois correspondence, and let $\widetilde{A}$ *and* $\widetilde{B}$ *denote the images of* g *and* f *respectively. Then the restricted maps*

$$\widetilde{A} \underset{g}{\overset{f}{\rightleftarrows}} \widetilde{B}$$

form an anti-isomorphism between the sub-posets $\widetilde{A}$ *and* $\widetilde{B}$*.*

Proof. We need to show that

(1) $f(g(b)) = b$ for every $b \in \widetilde{B}$, and
(2) $g(f(a)) = a$ for every $a \in \widetilde{A}$.

For (1), suppose $b \in \widetilde{B}$. Then we can find some $a \in A$ such that $b = f(a)$. Then the previous lemma gives

$$f(g(b)) = f(g(f(a))) = f(a) = b.$$

The proof of (2) is similar. □

For reasons that will become apparent later (Theorem 3.4), we refer to $\widetilde{A}$ and $\widetilde{B}$ as the sets of *closed elements* of A and B respectively. Characterizing the closed elements is an essential first step in understanding any particular Galois correspondence. Before studying the important *closure operation* in the next section, we give two additional examples of Galois correspondences:

Example 2.9 (The Galois pairing of V and V^*)**.** Let V be a vector space over k, and let V^* be the *dual space* of V, i.e., the set of all linear transformations from V to k. (Note that V^* is again a vector space over k with respect to pointwise addition and scalar multiplication.) Given any set $S \subseteq V$, define the *annihilator of* S *in* V^* by

$$\mathrm{Ann}_{V^*}(S) = \{\lambda \in V^* \mid \lambda(\mathbf{s}) = 0 \ \forall \mathbf{s} \in S\},$$

and similarly, for $T \subseteq V^*$ let

$$\mathrm{Ann}_V(T) = \{\mathbf{v} \in V \mid \tau(\mathbf{v}) = 0 \ \forall \tau \in T\}.$$

Then the pair $\{\mathrm{Ann}_{V^*}, \mathrm{Ann}_V\}$ is an abstract Galois correspondence between the power set of V and the power set of V^*.

Example 2.10 (The classical Galois correspondence)**.** Let E/F be an extension field, and let $\mathrm{Gal}(E/F)$ be its Galois group, i.e., the group of automorphisms of E fixing F pointwise. For any subset $K \subseteq E$, define

$$\gamma(K) = \{g \in \mathrm{Gal}(E/F) \mid g(k) = k \ \forall k \in K\},$$

and for any subset $H \subseteq \mathrm{Gal}(E/F)$ define

$$\phi(H) = \{x \in E \mid h(x) = x \ \forall h \in H\}.$$

Then the pair $\{\gamma, \phi\}$ is an abstract Galois correspondence between the power set of E and the power set of $\mathrm{Gal}(E/F)$.

3. The closure operation

Definition 3.1. Suppose that

$$A \underset{g}{\overset{f}{\rightleftarrows}} B$$

is an abstract Galois correspondence. For any $a \in A$, we define the *closure* of a to be the element

$$\overline{a} = g(f(a)).$$

Similarly, for $b \in B$ we define

$$\overline{b} = f(g(b)).$$

We shall now give a series of definitions and results relating to the closure operations. For concreteness of notation, we shall discuss the closure operation on A; however, note that since the definition of an abstract Galois correspondence is symmetric in A and B, all of our definitions and results carry over word for word to the closure operation on B.

Definition 3.2. An element $a \in A$ is *closed* if $\overline{a} = a$.

Theorem 3.3. *The closure $\overline{a}$ is a closed element of A.*

Proof. We need to show that $\overline{\overline{a}} = \overline{a}$. Using the definition of $\overline{a}$ together with Lemma 2.7 gives

$$\overline{\overline{a}} = g(f(g(f(a)))) = g(f(a)) = \overline{a}.$$

$\square$

Theorem 3.4. *An element $a \in A$ is closed if and only if it belongs to $\widetilde{A}$.*

Proof. Suppose a is closed. Then $a = \overline{a} = g(f(a))$ certainly belongs to the image of g. On the other hand, if $a \in \widetilde{A}$ then choose $b \in B$ with $a = g(b)$. Using Lemma 2.7 we obtain

$$\overline{a} = g(f(a)) = g(f(g(b))) = g(b) = a.$$

$\square$

Theorem 3.5. *Closure is an order-preserving operation, i.e. $a_1 \le a_2$ implies $\overline{a_1} \le \overline{a_2}$.*

Proof. Since f and g are order-reversing, we have

$$a_1 \le a_2 \implies f(a_1) \ge f(a_2) \implies g(f(a_1)) \le g(f(a_2)) \implies \overline{a_1} \le \overline{a_2}.$$

$\square$

Theorem 3.6. *The closure $\overline{a}$ is the smallest closed element greater than or equal to a.*

Proof. That $\overline{a} \geq a$ is part of the definition of an abstract Galois correspondence. It remains only to show that, for any closed element a' with $a \leq a'$ we also have $\overline{a} \leq a'$. To see this, choose any such a'. Then

$$a \leq a' \implies \overline{a} \leq \overline{a'} \implies \overline{a} \leq a'.$$

□

In the next section we shall determine the closed elements and closure operations for the Galois correspondence arising in affine algebraic geometry (Example 2.6).

Exercise 3.7. Determine the closed elements and closure operations for the Galois pairing between V and V^* (Example 2.9), at least in the case where V is finite-dimensional. As a challenge, determine the closed elements and closure operations for the classical Galois correspondence (Example 2.10). (In other words, discover and prove all of the fundamental results of Galois theory.)

4. Closure operations in algebraic geometry: the Hilbert Nullstellensatz

We now return to the situation in Section 1. Recall that we have the Galois correspondence

$$\{\text{Subsets of } \mathsf{k}^n\} \underset{\mathbb{V}}{\overset{\mathbb{I}}{\rightleftarrows}} \{\text{Subsets of } \mathsf{k}[x_1, \ldots, x_n]\}\ .$$

By Theorem 3.4, a closed subset of k^n is a set in the image of $\mathbb{V}$, which by definition is just an affine algebraic variety. So from Theorem 3.6 we immediately obtain

Theorem 4.1. *For any subset $S \subseteq \mathsf{k}^n$, the closure $\overline{S}$ is the smallest affine algebraic variety containing S. (We sometimes refer to $\overline{S}$ as the* Zariski closure *of S.)*

As a reminder, we note that the words "closed" and "closure" are used here in the sense of Section 3, not in the sense of topology. In fact, although it is true that the closed subsets of k^n form a topology on k^n (the so-called *Zariski topology*), we shall see later (Exercise 4.7) that the closed subsets of $\mathsf{k}[x_1, \ldots, x_n]$ do *not* form a topology on $\mathsf{k}[x_1, \ldots, x_n]$.

Determining the closed subsets of $\mathsf{k}[x_1, \ldots, x_n]$ is more difficult. Here are two easy preliminary results:

Theorem 4.2. *Suppose F is a closed subset of $\mathsf{k}[x_1, \ldots, x_n]$. Then F is an ideal.*

Proof. Since F is closed, it lies in the image of $\mathbb{I}$, so we can write $F = \mathbb{I}(S)$ for some $S \subset \mathsf{k}^n$. Clearly the zero polynomial lies in F. If $f_1, f_2 \in F$ then, for any $\mathbf{s} \in S$ we have $f_1(\mathbf{s}) = f_2(\mathbf{s}) = 0$. Consequently $(f_1 + f_2)(\mathbf{s}) = f_1(\mathbf{s}) + f_2(\mathbf{s}) = 0$. Since $\mathbf{s}$ was arbitrary in S this implies that $(f_1 + f_2) \in F$. Similarly, if $f \in F$ and h is any polynomial, then $(hf)(\mathbf{s}) = h(\mathbf{s})f(\mathbf{s}) = 0$ so that $hf \in F$. □

Theorem 4.3. *Suppose F is a closed subset of $\mathsf{k}[x_1, \ldots, x_n]$. If f is a polynomial such that $f^i \in F$ for some non-negative power i, then in fact $f \in F$.*

Proof. Write $F = \mathbb{I}(S)$, and suppose that $f^i \in F$. Then for any $\mathbf{s} \in S$ we have $f^i(\mathbf{s}) = (f(\mathbf{s}))^i = 0$. This implies that $f(\mathbf{s}) = 0$, and since $\mathbf{s}$ was arbitrary in S this means that $f \in F$. □

Ideals with the property described in the previous theorem are called *radical ideals*, since they contain all the ith roots of all of their elements. So we can say that every closed subset of $\mathsf{k}[x_1, \ldots, x_n]$ is a radical ideal. We will soon see (Theorem 4.6) that the closed subsets of $\mathsf{k}[x_1, \ldots, x_n]$ are *precisely* the radical ideals.

Definition 4.4. Let F be any subset of $\mathsf{k}[x_1, \ldots, x_n]$. The *ideal generated by* F, denoted $\langle F \rangle$, is the intersection of all ideals containing F. This is an ideal, and it is the smallest ideal containing F.

Definition 4.5. Let F be any subset of $\mathsf{k}[x_1, \ldots, x_n]$. The *radical* of F is the set

$$\sqrt{F} = \{f \in \mathsf{k}[x_1, \ldots, x_n] \mid f^i \in F \text{ for some } i \geq 0\}.$$

In other words, the radical of a set is the new set obtained by adding all the ith roots of all elements of the set. Using the binomial theorem, one can prove that the radical of an ideal is again an ideal, and that in fact it is a radical ideal.

We are now ready to describe the closure operation on $\mathsf{k}[x_1, \ldots, x_n]$.

Theorem 4.6 (the Hilbert Nullstellensatz). *Let F be any subset of $\mathsf{k}[x_1, \ldots, x_n]$. Then the closure of F is given by*

$$\overline{F} = \sqrt{\langle F \rangle}.$$

Proof. [**?**, Theorem 4.2.6]. □

It follows immediately that every radical ideal is closed. Applying Theorem 2.8, we see that the system of maps

$$\{\text{Algebraic varieties in } \mathsf{k}^n\} \underset{\mathbb{V}}{\overset{\mathbb{I}}{\rightleftarrows}} \{\text{Radical ideals in } \mathsf{k}[x_1, \ldots, x_n]\}\ .$$

is an anti-isomorphism of posets. In particular, *there is a one-to-one correspondence between algebraic varieties in k^n and radical ideals in $\mathsf{k}[x_1, \ldots, x_n]$.*

Exercise 4.7. Show that the radical ideals do *not* form a topology on $\mathsf{k}[x_1, \ldots, x_n]$. *(Hint: consider the union of two radical ideals.)*

5. Corresponding operations and the algebra-geometry dictionary

Definition 5.1. Suppose that

$$A \underset{g}{\overset{f}{\rightleftarrows}} B$$

is an abstract Galois correspondence, that $*$ is a binary operation on A, and that $\star$ is a binary operation on B. We say that $*$ and $\star$ are *corresponding operations* if f and g are homomorphisms of the resulting binary structures; that is, if

$$f(a_1 * a_2) = f(a_1) \star f(a_2)\ \forall a_1, a_2 \in A$$

and

$$g(b_1 \star b_2) = g(b_1) * g(b_2)\ \forall b_1, b_2 \in B.$$

Exercise 5.2. Consider the Galois correspondence

$$\{\text{Subsets of } \mathsf{k}^n\} \underset{\mathbb{V}}{\overset{\mathbb{I}}{\rightleftarrows}} \{\text{Subsets of } \mathsf{k}[x_1, \ldots, x_n]\}\ .$$

Prove that the operation $S * T = S \cap T$ on subsets of k^n corresponds to the operation $F \star G = \sqrt{\langle F \cup G \rangle}$ on subsets of $\mathsf{k}[x_1, \ldots, x_n]$.

The next result shows that it is not always possible to find an operation on B corresponding to a given operation on A:

Theorem 5.3. *Suppose that $*$ and $\star$ are corresponding operations. Then $*$ and $\star$ both take closed elements to closed elements (i.e. if a_1 and a_2 are closed then so is $a_1 * a_2$ and similarly for $\star$).*

Proof. Suppose that a_1 and a_2 are closed. Then by Theorem 3.4 we can find $b_1, b_2 \in B$ with $a_1 = g(b_1)$ and $a_2 = g(b_2)$. But then

$$a_1 * a_2 = g(b_1) * g(b_2) = g(b_1 \star b_2)$$

so that $a_1 * a_2$ is also closed. The proof for $\star$ is similar. □

It follows that if $*$ is an operation on A which does not take closed elements to closed elements then it is impossible to find any corresponding operation on B. However, this difficulty is easy to work around by defining a new operation $\widetilde{*}$ by the formula

$$a_1 \widetilde{*} a_2 = \overline{a_1 * a_2}.$$

It is common to abuse language and say that $*$ and $\star$ are corresponding operations when in fact we mean that $\widetilde{*}$ and $\widetilde{\star}$ are corresponding operations.

Example 5.4. Consider the Galois correspondence

$$\{\text{Subsets of } \mathsf{k}^n\} \underset{\mathbb{V}}{\overset{\mathbb{I}}{\rightleftarrows}} \{\text{Subsets of } \mathsf{k}[x_1, \ldots, x_n]\} \ .$$

The operation $S * T = S - T$ on subsets of k^n does not take closed sets to closed sets since the difference of two varieties need not be a variety. Consequently there is no operation on subsets of $\mathsf{k}[x_1, \ldots, x_n]$ corresponding to $*$. However, we can define a new operation $\widetilde{*}$ by the formula $S \widetilde{*} T = \overline{S - T}$, the smallest variety containing $S - T$. This new operation corresponds to the operation $F \star G = \sqrt{\langle F \rangle} : \sqrt{\langle G \rangle}$ (see [**?**, Section 4.4] and Exercise 5.5 below). We often speak carelessly and say that the colon operation corresponds to set difference.

We can make similar definitions for m-ary operations for any m (e.g. unary and even nullary operations). Finding pairs of corresponding operations is an essential second step in understanding any particular Galois correspondence.

Exercise 5.5. Consider the Galois correspondence

$$\{\text{Subsets of } \mathsf{k}^n\} \underset{\mathbb{V}}{\overset{\mathbb{I}}{\rightleftarrows}} \{\text{Subsets of } \mathsf{k}[x_1, \ldots, x_n]\} \ .$$

Find operations on subsets of $\mathsf{k}[x_1, \ldots, x_n]$ corresponding to the operations of projection, union, intersection, and set difference on subsets of k^n. (In other words, work out the rest of Chapter 4 of [**?**].)

Department of Mathematics, University of Massachusetts, 100 Morrissey Boulevard, Boston, MA 02125-3393

E-mail address: `jackson@math.umb.edu`