Chapter 3

Algebras Over Algebraic Curves

A beautiful result in classical algebraic geometry says that every compact complex manifold admits at most one algebraic structure and that every compact one-dimensional complex manifold has an algebraic structure and hence is unique. This is an application of the celebrated theorem of Chow, that the only complex analytic subsets of the complex projective space are algebraic varieties; see [46, Sec. 4B]. This theorem is an open-arm invitation by algebra to analysis so that algebraic tools are automatically available to analytic subsets of projective space.

A good example of such an analytic subset of the complex projective plane is the so-called elliptic curves: these are compact complex Lie groups. The uniqueness of the group law over elliptic curve states that if $+$ and $\oplus$ are two group laws defined over an elliptic curve and if they have the same identity element, then $x+y = x \oplus y$. This is an easy consequence of the powerful rigidity lemma of projective curves (see [44, 45]).

3.1 What Is a Uniqueness Theorem?

Patterned after this uniqueness of group laws, we formulate the natural concept of a *uniqueness theorem*: Let $\mathcal{A}$ be a mathematical structure, F a class of functions defined on $\mathcal{A}$, and Σ a set of sentences in the first-order theory of a given type, say τ. A uniqueness theorem for the triple $\langle \mathcal{A}, F, \Sigma \rangle$ states that if f and g are two n-ary functions belonging to the class F and if the reducts $\langle \mathcal{A}; f \rangle$ and $\langle \mathcal{A}; g \rangle$ both satisfy the properties in Σ, then $f = g$. See Table 3.1 for examples.

Table 3.1: Examples of Uniqueness of Algebraic Laws

Mathematical System $\mathcal{A}$	Class of Functions F	Laws Σ	Status
Elliptic curves	morphisms	group laws	True
Elliptic curves	n-ary morphisms	n-ary Steiner laws	True [a]
Elliptic curves	n-ary morphisms	n-group laws	Open
Elliptic curves	ternary morphisms	Mal'cev laws	True
Groups	group words	group laws	False
Abelian groups	group words	group laws	True
R, real field	polynomials	group laws	True
R, real field	polynomials	Mal'cev + cancel.	True
R, real field	polynomials	Steiner laws	True
C, complex field	polynomials	Steiner laws	False
$R \times R$, the plane	ring polynomials	group laws	True
$R \times R$, the plane	ring polynomials	Mal'cev + cancel.	Open
$R \times R$, the plane	ring polynomials	Steiner laws	Open
$R \times R \times R$	ring polynomials	group laws	False [b]
Unit circle	continuous	group laws	True [c]
Unit circle	continuous	Mal'cev laws	Open
Join semilattice	binary functions	lattice meet	True
Join semilattice	binary functions	quasilattice meet	False [d]
$\{x+x=x, x+y=y+x\}$	binary functions	WA-lattice meet	True [e]
$\{x+x=x, x+y=y+x\}$	binary functions	TN-lattice meet	False [f]

[a] First proved by OTTER for the cases $n = 5, 8$; see Sec. 3.5.

[b] For example, $(x_1, x_2, x_3) + (y_1, y_2, y_3) = (x_1 + y_1, x_2 + y_2 + x_1 + y_3, x_3 + y_3)$ is a non-commutative group law defined on $R \times R \times R$.

[c] A rule of inference analogous to (gL) is not known for continuous functions on circles.

[d] Example obtained by MACE; see Example QLT-7.

[e] First proof obtained by OTTER; see Thm. WAL-2.

[f] Example obtained by MACE; see Example TNL-2.

3.1.1 The Rigidity Lemma

An elliptic curve, viewed as a plane algebraic curve in the complex projective plane, is given by a nonsingular cubic equation. In this chapter, we bring out the equational properties of the algebraic laws naturally definable on cubic curves (i.e., by means of synthetic constructions) from the point of view of equational logic. One may wonder what equational logic—a topic in universal algebra—has to do with cubic curves—a topic in classical algebraic geometry.

The subject of elliptic curves ignores interdisciplinary boundaries; it is a place where rationally defined quasigroup laws, certain combinatorial configurations, formal groups, number theory, incidence theorems, and coding theory all happily coexist. We say that an algebraic curve Γ admits an algebraic law (of arity n), if there exists an n-ary morphism $(x_1, x_2, \cdots, x_n)$ on the curve Γ; that is, $(x_1, x_2, \cdots, x_n)$ is the completion of a regular function on the product set $\Gamma_n = \Gamma \times \Gamma \times \cdots \times \Gamma$. The nonsingular cubic curves are ripe with a number of such algebraic laws all of which are morphisms of the curve. For example, the famous Cayley-Bacharach theorem of classical algebraic geometry says that every algebraic curve induces a rational operation on cubic curves via a complete intersection cycle (e.g., see Fig. 3.6, p. 57 for the 5-ary conic process). Let us list a few equational properties enjoyed by such algebraic laws defined on nonsingular cubic curves.

1. Any two group laws sharing the same identity element are equal.
2. Any group law definable on an elliptic curve must be commutative.
3. Every quasigroup law definable on such a curve gives rise to a group law.
4. Every cancellative di-associative groupoid on an elliptic curve must be associative.
5. Every groupoid having a two-sided identity element is a group law.
6. Any two binary Steiner quasigroup laws having a common idempotent are equal; that is,
$$\left\{\begin{array}{l} f(x, f(y,x)) = y,\ f(e,e) = e \\ g(x, g(y,x)) = y,\ g(e,e) = e \end{array}\right\} \overset{(gL)}{=\!\!\Longrightarrow} \{f(x,y) = g(x,y)\}.$$
7. Any two 5-ary Steiner quasigroup laws having a common idempotent are equal (see Lem. UAL-6 below for details).

One of the purposes of this project is to develop a new geometric theorem-prover based on certain local-to-global principles of classical algebraic geometry so that we can formulate and prove properties like the above purely within the realm of first-order logic with equality. To this end we need additional context-sensitive rules of inference. One such rule is the famous rigidity lemma for the morphisms of projective curves, in particular for elliptic curves (see, e.g., [44, p. 104], [45, p. 43], or [64, p. 152]):

$$\exists y_0 z_0 \forall \mathbf{x}(f(\mathbf{x}, y_0) = z_0) \Rightarrow \forall \mathbf{x}\mathbf{z}y(f(\mathbf{x}, y) = f(\mathbf{z}, y)) \qquad \text{(rigidity)}$$

That is, from local equality $f(\mathbf{x}, y_0) = z_0$ for some term f and some elements y_0, z_0, we can derive the global multivariable identity $f(\mathbf{x}, y) = f(\mathbf{z}, y)$, in which $\mathbf{x}$ and $\mathbf{z}$ can be a vectors of variables.

On an elementary level, the rigidity lemma is clearly valid for the so-called affine algebras: $p(x_1, x_2, \cdots, x_m) = n_i x_i + k$, where the n_i's are group homomorphisms of a group $\langle G; +\rangle$. The rigidity lemma says essentially that if an identity happens to be true in a dense open subset of a topological space, then it is globally valid.

In fact, this is the essence of almost all proofs of the associativity of the group law on cubics (see, e.g., [62, p. 36]): one first proves the associativity for distinct points (using, say the Bezout theorem), then notices that $+$ being a morphism is a continuous function, then appeals to the continuity to extend the validity of the associativity to all points, that is, the two ternary continuous functions $(x+y)+z$ and $x+(y+z)$ agree on a dense open subset of the curve and hence they agree everywhere. Such local-to-global principles have been well known in function theory and algebraic geometry for a long time.

3.1.2 Applications to Cubic Curves

As an example of the rigidity lemma let us show a rather syntactic proof of the powerful four-variable median law $(xy)(zu) = (xz)(yu)$ for the classical binary morphism of chord-tangent construction (Fig. 3.2) on nonsingular cubics from just the relatively weak two-variable Steiner quasigroup laws $\{x(yx) = y,\ (yz)z = y\}$ without any reference to the geometry or the topology of curves.

Theorem MED-2. Median law for chord-tangent construction (1).

$$\left\{ \begin{array}{l} x(yx) = y \\ (yz)z = y \end{array} \right\} \Longleftarrow\!\!\text{(rigidity)}\!\!\Longrightarrow \{(xy)(zw) = (xz)(yw)\}.$$

Proof. Define the 5-ary composite operation f by

$$f(x,y,z,w,u) = ((xy)(zw))(u((xz)(yw))).$$

Now we have, by the law $x(yx) = y$, $f(x,y,y,w,u) = u$ for all x. Thus by the rigidity property, the 5-ary expression $f(x,y,z,w,u)$ does not depend upon x for all y,z,w,u. In particular, we have

$$\begin{array}{lll} f(x,y,z,w,u) & = f(x_1,y,z,w,u) & \forall x \forall x_1 \\ ((xy)(zw))(u((xz)(yw))) & = ((x_1y)(zw))(u((x_1z)(yw))) & \forall x \forall x_1 \\ & = (((yz)y)(zw))(u(((yz)z)(yw))) & \text{letting } x_1 = yz \\ & = w(uw) & \text{by the Steiner laws} \\ & = u & \\ & = ((xz)(yw))(u((xz)(yw))) & \end{array}$$

and hence one right-cancellation of the common term $(u((xz)(yw)))$ immediately yields the desired median law $(xy)(zw) = (xz)(yw)$. Q.E.D.

Since a nonsingular cubic curve defined over an algebraically closed field is a projective curve and since the chord-tangent law of composition obviously satisfies the Steiner laws, we have the following.

Corollary. *The classical binary morphism of chord tangent construction defined on a nonsingular cubic curve is medial* (see Fig. 3.1).

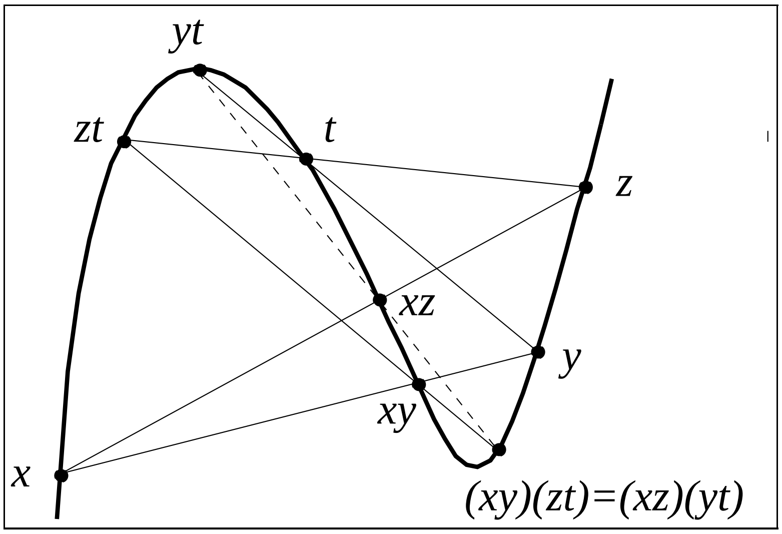

Figure 3.1: The Median Law

Historical remark. This important identity for cubics is usually proved by using some sophisticated machinery such as the Bezout theorem, the Riemann-Roch theorem, or Weierstrass elliptic functions. It was first proved for plane cubic curves by I. M. S. Etherington using the Bezout theorem (see [9]). In [51], Padmanabhan gave a proof for elliptic curves over an arbitrary algebraically closed field. See also an elaborate proof of this identity by using the important concept of intersection multiplicities in [22, pp. 68–70]. The associativity of the classical group law is a simple consequence of this identity. Now let us connect this basic binary operation of chord-tangent construction with the classical group law on elliptic curves.

It turns out that the rigidity property is closely related to the so-called "term condition", a universally quantified implication recently discovered in universal algebra while attempting to generalize the group theory concept of commutators to modular congruence varieties (for a history and comparison, see [61] and [40, Abelian algebras]). In fact, modulo nonsingular cubic curves over an algebraically closed field, these two properties turn out to be equivalent (see Thm. 3.3 below). Thus, hindsight suggests that the term condition, called (gL) here (for "geometric Logic") does not originate in universal algebra but rather comes from the classical algebraic geometry of complex projective varieties. After all, the uniqueness of group law for elliptic curves has been known for a long time.

The following three properties are of interest to us.

$$F(\mathbf{x}, b) = c \ \Rightarrow\ F(\mathbf{x}, z) = F(\mathbf{y}, z) \qquad \text{(rigidity)}$$
$$F(a, \mathbf{x}) = F(a, \mathbf{y}) \ \Rightarrow\ F(z, \mathbf{x}) = F(z, \mathbf{y}) \qquad \text{(weak-}gL)$$
$$F(a, b) = F(a, c) \ \Rightarrow\ F(z, b) = F(z, c) \qquad (gL)$$

Here, $\mathbf{x}$, and $\mathbf{y}$ are vectors of variables, and a, b, and c are terms not containing members of $\mathbf{x}$ or $\mathbf{y}$. It is clear that $(gL) \Rightarrow$ (weak-gL) $\Rightarrow$ (rigidity).

Theorem 3.1. *Let C be an elliptic curve in the complex projective plane. Then the morphisms of C satisfy the property* (weak-gL).

Proof. Without loss of generality we can assume that C is a nonsingular cubic curve, because it is well-known that there always exists a biregular correspondence between an elliptic curve and a smooth cubic in the complex projective plane (e.g., [46, Corollary 7.8]).

Let $F : C \times C \longrightarrow C$ be a binary morphism such that $F(a, x) = F(a, y)$ for some point a in C. Form the composite ternary morphism $f : C \times C \times C \longrightarrow C$ by the rule $f(x, y, z) = (F(z, x) \cdot e) \cdot F(z, y)$ where '$\cdot$' is the synthetic binary morphism of chord-tangent construction on the cubic, and e is an inflection point which we choose to be the origin of the group law. Now,

$$\begin{aligned} f(x, y, a) &= (F(a, x) \cdot e) \cdot F(a, y) \\ &= (F(a, x) \cdot e) \cdot F(a, x) && [\text{since } F(a, x) = F(a, y)] \\ &= e && [\text{since } (u \cdot e) \cdot u = e] \end{aligned}$$

Thus we have

$$f(x, y, a) = e \qquad [\forall x, y \in C]$$

and hence,

$$\begin{aligned} f(x, y, z) &= f(u, v, z) && [\text{by rigidity}] \\ &= f(e, e, z) && [\text{letting } v = u = e] \\ &= (F(z, e) \cdot e) \cdot F(z, e) \\ &= e \end{aligned}$$

In other words, $(F(z, x) \cdot e) \cdot F(z, x) = (F(z, x) \cdot e) \cdot F(z, y)$ and thus, after one left cancellation, we get the desired equality $F(z, x) = F(z, y)$ for all x, y and z. Q.E.D.

Let us illustrate this deduction procedure with one typical example. Suppose we wish to find all binary morphisms $s(x, y)$ of an elliptic curve $\langle C; e\rangle$ satisfying the two equational identities $s(x, e) = x$ and $s(x, x) = e$. One obvious candidate for $s(x, y)$ is subtraction $x - y$, where the corresponding group addition has e as its identity. It turns out that this is the only possibility.

Theorem 3.2.

$$\left\{ \begin{array}{l} s(x, e) = x \\ s(x, x) = e \end{array} \right\} = \!\!(\text{rigidity})\!\!\Rightarrow \{s(x, y) = x - y\},$$

where $x - y$ is the usual subtraction on C corresponding to the group law $+$ having e as its identity element.

First Proof. Define $F(x, z) = s(x, s(x, z))$. We have $F(x, e) = s(x, s(x, e)) = s(x, x) = e$. Hence, by the rigidity property, we have $F(x, z) = F(y, z)$ for all x, y and z. In particular, we have $F(x, z) = F(z, z) = s(z, (s(z, z)) = s(z, e) = z$. Thus we have $s(x, s(x, z)) = z$. Now define $m(x, y) = s(x, s(e, y))$. It is clear that $m(x, e) = x$ and $m(e, y) = s(e, s(e, y)) = y$. Appealing to [45, appendix to

Sec. 4], we obtain the equality $m(x,y) = x + y$, the unique group law with e as its identity. Thus $s(x, s(e,y)) = x + y$. Now,

$$x + s(e,x) = s(x, s(e, s(e,x))) = s(x,x) = e$$

and hence $s(e,x) = -x$. Finally, $x - y = x + (-y) = s(x, s(e,-y) = s(x, s(e, s(e,y))) = s(x,y)$. Q.E.D.

Second Proof. See Thm. ABGT-5 (p. 62) where OTTER shows that $\{s(x,e) = x, s(x,x) = e\}$ is a (gL)-basis for the equational theory of Abelian groups where $s(x,y) = x - y$.

Theorem 3.3. *Let C be a nonsingular cubic curve in the complex projective plane. Then the morphisms of C satisfy the rule (gL).*

Proof. Let F be an arbitrary binary morphism of a nonsingular cubic curve $\langle C; e\rangle$ and let $F(a,b) = F(a,c)$. Form the composite 4-ary morphism $h(x,y,z,u) = F(x,y) \cdot (u \cdot F(x,z))$. Now, $h(x,e,e,e) = F(x,e) \cdot (e \cdot F(x,e)) = e$ and hence, by rigidity, $h(x,y,z,u) = h(w,y,z,u)$ and thus it does not depend upon x. Thus, in particular, we have the equality $F(x,y) \cdot (u \cdot F(x,z)) = F(a,y) \cdot (u \cdot F(a,z))$. So,

$$\begin{aligned} F(x,b) \cdot (u \cdot F(x,c)) &= F(a,b) \cdot (u \cdot F(a,c)) \\ &= F(a,c) \cdot (u \cdot F(a,c)) \\ &= u \\ &= F(x,c) \cdot (u \cdot F(x,c)). \end{aligned}$$

Since '$\cdot$' is cancellative on both sides, we immediately get the desired equality $F(x,b) = F(x,c)$. Q.E.D.

The property (gL) is implemented as an inference rule in OTTER (see Sec. 2.2.4 for details), and we write $=\!\!(gL)\!\!\Rightarrow$ for model-theoretic consequence under (gL). The rule derives an equation from an equation, so it is strictly within the language of equational logic, yet it captures the essence of the rigidity principle valid for complex projective curves. Using the rule, OTTER can find formal equational proofs for the uniqueness of many geometrically constructed operations over nonsingular cubic curves and obtain elegant equational characterizations for these synthetic geometric constructions. It is this blend of universal algebra, algebraic geometry, and computer science on which we focus; it provides a rich source of examples for universal algebra and a new equational tool for algebraic geometry.

We now present in detail one example of a (gL)-derivation. One of the beauties of the group law on a nonsingular cubic curve C is that it is harmoniously blended with the geometry on the curve; in particular, $a + b + c = e$ if and only if there exists a line L such that $C \cap L = \{a,b,c\}$. Expressing this in our algebraic language, we have $a + b = e \cdot (a \cdot b)$. In [45, appendix to Sec. 4], D. Mumford and C. P. Ramanujam show that if $m(x,y)$ is a binary morphism of a complete variety and if m admits a two-sided identity then it must be an Abelian group morphism. We capture a fragment of this deep theorem in the following implication.

$$\left\{ \begin{array}{l} m(x,e) = x \\ m(e,x) = x \\ x \cdot (y \cdot x) = y \\ x \cdot y = y \cdot x \end{array} \right\} =\!\!(gL)\!\!\Rightarrow \{m(x,y) = e \cdot (x \cdot y)\}.$$

(Note that the hypotheses assert no connection at all between m and '$\cdot$'.)

Proof (found by Otter 3.0.4 on gyro at 8.07 seconds).

2	$m(x,e) = x$	
3	$m(e,x) = x$	
4	$x \cdot (y \cdot x) = y$	
5	$x \cdot y = y \cdot x$	
6	$m(A,B) \neq e \cdot (A \cdot B)$	
11	$m(e,x) \cdot (y \cdot x) = y$	[3 → 4]
17	$x \cdot m(e, y \cdot x) = y$	[3 → 4]
28,27	$m(e, x \cdot y) = y \cdot x$	[3 → 5]
29	$x \cdot (x \cdot y) = y$	[17 :28]
35	$m(x,y) \cdot (z \cdot y) = m(x,u) \cdot (z \cdot u)$	[11 → 11 :(gL)]
53	$x \cdot (y \cdot e) = m(x,z) \cdot (y \cdot z)$	[2 → 35]
106	$m(x,y) \cdot (m(x,z) \cdot y) = z$	[35 → 29]
180,179	$m(x,y) \cdot (z \cdot y) = x \cdot (e \cdot z)$	[5 → 53, flip]
194	$x \cdot (e \cdot m(x,y)) = y$	[106 :180]
225	$e \cdot m(x,y) = x \cdot y$	[194 → 29, flip]
231	$m(x,y) = e \cdot (x \cdot y)$	[225 → 29, flip]
233	$\square$	[231,6]

In Thm. ABGT-3 (p. 48), we show as well that each element has an inverse.

The logic of this project is now clear. First we transform the geometric concepts and statements associated with an elliptic curve into equivalent algebraic ones via a system of equational definitions. See Fig. 3.2 and Table 3.2.

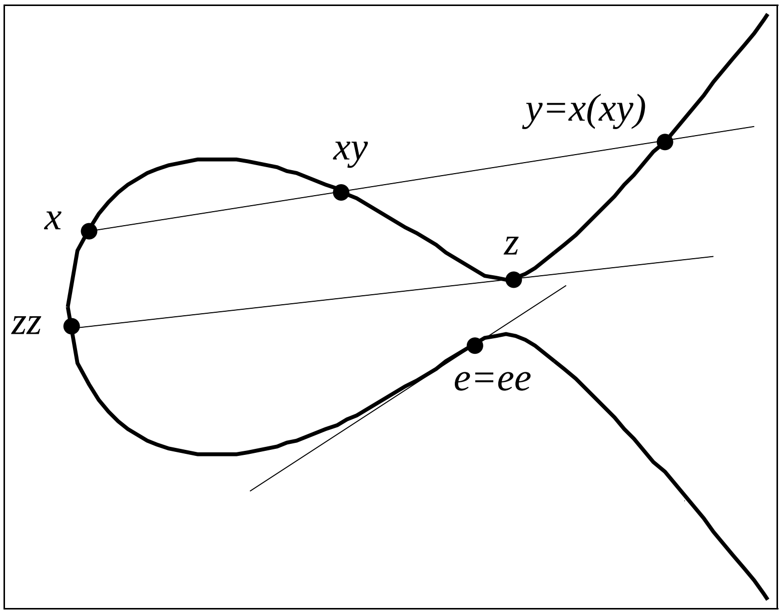

Figure 3.2: Chord-Tangent Operation on a Cubic Curve

Table 3.2: Equationally Definable Concepts in Cubic Curves

Geometry	Algebra
Points	elements
Chords	$\{(P,Q) \mid P,Q$ elements$\}$
Tangents	$\{(P,P) \mid P$ an element$\}$
P,Q,R collinear	$R = P \cdot Q$
P lies on the tangent at Q	$P = Q \cdot Q$
Inflection point	$\{P \mid P \cdot P = P\}$ (idempotent elements)
Singular point	$\{P \mid \forall Q,\ P \cdot Q = P\}$ (absorbing element)
Nonsingular curve	no absorbing elements
Conic	$\{(P,Q,R,S,T)\}$ (all 5-tuples)
Sextatic point P	$\{P \mid ((P \cdot P) \cdot (P \cdot P)) \cdot P = P\}$
Configuration theorem	equation or implication
Bitangents PQ	$2P + 2Q = 0$ under the induced group law (for elliptic quartics)

After transforming the geometric statements into the language of algebra, we formally derive the equational conditions that correspond to the required geometric conclusions. Let us start with a simple example of a well-known geometric property.

The following configuration theorem is a simple consequence of a Steiner law and (gL). The conclusion $S \cdot S = R \cdot Q$ means that the tangent at S and the