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.

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. 55 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,
$$\left\{ \begin{array}{l} f(x, f(y, x)) = y, \; f(e, e) = e \\ g(x, g(y, x)) = y, \; g(e, e) = e \end{array} \right\} \stackrel{(gL)}{=\!\!\Longrightarrow} \{f(x, y) = g(x, y)\}.$$
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-sensitve 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]):

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

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

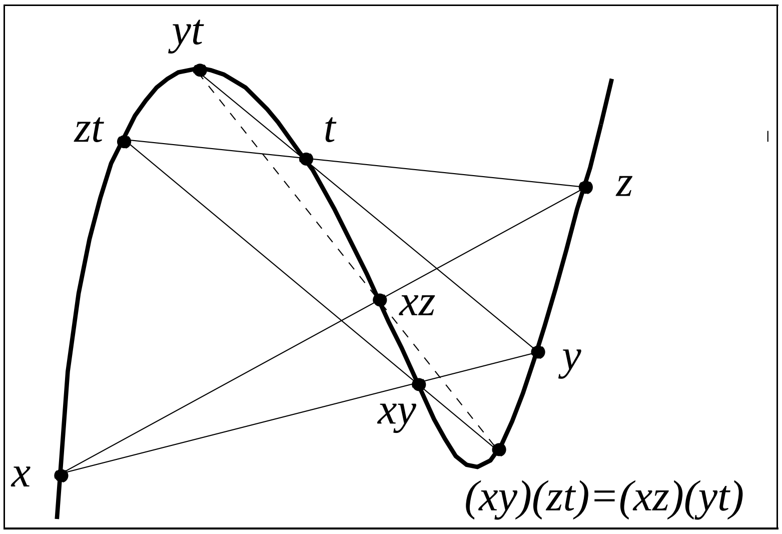

Figure 3.1: The Median Law

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, which we also call (weak-gL), is closely related to the *term condition*, an implication recently discovered in universal algebra (for a history and comparison, see [61]):

$$F(a, \mathbf{x}) = F(a, \mathbf{y}) \ \vdash \ F(z, \mathbf{x}) = F(z, \mathbf{y}) \qquad (gL)$$

That is, if $F(a, \mathbf{x}) = F(a, \mathbf{y})$ for some term a, then derive $F(z, \mathbf{x}) = F(z, \mathbf{y})$, where z is a new variable. It is clear that the term condition implies the rule (weak-gL). In fact, for the morphisms of elliptic curves over an algebraically closed field, the term condition and (weak-gL) are equivalent.

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

Proof. Without loss of generality we can assume that C is a nonsingular cubic curve, since it is well known that a complex elliptic curve is birationally equivalent to a nonsingular cubic curve, say, obtained via the classical parameterization by the elliptic functions of Weierstrass.

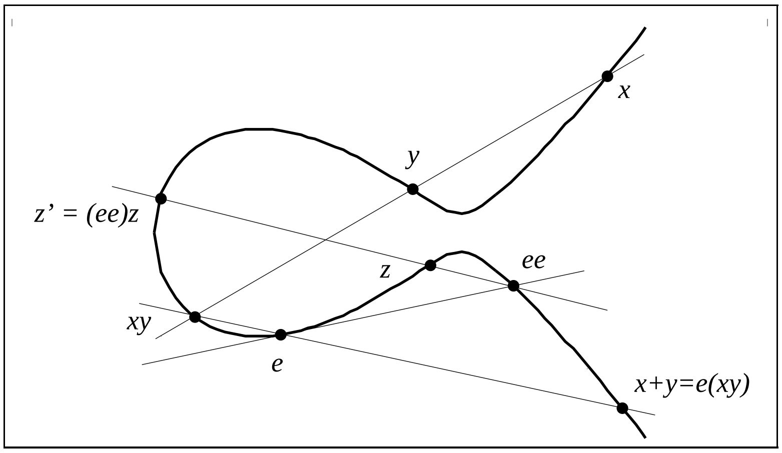

Figure 3.5: A Group $\langle G; +,', e\rangle$ on a Cubic Curve

Putting together Thms. ABGT-2 and ABGT-3, we have the following.

Corollary ABGT-3a. Mumford-Ramanujam theorem for elliptic curves.
If $m : C \times C \longrightarrow C$ is a binary morphism of a nonsingular cubic curve C defined over the complex projective plane, and if for some e in C, $m(x, e) = m(e, x) = x$ for all x, then the structure $\langle C; m, e\rangle$ is an Abelian group.

This is a special case of a result of D. Mumford and C. P. Ramanujam that any complete variety with a binary morphism admitting a two-sided identity must be an Abelian group variety [45, appendix to Sec. 4].

3.4 Uniqueness of Group Laws

Theorem UAL-1. Uniqueness of inversive groupoids under (gL).
(Note that the two group operations have the same identity element.)

$$\left\{\begin{array}{ll} f(e,x) = x, & F(e,x) = x \\ f(x,e) = x, & F(x,e) = x \\ f(g(x),x) = e, & F(G(x),x) = e \\ f(x,g(x)) = e, & F(x,G(x)) = e \end{array}\right\} \overset{(gL)}{\Longrightarrow} \left\{\begin{array}{l} f(x,y) = F(x,y) \\ g(x) = G(x) \end{array}\right\}.$$

Proof (found by Otter 3.0.4 on gyro at 13.58 seconds).

2 $f(e, x) = x$
3 $f(x, e) = x$
4 $f(g(x), x) = e$
5 $f(x, g(x)) = e$
6 $F(e, x) = x$
7 $F(x, e) = x$

8	$F(G(x),x)=e$	
9	$F(x,G(x))=e$	
10	$f(A,B)=F(A,B),\ g(A)=G(A)\ \rightarrow\ \Box$	
28,27	$f(x,e)=F(e,x)$	[3 → 6, flip]
32,31	$f(e,x)=F(e,x)$	[2 → 6, flip]
40	$F(e,x)=F(x,e)$	[7 → 6]
41	$f(g(F(x,e)),x)=e$	[7 → 4]
43	$f(g(x),F(x,e))=e$	[7 → 4]
82	$f(x,F(e,g(x)))=e$	[6 → 5]
94,93	$F(x,f(y,g(y)))=x$	[5 → 7]
112,111	$G(e)=e$	[5 → 8 :94]
139,138	$G(F(G(x),x))=e$	[8 → 111]
144	$F(e,g(e))=e$	[111 → 5 :112,32]
176	$F(G(x),x)=F(y,G(y))$	[9 → 8]
184,183	$F(F(x,G(x)),y)=y$	[9 → 6]
186,185	$g(e)=e$	[9 → 144 :184]
214,213	$f(F(G(x),x),y)=F(e,y)$	[8 → 31]
231	$f(g(F(x,y)),x)=f(g(F(z,y)),z)$	[41 → 41 :(gL)]
236,235	$f(g(F(x,y)),x)=F(e,g(y))$	[9 → 231 :184,28, flip]
243	$F(e,g(F(x,e)))=F(e,g(x))$	[40 → 231 :28,236]
248,247	$F(e,g(x))=F(e,G(x))$	[8 → 231 :186,32,236, flip]
268,267	$F(x,g(F(y,e)))=F(x,g(y))$	[243 :(gL)]
277	$f(x,F(e,G(x)))=e$	[82 :248]
289	$f(g(x),F(x,y))=f(g(z),F(z,y))$	[43 → 43 :(gL)]
291,290	$g(x)=F(e,G(x))$	[9 → 267 :268,184,248]
292	$f(F(e,G(x)),F(x,y))=f(F(e,G(z)),F(z,y))$	[289 :291,291]
311	$f(A,B)=F(A,B)\ \rightarrow\ \Box$	[10 :291 :6]
312	$f(F(A,e),B)=F(A,B)\ \rightarrow\ \Box$	[7 → 311]
350,349	$f(x,G(x))=e$	[9 → 277 :184]
409	$f(F(x,G(y)),F(y,z))=f(F(x,G(u)),F(u,z))$	[292 :(gL)]
443,442	$f(F(x,G(y)),F(y,z))=f(F(x,e),F(e,z))$	[349 → 409 :350,112, flip]
446,445	$f(F(x,e),F(e,y))=f(F(x,e),y)$	[176 → 409 :139,184,443, flip]
449,448	$f(F(x,e),y)=F(e,F(x,y))$	[176 → 409 :214,443,446, flip]
478	$F(e,F(A,B))=F(A,B)\ \rightarrow\ \Box$	[312 :449]
479	$\Box$	[478,6]

Corollary UAL-2. Uniqueness of group laws under (gL).

By Thm. UAL-1, there do not exist two distinct (gL)-groups with the same identity element.

Theorem MCV-1. Associativity of Mal'cev polynomial under (gL).

$$\left\{\begin{array}{l} m(x,y,y)=x \\ m(x,x,y)=y \end{array}\right\} \overset{(gL)}{\Longrightarrow} \{m(x,y,m(z,u,v))=m(v,u,m(x,y,z))\}.$$

Proof (found by Otter 3.0.4 on gyro at 17.08 seconds).

2	$m(x,y,y) = x$	
3	$m(x,x,y) = y$	
4	$m(A,B,m(C,D,E)) \neq m(E,D,m(A,B,C))$	
25	$m(x,x,y) = m(y,z,z)$	$[2 \to 3]$
70	$m(x,y,z) = m(z,y,x)$	[(gL) 25]
98	$m(x,x,m(y,z,u)) = m(u,z,y)$	$[3 \to 70]$
99	$m(m(x,y,z),u,u) = m(z,y,x)$	$[2 \to 70]$
135	$m(m(C,D,E),B,A) \neq m(E,D,m(A,B,C))$	$[70 \to 4]$
183	$m(x,y,m(z,u,y)) = m(x,u,z)$	[(gL) 98]
291	$m(m(x,y,z),x,u) = m(z,y,u)$	[(gL) 99]
304	$m(m(x,y,z),u,v) = m(z,y,m(v,u,x))$	$[183 \to 291]$
305	$\square$	[304,135]

Theorem UAL-3. Uniqueness of Mal'cev law under (gL).

The type is $\langle 3,3\rangle$ with two ternary operations m_1 and m_2.

$$\left\{ \begin{array}{l} m_1(x,y,y) = x,\ \ m_1(x,x,z) = z \\ m_2(x,y,y) = x,\ \ m_2(x,x,z) = z \end{array} \right\} \overset{(gL)}{=\!\!\Rightarrow} \{m_1(x,y,z) = m_2(x,y,z)\}.$$

Proof (found by Otter 3.0.4 on gyro at 103.43 seconds).

2	$m_1(x,y,y) = x$	
3	$m_1(x,x,z) = z$	
4	$m_2(x,y,y) = x$	
5	$m_2(x,x,z) = z$	
6	$m_2(A,B,C) \neq m_1(A,B,C)$	
15	$m_1(x,x,y) = m_1(y,z,z)$	$[2 \to 3]$
30	$m_1(x,y,m_2(y,z,z)) = x$	$[4 \to 2]$
37	$m_2(x,x,y) = m_2(y,z,z)$	$[4 \to 5]$
51	$m_1(x,y,z) = m_1(z,y,x)$	[(gL) 15]
52	$m_1(x,y,m_2(z,z,u)) = m_1(u,y,x)$	$[5 \to 51$, flip]
60	$m_2(x,y,z) = m_2(z,y,x)$	[(gL) 37]
65	$m_2(x,x,m_2(y,z,u)) = m_2(u,z,y)$	$[5 \to 60]$
71	$m_1(x,y,m_2(z,z,u)) = m_1(u,y,m_2(v,v,x))$	$[5 \to 52]$
419	$m_2(x,y,m_2(z,x,u)) = m_2(u,y,z)$	[(gL) 65]
516	$m_2(x,y,m_2(y,x,z)) = z$	$[4 \to 419]$
937	$m_1(x,y,m_2(z,u,v)) = m_1(v,y,m_2(z,u,x))$	[(gL) 71]
964	$m_1(x,y,m_2(y,x,z)) = z$	$[30 \to 937$, flip]
989	$m_2(x,y,z) = m_1(x,y,z)$	$[516 \to 964$, flip]
990	$\square$	[989,6]

Appendix A

Theorems Proved

We list here the results that are new and interesting to us. Some are entirely new, and some are new kinds of proof for previously known theorems.

A.3 Algebras over Algebraic Curves

Theorem MED-2 (p. 34). Median law for chord-tangent construction (1).

Theorem MED-4 (p. 42). Median law for chord-tangent construction (3).

Theorem MED-5 (p. 43). Median law for four group operations.

Theorem ABGT-2 (p. 45). Identity with (gL) is a commutative monoid.

Theorem ABGT-3 (p. 46). Existence of inverses under (gL).

Corollary ABGT-3a (p. 47). Mumford-Ramanujam theorem for elliptic curves.

Theorem UAL-1 (p. 47). Uniqueness of inversive groupoids under (gL).

Theorem MCV-1 (p. 48). Associativity of Mal'cev polynomial under (gL).

Theorem UAL-3 (p. 49). Uniqueness of Mal'cev law under (gL).

Theorem UAL-4 (p. 50). Uniqueness of binary Steiner law under (gL).

Theorem UAL-6 (p. 53). Uniqueness of 5-ary Steiner law under (gL).

Corollary UAL-7 (p. 55). A ruler construction for cubic and conic.

[32] W. McCune. Single axioms for the left group and right group calculi. *Notre Dame J. Formal Logic*, 34(1):132–139, 1993.

[33] W. McCune. A Davis-Putnam program and its application to finite first-order model search: Quasigroup existence problems. Tech. Memo. ANL/MCS-TM-194, Argonne National Laboratory, Argonne, Ill., 1994.

[34] W. McCune. Models And Counter-Examples (MACE). http://www.mcs.anl.gov/home/mccune/ar/mace/, 1994.

[35] W. McCune. OTTER 3.0 Reference Manual and Guide. Tech. Report ANL-94/6, Argonne National Laboratory, Argonne, Ill., 1994.

[36] W. McCune and R. Padmanabhan. Single identities for lattice theory and for weakly associative lattices. Preprint MCS-P493-0395, Argonne National Laboratory, Argonne, Ill., 1995.

[37] W. McCune and L. Wos. The absence and the presence of fixed point combinators. *Theoretical Computer Science*, 87:221–228, 1991.

[38] W. McCune and L. Wos. Application of automated deduction to the search for single axioms for exponent groups. In A. Voronkov, editor, *Logic Programming and Automated Reasoning, Springer-Verlag Lecture Notes in Artificial Intelligence, Vol. 624*, pages 131–136, New York, July 1992. Springer-Verlag.

[39] R. N. McKenzie. Equational bases for lattice theories. *Math. Scand.*, 27:24–38, 1970.

[40] R. N. McKenzie, G. F. McNulty, and W. F. Taylor. *Algebras, Lattices, Varieties*, volume I. Wadsworth & Brookes/Cole, California, 1987.

[41] G. McNulty. The decision problem for equational bases of algebras. *Ann. Math. Logic*, 11:193–259, 1976.

[42] N. S. Mendelsohn, R. Padmanabhan, and B. Wolk. Straight edge constructions on cubic curves. *C. R. Math. Rep. Acad. Sci. Canada*, 10:77–82, 1988.

[43] N. S. Mendelsohn, R. Padmanabhan, and B. Wolk. Placement of the Desargues configuration on a cubic curve. *Geometriae Dedicata*, 40:165–170, 1991.

[44] J. S. Milne. Abelian varieties. In *Arithmetic, Geometry*, pages 103–150. Springer-Verlag, New York, 1986.

[45] D. Mumford. *Abelian Varieties* (Second Edition). Oxford University Press, 1974.

[46] D. Mumford. *Algebraic Geometry I, Complex Projective Varieties*. Springer-Verlag, 1976.