Uniqueness of the 5-ary Steiner Law on Elliptic Curves

W. McCune[*]
Mathematics and Computer Science Division
Argonne National Laboratory
Argonne, Illinois 60439-4844
U.S.A.

R. Padmanabhan[†]
Department of Mathematics
University of Manitoba
Winnipeg, Manitoba R3T 2N2
Canada

April 27, 1995

Abstract. An n-ary Steiner law $f(x_1, x_2, \cdots, x_n)$ on a projective curve Γ over an algebraically closed field k is a totally symmetric n-ary morphism f from Γ^n to Γ satisfying the universal identity

$$f(x_1, x_2, \cdots, x_{n-1}, f(x_1, x_2, \cdots, x_n)) = x_n.$$

An element e in Γ is called an idempotent for f if $f(e, e, \cdots, e) = e$. The binary morphim $x * y$ of the classical chord-tangent construction on a non-singular cubic curve (Fig. 1) is an example of a binary Steiner law on the curve and the idempotents of $*$ are precisely the inflexion points of the curve. In this paper, we prove that if f and g are two 5-ary Steiner laws on an elliptic curve Γ sharing a common idempotent then $f = g$. We use a new rule of inference rule $=\!\!(gL)\!\!\Rightarrow$, extracted from a powerful local-to-global principle in algebraic geometry. This rule is implemented in theorem-proving program OTTER. Then we use OTTER to automatically prove the

[*]Supported by the Office of Scientific Computing, U.S. Department of Energy, under Contract W-31-109-Eng-38.
[†]Supported by an operating grant from NSERC of Canada (#A8215).

uniqueness of the 5-ary Steiner law on an elliptic curve. Very much like the binary case, this theorem provides an algebraic characterization of a geometric construction process involving conics and cubics. The well-known theorem of the uniqueness of the group law on such a curve is shown to be a consequence of this result.

1 Introduction

The so-called identity theorems of classical function theory state that if two functions (belonging to a "nice" class) agree on a dense open set they they agree everywhere. This is the heart and soul of several uniqueness theorems of algebraic structures in mathematics. An analog in algebraic geometry is the so-called Chow's theorem [7, page 67]: "every compact complex manifold has at most one algebraic structure and moreover, every compact 1-dimensional complex manifold admits a unique algebraic structure". These are analytically isomorphic to projective varieties. This is a deep theorem and the uniqueness of a group law on an elliptic curve Γ is a special case. We say that an algebraic curve Γ admits an algebraic law, say $f(x_1, x_2, \cdots, x_n)$ if f is a n-ary morphism (= a regular function or a rational function) on the curve Γ. The non-singular cubic curves are pregnant with a number of universal algebras all of which are morphisms of the curve: every algebraic curve induces a rational operation on cubic curves via a complete intersection cycle (see e.g. Fig. 1 for the binary linear process and Fig. 3 for the 5-ary conic process).

In this paper, we give a pure equational characterization for the 5-ary morphism determined by the conic process. We believe that the blending of universal algebra and algebraic geometry is an important application of universal algebra and a new tool for algebraic geometry. And the addition of automated theorem proving will do a great deal to bring attention to the role of computers in symbolic reasoning in real mathematical questions. With this theme as our backdrop, let us now rephrase the uniqueness of the group law in the language of first order logic with equality:

$$\{f(x,y) \text{ is a group law on } \Gamma\} \Rightarrow \{f(x,y) = f(y,x)\}$$

$$\{f(x,y) \text{ and } g(x,y) \text{ are group laws, with a common identity, on } \Gamma\} \Rightarrow \{f(x,y) = g(x,y)\}.$$

This gives rise to a model-theoretic question of whether one can extract some first order properties from the theory of projective curves and formulate and

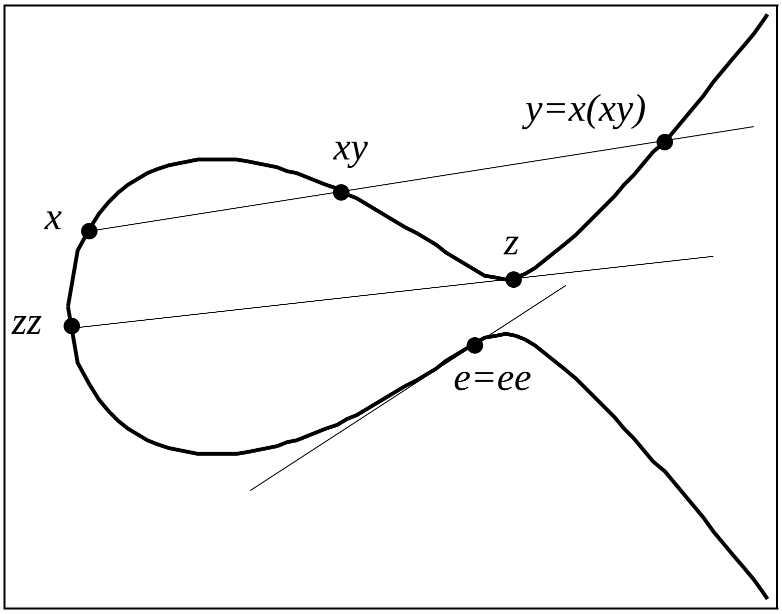

Figure 1: Chord-Tangent Construction

prove the various uniqueness theorems within the framework of first order logic with equality. And the answer is an emphatic *yes*: it is the rigidity lemma—a powerful local-to-global principle valid for morphisms of complete varieties—which proves the validity of the above implications:

Lemma 1 *Let X be a projective curve and Y and Z be irreducible algebraic varieties, all defined over an algebraically closed field k. Let f be a regular mapping from $X \times Y$ into Z such that $f(X \times \{y_0\})$ is a singleton z_0 for some $y_0 \in Y$. Then $f(X \times \{y\})$ is a singleton for every $y \in Y$.*

Proofs of this basic fact may be found in [10, p. 156], [5, p. 104], or in [11, p. 156].

2 Methodology and Theorems

We now rewrite the rigidity lemma as a formal implication ((gL) for "Local to global", "geometric Logic", "geometric Law").

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

We view the rule (gL) as an equation-deriving principle extending the scope of the usual equational logic: whenever the program meets the local equality $f(x, y_0) = z_0$ for some word f and some elements y_0, z_0, it churns out the global multivariable identity $f(x, y) = f(z, y)$ (multivariable because here x, y, or z could be vectors, namely, $x = (x_1, x_2, .., x_m)$, because x, y, or z could themselves be product spaces). This idea of viewing (gL) as an inference rule was first stated and systematically used by R. Padmanabhan in [7]. See R. W. Quackenbush [9] for the history of a closely related and recently discovered concept of "term condition".

We use the following notation. If Σ is a set of identities and if σ is an identity in the language of Σ, then we write

$$\Sigma \ =\!\!(gL)\!\!\Rightarrow \ \sigma$$

if $\Sigma \cup (\mathrm{gL}) \Rightarrow \sigma$ in the usual equational logic. Whenever convenient, we also say that the axioms Σ "(gL)-implies" σ, etc.

Using the rule (gL), let us now give a "mindless" proof of the powerful four-variable median law just from the relatively weak two-variable Steiner quasigroup laws $\{x \cdot (y \cdot x) = y, (y \cdot z) \cdot z = y\}$.

Theorem 1 $\{x(yx) = y,\ (yz)z = y\} \ =\!\!(gL)\!\!\Rightarrow \ \{(xy)(zt) = (xz)(yt)\}$.

Proof. Define the 5-ary composite operation f by

$$f(x, y, z, t, u) = ((xy)(zt))(u((xz)(yt))).$$

Now we have, by the law $x(yx) = y$, $f(x, c, c, t, d) = d$ for all x. Thus by the rule (gL), the 5-ary expression $f(x, y, z, t, u)$ does not depend upon x *for all* y, z, t, u. In particular, we have

$$\begin{array}{lll} f(x, y, z, t, u) & = f(x_1, y, z, t, u) & \forall x \forall x_1 \\ ((xy)(zt))(u((xz)(yt))) & = ((x_1 y)(zt))(u((x_1 z)(yt))) & \forall x \forall x_1 \\ & = (((yz)y)(zt))(u(((yz)z)(yt))) & \text{letting } x_1 = yz \\ & = t(ut) & \text{by the Steiner laws} \\ & = u & \\ & = ((xz)(yt))(u((xz)(yt))) & \end{array}$$

and hence one right-cancellation of the common term $(u((xz)(yt)))$ immediately yields the desired median law $(xy)(zt) = (xz)(yt)$.

Let us now apply this to the geometry of plane cubic curves without any further reference to the geometry or the topology of curves.

Corollary 1 *Every binary morphism "·" defined on a nonsingular cubic curve* Γ *over an algebraically closed field satisfying the Steiner quasigroup identities must be medial (see Fig. 2).*

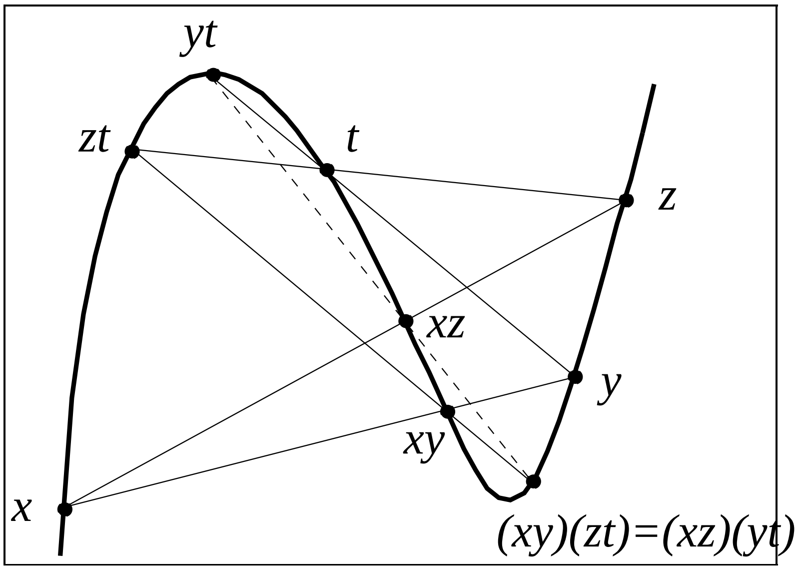

Figure 2: The Medial Law

Historical remark. This corollary was first proved for plane cubic curves by I. M. S. Etherington using the classical Bezout theorem (see [1]). In [7], Padmanabhan gave a proof for elliptic curves over an arbitrary algebraically closed field k (see also Knapp [2, p. 67–74]).

Proof. A nonsingular cubic curve is an Abelian variety and hence, as mentioned in the introduction, satisfies (the rigidity lemma and consequently) the rule (gL) for all morphisms.

3 Otter and the Implementation of $=\!(gL)\!\Rightarrow$

Otter [3] is a computer program that attempts to prove theorems stated in first-order logic with equality. Here we restrict our attention to its capabilities in equational logic. The user inputs axioms and the denial of the goal(s), and OTTER searches for a contradiction by working both forward from the axioms and backward from the goal(s). Equational reasoning is accomplished by paramodulation and demodulation. Paramodulation is equality substitution extended with unification: if the two terms in question can be made identical by instantiating variables, then equality substitution is applied to the corresponding instances. Demodulation is the use of equalities as rewrite rules to simplify other equalities. The following example illustrates the interplay between paramodulation and demodulation. Consider $\{f(x, f(g(x), y)) = y, f(u, g(u)) = e, f(w, e) = w\}$, where e is a constant; OTTER can infer $x = g(g(x))$ "in one step" by unifying $f(u, g(u))$ and $f(g(x), y))$ (which instantiates u to $g(x)$ and y to $g(g(x))$), replacing $f(g(x), g(g(x)))$ with e, and then demodulating with $f(w, e) = w$.

The rule (gL) was implemented in OTTER in two ways that are analogous to paramodulation and demodulation. Let $F[a_1, x]$ represent a term that contains a subterm a_1 at a particular position, with x representing everything else in the term. Suppose we have $F[a_1, x] = F[a_2, y]$, (i.e., a_1, and a_2 are in corresponding positions), with a_1 and a_2 unifiable. By (gL) we infer $F[z, x'] = F[z, y']$, where z is a new variable, and x' and y' are the appropriate instances of x and y. For example, from

$$f(f(x, y), f(z, f(x, z))) = f(u, f(y, u)),$$

we can (gL)-infer

$$f(f(x, y), f(z, w)) = f(f(x, z), f(y, w))$$

by unifying u and $f(x, z)$ and introducing the variable w. We also use (gL) as a rewrite rule whenever possible. That is, we rewrite $F[a, x] = F[a, y]$ to $F[z, x] = F[z, y]$ (again, z is a new variable).

OTTER **Proof Notation.** Each derived clause has a justification. The notation "$m \to n$" indicates paramodulation from m into n; ": $i, j, k, \ldots$" indicates rewriting with the demodulators $i, j, k, \ldots$; and ",flip" indicates that equality was reversed (usually so that the complex sides occurs on the left). The justification "[(gL)" indicates the use of $=\!\!(gL)\!\!\Rightarrow$ as an inference rule, and ":(gL)" indicates its use as an rewrite rule.

4 Uniqueness of 5-ary Steiner Law

Let Γ be a non-singular cubic and let x, y, z, t, u be five points on the curve. Let Q be the unique conic determined by these 5 points. By the celebrated Bezout theorem of classical geometry, we have $|\Gamma \cap Q| = 6$, counting multiplicities. Let now $F(x, y, z, t, u)$ be the 5-ary morphism on Γ defined by the complete intersection cycle $\Gamma \cap Q = \{x, y, z, t, u, F(x, y, z, t, u)\}$. Then the unique sixth point $F(x, y, z, t, u)$ can be found by a simple ruler construction as shown in Fig. 3; a proof using the rigidity lemma was given by

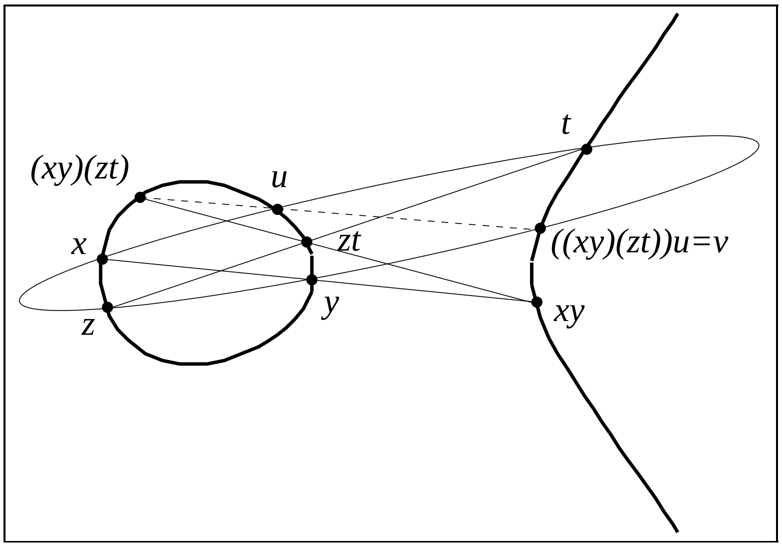

Figure 3: The Sixth Point of Intersection

N. S. Mendelsohn, R. Padmanabhan and B. Wolk in [4]). Here we would like characterize the above synthetic geometric process by means of equational identities.

The 5-ary law is totally symmetric in all of its 5 arguments and every inflexion point is an idempotent for f: $f(e, e, e, e, e) = e$. The geometric reason for this is that the intersection multiplicity at an inflexion point e is six. Moreover, it satisfies the Steiner identity $f(e, e, e, x, f(e, e, e, x, y)) = y$. We claim that a non-singular cubic curve over an algebraically closed field admits at most one such 5-ary morphism. First we prove the universal Steiner identity.

Lemma 2

$$\left\{\begin{array}{l} f(u,v,w,x,y)=f(u,v,w,y,x) \\ f(e,e,e,e,e)=e \\ f(e,e,e,x,f(e,e,e,x,y))=y \end{array}\right\} =\!(gL)\!\Rightarrow \{f(u,v,w,x,f(u,v,w,x,y))=y\}.$$

Proof (found by Otter 3.0.3+ on gyro at 3.93 seconds).

3	$f(x,y,z,u,v)=f(x,y,z,v,u)$	
4	$f(e,e,e,e,e)=e$	
7,6	$f(e,e,e,x,f(e,e,e,x,y))=y$	
9,8	$f(e,e,e,x,f(e,e,e,y,x))=y$	[3 → 6]
12	$f(x,y,z,u,f(e,e,e,u,e))=f(x,y,z,e,e)$	[6 → 4 :(gL) :(gL) :(gL), flip]
21	$f(e,e,e,x,f(y,z,u,f(v,w,v_6,e,e),x))=f(v,w,v_6,v_7,f(y,z,u,v_7,e))$	[8 → 12 :(gL) :(gL) :(gL), flip]
214	$f(x,y,z,f(x,y,z,e,e),u)=f(e,e,e,e,u)$	[(gL) 21, flip]
255	$f(x,y,z,u,f(x,y,z,u,e))=e$	[214 → 21 :9, flip]
332	$f(x,y,z,u,f(x,y,z,u,v))=v$	[6 → 255 :(gL) :7]

Line 332 is the universal Steiner identity.

Theorem 2 *Let S be the set of identities of type (5,5,0) defined by*

$$S=\left\{\begin{array}{lll} f(e,e,e,e,e)=e, & f \text{ is symmetric}, & f(e,e,e,x,f(e,e,e,x,y))=y, \\ g(e,e,e,e,e)=e, & g \text{ is symmetric}, & g(e,e,e,x,g(e,e,e,x,y))=y \end{array}\right\}.$$

Then $S =\!(gL)\!\Rightarrow \{f(x,y,z,t,u)=g(x,y,z,t,u)\}$.

By Lemma 2, we may assume the general 5-ary Steiner laws

$$f(u,v,w,x,f(u,v,w,x,y))=y,$$
$$g(u,v,w,x,g(u,v,w,x,y))=y.$$

Full symmetry of the operations causes an explosion in the Otter search space; to constrain the search, we incompletely specify symmetry with

$$f(u,v,w,x,y)=f(u,v,w,y,x)$$
$$g(u,v,w,x,y)=g(u,v,w,y,x)$$
$$g(x,y,z,u,w)=f(x,y,z,u,v)\rightarrow g(y,z,u,w,x)=f(y,z,u,v,x).$$

Proof (found by Otter 3.0.3+ on gyro at 400.44 seconds).

2	$g(x,y,z,u,w)=f(x,y,z,u,v) \;\rightarrow\; g(y,z,u,w,x)=f(y,z,u,v,x)$	
3	$f(u,v,w,x,y)=f(u,v,w,y,x)$	
4	$f(e,e,e,e,e)=e$	
5	$f(u,v,w,x,f(u,v,w,x,y))=y$	
6	$g(u,v,w,x,y)=g(u,v,w,y,x)$	
7	$g(e,e,e,e,e)=e$	
8	$g(u,v,w,x,g(u,v,w,x,y))=y$	
11	$f(x,y,z,u,g(e,e,e,e,e))=f(x,y,z,e,u)$	[7 $\rightarrow$ 3]
12	$f(e,e,e,e,g(e,e,e,e,e))=e$	[7 $\rightarrow$ 4]
15	$f(x,y,z,e,g(u,v,w,v_6,g(u,v,w,v_6,v_7)))=f(x,y,z,v_7,g(e,e,e,e,e))$	[8 $\rightarrow$ 11, flip]
21	$f(x,y,z,e,g(u,v,w,v_6,g(u,v,w,v_7,v_6)))=f(x,y,z,v_7,g(e,e,e,e,e))$	[6 $\rightarrow$ 15]
25	$f(x,y,z,e,g(u,v,w,v_6,g(u,v,w,e,v_7)))=f(x,y,z,v_7,g(e,e,e,v_6,e))$	[(gL) 15]
46	$f(x,y,z,e,g(u,v,w,e,v_6))=f(x,y,z,v_7,g(u,v,w,v_7,v_6))$	[21 $\rightarrow$ 25 :(gL) :(gL) :(gL) :(gL)]
53	$f(x,y,z,u,g(v,w,v_6,u,v_7))=f(x,y,z,v_8,g(v,w,v_6,v_8,v_7))$	[46 $\rightarrow$ 46]
65	$f(e,e,e,x,g(e,e,e,x,e))=e$	[12 $\rightarrow$ 46, flip]
70	$f(e,e,e,x,g(e,e,e,e,x))=e$	[6 $\rightarrow$ 65]
71	$g(e,e,e,x,e)=f(e,e,e,x,e)$	[65 $\rightarrow$ 5, flip]
77	$f(x,y,z,u,g(v,w,v_6,v_7,u))=f(x,y,z,v_8,g(v,w,v_6,v_7,v_8))$	[70 $\rightarrow$ 70 :(gL) :(gL) :(gL) :(gL) :(gL) :(gL) :(gL)]
83	$g(e,e,x,e,e)=f(e,e,x,e,e)$	[71,2]
100	$f(e,e,x,e,g(e,e,x,e,e))=e$	[83 $\rightarrow$ 5]
116	$f(e,e,x,y,g(e,e,x,e,y))=e$	[77 $\rightarrow$ 100]
117	$f(x,y,z,u,g(v,w,z,v_6,v_7))=f(x,y,v_8,u,g(v,w,v_8,v_6,v_7))$	[100 $\rightarrow$ 100 :(gL) :(gL) :(gL) :(gL) :(gL) :(gL) :(gL)]
149	$f(e,e,x,y,g(e,e,x,y,e))=e$	[65 $\rightarrow$ 117, flip]
171	$g(e,e,x,e,y)=f(e,e,x,y,e)$	[116 $\rightarrow$ 5, flip]
174	$f(x,y,z,u,g(v,w,z,u,v_6))=f(x,y,v_7,v_8,g(v,w,v_7,v_8,v_6))$	[149 $\rightarrow$ 149 :(gL) :(gL) :(gL) :(gL) :(gL)]
182	$g(e,e,x,e,y)=f(e,e,x,e,y)$	[3 $\rightarrow$ 171]
221	$f(e,e,x,e,g(e,e,x,e,y))=y$	[8 $\rightarrow$ 182, flip]
249	$f(e,e,x,y,g(e,e,x,y,z))=z$	[174 $\rightarrow$ 221]
252	$g(e,e,x,y,z)=f(e,e,x,y,z)$	[8 $\rightarrow$ 249, flip]
256	$g(e,x,y,z,e)=f(e,x,y,z,e)$	[252,2]
269	$g(x,y,z,e,e)=f(x,y,z,e,e)$	[256,2]
272	$f(e,x,y,z,g(e,x,y,z,e))=e$	[256 $\rightarrow$ 5]
280	$f(x,y,z,e,g(x,y,z,e,e))=e$	[269 $\rightarrow$ 5]
300	$f(x,y,z,u,g(v,y,z,u,w))=f(x,v_6,v_7,v_8,g(v,v_6,v_7,v_8,w))$	[272 $\rightarrow$ 272 :(gL) :(gL) :(gL)]
339	$f(x,y,z,u,g(x,y,z,u,e))=e$	[53 $\rightarrow$ 280]
363	$g(x,y,z,u,e)=f(x,y,z,u,e)$	[339 $\rightarrow$ 5, flip]

375	$g(x,y,z,e,u) = f(x,y,z,e,u)$	[363,2]
408	$f(x,y,z,e,g(x,y,z,e,u)) = u$	[8 $\rightarrow$ 375, flip]
471	$f(x,y,z,u,g(x,y,z,u,v)) = v$	[300 $\rightarrow$ 408]
652	$g(x,y,z,u,v) = f(x,y,z,u,v)$	[8 $\rightarrow$ 471, flip]

Line 652 completes the proof of Theorem 2.

We now apply Theorem 2 to derive a ruler construction to locate the unique sixth point $f(x,y,z,t,u)$ on the cubic.

Corollary 2 *$f(x,u,z,t,u) = ((x*y)*(z*t))*u$, where "$*$" stands for the binary morphism of secant-tangent construction on the cubic.*

Proof. Define $g(x,y,z,t,u) = ((x*y)*(z*t))*u$. It is clear that g is totally symmetric and that every inflexion point is an idempotent for g and moreover, g satisfies the 5-ary Steiner law $g(e,e,e,x,g(e,e,e,x,y)) = y$. Hence, by the theorem, $f = g$.

In a similar fashion, we can derive the well-known theorem of the uniqueness of the group law on such a curve is shown to be a consequence of this result.

Corollary 3 *If $x+y$ and $x \cdot y$ are two group law on an elliptic curve, and if $e+e = e \cdot e = e$, where e is an inflexion point, then $x+y = x \cdot y$ for all points x and y on the curve.*

Proof. Define $f(x,y,z,u,v) = x+y+z+u+v$, and $g(x,y,z,u,v) = x \cdot y \cdot z \cdot u \cdot v$. It is clear that both f and g satisfy the Steiner identities, that both f and g are totally symmetric (because group laws on elliptic cureves are commutative), that e is the identity element for both groups laws, and that e is an idempotent for both f and g. Therefore, $x+y+z+u+v = x \cdot y \cdot z \cdot u \cdot v$. Let z, u, and v all be e, then simplify, obtaining $x+y = x \cdot y$. Let $-$ and $'$ be the inverses. With the identity $x' + (--x) = e$, add $-x$ to both sides, then simplify to $x' = -x$.

The second part of the proof, after $x+y+z+u+v = x \cdot y \cdot z \cdot u \cdot v$, was first proved by OTTER.

References

[1] I. M. S. Etherington. Quasigroups and cubic curves. *Proc. Edinburgh Math. Soc.*, 14:273–291, 1965.

[2] A. Knapp, editor. *Elliptic Curves*. Princeton University Press, 1993.

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

[4] 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.

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

[6] D. Mumford. *Algebraic Geometry I, Complex Projective Varieties*. Springer-Verlag, 1970.

[7] R. Padmanabhan. Logic of equality in geometry. *Discrete Mathematics*, 15:319–331, 1982.

[8] R. Padmanabhan and W. McCune. Automated reasoning about cubic curves. *Computers and Mathematics with Applications*, 29(2):17–26, 1995.

[9] R. W. Quackenbush. Quasi-affine algebras. *Algebra Universalis*, 20:318–327, 1985.

[10] I. R. Shafarevich. *Basic Algebraic Geometry*. Springer-Verlag, New York, 1977.

[11] T. A. Springer. *Linear Algebraic Groups*. Birkhauser, Boston, 1980.

[12] W. Wechler. *Universal Algebra for Computer Scientists*. Springer-Verlag, New York, 1992.