JOURNAL OF ALGABRA **107**, 106–116 (1987)

Addition Laws on Elliptic Curves in Arbitrary Characteristics

H. LANGE AND W. RUPPERT

Mathematisches Institut, Bismarckstr. 1½, D-8520 Erlangen, West Germany

Communicated by Michael Artin

Received May 2, 1985

INTRODUCTION

Let E be an elliptic curve over a field k which we assume to be algebraically closed for simplicity. If L is a very ample line bundle on E, we denote by $i_L: E \to \mathbb{P}^n$ the associated complete embedding. An *addition law* of bidegree (μ, ν) on E with respect to L is an $(n+1)$-tuple of polynomials $p_0,..., p_n \in k[X_0,..., X_n, Y_0,..., Y_n]$, not all zero, and bihomogeneous of degree μ in $X_0,..., X_n$ and ν in $Y_0,..., Y_n$, such that on an open nonempty set $U \subset E \times E$ we have

$$x + y = (p_0(x, y): \cdots : p_n(x, y))$$

for all $(x, y) \in U$, considered as points of $\mathbb{P}^n \times \mathbb{P}^n$. Here "+" denotes the group law of E. A set of addition laws $\{(p_0^i,..., p_n^i);\ i = 1,..., s\}$ of bidegree (μ, ν) on E with respect to L is called a *complete system of addition laws* if the defining open sets $U_i \subset E \times E$ form a covering of $E \times E$.

It is the aim of this note to work out explicitly a complete system of addition laws of bidegree (2, 2) with respect to $L = \mathcal{O}_E(3 \cdot o)$ (o denoting the zero point of E) valid in every characteristic. Here the coordinates of $\mathbb{P}^2$ are chosen in such a way that the equation of E is in Weierstrass form in the sense of Tate (cf. [6]). Moreover we study the behaviour of the addition laws in case E degenerates to a singular cubic, i.e., to the additive group $\mathbb{G}_a$ or the multiplicative group $\mathbb{G}_m$. The starting point for the computations is a general existence theorem for addition laws on abelian varieties (cf. [[2]). This theorem in the special case of an elliptic curve admits an easy proof, which we give in Section 1 and which is based on the fact that the diagonal is a divisor on $E \times E$. Consequently the proof is not a special case of the more general one given in [2]. Section 2 contains the above-mentioned explicit addition laws and Section 3 its degenerations to $\mathbb{G}_a$ and

0021-8693/87 $3.00

Copyright © 1987 by Academic Press, Inc.
All rights of reproduction in any form reserved.

$\mathbb{G}_m$. It should be mentioned that the results admit some applications to the theory of transcendental numbers as outlined in [2] and which shall not be repeated here (cf. [3–5, 8]).

1

Throughout the paper let k denote an algebraically closed field. It should be noted, however, that the results and formulas are correct for arbitrary ground fields under mild rationality hypotheses which we omit for the sake of simplicity. Let E denote an elliptic curve over k and L a line bundle of degree $d \geqslant 3$ on E. Then we have

THEOREM 1.1. (1) *Let μ and ν be integers $\geqslant 2$ with one of them $\geqslant 3$. Then there is a complete system of addition laws of bidegree (μ, ν) on E with respect to L.*

(2)(i) *If L is not symmetric* (i.e., $(-1)^*L \neq L$), *there is no addition law of bidegree* (2, 2) *on E with respect to L.*

(ii) *If L is symmetric, there is a complete system of addition laws of bidegree* (2, 2) *on E with respect to L.*

For the proof we need some auxiliary results.

LEMMA 1.2. *There is a complete system of addition laws (resp. an addition law) of bidegree (μ, ν) on E with respect to L if and only if the line bundle $F(\mu, \nu) := m^*L^{-1} \otimes p_1^*L^{\mu} \otimes p_2^*L^{\nu}$ on $E \times E$ is basepoint-free (resp. admits a nonzero global section).*

Here m, p_1, and p_2 denote the addition map $E \times E \to E$ and the natural projections of $E \times E$. For the proof we refer to [2, Sect. 2]. Note only that any completely embedded elliptic curve in $\mathbb{P}^n$ is projectively normal.

If f_i denotes a fibre in $E \times E$ with respect to p_i for $i = 1$ and 2, $\Delta = \{(x, x) \in E \times E\}$ the diagonal, and $A = \{(x, -x) \in E \times E\}$ the antidiagonal of $E \times E$, then we have

LEMMA 1.3. $A \equiv 2f_1 + 2f_2 - \Delta$, *where "$\equiv$" denotes numerical equivalence.*

Proof. It is well known (cf., e.g., [7]) that the rank of the group $\mathrm{Num}(E \times E)$ of divisors on $E \times E$ modulo numerical equivalence is 3, 4, or 6 if respectively E is without complex multiplication, singular, or supersingular. A base of $\mathrm{Num}(E \times E)$ is given by the classes (denoted by the same letter) of f_1, f_2, Δ, and $\Gamma_1, \ldots, \Gamma_s$, where the $\Gamma_i \subset E \times E$ denote graphs

of suitable endomorphisms φ_i of E and $s=0$, 1, or 3, respectively. For the intersection numbers we have

$$(f_1^2)=(f_2^2)=(\Delta^2)=(\Gamma_i^2)=0, \qquad (\Delta\cdot f_1)=(\Delta\cdot f_2)=(f_1\cdot f_2)=1,$$

and (1)

$$(f_1\cdot\Gamma_i)=1, \qquad (f_2\cdot\Gamma_i)=\deg\varphi_i, \qquad (\Delta\cdot\Gamma_i)=\deg(\varphi_i-1) \qquad \text{for} \quad i=1,\ldots,s$$

Then $A\equiv\alpha f_1+\beta f_2+\delta\Delta+\gamma_1\Gamma_1+\cdots+\gamma_s\Gamma_s$ with uniquely determined integers $\alpha, \beta, \delta, \gamma_1,\ldots,\gamma_s$ which we have to determine. For doing this, note that

$$(A\cdot f_1)=(A\cdot f_2)=1, \qquad (A\cdot\Gamma_i)=\deg\varphi_i, \qquad \text{and} \qquad (A\cdot\Delta)=4, \quad (2)$$

the last equation following from the fact that there are exactly four 2-division-points of E (counted with multiplicity in characteristic 2).

Writing out Eqs. (2) and inserting the intersection numbers (1) we get a system of $3+s$ linear equations in the $3+s$ variables $\alpha, \beta, \delta, \gamma_1,\ldots,\gamma_s$, which has a unique solution, since $f_1, f_2, \Delta, \Gamma_1,\ldots,\Gamma_s$ are a basis of $\mathrm{Num}(E\times E)$. But it is easily seen that $\alpha=\beta=2$, $\delta=-1$, $\gamma_1=\cdots=\gamma_s=0$ is a solution (note that $\deg(\varphi_i+1)=(\varphi_i+1)(\bar\varphi_i+1)=2+2\varphi_i\bar\varphi_i-(\varphi_i-1)(\bar\varphi_i-1)=2+2\deg\varphi_i-\deg(\varphi_i-1)$), which completes the proof of Lemma 1.3.

COROLLARY 1.4. *If L is a line bundle of degree d on E, then we have for all integers x and y:*

$$\chi(E\times E, m^*L^{-1}\otimes p_1^*L^x\otimes p_2^*L^y)=d^2(xy-x-y),$$

χ denoting the Euler–Poincaré-characteristic.

Proof. By Riemann–Roch

$$\chi(E\times E, m^*L^{-1}\otimes p_1^*L^x\otimes p_2^*L^y)=\tfrac{1}{2}(m^*L^{-1}\otimes p_1^*L^x\otimes p_2^*L^y)^2.$$

Since $L\simeq\mathcal{O}_E(d\cdot p)$ for some point p on E and the intersection number on the right-hand side does not change under algebraic equivalence, we may assume $L\simeq\mathcal{O}_E(d\cdot o)$. But then according to Lemma 1.3

$$m^*L^{-1}\otimes p_1^*L^x\otimes p_2^*L^y\equiv\mathcal{O}_{E\times E}(d[(x-2)f_1+(y-2)f_2+\Delta])$$

which gives the assertion since

$$\tfrac{1}{2}(((x-2)f_1+(y-2)f_2+\Delta)^2)=xy-x-y.$$

Finally, we need the following lemma, for the (easy) proof of which we refer to [2].

LEMMA 1.5. *Let* $F = m^*L^{-1} \otimes p_1^*L^2 \otimes p_2^*L^2$. *Then we have*

(a) $\Delta \subseteq K(F)$ $(= \{(x, y) \in E \times E \mid T^*_{(x,y)}F \simeq F\}$ *by definition,* T *denoting the translation map*).

(b) L *is symmetric if and only if* $F|\Delta \simeq \mathcal{O}_\Delta$.

(c) *Let* L *be symmetric and* $\pi\colon E \times E \to E \times E/\Delta$ *the natural map. Then we have with respect to a suitable isomorphism* $\psi\colon E \times E/\Delta \to E$:

$$F \simeq (\psi\pi)^*L.$$

Now we are in a position to prove Theorem 1.1:

Proof of (1). According to Lemma 1.2 have to show that $F(\mu, \nu)$ is basepoint-free. But $L = N^d$ for some line bundle N of degree 1 on E and hence

$$F(\mu, \nu) = G^d$$

with $G = m^*N^{-1} \otimes p_1^*N^\mu \otimes p_2^*N^\nu$. Applying, for example, Nakai's criterion we see that $G \equiv \mathcal{O}_{E \times E}((\mu - 2) f_1 + (\nu - 2) f_2 + \Delta)$ is ample. It follows that G^d is very ample, since $d \geqslant 3$.

Proof of (2). Part (i) follows by Lemma 1.5(a) and (b) from a theorem of Kempf (cf. [1, Theorem 1(i)]), which says that if Y is a connected component of $K(F)$ and $F|Y$ trivial, then F has no cohomology.

Part (ii) is a direct consequence of Lemma 1.2 and Lemma 1.5(c).

2

In this section we want to give explicit formulas for a complete set of addition laws for an elliptic curve E in Weierstrass form

$$x_0x_2^2 + a_1x_0x_1x_2 + a_3x_0^2x_2 = x_1^3 + a_2x_0x_1^2 + a_4x_0^2x_1 + a_6x_0^3 \qquad (1)$$

over k in the sense of Tate (cf. [6]). Here the characteristic of k is arbitrary. The a_i are elements of k of weight i and to x_0, x_1, x_2 the weights 0, 2, and 3 respectively are associated, so that Eq. (1) is of weight 6. Since the embedding line bundle $L = \mathcal{O}_E(3 \cdot o)$ is symmetric, there must be a complete system of addition laws of bidegree (2, 2) on E with respect to L according to Theorem 1.1. For its formulation we write

$$(z_0 : z_1 : z_2) = (x_0 : x_1 : x_2) + (y_0 : y_2 : y_2)$$

and define the following sets of quantities. Note that subscripts indicate weights:

(i) $b_2 = a_1^2 + a_2$; $b_3 = a_1 a_2 - 3a_3$; $b_4 = a_1 a_3 + a_4$;

$b_5 = a_1 a_4 - a_2 a_3$; $b_6 = a_3^2 + 3a_6$; $b_7 = 3a_1 a_6 - a_3 a_4$;

$b_8 = a_2 b_6 - a_4 b_4 + a_6 b_2$; $b_9 = a_1 b_8 - a_3 b_6$;

$b_{10} = (a_2 + b_2)\, b_8 - a_3^2 b_4 - 2a_4 b_6$; $b_{12} = b_4 b_8 - b_6^2$.

(ii) $S_0 = x_0^2$; $S_2 = x_0 x_1$; $S_3 = x_0 x_2$; $S_4 = x_1^2$; $S_5 = x_1 x_2$ $S_6 = x_2^2$;

$T_0 = y_0^2$; $T_2 = y_0 y_1$; $T_3 = y_0 y_2$; $T_4 = y_1^2$; $T_5 = y_1 y_2$; $T_6 = y_2^2$;

$P_{ij} = S_i T_j$; $Q_{ij} = P_{ij} - P_{ji}$; $R_{ij} = P_{ij} + P_{ji}$.

PROPOSITION 2.1. *Suppose the characteristic of k is different from* 2. *Then the following three addition laws form a complete set of addition laws of bidegree* (2, 2) *on E in Tate–Weierstrass form* (1):

$(Z^{(1)})$:

$$z_0 = a_4 Q_{02} - a_3 Q_{03} + a_2 Q_{04} - a_1 Q_{05} - Q_{06} + 3Q_{24}$$

$$z_1 = -3a_6 Q_{02} - a_4 Q_{04} + a_3 Q_{05} - 2a_3 Q_{23} - a_2 Q_{24} - Q_{26} + a_1 Q_{34} + 2Q_{35}$$

$$z_2 = b_7 Q_{02} + b_6 Q_{03} + b_5 Q_{04} + a_4 Q_{05} + 2b_4 Q_{23} + b_3 Q_{24} + 2a_2 Q_{25} - b_2 Q_{34} - 2a_1 Q_{35} - Q_{36} + 3Q_{45}$$

$(Z^{(2)})$:

$$z_0 = b_6 Q_{02} + b_4 Q_{04} + a_3 Q_{05} + b_2 Q_{24} + 2a_1 Q_{25} + Q_{26} + a_1 Q_{34} + 2Q_{35}$$

$$z_1 = -b_8 Q_{02} - b_6 Q_{04} - b_4 Q_{24} - a_3 Q_{34} + a_1 Q_{45} + Q_{46}$$

$$z_2 = b_9 Q_{02} + b_8 Q_{03} + b_7 Q_{04} + 3a_6 Q_{05} + 2b_6 Q_{23} + b_5 Q_{24} + 2a_4 Q_{25} - b_4 Q_{34} - 2a_3 Q_{35} + a_2 Q_{45} + Q_{56}$$

$(Z^{(3)})$:

$$\begin{aligned} z_0 = {} & a_3 b_6 R_{00} + 3(a_1 a_3^2 + a_1 a_6 + a_3 a_4)\, R_{02} + 3(a_3^2 + 2a_6)\, R_{03} \\ & + (a_1 b_4 + a_2 a_3)(R_{04} + 2R_{22}) + 2b_4(R_{05} + 2R_{23}) + a_3(R_{06} + 2R_{33}) \\ & + (a_1^3 + 3a_1 a_2 + 3a_3)\, R_{24} + (a_1^2 + 2a_2)(2R_{25} + R_{34}) + a_1(R_{26} + 2R_{35}) \\ & + 3a_1 R_{44} + 2R_{36} + 6R_{45} \end{aligned}$$

$$z_1 = -a_3b_8R_{00} - (b_9 + 3a_3(a_6 + b_6))R_{02} - 2b_8R_{03} - (a_1b_6 + a_3b_4)(R_{04} + 2R_{22})$$
$$- (a_3^2 + 6a_6)(R_{05} + 2R_{23}) - (3a_1a_4 + a_3b_2)\,R_{24} - 2a_4(2R_{25} + R_{34})$$
$$+ a_3(R_{26} + 2R_{35}) - a_1a_2R_{44} + (a_1^2 - 2a_2)\,R_{45} + a_1R_{46} + 2a_1R_{55} + 2R_{56}$$

$$z_2 = b_{12}R_{00} + b_{10}R_{02} + b_9R_{03} + (2b_8 + a_6b_2 - a_2b_6)(R_{04} + 2R_{22})$$
$$+ b_7(R_{05} + 2R_{23}) + (a_1^2a_4 - 2a_2b_4 + 3b_6 + 9a_6)\,R_{24} + b_5(2R_{25} + R_{34})$$
$$- (a_2^2 - 3a_4)\,R_{44} + a_3R_{36} + (a_1a_2 - 3a_3)\,R_{45} + a_1R_{56} + R_{66}$$

Note that z_0, z_1, and z_2 are of weight k, $k+2$, and $k+3$ respectively with $k=6$ for $(Z^{(1)})$, $k=8$ for $(Z^{(2)})$, and $k=9$ for $(Z^{(3)})$. As for the proof, we give only a sketch, since some of the computations are a little tedious.

Proof. According to Lemma 1.2 an addition law of bidegree (2, 2) on E with respect to $L = \mathcal{O}_E(3 \cdot o)$ may be interpreted as a nontrivial section of $F = m^*L^{-1} \otimes p_1^*L^2 \otimes p_2^*L^2$. Since $H^0(E \times E, F)$ is of dimension 3 (apply Lemma 1.5(c)) and since F is basepoint-free on $E \times E$, any three linearly independent global sections of F give a complete system of addition laws.

Assume first that the characteristic of k is different from 2 and 3. We want to "add" the points $(x_0 : x_1 : x_2)$ and $(y_0 : y_1 : y_2)$. For this we transform the curve (1) into the curve

$$u_0u_2^2 = 4u_1^3 - g_2u_0^2u_1 - g_3u_0^3 \tag{2}$$

with

$$\tilde{b}_2 = a_1^2 + 4a_2, \qquad \tilde{b}_4 = a_1a_3 + 2a_4, \qquad \tilde{b}_6 = a_3^2 + 4a_6,$$
$$g_2 = \tfrac{1}{12}(\tilde{b}_2^2 - 24\tilde{b}_4), \qquad g_3 = \tfrac{1}{216}(-\tilde{b}_2^3 + 36\tilde{b}_2\tilde{b}_4 - 216\tilde{b}_6)$$

(cf. [3, p. 180]). Here $(x_0 : x_1 : x_2)$ and $(y_0 : y_1 : y_2)$ are transformed into the points $(u_0 : u_1 : u_2)$ and $(v_0 : v_1 : v_2)$ with

$$u_0 = x_0,$$
$$u_1 = \tfrac{1}{12}\tilde{b}_2x_0 + x_1,$$
$$u_2 = a_3x_0 + a_1x_1 + 2x_2$$

and v_0, v_1, v_2 analogously.

For the curve (2) a complete system of three addition laws of bidegree (2, 2) on E with respect to L has been given in [2, Sect. 3]. This we take and transform back, i.e., let $(w_0 : w_1 : w_2) = (u_0 : u_1 : u_2) + (v_0 : v_1 : v_2)$ and

$$z_0 = w_0,$$

$$z_1 = -\frac{1}{12}\tilde{b}_2 w_0 + w_1,$$

$$z_2 = \frac{1}{24}(a_1\tilde{b}_2 - 12a_3)\, w_0 - \frac{1}{2}a_1 w_1 + \frac{1}{2}w_2,$$

Let the corresponding three addition laws be denoted by $(\tilde{Z}^{(1)})$, $(\tilde{Z}^{(2)})$, and $(\tilde{Z}^{(3)})$. In order to obtain better coefficients we choose

$$(Z^{(1)}) = \frac{1}{4}(\tilde{Z}^{(1)}),$$

$$(Z^{(2)}) = \frac{1}{48}((a_1^2 + 4a_2)(\tilde{Z}^{(1)}) + 3(\tilde{Z}^{(2)})),$$

$$(Z^{(3)}) = \frac{1}{16}(\tilde{Z}^{(3)})$$

to get the three addition laws as stated in Proposition 2.1. It is clear that they form a complete set of addition laws in every characteristic different from 2 and 3 it remains to show that it does so also if the characteristic is 3.

First of all note that every addition law $(Z^{(i)})$ is in fact an addition law for E with respect to L in all characteristics including 2 and 3. For this we have to mention only that the equations $(Z^{(i)})$ are defined over $\mathbb{Z}$ and make sense in every characteristic. To be more precise, let $\mathscr{E} \to S$ be a family of elliptic curves over a base scheme S, such that $\mathscr{L} = \mathscr{O}_E(3 \cdot \mathrm{o})$ is relatively very ample (o = zero section) and thus yields an embedding $i\colon \mathscr{E} \to \mathbb{P}^2_S$ over S, and let $m\colon \mathscr{E} \times_S \mathscr{E} \to \mathscr{E}$ denote the addition map. Then an addition law can be interpreted by the composite rational map

$$\mathscr{E} \times_S \mathscr{E} \xrightarrow{m} \mathscr{E} \xrightarrow{i} \mathbb{P}^2_S$$

defined by a basis of global sections of $m^*\mathscr{L}$. The open defining set of the addition law is the set of all points where not every global section of the basis vanishes. Since z_0, z_1, z_2 represent just this basis and since they do not vanish simultaneously everywhere neither in characteristic 2 nor 3, the above assertion follows from the fact that every curve in positive characteristic can be lifted to characterize zero.

It remains to show that $(Z^{(1)})$, $(Z^{(2)})$, and $(Z^{(3)})$ are linearly independent in characteristic 3. But $z_0^{(1)}$ contains $-Q_{06}$, and $z_0^{(2)}$ does not, whereas $z_0^{(2)}$ contains Q_{26}, and $z_0^{(1)}$ does not, which implies that $(Z^{(1)})$ and $(Z^{(2)})$ are linearly independent. Since $(Z^{(1)})$ and $(Z^{(2)})$ are antisymmetric and $(Z^{(3)})$

symmetric with respect to x and y, $(Z^{(3)})$ is linearly independent from $(Z^{(1)})$ and $(Z^{(2)})$. This completes the proof of Proposition 2.1.

If the characteristic of k is 2, $(Z^{(1)})$, $(Z^{(2)})$, and $(Z^{(3)})$ still are addition laws of E with respect to L, as was shown within the proof of Proposition 2.1, and $(Z^{(1)})$ and $(Z^{(2)})$ still are linearly independent over k. However,

$$(Z^{(3)}) \equiv a_3(Z^{(1)}) - a_1(Z^{(2)}) \qquad (\text{mod } 2),$$

so that Proposition 2.1 is not correct in characteristic 2. But choosing, for example,

$$(Z^{(4)}) = \tfrac{1}{2}((Z^{(3)}) + a_1(Z^{(2)}) - a_3(Z^{(1)})),$$

one immediately checks that $(Z^{(4)})$ is an addition law in characteristic 2, linearly independent of $(Z^{(1)})$ and $(Z^{(2)})$. The same argument as in the above proof then yields

THEOREM 2.2. *The three addition laws* $(Z^{(1)})$, $(Z^{(2)})$, *and* $(Z^{(4)})$ *form a complete set of addition laws of bidegree* $(2, 2)$ *on the elliptic curve* E *in Tate–Weierstrass form* (1) *in arbitrary characteristics.*

3

Finally, we want to study the behaviour of the addition laws $(Z^{(1)})$, $(Z^{(2)})$, and $(Z^{(3)})$, when the curve E degenerates to the singular cubics $x_0x_2^2 = x_1^3$ and $x_0x_2^2 = x_1^3 + x_0x_1^2$. Whereas it is well known that the "ordinary" addition law of E degenerates to the addition laws on the singular cubics (cf. [6]), it does not seem clear (at least to us) that this is always the case. However, as we shall see it is the case for $(Z^{(1)})$, $(Z^{(2)})$, and $(Z^{(3)})$.

(a) $x_0x_2^2 = x_1^3$. Suppose E is a plane cubic with a cusp over k. Then the coordinates of $\mathbb{P}^2$ can be chosen in such a way that E is given by the equation

$$x_0x_2^2 = x_1^3.$$

According to [6, p. 182] we get a group isomorphism of $E - \{\text{cusp}\}$ onto the additive group $\mathbb{G}_a$ as follows:

$$x \mapsto ((\text{slope } \overline{xc}) - (\text{slope of the tangent at } c))^{-1} = x_1/x_2 =: t$$

where $x=(x_0:x_1:x_2)$ and c is the cusp of E. This yields the parametrization

$$t \mapsto (t^3:t:1).$$

So let $(x_0:x_1:x_2)=(s^3:s:1)$ and $(y_0:y_1:y_2)=(t^3:t:1)$ denote points of $E-\{\text{cusp}\}$. Then the laws of Proposition 2.1 say in this case (where all a_i and b_j vanish):

$(Z^{(1)})$:

$$\begin{aligned} z_0 &= -Q_{06}+3Q_{24}=(t-s)^3(t+s)^3 \\ z_1 &= -Q_{26}+2Q_{35}=(t-s)^3(t+s) \\ z_2 &= -Q_{36}+3Q_{45}=(t-s)^3\cdot 1 \end{aligned}$$

$(Z^{(2)})$:

$$\begin{aligned} z_0 &= Q_{26}+2Q_{35}=(s-t)(t+s)^3 \\ z_1 &= Q_{46} \qquad\quad =(s-t)(t+s) \\ z_2 &= Q_{56} \qquad\quad =(s-t)\cdot 1 \end{aligned}$$

$(Z^{(3)})$:

$$\begin{aligned} z_0 &= 2R_{36}+6R_{45}=2(t+s)^3 \\ z_1 &= 2R_{56} \qquad\quad =2(t+s) \\ z_2 &= R_{66} \qquad\quad =2\cdot 1 \end{aligned}$$

Hence in all cases $(z_0:z_1:z_2)=((t+s)^3:(t+s):1)$ as it should be. The same follows for $(Z^{(4)})$ in characteristic 2.

(b) $x_0x_2^2=x_1^3+x_0x_1^2$. Let E be a plane cubic with an ordinary double point. Then the coordinates of $\mathbb{P}^2$ can be chosen in such a way that E is given by the equation

$$x_0x_2^2=x_1^3+x_0x_1^2.$$

According to [6, p. 182] we get a group isomorphism of $E-\{\text{double point}\}$ onto the multiplicative group $\mathbb{G}_m$ as follows:

$$(x_0:x_1:x_2)\mapsto \frac{x_2+x_1}{x_2-x_1}=:t.$$

This yields a parametrization

$$t \mapsto ((t-1)^3:4t(t-1):4t(t+1)).$$

So let

$$(x_0 : x_1 : x_2) = ((s-1)^3 : 4s(s-1) : 4s(s+1))$$

and

$$(y_0 : y_1 : y_2) = ((t-1)^3 : 4t(t-1) : 4t(t+1))$$

denote points of $E - \{\text{double point}\}$. Then the addition laws of Proposition 2.1 say in this case (where $a_2 = b_2 = 1$ and all other a_i and b_j vanish):

$(Z^{(1)})$:

$$\begin{aligned} z_0 &= Q_{04} - Q_{06} + 3Q_{24} && = 64(t-s)^3 \cdot (st-1)^3 \\ z_1 &= -Q_{24} - Q_{26} + 2Q_{35} && = 64(t-s)^3 \cdot 4st(st-1) \\ z_2 &= 2Q_{25} - Q_{34} - Q_{36} + 3Q_{45} && = 64(t-s)^3 \cdot 4st(st+1) \end{aligned}$$

$(Z^{(2)})$:

$$\begin{aligned} z_0 &= Q_{24} + Q_{26} + 2Q_{35} && = 256st(s-t) \cdot (st-1)^3 \\ z_1 &= Q_{46} && = 256st(s-t) \cdot 4st(st-1) \\ z_2 &= Q_{45} + Q_{56} && = 256st(s-t) \cdot 4st(st+1) \end{aligned}$$

$(Z^{(3)})$:

$$\begin{aligned} z_0 &= 4R_{25} + 2R_{34} + 2R_{36} + 6R_{45} && = 512st(s+t) \cdot (st-1)^3 \\ z_1 &= -2R_{45} + 2R_{56} && = 512st(s+t) \cdot 4st(st-1) \\ z_2 &= -R_{44} + R_{66} && = 512st(s+t) \cdot 4st(st+1) \end{aligned}$$

Hence in all cases $(z_0 : z_1 : z_2) = ((st-1)^3 : 4st(st-1) : 4st(st+1))$ as it should be. Again we have to exclude the characteristic 2 case, in which, however, it is easy to make the suitable modifications.

ACKNOWLEDGMENT

We would like to thank D. Bertrand, who suggested that one should compute the formulas and study its degenerations.

REFERENCES

1. G. KEMPF, Appendix to Varieties defined by quadratic equations, by D. Mumford, *in* "Questions on Algebraic Varieties," pp. 29–100, CIME, Roma, 1970.

2. H. LANGE AND W. RUPPERT, Complete systems of addition laws on abelian varieties, *Invent. Math.* **79** (1985), 603–610.
3. D. W. MASSER, AND G. WÜSTHOLZ, Zero estimates on group varieties, I, Invent. Math. 64 (1981), 489–516.
4. J.-C. MOREAU, Démonstrations géométriques de lemmes de zéro, II, *Progr. Math.* **31** (1983), 191–198.
5. P. PHILLIPON, Lemmes de zéros dans les groupes algébriques commutatifs, preprint, 1985.
6. J. TATE, The arithmetic of elliptic curves, *Invent. Math.* **23** (1974), 179–206.
7. A. WEIL, "Courbes algébriques et variétés abéliennes," Hermann, Paris, 1971.
8. G. WÜSTHOLZ, Multiplicity estimates on group varieties, preprint, 1984.