ALGEBRAIC POINTS ON QUARTIC CURVES OVER FUNCTION FIELDS

by ANDREW BREMNER

(Recieved 4 October, 1984)

1. The following general problem is of interest. Let Γ be an irreducible algebraic variety of degree d, in projective n-space $\mathbf{P}^n$, defined over a field k; and suppose that K is a finite extension of k with $[K:k]$ prime to d. If Γ has a point defined over K, then does it necessarily have a point defined over k?

It has been studied in various instances by several authors: see, for example, Cassels [**2**], Coray [**3, 4**], Pfister [**5**], Bremner, Lewis, Morton [**1**]. Coray [**3**] shows that a quartic curve Γ over $\mathbf{Q}$ may possess points in extension fields of $\mathbf{Q}$ of every odd degree greater than one, but have no points in $\mathbf{Q}$ itself. Some further examples of this instance occur in the paper of Bremner, Lewis, Morton, with the additional property that the curve Γ also possesses points in every p-adic completion $\mathbf{Q}_p$ of $\mathbf{Q}$.

When the ground field is the function field $k = \mathbf{Q}(\lambda)$ of transcendence degree 1, then Bremner, Lewis, Morton again give (although rather as a rabbit from a hat) two examples to show that a quartic curve Γ defined over k may possess points in extension fields of k of every odd degree greater than one, but have no points in k itself. It is the purpose of this note to give a method whereby an infinite family of such curves Γ may be produced (of which the two examples of Bremner, Lewis, Morton are special cases).

2. From Coray [**3**] it follows that if the quartic curve Γ (of genus 3, when irreducible) possesses a point in a cubic extension of k, then it will possess points in extension fields of k of every odd degree greater than one. So it will suffice to produce a family of curves having points in a cubic extension of k. We search for polynomial identities of the following type:

$$(x^3+ax^2+bx+c)(x^3-ax^2+bx-c)(x^2+d) = (x^2+e)^4+Mx^4+N. \qquad (1)$$

Such an identity implies that the diagonal form $X^4+MY^4+NZ^4=0$ representing a quartic curve does indeed have zeros in the field defined by a root of the cubic polynomial x^3+ax^2+bx+c. It will then remain to ensure that this cubic is irreducible, and that there are no global points on the quartic curve.

Equating coefficients at (1) gives

$$d+2b-a^2=4e \qquad (2)$$

$$b^2-2ac+(2b-a^2)d=6e^2+M \qquad (3)$$

$$d(b^2-2ac)-c^2=4e^3 \qquad (4)$$

$$-dc^2=e^4+N \qquad (5)$$

and eliminating d between (2), (4) gives

$$c^2+2c(a^3-2ab+4ae)+4e^3-4eb^2+2b^3-a^2b^2=0.$$

Thus

$$c=-a^3+2ab-4ae+\Delta \tag{6}$$

where

$$\Delta^2=a^6-4a^4(b-2e)+a^2(5b^2-16be+16e^2)+(-2b^3+4be^2-4e^3). \tag{7}$$

Put now

$$\lambda=b/e, \qquad p(\lambda)=\lambda^3-2\lambda^2+2 \tag{8}$$

and

$$\rho=-2p(\lambda)e/a^2, \qquad \sigma=2p(\lambda)\,\Delta/a^3. \tag{8$'$}$$

Then (7) becomes

$$\sigma^2=\rho^3+(5\lambda^2-16\lambda+16)\rho^2+8(\lambda-2)(\lambda^3-2\lambda^2+2)\rho+4(\lambda^3-2\lambda^2+2)^2; \tag{9}$$

and from (2)–(6), (8), (8′)

$$\begin{aligned}
b&=-\lambda a^2\rho/2p(\lambda)\\
c&=-a^3(p(\lambda)+(\lambda-2)\rho-\tfrac{1}{2}\sigma)/p(\lambda)\\
d&=a^2(p(\lambda)+(\lambda-2)\rho)/p(\lambda)\\
e&=a^2\rho/2p(\lambda)\\
4p(\lambda)^2M/a^4&=4p(\lambda)^2-8p(\lambda)\rho-(3\lambda^2-8\lambda+6)\rho^2-4p(\lambda)\sigma\\
16p(\lambda)^4N/a^8&=-32p(\lambda)^4-96(\lambda-2)p(\lambda)^3\rho-4(25\lambda^2-96\lambda+96)p(\lambda)^2\rho^2\\
&\quad-8(5\lambda^3-26\lambda^2+48\lambda-31)p(\lambda)\rho^3-(2\lambda^2-6\lambda+5)(2\lambda^2-2\lambda-3)\rho^4\\
&\quad+16[p(\lambda)+(\lambda-2)\rho]^2p(\lambda)\sigma.
\end{aligned} \tag{10}$$

Now (9) represents the equation of an elliptic curve E over the field $\mathbf{Q}(\lambda)$, and any point of E defined over $\mathbf{Q}(\lambda)$ gives rise via the maps (10) to an identity (1). For example, let A be the point of E given by

$$A=(0,2p(\lambda)). \tag{11}$$

Then $(M,N)=(-a^4,0)$ and the associated quartic curve may be taken in the form $X^4-Y^4=0$. Similarly $-A=(0,-2p(\lambda))$ gives rise to the quartic curve $X^4+3Y^4-4Z^4=0$. These two curves, however, clearly possess points rational over $\mathbf{Q}(\lambda)$ (indeed, over $\mathbf{Q}$). But consider instead the point $2A=(-\lambda^2,-4)$ on E; this gives rise to the example given as III(a) in Bremner, Lewis, Morton [**1**]. Further, the point at infinity on E gives rise to the example III(b).

3. If we let B be the point of E given by

$$B=(-\lambda^2+1,\lambda^2+1) \tag{12}$$

then

$$A-B=\left(\frac{4(\lambda^3-2\lambda^2+2)}{(\lambda-1)^2},\frac{-2(\lambda^3-2\lambda^2+2)(\lambda^3+\lambda^2-7\lambda+9)}{(\lambda-1)^3}\right). \tag{13}$$

Denoting this point by P, it is easy to verify that P has infinite order in the group of $\mathbf{Q}(\lambda)$-rational points of E.

REMARKS. It is well-known that the group of $\mathbf{Q}(\lambda)$-points on E is finitely generated; it seems plausible that the rank of the group is 2 with generators A, B at (11), (12), but this has not been specifically checked.

THEOREM. *Let $m\in\mathbf{Z}$, $m\equiv 1 \bmod 9$. Then the point mP of E gives rise in the manner described above to a quartic curve $\Gamma: X^4+MY^4+NZ^4=0$ which possesses no point defined over $\mathbf{Q}(\lambda)$, but does have a point defined over a cubic extension of $\mathbf{Q}(\lambda)$.*

Proof. The method is to localize at the prime ideal (λ) of $\mathbf{Q}[\lambda]$, thereby restricting attention to the constant terms of all the polynomials.

Indeed, P specializes to the point

$$P_0=(8,36)$$

on the curve

$$E_0: S^2=R^3+16R^2-32R+16. \tag{14}$$

Considering the further reduction modulo 5, P_0 corresponds to the point

$$\tilde{P}_0=(3,1)$$

on the curve

$$\tilde{E}_0: s^2=r^3+r^2+3r+1.$$

Now $2\tilde{P}_0=(2,2)$; $3\tilde{P}_0=(0,1)$; $4\tilde{P}_0=(1,4)$; $5\tilde{P}_0=(1,1)$, so that $\tilde{P}_0$ is of order 9 on $\tilde{E}_0$. It follows that for $k\in\mathbf{Z}$, then $Q_k=(9k+1)P_0\equiv P_0\equiv(3,1) \bmod 5$. Such points Q_k give rise to quartic curves

$$\Gamma: X^4+MY^4+NZ^4=0 \tag{15}$$

where from (10), with obvious notation, $M_0\equiv a^4$, $N_0\equiv a^8 \bmod 5$.

In particular, taking a non-zero mod 5, then

$$M_0\equiv N_0\equiv 1 \bmod 5. \tag{16}$$

Suppose now (x, y, z) is a point of (15) defined over $\mathbf{Q}(\lambda)$, where x, y, z have no common factor. Then specializing to $\lambda=0$ results in the rational identity

$$x_0^4+M_0y_0^4+N_0z_0^4=0 \tag{17}$$

which by (16) forces $x_0=y_0=z_0=0$. Then x, y, z are all divisible by λ, a contradiction. Thus Γ has no non-trivial $\mathbf{Q}(\lambda)$-point.

To show (15) has a point defined over a cubic extension of $\mathbf{Q}(\lambda)$, it suffices to show from (1) that the corresponding cubic x^3+ax^2+bx+c is irreducible over $\mathbf{Q}(\lambda)$. But from (10), specializing to $\lambda=0$,

$$(a_0, b_0, c_0) \equiv (a_0, 0, a_0^3) \bmod 5.$$

Now the cubic polynomial $\chi^3+a_0\chi^2+a_0^3$ is irreducible mod 5, and so x^3+ax^2+bx+c is irreducible over $\mathbf{Q}(\lambda)$.

4. Remark. Although (15) is locally insolvable at the prime (λ), it is solvable modulo $\mathfrak{p}$ for those prime divisors $\mathfrak{p}$ of M, N. For from (2)–(5)

$$M=(4e^3+c^2)/d+(4c-d)d-6e^2$$
$$N=-dc^2-e^4;$$

then on eliminating d:

$$(c^2+e^3)^4+M(ce)^4 \equiv 0 \bmod N$$

and on eliminating c^2:

$$(d-e)^4+N.1^4 \equiv 0 \bmod M.$$

These lift by Hensel's Lemma to $\mathfrak{p}$-adic solutions (at least, in the former instance, for $(ce, N)=1$).

Finding an infinite family of examples where each member is everywhere locally solvable, seems quite a difficult problem.

REFERENCES

1. A. Bremner, D. J. Lewis and P. Morton, Some varieties with points only in a field extension, *Archiv der Math.* **43** (1984), 344–350.

2. J. W. S. Cassels, On a problem of Pfister about systems of quadratic forms, *Archiv der Math.* **33** (1979), 29–32.

3. D. F. Coray, Algebraic points on cubic hypersurfaces, *Acta Arith.* **30** (1976), 267–296.

4. D. F. Coray, On a problem of Pfister about intersections of three quadrics, *Archiv der Math.* **34** (1980), 403–411.

5. A. Pfister, *Systems of quadratic forms, Colloque sur les formes quadratiques,* 2 Bull. Soc. Math. France, Mem. No. 59, (1979), 115–123.

Department of Mathematics
Arizona State University
Tempe AZ 85287
U.S.A.