Arch. Math., Vol. 43, 344–350 (1984)

0003-889X/84/4304-0344 $ 2.90/0


# Some varieties with points only in a field extension

By

ANDREW BREMNER, D. J. LEWIS and PATRICK MORTON

We are interested in the following problem. Let $\Gamma$ be an irreducible algebraic variety of degree $d$, in projective $n$-space $\mathbb{P}^n$, defined over a field $k$; and suppose $K$ is a finite extension of $k$ with $[K:k]$ prime to $d$. If $\Gamma$ has a point defined over $K$, then does it necessarily have a point defined over $k$?

Several instances of this phenomenon are known, in particular when $\Gamma$ is a quadric in $\mathbb{P}^n$ [12], or a cubic plane curve [11]. Brumer [3] and Amer [1] have shown that the result holds for the intersection of two quadrics, while Pfister [10] has shown that results of this nature do not continue to generalize by giving an example of three quadrics in $\mathbb{P}^2$ having a zero in $\mathbb{Q}(\sqrt[3]{2})$, but no zero in $\mathbb{Q}$. Further such counterexamples involving systems of quadrics are given by Cassels [4] and Coray [5].

Cassels and Swinnerton-Dyer have conjectured that if $\Gamma$ is a cubic hypersurface in $\mathbb{P}^n$, then the existence of a point defined over $K$ with $[K:k]$ prime to 3, implies the existence of a $k$-rational point on $\Gamma$. This conjecture is still unresolved, but Coray [6] has shown that when $n = 3$, then a point on $\Gamma$ defined over such a field $K$ implies that $\Gamma$ has a point over a field extension $L$ of $k$ with $[L:k] = 1$, 4, or 10. Finally, Coray in [6] gives an example of a quartic curve over $\mathbb{Q}$ possessing no rational point (because it possesses no 5-adic point), yet having a point over a cubic extension of $\mathbb{Q}$.

We give in this note some further examples of instances where points on a variety defined over an extension field do not imply the existence of points defined over the base field. In (I) we give two cubics in $\mathbb{P}^2$ defined over $\mathbb{Q}$, having a common zero over a quadratic extension of $\mathbb{Q}$, but having no common zero in $\mathbb{Q}$. In (II) and (III) we are concerned with quartic curves in $\mathbb{P}^2$. Coray [6] has shown [Cor. 6.5] that a point on such a curve $\Gamma$ defined over a field $K$ where $[K:k]$ is odd, implies that $\Gamma$ has a point over a field extension $L$ of $k$ with $[L:k] = 1$ or 3. In (II) we give an example of such a curve in $\mathbb{P}^2$ which is everywhere locally solvable, has no point defined over $\mathbb{Q}$, but does have a point defined over a cubic extension of $\mathbb{Q}$. In (III) we give two similar examples defined over the function field $\mathbb{Q}(t)$. In (IV) we give a quartic form in 16 variables with a point over a cubic extension of $\mathbb{Q}$, but with no point actually in $\mathbb{Q}$.

**I.** Let $\Gamma$ be the intersection of the two cubics:

$$x^3 + y^3 + z^3 = 0, \quad x y^2 - z(y^2 - yz + z^2) = 0.$$

Then $\Gamma$ contains the point $(x, y, z) = (0, \omega, 1)$ where $\omega = \dfrac{1 + \sqrt{-3}}{2}$. But as is well known

[9], any rational point on $\Gamma$ must have $xyz = 0$, and it is immediate to deduce that $x = y = z = 0$.

**II (a).** Let $\Gamma$ be the quartic curve over $\mathbb{Q}$ defined by

$$(1) \qquad \Gamma\colon 3x^4 + 4y^4 = 19z^4.$$

Now (1) is everywhere locally solvable. Indeed, it represents a curve of genus 3, so by Weil's estimate [13] the number $N_p$ of points modulo $p$ on (1) satisfies the inequality

$$N_p \geqq p + 1 - [6\sqrt{p}],$$

and thus there is a $p$-adic point on $\Gamma$ provided $p \geqq 37$. It is easy to check solvability for the remaining primes.

Define the cubic irrational $\theta$ by

$$\theta^3 + 2\theta^2 + 2\theta - 32 = 0.$$

Then by direct calculation, $(x, y, z) = (\theta^2 + 2, 3\theta, 6)$ is a point on $\Gamma$. However we now show that $\Gamma$ has no points defined over $\mathbb{Q}$.

We work in the extension $K = \mathbb{Q}(\alpha)$, where $\alpha^4 = -12$. The following facts about $K$ are relegated to an appendix. An integral basis is $\{1, \alpha, \omega_1, \omega_2\}$ where $\omega_1 = \frac{1}{2} + \frac{1}{4}\alpha^2$, $\omega_2 = \frac{1}{2}\alpha + \frac{1}{4}\alpha^3$ (notice that $\omega_1$ is a root of unity); the class number of $K$ is 1; a fundamental unit is $\varepsilon = -3 + 4\omega_1 + 2\omega_2$; and there are the ideal factorizations

$$(2) = \mathfrak{p}_2^2, \quad (19) = (4 - \sqrt{-3})(4 + \sqrt{-3}) = (4 - \sqrt{-3})\,\mathfrak{p}_{19}\bar{\mathfrak{p}}_{19},$$
$$(4 + \alpha - 4\omega_1 - 2\omega_2) = \mathfrak{p}_2\mathfrak{p}_{19}.$$

We now suppose $x, y, z$ are integers with no common factor, and satisfy (1). Then

$$(2) \qquad x \equiv z \equiv 1 \bmod 2, \qquad y \equiv 0 \bmod 2.$$

Write (1) in the form

$$\mathrm{Norm}_{K/Q}(2y + x\alpha) = 2^2 \cdot 19 z^4.$$

Since the only possible common ideal factor of $(2y + x\alpha)$ and its conjugates is $\mathfrak{p}_2$, we deduce the ideal equation

$$(3) \qquad (2y + x\alpha) = \mathfrak{p}_2\mathfrak{p}_{19}\mathfrak{a}^4$$

for some integral ideal $\mathfrak{a}$ of $K$ (where we have chosen the sign of $x$ to ensure divisibility by $\mathfrak{p}_{19}$). Since $K$ has class number 1, then (3) takes the non-ideal form

$$(4) \qquad \pm(2y + x\alpha) = (4 + \alpha - 4\omega_1 - 2\omega_2)\,\varepsilon^r \omega_1^s A^4,$$

where $\omega_1$ is the primitive root of unity in $K$, $r$ and $s$ are integers, and $A$ is an integer of $K$ with norm equal to $z$. Using $\omega_1 = \omega_1^4$ then (4) may be written

$$(5) \qquad \pm(2y + x\alpha) = (4 + \alpha - 4\omega_1 - 2\omega_2)\,\varepsilon^r A^4$$

where without loss of generality, $0 \leqq r \leqq 3$. Then modulo 4, we obtain from (2) and (5), using the fact that $\alpha \cdot 2\omega_2 = 4\omega_1 - 8$,

$$\pm x\alpha \equiv (\alpha - 2\omega_2)(1 + 2\omega_2)^r A^4$$

$$\equiv (\alpha - 2\omega_2) A^4. \tag{6}$$

Then modulo 2, $\alpha \equiv \alpha A^4$, whence $A^4 \equiv 1 \bmod \mathfrak{p}_2$. However, Norm $\mathfrak{p}_2 = 4$ and $(A, \mathfrak{p}_2) = 1$ imply $A^3 \equiv 1 \bmod \mathfrak{p}_2$; thus $A \equiv 1 \bmod \mathfrak{p}_2$ from which it follows that $A^4 \equiv 1 \bmod 4$. Equation (6) now gives

$$\pm x\alpha \equiv \alpha - 2\omega_2 \bmod 4,$$

a contradiction on comparing coefficients of $\omega_2$.

Remark. Let $p$ be a prime, $p \equiv 3 \bmod 16$, satisfying the condition

$$4p = \mathrm{Norm}_{K/Q}(2r + s\alpha + 2t\omega_1 + u\omega_2)$$

where $r, s, t, u$ are integers with $u \equiv 2 \bmod 4$, $s \equiv 1 \bmod 2$. Such primes include 19, 163, 403, ... Then a similar argument to the above shows there can be no rational point on the curve

$$\Gamma_p\colon 3x^4 + 4y^4 = pz^4.$$

However it is not clear whether in general $\Gamma_p$ contains points defined over some cubic extension of $\mathbb{Q}$; it is possible for a rational quartic curve with points over $\mathbb{R}$ not to possess points over any cubic extension of $\mathbb{Q}$ (and hence to possess points only over extension fields of $\mathbb{Q}$ of even degree).

**II (b).** Another quartic curve with the properties of (1) is

$$\Gamma\colon 4x^4 + 97y^4 = z^4.$$

This has the point $(x, y, z) = (\theta^2, 3\theta, 5\theta + 96)$ over the cubic extension $\mathbb{Q}(\theta)$ where $\theta^3 + 2\theta^2 - 60\theta - 576 = 0$. But $\Gamma$ has no rational points; we do not give the details.

Notice that there are obvious maps from $\Gamma$ to each of the three elliptic curves

$$E_1\colon 4X^2 + 97y^4 = z^4$$

$$E_2\colon 4x^4 + 97Y^2 = z^4$$

$$E_3\colon 4x^4 + 97y^4 = Z^2.$$

Each of these curves has positive rational rank for it may be checked that the following are points of infinite order on each $E_i$ respectively:

$$(X, y, z) = (24, 1, 7)$$

$$(x, Y, z) = (66, 1751, 139)$$

$$(x, y, Z) = (2, 3, 89).$$

So certainly $\Gamma$ is trying hard to have rational points! This phenomenon occurs also in II (a) in virtue of the identities:

$$3.10^2 + 4.1^4 = 19.2^4$$

$$3.1^4 + 4.2^2 = 19.1^4$$

$$3.5^4 + 4.8^4 = 19.31^2.$$

See Bremner and Morton [2] for further examples of this type.

**III (a).** Let $\Gamma$ be the quartic curve over the function field $\mathbb{Q}(t)$ defined by

$$X^4 + (4t^3 - 4t^2 + 1)^2 (4t^6 - 6t^4 + 16t^3 - 12t^2 + 3) Y^4 = (t^8 + 16t^3 - 16t^2 + 4) Z^4 .$$

Define $\theta$ by

$$\theta^3 + (4t^3 - 4t^2 + 1)\theta^2 + 2t^3(4t^3 - 4t^2 + 1)\theta - 2(4t^3 - 4t^2 + 1)^2 = 0 .$$

Since this polynomial is irreducible over $\mathbb{Q}(t)$ (by considering, for example, specialization at $t = 1$), $\theta$ is cubic over $\mathbb{Q}(t)$. And calculation shows that the following is a point of $\Gamma$:

$$(X, Y, Z) = (\theta^2 + t^2(4t^3 - 4t^2 + 1),\ \theta,\ 4t^3 - 4t^2 + 1) .$$

However, specialization of $\Gamma$ at $t = \frac{1}{2}$ results in the equation

$$3(4x)^4 + 4(3y)^4 = 19(3z)^4 \tag{7}$$

where $x = X(\frac{1}{2})$, $y = Y(\frac{1}{2})$, $z = Z(\frac{1}{2})$; and by example II (a), equation (7) has no non-trivial rational solution. Accordingly, $\Gamma$ has no point defined over $\mathbb{Q}(t)$.

**III (b).** Let $\Gamma$ be the quartic curve over $\mathbb{Q}(t)$ defined by

$$4(3t^2 - 8t + 6)(t^3 - 2t^2 + 2)^2 X^4 + (4t^4 - 16t^3 + 16t^2 + 8t - 15) Y^4 = Z^4 .$$

Define $\theta$ by

$$\theta^3 - 2t(t^3 - 2t^2 + 2)\theta + 4(t^3 - 2t^2 + 2)^2 = 0.$$

By considering specialization at $t = 0$, $\theta$ is cubic over $\mathbb{Q}(t)$. And the following is a point of $\Gamma$:

$$(X, Y, Z) = (\theta,\ 2(t^3 - 2t^2 + 2),\ \theta^2 - 2(t^3 - 2t^2 + 2)) .$$

However, specialization of $\Gamma$ at $t = 3$ results in an equation

$$484x^4 + 5y^4 = 9z^4 \tag{8}$$

and we now show that (8) has no non-trivial rational solution, whence $\Gamma$ has no point over $\mathbb{Q}(t)$. A similar argument may be used to that of II (a), working with the quartic field $\mathbb{Q}(\sqrt[4]{-2420})$, but instead we give a more elementary proof along lines suggested by Cassels.

Certainly in (8) we may suppose $(x, y, z) = 1$; and it follows that $x \equiv y \equiv z \equiv 1 \bmod 2$. Then

$$(3z^2 + 22x^2)(3z^2 - 22x^2) = 5y^4 \quad \text{and}$$
$$(3z^2 + 22x^2, 3z^2 - 22x^2) = (3z^2 + 22x^2, 6z^2) = 1,$$

so that there exist odd, coprime integers $u, v$ satisfying

$$3z^2 \pm 22x^2 = 5u^4$$
$$3z^2 \mp 22x^2 = v^4$$
$$y = uv .$$

Modulo 8, the upper sign is impossible, and so

$$v^4 + 5u^4 = 6z^2$$
$$v^4 - 5u^4 = 44x^2.$$

Write the latter equation in the form

$$(v^2 - 15u^2 - 22x)^2 = 2(4v^2 - 5u^2 + 22x)(7v^2 + 5u^2 - 44x).$$

The highest common factor of the three terms divides

$$\begin{vmatrix} 1 & -15 & -22 \\ 4 & -5 & 22 \\ 7 & 5 & -44 \end{vmatrix} = -2.5^2\,11^2.$$

Now certainly $v^2 \equiv 4u^2 \bmod 11$, and the sign of $x$ may be chosen so that $v^2 \equiv 2x \bmod 5$. Then each term is divisible by 55, and since $u, v$ are odd, then $4v^2 - 5u^2 + 22x \equiv 1 \bmod 2$. Thus

$$\begin{aligned} v^2 - 15u^2 - 22x &= 110R \\ 4v^2 - 5u^2 + 22x &= 55S \qquad (9) \\ 7v^2 + 5u^2 - 44x &= 110T \end{aligned}$$

where $R^2 = ST$; and then

$$u^2 = -6R - S + 2T$$
$$v^2 = -2R + 7S + 8T$$
$$x = -R + S - T.$$

Since $(u, v) = 1$ then $(S, T) = 1$ and so there exist coprime integers $a, b$ with $R = ab$, $S = \pm b^2$, $T = \pm a^2$. Then from (9) using a congruence modulo 4, it must be the case that $S = -b^2$, $T = -a^2$. But now

$$v^2 = -8a^2 - 2ab - 7b^2$$

forcing $a = b = 0$, $v = u = 0$, impossible.

Remark. As in II(b), each of the three elliptic curves associated with (8) has positive rational rank, in virtue of the arithmetic identities:

$$484.11^2 + 5.11^4 = 9.11^4$$
$$484.1^4 + 5.7^4 = 9.3^4$$
$$484.1^4 + 5.4^4 = 9.14^2.$$

We have not been able to verify whether the elliptic curves over $\mathbb{Q}(t)$ associated with the examples of III, also have positive rank.

**IV.** Consider the quartic surface $V$ defined by $F = 0$ where

$$F(x, y, z, t) = x^4 + 511y^4 - 134z^4 - 14t^4.$$

Then $V$ contains the point $(x, y, z, t) = (\theta^2 - 2, 2, \theta, \theta)$ where $\theta$ is the cubic irrational given by $\theta^3 + 2\theta^2 + 2\theta + 32 = 0$. However, modulo 5 we have that $F(x, y, z, t) \equiv x^4 + y^4 + z^4 + t^4$, and consequently $V$ cannot contain a rational point. It is now evident that the form

$$F(x_1, y_1, z_1, t_1) + 5F(x_2, y_2, z_2, t_2) + 5^2 F(x_3, y_3, z_3, t_3) + 5^3 F(x_4, y_4, z_4, t_4),$$

cannot represent zero over $\mathbb{Q}$, but does contain a point defined over the cubic extension $\mathbb{Q}(\theta)$. For diagonal quartic forms this is best possible in view of the result of Davenport and Lewis [7] which states that a diagonal quartic form over $\mathbb{Q}$ in at least seventeen variables, has a zero over $\mathbb{Q}$.

Appendix. We give now the arithmetic details of the number field $K = \mathbb{Q}(\alpha)$, $\alpha^4 = -12$. That $\{1, \alpha, \omega_1, \omega_2\}$ is an integral basis can be seen as follows. Certainly $\omega_1 = \frac{1}{2} + \frac{1}{4}\alpha^2 = \dfrac{1 + \sqrt{-3}}{2}$, $\omega_2 = \alpha\omega_1$, are integers of $K$. The discriminant of the basis $\{1, \alpha, \omega_1, \omega_2\}$ is $2^6 3^3$; since the prime (3) is totally ramified in $K$, it suffices to show that if

$$r + s\alpha + t\omega_1 + u\omega_2 \equiv 0 \bmod 2 \tag{10}$$

for integers $r, s, t, u$, then $r \equiv s \equiv t \equiv u \equiv 0 \bmod 2$.

Now $(2) = \mathfrak{p}_2^2$ in $K$, with $\alpha \equiv 0 \bmod \mathfrak{p}_2$, and thus from (10) we have $r + t\omega_1 \equiv 0 \bmod \mathfrak{p}_2$, whence $r \equiv t \equiv 0 \bmod 2$. Then $s + u\omega_1 \equiv 0 \bmod \mathfrak{p}_2$ and $s \equiv u \equiv 0 \bmod 2$.

As regards the class number of $K$, the Minkowski bound gives that every ideal class contains an ideal of norm at most 6. But $(2) = (\alpha + 2\omega_1)^2$, $(3) = (1 - 2\omega_1 + \omega_2)^4$, and (5) remains prime; so the class number of $K$ is indeed one. Finally, note that $\varepsilon = -3 + 4\omega_1 + 2\omega_2$ has norm 1, so is a unit of $K$. Further, $|\varepsilon| = 7.32\ldots$; but by a result of Delone and Faddeev [8], p. 371, there exists a fundamental unit in $K$ with absolute value greater than $2\sqrt[4]{11} = 3.64\ldots$ and hence it is clear that $\varepsilon$ is itself a fundamental unit.

The authors were supported by an NSF Grant during some of the research for this paper.

## References

[1] M. Amer, Quadratische Formen über Funktionenkörpern. Dissertation, Mainz 1976.
[2] A. Bremner and P. Morton, A new characterization of the integer 5906. Manuscripta Math. **44**, 187–229 (1983).
[3] A. Brumer, Remarques sur les couples de formes quadratiques. C.R. Acad. Sci. Paris **286** A, 679–681 (1978).
[4] J. W. S. Cassels, On a problem of Pfister about systems of quadratic forms. Arch. Math. **33**, 29–32 (1979).
[5] D. F. Coray, On a problem of Pfister about intersections of three quadrics. Arch. Math. **34**, 403–411 (1980).
[6] D. F. Coray, Algebraic points on cubic hypersurfaces. Acta Arith. **30**, 267–296 (1976).
[7] H. Davenport and D. J. Lewis, Homogeneous additive equations. Proc. Royal Soc. A. **274**, 443–460 (1963).
[8] B. N. Delone and D. K. Faddeev, Theory of irrationalities of the third degree. Amer. Math. Soc. Transl. 1964.

[9] A. M. LEGENDRE, Mém. Acad. Roy. Sc. de l'Inst. de France **6**, 41, Sec. 49 (1823).
[10] A. PFISTER, Systems of Quadratic Forms. Colloque sur les Formes Quadratiques, 2 Bull. Soc. Math. France Mem. **59**, 115–123 (1979).
[11] H. POINCARÉ, Sur les propriétés arithmétiques des courbes algébriques. J. Math. Pures Appl. **7**, 161–233 (1901).
[12] T. A. SPRINGER, Sur les formes quadratiques d'indice zéro. C.R. Acad. Sci. Paris **234**, 1517–1519 (1952).
[13] A. WEIL, Sur les courbes algébriques et les variétés qui s'en déduisent. Paris 1948.

Eingegangen am 9. 12. 1983

Anschrift der Autoren:

A. Bremner
Dept. of Pure Mathematics
and Mathematical Statistics
16 Mill Lane
Cambridge
England

D. J. Lewis
Dept. of Mathematics
The University of Michigan
Ann Arbor
Michigan 48 109
USA

P. Morton
Department of Mathematics
California Institute of Technology
Pasadena, California
USA