SUPERSIMPLICITY AND QUADRATIC EXTENSIONS

A. MARTIN-PIZARRO[†] AND F. O. WAGNER[‡]

Abstract. Elliptic curves over a supersimple field with exactly one extension of degree 2 have s-generic rational points.

1. Introduction

Shelah's simple theories [11] were shown to be a good setting to adapt some of the ideas of geometric model theory after the results of Kim and Pillay [5]. In doing so, new ideas and methods need to be developed, because of the weakness of simplicity (or rather, strength of stability) when carrying over some of the arguments.

Typical examples of simple unstable structures are, among others, the Random graph, pseudo-finite fields [1] (i.e. infinite models of the theory of all finite fields, or equivalently, perfect PAC fields with absolute Galois group) and more generally [3], perfect PAC fields with bounded absolute Galois group (i.e. only finitely many open subgroups of index n for every n). All the above examples are supersimple of SU-rank 1. Unfortunately, an algebraic characterization of supersimple fields is far from being obtained as in the superstable case [2, 6]. It has been conjectured in 1995 by A. Pillay that all supersimple fields lie in the above category. In [9] it was shown that supersimple fields are perfect and have bounded absolute Galois group. Therefore, only the PAC condition is left to be proved (or disproved for those who have little faith in the universum behaving as it should). Recall that a perfect field K is PAC (it stands for **P***seudo* **A***lgebraically* **C***losed*) if every absolutely irreducible variety defined over K has a K-rational point,

Date: July 12, 2005.

1991 *Mathematics Subject Classification.* 03C45.

Key words and phrases. supersimple, field, elliptic curve, generic point.

Work done during the semester on Model Theory and Applications in Algebra and Analysis at the Isaac Newton Institute for the Mathematical Sciences, whose hospitality is gratefully acknowledged.

[†]Research supported by a DFG-Forschungsstipendium MA3310/1-1

[‡]Membre junior de l'Institut universitaire de France.

or equivalently, if every absolutely irreducible plane curve over K has such a point.

Special families of curves have been already considered: [10] dealt with the genus 0 case successfully and showed that all genus 0 curves are birationally isomorphic to $\mathbb{P}^1$. In [7, 8] some families of elliptic and hyperelliptic curves were treated, in particular those whose rational isomorphism class was generic in the appropriate moduli space. In this note, we will prove the following:

Main Theorem. *Let K be a supersimple field with exactly one extension of degree 2 (up to isomorphism). Any elliptic curve E defined over K has an s-generic K-rational point, i.e. a point P in $E(K)$ such that $SU(P/F) = SU(K)$, where F is some small set of parameters over which E is defined.*

The relevance of the above theorem is that it holds for all elliptic curves and not only for those with generic modulus. On the other hand, it is restrictive in the sense that we require K to have a unique extension of degree 2. It is still open to generalize this result to a an arbitrary number of extension of degree 2. Moreover, it is still not clear how to transfer the techniques here exhibited for curves of larger genus, since we strongly use the group law in an elliptic curve.

We should like to thank Thomas Scanlon for helpful discussions, and Juan Pons-Llopis for a careful proof-reading of a previous version of this work.

2. Equations and group law

Throughout this section, we fix a perfect field K and some algebraic closure $\overline{K}$. The material for this section has been obtained from [4, 12].

An *elliptic curve* over K is a pair (E, O) consisting of a projective nonsingular curve E of genus 1 defined over K and a distinguished K-rational point O.

By Riemann-Roch, there exist x and y in $K(E)$ such that x has a pole of degree 2 at O and y a pole of degree 3 at O, and they satisfy the following relation:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

for some a_i in K. Such an equation is a *Weierstrass equation* for the elliptic curve (E, O), where we identify O with the projective point

$[0, 1, 0]$. Depending on the characteristic of K further reductions of the equation may be done.

An elliptic curve E over K admits a commutative group structure, uniquely determined from the choice of the point O. Let P and Q be points in $E(K)$ and ℓ the line connecting them (if P equals Q then ℓ is the tangent line to E at P). By Bezout's Theorem, ℓ intersects E in 3 points (counted with multiplicities). Let R be the third point of $\ell \cap E$ and ℓ' be the line determined by R and O. We define $P + Q$ to be the third point in $\ell' \cap E$. This operation so defined makes E into an abelian variety defined over K such that O is the identity element.

Fact 2.1. *Given an elliptic curve E defined by an equation as above and $P = (x, y)$ in E, then the additive inverse is $-P = (x, -y - a_1x - a_3)$.*

Likewise, for distinct points P and Q in E which are not inverses of each other, we have that:

$$x(P+Q) = \left(\frac{y(Q) - y(P)}{x(Q) - x(P)}\right)^2 + a_1\left(\frac{y(Q) - y(P)}{x(Q) - x(P)}\right) - a_2 - x(P) - x(Q).$$

3. Results

In this section we shall prove the main theorem. So let K be a supersimple field of any characteristic definable inside some sufficiently saturated structure. We suppose that K has (up to isomorphism) a unique quadratic extension $L = K(\delta)$. Since K is perfect [9], we may choose δ such that $\delta^2 = d \in K^\times \setminus (K^\times)^2$ (in characteristic different from two), or $\delta^2 + \delta = d \in K^+ \setminus \{k^2 + k : k \in K\}$ (in characteristic two). Let σ be a generator of the Galois group of L over K, and N the generalized norm map

$$N : E(L) \to E(K), \qquad P \mapsto P + P^\sigma.$$

We first treat the case where the characteristic is different from 2 and 3. By [7], after a K-rational change of variables, a *Weierstrass equation* for E over K takes the form

$$y^2 = x^3 + ax + b$$

for some non-zero a and b in K with discriminant $\Delta = -16(4a^3 + 27b^2) \neq 0$.

Let us consider the restriction of scalars of E (viewed as defined over L) over K. A pair $(x_1 + \delta x_2, y_1 + \delta y_2)$ is in $E(L)$ if and only if it satisfies

the following equations:

$$y_1^2 + dy_2^2 = x_1^3 + 3dx_1x_2^2 + ax_1 + b$$
$$2y_1y_2 = x_2(3x_1^2 + dx_2^2 + a).$$

By [10] there are x_1 and x_2 in K with x_1 generic over $\{a, b\}$ such that $3x_1^2 + dx_2^2 + a = 0$. By our assumptions on the number of quadratic extensions of K, the quantity $x_1^3 + 3dx_1x_2^2 + ax_1 + b$ is either a square or it lies in $d \cdot (K^\times)^2$. In either case there exists some y in K and ϵ in $\{1, \delta\}$ such that

$$(\epsilon y)^2 = x_1^3 + 3dx_1x_2^2 + ax_1 + b$$
$$0 = 3x_1^2 + dx_2^2 + a.$$

Then $P = (x_1 + \delta x_2, \epsilon y) \in E(L)$ and $SU(P/\{a, b\}) = SU(K)$. Substituting the second into the first equation, we obtain

$$(\epsilon y)^2 = -8x_1^3 - 2ax_1 + b = (-2x_1)^3 + a(-2x_1) + b,$$

so if $\epsilon = 1$ the point $(-2x_1, y)$ is s-generic in $E(K)$.

If $\epsilon = \delta$, we compute the x-coordinate of $N(P) = P + P^\sigma \in E(K)$:

$$\begin{aligned} x(N(P)) &= \left(\frac{y(P^\sigma) - y(P)}{x(P^\sigma) - x(P)}\right)^2 - x(P) - x(P^\sigma) \\ &= (\frac{-2\delta y}{-2\delta x_2})^2 - 2x_1 = \frac{-8x_1^3 - 2ax_1 + b}{-3x_1^2 - a} - 2x_1 = \frac{2x_1^3 - b}{3x_1^2 + a}, \end{aligned}$$

and $N(P)$ is s-generic in $E(K)$, since x_1 and $x(N(P))$ are interalgebraic over $\{a, b\}$.

If the characteristic is three, the equation for E can be reduced to the form

$$y^2 = x^3 + ax^2 + b$$

with non-zero a and b in K. By restriction of scalars of E, we obtain this time

$$y_1^2 + dy_2^2 = x_1^3 + adx_2^2 + ax_1^2 + b$$
$$2y_1y_2 = x_2(dx_2^2 + 2ax_1).$$

Choose x_2 in K generic over $\{a, b\}$, and define $x_1 = a^{-1}dx_2^2$. Since the characteristic is three, $dx_2^2 + 2ax_1 = 0$; as there is a unique extension of degree two,

$$x_1^3 + adx_2^2 + ax_1^2 + b = x_1^3 + ax_1^2 + a^2x_1 + b = (x_1 - a)^3 + a(x_1 - a)^2 + b$$

is either a square or in $d \cdot (K^\times)^2$. Hence there is $\epsilon \in \{1, \delta\}$ and $y \in K$ such that the point $P = (x_1 + \delta x_2, \epsilon y)$ is in $E(L)$. If $\epsilon = 0$, then

$(x_1 - a, y)$ is an s-generic point in $E(K)$. If $\epsilon = \delta$, we calculate the image $P + P^\sigma$ of P under the norm map :

$$\begin{aligned} x(P + P^\sigma) &= \left(\frac{y(P^\sigma) - y(P)}{x(P^\sigma) - x(P)}\right)^2 - a - x(P) - x(P^\sigma) \\ &= (\frac{-2\delta y}{-2\delta x_2})^2 - a - 2x_1 = \frac{dy^2}{dx_2^2} - a - 2x_1 \\ &= \frac{x_1^3 + ax_1^2 + a^2x_1 + b}{ax_1} - a - 2x_1 = \frac{x_1^3 - ax_1^2 + b}{ax_1}, \end{aligned}$$

so $P + P^\sigma$ is s generic in $E(K)$, as $x(P + P^\sigma)$ and x_1 are interalgebraic over $\{a, b\}$.

Finally, in characteristic two the *Weierstrass equation* for E over K takes the form

$$y^2 + xy = x^3 + ax^2 + b$$

with a and b in K and b nonzero [7].

Putting $y = xz$ and dividing by x^2, this equation can be rewritten as

$$z^2 + z = \frac{x^3 + ax^2 + b}{x^2} = x + a + \frac{b}{x^2}.$$

Recall that the inverse of an element $x_1 + x_2\delta$ in L is

$$\frac{x_1 + x_2 + \delta x_2}{x_1^2 + dx_2^2 + x_1x_2}.$$

Again by restriction of scalars of E over K we obtain

$$\begin{aligned} z_1^2 + z_1 + dz_2^2 &= x_1 + a + b\frac{(x_1^2 + (d+1)x_2^2)}{(x_1^2 + dx_2^2 + x_1x_2)^2} \\ z_2^2 + z_2 &= x_2 + \frac{b}{(x_1^2 + dx_2^2 + x_1x_2)^2}x_2^2. \end{aligned}$$

Consider the equation

$$bx_2 = (x_1^2 + dx_2^2 + x_1x_2)^2 = x_1^4 + d^2x_2^4 + x_1^2x_2^2,$$

or equivalently

$$\frac{b}{x_2^3} = (\frac{x_1}{x_2})^4 + (\frac{x_1}{x_2})^2 + d^2.$$

By [7, 10] there is a solution (x_1, x_2) in K with x_2 generic over $\{a, b\}$, since the left-hand side is a coset of a multiplicative subgroup of bounded index, and the right-hand side represents a coset of an additive subgroup of bounded index (recall that K is perfect, so $K^2 = K$). By

uniqueness of L there is ϵ in $\{0,1\}$ and $z \in K$ such that the point $P = (x_1 + \delta x_2, (x_1 + \delta x_2)(z + \epsilon\delta))$ is in $E(L)$. Note that

$$\begin{aligned} z^2 + z + \epsilon\, d &= x_1 + a + b\frac{(x_1^2 + (d+1)x_2^2)}{(x_1^2 + dx_2^2 + x_1x_2)^2} = x_1 + x_2 + a + \frac{x_1^2 + dx_2^2}{x_2} \\ &= a + x_2 + \frac{x_1^2 + dx_2^2 + x_1x_2}{x_2} = a + x_2 + \frac{\sqrt{bx_2}}{x_2} \\ &= a + x_2 + \sqrt{\frac{b}{x_2}} = a + \sqrt{\frac{b}{x_2}} + \frac{b}{\sqrt{b/x_2}^2} \end{aligned}$$

(the square root of b/x_2 exists since K is perfect; note that it is again generic over $\{a,b\}$). In particular, for $\epsilon = 0$ the point $(\sqrt{b/x_2}, \sqrt{b/x_2}z)$ is s-generic in $E(K)$.

If $\epsilon = 1$, consider $N(P) = P + P^\sigma \in E(K)$. Put

$$\begin{aligned} \lambda :&= \frac{y(P^\sigma) - y(P)}{x(P^\sigma) - x(P)} = \frac{x(P^\sigma)z(P^\sigma) - x(P)z(P)}{x(P^\sigma) - x(P)} \\ &= \frac{(x_1 + (\delta+1)x_2)(z + \delta + 1) - (x_1 + \delta x_2)(z + \delta)}{x_1 + (\delta+1)x_2 - x_1 - \delta x_2} \\ &= \frac{x_2(z + \delta + 1) + x_1 + \delta x_2}{x_2} = \frac{x_1}{x_2} + z + 1. \end{aligned}$$

Then

$$\begin{aligned} x(P + P^\sigma) &= \lambda^2 + \lambda + a + x(P) + x(P^\sigma) \\ &= \frac{x_1^2}{x_2^2} + z^2 + 1 + \frac{x_1}{x_2} + z + 1 + a + (x_1 + \delta x_2) + (x_1 + (\delta+1)x_2) \\ &= (\frac{x_1^2}{x_2^2} + \frac{x_1}{x_2}) + (z^2 + z) + a + x_2 \\ &= (\sqrt{\frac{b}{x_2^3}} + d) + (a + x_2 + \sqrt{\frac{b}{x_2}} + d) + a + x_2 \\ &= \sqrt{\frac{b}{x_2^3}}\,(1 + x_2), \end{aligned}$$

which is interalgebraic with x_2 over $\{a,b\}$. Hence $N(P)$ is s-generic in $E(K)$. □

References

[1] Z. Chatzidakis, L. van den Dries, A. Macintyre, *Definable sets over finite fields*, J. Reine Angew. Math. **427**:107–135, 1992.

[2] G. Cherlin, S. Shelah, *Superstable fields and groups*, Ann. Math. Logic **18**(3):227–270, 1980.
[3] E. Hrushovski, Pseudo-finite fields and related structures, preprint, 1991.
[4] D. Husemöller, *Elliptic Curves*, Springer-Verlag, Berlin, Germany, 2000.
[5] B. Kim, A. Pillay, *Simple theories*, Ann. Pure Appl. Logic **88**(2–3):149–164, 1997.
[6] A. Macintyre, *On* ω_1-categorical theories of fields, Fund. Math. **71**(1):1–25, 1971.
[7] A. Martin-Pizarro, A. Pillay, *Elliptic and Hyperelliptic curves over supersimple fields*, J. London Math. Soc. (2) **69**(1):1–13, 2004.
[8] A. Martin-Pizarro, *Elliptic and Hyperelliptic curves over supersimple fields in characteristic 2*, to appear in J. Pure and Applied Algebra.
[9] A. Pillay, B. Poizat, *Corps et chirurgie*, J. Symbolic Logic **60**(2):528–533, 1995.
[10] A. Pillay, T. Scanlon, F. Wagner, *Supersimple fields and division rings*, Math. Research Letters **5**:473-483, 1998.
[11] S. Shelah, *Simple unstable theories*, Ann. Math. Logic **19**(3):177–203, 1980.
[12] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, Berlin, Germany, 1986.
[13] F.O. Wagner, *Simple Theories*, Kluwer Academic Publishers, Dordrecht, The Nederlands, 2000.

A. Martin Pizarro, Institut für Mathematik, Humboldt-Universität zu Berlin, D–10099 Berlin, Germany

E-mail address: pizarro@mathematik.hu-berlin.de

F. O. Wagner, Institut Camille Jordan, Université Claude Bernard Lyon-1, 43 boulevard du 11 novembre 1918, F–69622 Villeurbanne Cedex, France

E-mail address: wagner@math.univ-lyon1.fr