THE IRREDUCIBILITY OF A CUBIC OVER $\mathbb{F}_q$

DAVID G. A. JACKSON

1. Introduction

It has been over 450 years since Cardano first gave his method for systematically determining the roots of a cubic equation. Finite fields have been around for at least 150 years. One would have thought that the question of deciding whether a cubic polynomial over a finite field is reducible would have been studied to death. Apparently not so.

The attention of the author was drawn to this subject when studying a paper of Chang [2] on the classification of the conjugacy classes of a Chevalley group of type G_2 over a finite field. On pages 197–198 of this paper Chang implicitly gives necessary and sufficient conditions for the polynomial $x^3 - 3x - \zeta$ to be irreducible over the field $\mathbb{F}_q$ for $q \equiv -1 \mod 3$. In the author's PhD thesis [4], a generalization of this result was needed which dealt with a general cubic, and this was subsequently extended further to include the case $q \equiv 1 \mod 3$. At this point Tonny Springer pitched in and gave a reformulation of the main result which was aesthetically quite pleasing. It is amusing that these results do not appear in the standard literature as they are quite elementary and could easily have been written down 100 years ago.

2. A refresher on Cardano's method

It is worthwhile reminding the reader on how Cardano solved his cubics. Cardano would have dealt with polynomials whose coefficients were real numbers. The coefficients of our cubics are however to be chosen from the finite field $k := \mathbb{F}_q$ (where q is some power of a prime p). It will be necessary to restrict the characteristic p of this field to be different from 2 or 3. Let our cubic be

$$g(y) := y^3 + a_2y^2 + a_1y + a_0$$

where a_0, a_1, $a_2 \in k$. By the substitution $y = x - a_2/3$, we are reduced to finding the roots of the cubic

$$f(x) := x^3 + \xi x + \eta$$

with ξ, $\eta \in k$. It is worthwhile noting at this point that if $\eta = 0$ then $f(x)$ is clearly reducible and it is well-known (see for example [3, p. 251]) that f has multiple roots (in k) if and only if $4\xi^3 + 27\eta^2 = 0$. Cardano's formulae (see for example [3, p. 258]) state that the three roots of f are

$$x_0 = v + w,\ x_1 = \omega v + \omega^{-1} w,\ x_{-1} = \omega^{-1} v + \omega w,$$

where $\omega \in \mathbf{F}_{q^2}$ is a primitive cube root of unity and v, w are such that $vw = -\frac{1}{3}\xi$ and $t = v^3$, $u = w^3$ are the roots of the auxiliary quadratic polynomial

$$X^2 + \eta X - \frac{1}{27}\xi^3.$$

It should be noted that ω is given by the formula

$$\omega = \frac{-1 + \sqrt{-3}}{2}$$

in which $\sqrt{-3}$ stands for any root in $\mathbb{F}_{q^2}$ of the polynomial $x^2 + 3$. If $q \equiv 1 \bmod 3$ then ω in fact lies in $\mathbb{F}_q$. A neat way of seeing this is to note that $\omega^q = \omega^{q \bmod 3}$ and hence that $\omega^q = \omega$ if and only if $q \equiv 1 \bmod 3$. But $\omega^q = \omega$ if and only if $\omega \in k$ since the elements of k are precisely the q roots of the polynomial $x^q - x$.

Also note that $t \in k$ if and only if $u \in k$. It makes sense therefore to make the following two definitions.

$$\epsilon_f := \begin{cases} 1 & \text{if } t, u \in k, \\ -1 & \text{otherwise;} \end{cases}$$

$$k_\epsilon := \begin{cases} k & \text{if } \epsilon = 1, \\ \mathbb{F}_{q^2} & \text{if } \epsilon = -1. \end{cases}$$

For simplicity we will write k_f instead of k_{ϵ_f}.

3. The Main Result: Version 1

Theorem 1. *Let $f(x) = x^3 + \xi x + \eta$ with $\xi, \eta \in k$. Let t be a root of the quadratic polynomial*

$$X^2 + \eta X - \frac{1}{27}\xi^3$$

(with the understanding that we choose the root $-\eta$ in case $\xi = 0$). Then f is irreducible over k if and only if the following conditions are satisfied:

(a) $\eta(4\xi^3 + 27\eta^2) \neq 0$,

(b) $q \equiv \epsilon_f \bmod 3$,

(c) $t \notin (k_f^\times)^3$.

Proof. Case 1. $\xi = 0$.

First observe that in this case $t = -\eta \in k$ and so $\epsilon_f = 1$. Now f is irreducible if and only if $t = -\eta$ is a noncube in k. Since noncubes exist in k if and only if $q \equiv 1 \bmod 3$ we are done in this case.

Case 2. $\xi \neq 0$, $\epsilon_f = 1$.

Suppose first that f is irreducible. We have seen above that this implies that (a) holds. A consequence of (a) is that $t \neq u$ and both t, u are nonzero.

Since $\epsilon_f = 1$, we have $t \in k$ and $(v^q)^3 = t^q = t$. We cannot have $v^q = v$ (that is $t \in (k^\times)^3$), otherwise the root x_0 would lie in k. We thus find that (c) holds and $v^{-1}v^q$ is a primitive cube root which we may assume to be ω. Since $vw \in k$ we must have $v^q w^q = vw$ and hence $w^q = \omega^{-1}w$. If $q \equiv -1 \bmod 3$ we would have

$$x_{-1}^q = \omega^{-q+1}v + \omega^{q-1}w = x_{-1}$$

and f would be reducible. This shows that (a), (b) and (c) hold if f is irreducible.

Now suppose that (a), (b) and (c) hold. We see from (c) that we cannot have $v^q = v$. We may then again assume that $v^q = \omega v$ and $w^q = \omega^{-1}w$. It is now straightforward to check that, from (b), $x_i^q \neq x_i$ for $i = 0, 1, -1$. For example, if $x_0^q = x_0$ then

$$\omega v + \omega^{-1}w = v + w$$

and hence $w/v = \omega$ (remember that from (a), $v \neq 0$). Raising to the qth power then gives $w/v = \omega^{q+2}$. Hence $\omega^{q+2} = \omega$ which contradicts (b). The other two cases are dealt with in a similar fashion. Hence f is irreducible and we have settled the case $\epsilon_f = 1$.

Case 3. $\xi \neq 0$, $\epsilon_f = -1$.

We now have $k_f \neq k$. The operation F of raising to the qth power takes f to the polynomial $(x^q)^3 + \xi x^q + \eta$ and hence F induces a permutation σ on the roots of f. The operation F^2 (that is, raising to the q^2th power) induces the permutation σ^2 on the roots. It is easy to see that σ has a fixed point if and only if σ^2 has a fixed point. Hence f is irreducible over k if and only it is irreducible over k_f.

Working over k_f we see, by replacing q by q^2 and ϵ_f by 1 in the argument for ϵ_1, that f is irreducible if (a), (b) and (c) hold (notice that k_f has q^2 elements and that $q^2 \equiv 1 \bmod 3$).

Now suppose f is irreducible over k and hence over k_f. As for the case $\epsilon_f = 1$ we find that (a) and (c) hold (for (c) we show that $v^{q^2} \neq v$ otherwise $x_0 \in k_f$). The proof that (b) holds is, however, slightly different. Since $t, u \in k_f \backslash k$ are roots of a quadratic polynomial over k, we have $t^q = u$ and $u^q = t$. Hence $(v^q)^3 = t^q = u = w^3$. If $v^q = w$ then $w^q = v$ (since $vw \in k$) and $x_0 \in k$. We may then assume that $v^q = \omega w$ and $w^q = \omega^{-1} v$. We want to show that $q \equiv -1 \bmod 3$. Suppose to the contrary that $q \equiv 1 \bmod 3$. Then

$$x_1^q = \omega^{-q-1} v + \omega^{q+1} w = x_1$$

and hence f is reducible, a contradiction. This finishes the proof. □

It should be noted that an argument of the same sort shows that f has three distinct roots in k if and only if $4\xi^3 + 27\eta^2 \neq 0$, (b) holds and (c) doesn't hold.

4. The Main Result: Version 2

In the case $\xi = -3$ it is possible to reformulate the statement of the Main Theorem in a manner that readily generalizes to the case of an arbitrary cubic. To state the other formulation requires the following lemma.

Lemma 2. *Let $\epsilon = \pm 1$ and suppose that $q \equiv \epsilon \mod 3$. Then t is a noncube in k_ϵ such that $t^{q-\epsilon} = 1$ if and only if $t = \nu^{3j \pm 1}$ where $\nu = \zeta^{q+\epsilon}$ and ζ generates the group $\mathbb{F}_{q^2}^\times$.*

Proof. If $\epsilon = 1$ then ν generates $\mathbb{F}_q^\times$ and the condition $t^{q-\epsilon} = 1$ is equivalent to $t \in \mathbb{F}_q$. Since $q \equiv 1 \mod 3$, t is a noncube in $\mathbb{F}_q$ if and only if $t = \nu^{3j\pm 1}$ for some $j \in \mathbb{Z}$.

Now suppose $\epsilon = -1$. Since $q \equiv -1 \mod 3$, $q^2 \equiv 1 \mod 3$ and hence ζ^i is a cube in $\mathbb{F}_{q^2}$ if and only if $3 \mid i$. Hence $\nu^{3j\pm1}$ is a noncube in $\mathbb{F}_{q^2}$. We have

$$\nu^{(3j\pm1)(q+1)} = \zeta^{(q-1)(q+1)(3j\pm1)} = \zeta^{(q^2-1)(3j\pm1)} = 1.$$

Hence $\nu^{3j\pm1}$ satisfies the conditions. Conversely, let $t = \xi^i$ be such that $t^{q+1} = 1$. Then $t^{q+1} = \zeta^{i(q+1)} = 1$ implies that $q^2 - 1 \mid i(q+1)$ which in turn implies that $q - 1 \mid i$ and hence $t = \zeta^{(q-1)k} = \nu^k$ for some k. Also, t is a noncube if and only if $3 \nmid (q-1)k \iff 3 \nmid k$ and hence $t = \nu^{3j\pm1}$ for some $j \in \mathbb{Z}$. □

Using this lemma, we arrive at the following reformulation in the case $\xi = -3$.

Corollary 3. *Suppose $q \equiv \epsilon \mod 3$. If $\eta \in \mathbb{F}_q$ then the polynomial $x^3 - 3x - \eta$ is irreducible over $\mathbb{F}_q$ if and only if $\eta = \nu^{3j+1} + \nu^{-3j-1}$ for some $j \in \mathbb{Z}$ where $\nu = \zeta^{q+\epsilon}$ and ζ generates the group $\mathbb{F}_{q^2}^\times$.*

Proof. Suppose $f(x) = x^3 - 3x - \eta$ is irreducible. Then $\eta \neq 0, \pm 2$ and hence $\xi\eta(4\xi^3 + 27\eta^2) \neq 0$. The auxiliary quadratic becomes $X^2 - \eta X + 1$ and hence $u = t^{-1}$ and $\eta = t + t^{-1}$. Since $\eta \in k$ we must either have $t^{q-1} = 1$ or $t^{q+1} = 1$. Since $\eta \neq 0, \pm 2$ we see that $t \neq \pm 1$ and hence, if $t^{q+1} = 1$ then $t \notin k$. We thus have $t^{q-\epsilon_f} = 1$. Theorem 1 implies that $q \equiv \epsilon_f \bmod 3$ and hence $\epsilon_f = \epsilon$. Lemma 2 then implies that $t = \nu^{3j\pm1}$ for some $j \in \mathbb{Z}$ and hence $\eta = \nu^{3j+1} + \nu^{-3j-1}$.

Conversely, suppose $\eta = \nu^{3j+1} + \nu^{-3j-1}$ for some $j \in \mathbb{Z}$. Then $\eta \neq 0$ and if $\eta = t + t^{-1}$ then $t = \nu^{\pm(3j+1)} = \nu^{3k\pm1}$ for a suitable $k \in \mathbb{Z}$. Lemma 2 then implies that (i) $t \neq \pm 1$; (ii) if $q \equiv 1 \mod 3$ then $t \in k$ and t is a noncube in k and (iii) if $q \equiv -1 \mod 3$ then $t \notin k$ and t is a noncube in k_ϵ. From (i) and the fact that $\eta \neq 0$ it follows that condition (a) of Theorem 1 is satisfied. From (ii) and (iii) it follows that conditions (b) and (c) are satisfied. Hence f is irreducible and we are done. □

We can now generalize this result to deal with an arbitrary cubic over $\mathbb{F}_q$.

Theorem 4. *Let ζ generate $\mathbb{F}_{q^2}^\times$ and let $\nu = \zeta^{q\pm1}$ according as $q \equiv \pm 1 \mod 3$. Let $f(x) = a_0x^3 + 3a_1x^2 + 3a_2x + a_3$ with $a_0 \neq 0$ be a cubic polynomial over $\mathbb{F}_q$. If*

$\alpha = a_0a_2 - a_1^2$ and $\beta = a_0^2a_3 - 3a_0a_1a_2 + 2a_1^3$ then $f(x)$ is irreducible over $\mathbb{F}_q$ if and only if one of the following two conditions hold.

(a) $\alpha = 0$ and β is a noncube in $\mathbb{F}_q$ (impossible if $q \equiv -1 \mod 3$);

(b) $\alpha \neq 0$, $\beta \neq 0$ and $-\frac{\beta^2}{\alpha^3} - 2 = \nu^{3j+1} + \nu^{-3j-1}$ for some $j \in \mathbb{Z}$.

Proof. By a standard argument (see, for example, [1, 12.1]) we form the polynomial

$$f_1(x) := a_0^2 f(\frac{x - a_1}{a_0}) = x^3 + 3\alpha x + \beta$$

and $f(x)$ is irreducible if and only if $f_1(x)$ is. If $\beta = 0$, it is clear that $f_1(x)$ is reducible, so assume from now on that $\beta \neq 0$. Then $f_1(x)$ is irreducible if and only if $f_2(x) := x^3 f_1(x^{-1}) = \beta x^3 + 3\alpha x^2 + 1$ is irreducible, that is, if and only if

$$f_3(x) := \beta^2 f_2(\frac{x - \alpha}{\beta}) = x^3 - 3\alpha^2 x + (2\alpha^3 + \beta^2)$$

is irreducible. If $\alpha = 0$ then $f_3(x)$ and hence $f(x)$ is reducible if and only if β^2 and hence β is a cube in $\mathbb{F}_q$. So assume that $\alpha \neq 0$. Then $f_3(x)$ is irreducible if and only if $f_4(x) := \alpha^{-3} f_3(\alpha x) = x^3 - 3x + (\frac{\beta^2}{\alpha^3} + 2)$ is irreducible. By Corollary 3, this is irreducible if and only if $-\frac{\beta^2}{\alpha^2} - 2$ is of the form $\nu^{3j+1} + \nu^{-3j-1}$ for some $j \in \mathbb{Z}$. $\square$

References

[1] J. W. Archbold. *Algebra.* Pitman, Bath, 1964.

[2] Bomshik Chang. The conjugate classes of Chevalley groups of type (G_2). *J. Algebra*, 9:190–211, 1968.

[3] N. Jacobson. *Basic Algebra I.* W. H. Freeman and Company, San Francisco, 1974.

[4] D. G. A. Jackson. On nilpotent orbits of type G_2. PhD Thesis, Sydney University, 1997.

School of Mathematics and Statistics
University of Sydney
Australia 2006