Journal of Number Theory 130 (2010) 2745–2752

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

The characteristic polynomials of abelian varieties of dimensions 3 over finite fields

Safia Haloui

Institut de Mathématiques de Luminy, Marseille, France

ARTICLE INFO

Article history:
Received 26 February 2010
Accepted 15 June 2010
Communicated by David Goss

MSC:
14G15
11C08
11G10
11G25

Keywords:
Abelian varieties over finite fields
Weil polynomials

ABSTRACT

We describe the set of characteristic polynomials of abelian varieties of dimension 3 over finite fields.

1. Introduction and results

The isogeny class of an abelian variety over a finite field is determined by its characteristic polynomial (i.e. the characteristic polynomial of its Frobenius endomorphism). We describe the set of characteristic polynomials which occur in dimension 3; this completes the work of Xing [10] (we will recall his results in this section). Since the problem has been solved in dimensions 1 and 2 (see [8,6] and [3]), it is sufficient to focus on simple abelian varieties.

Let $p(t)$ be the characteristic polynomial of an abelian variety of dimension g over $\mathbb{F}_q$ (with $q = p^n$). Then the set of its roots has the form $\{\omega_1, \overline{\omega_1}, \ldots, \omega_g, \overline{\omega_g}\}$ where the ω_i's are q-Weil numbers. A monic polynomial with integer coefficients which satisfies this condition is called a *Weil polynomial*. Thus every Weil polynomial of degree 6 has the form

$$p(t) = t^6 + a_1 t^5 + a_2 t^4 + a_3 t^3 + q a_2 t^2 + q^2 a_1 t + q^3$$

E-mail address: haloui@iml.univ-mrs.fr.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2010.06.008

for certain integers a_1, a_2 and a_3. The converse is false; indeed, since the absolute value of the roots of $p(t)$ is prescribed (equal to $\sqrt{q}$), its coefficients have to be bounded. Section 2 is dedicated to the proof of the following proposition:

Theorem 1.1. *Let $p(t) = t^6 + a_1t^5 + a_2t^4 + a_3t^3 + qa_2t^2 + q^2a_1t + q^3$ be a polynomial with integer coefficients. Then $p(t)$ is a Weil polynomial if and only if either*

$$p(t) = \left(t^2 - q\right)^2\left(t^2 + \beta t + q\right)$$

where $\beta \in \mathbb{Z}$ and $|\beta| < 2\sqrt{q}$, or the following conditions hold:

(1) $|a_1| < 6\sqrt{q}$,
(2) $4\sqrt{q}|a_1| - 9q < a_2 \leqslant \frac{a_1^2}{3} + 3q$,
(3) $-\frac{2a_1^3}{27} + \frac{a_1a_2}{3} + qa_1 - \frac{2}{27}(a_1^2 - 3a_2 + 9q)^{3/2} \leqslant a_3 \leqslant -\frac{2a_1^3}{27} + \frac{a_1a_2}{3} + qa_1 + \frac{2}{27}(a_1^2 - 3a_2 + 9q)^{3/2}$,
(4) $-2qa_1 - 2\sqrt{q}a_2 - 2q\sqrt{q} < a_3 < -2qa_1 + 2\sqrt{q}a_2 + 2q\sqrt{q}$.

The Honda–Tate theorem gives us a bijection between the set of conjugacy classes of q-Weil numbers and the set of isogeny classes of simple abelian varieties over $\mathbb{F}_q$. Moreover, the characteristic polynomial of a simple abelian variety of dimension 3 over $\mathbb{F}_q$ has the form $p(t) = h(t)^e$ where $h(t)$ is an irreducible Weil polynomial and e is an integer. Obviously e must divide 6.

As remarked by Xing [10], e cannot be equal to 2 or 6, otherwise $p(t)$ would have a real root and real q-Weil numbers ($\pm\sqrt{q}$) correspond to dimension 1 or 2 (according to the parity of n) abelian varieties (see [8]).

When $e = 3$, using a result from Maisner and Nart [3, Proposition 2.5], we get the following proposition, proved by Xing, which gives us the form of $h(t)$.

Proposition 1.2 *(Xing). Let $\beta \in \mathbb{Z}$, $|\beta| < 2\sqrt{q}$. There exists a simple abelian variety of dimension 3 over $\mathbb{F}_q$ with $h(t) = t^2 + \beta t + q$ if and only if 3 divides n and $\beta = aq^{1/3}$, where a is an integer coprime with p.*

It follows that a simple abelian variety of dimension 3 with a reducible characteristic polynomial has p-rank 0; this fact was proved by González [2]. Note that the Newton polygon of a polynomial from Proposition 1.2 is of type 1/3 (see Fig. 4, Section 4).

It remains to see what happens when $p(t)$ is irreducible ($e = 1$). First, we need an irreducibility criterion for Weil polynomials. In Section 3, we prove the following proposition:

Proposition 1.3. *Set*

$$r = -\frac{a_1^2}{3} + a_2 - 3q \quad \textit{and} \quad s = \frac{2a_1^3}{27} - \frac{a_1a_2}{3} - qa_1 + a_3$$

and

$$\Delta = s^2 - \frac{4}{27}r^3 \quad \textit{and} \quad u = \frac{-s + \sqrt{\Delta}}{2}\cdot$$

Then $p(t)$ is irreducible over $\mathbb{Q}$ if and only if $\Delta \neq 0$ and u is not a cube in $\mathbb{Q}(\sqrt{\Delta})$.

Next, we determine the possible Newton polygons for $p(t)$; this is the aim of Section 4.

Theorem 1.4. *Let $p(t) = t^6 + a_1t^5 + a_2t^4 + a_3t^3 + qa_2t^2 + q^2a_1t + q^3$ be an irreducible Weil polynomial. Then $p(t)$ is the characteristic polynomial of an abelian variety of dimension 3 if and only if one of the following conditions holds*:

(1) $v_p(a_3) = 0$,
(2) $v_p(a_2) = 0$, $v_p(a_3) \geqslant n/2$ *and* $p(t)$ *has no root of valuation* $n/2$ *in* $\mathbb{Q}_p$,
(3) $v_p(a_1) = 0$ $v_p(a_2) \geqslant n/2$, $v_p(a_3) \geqslant n$ *and* $p(t)$ *has no root of valuation* $n/2$ *in* $\mathbb{Q}_p$,
(4) $v_p(a_1) \geqslant n/3$, $v_p(a_2) \geqslant 2n/3$, $v_p(a_3) = n$ *and* $p(t)$ *has no root* $\mathbb{Q}_p$,
(5) $v_p(a_1) \geqslant n/2$, $v_p(a_2) \geqslant n$, $v_p(a_3) \geqslant 3n/2$ *and* $p(t)$ *has no root nor factor of degree* 3 *in* $\mathbb{Q}_p$.

The p*-ranks of abelian varieties in cases* (1), (2), (3), (4) *and* (5) *are respectively* 3, 2, 1, 0 *and* 0. *The abelian varieties in case* (5) *are supersingular.*

It is possible to make condition (5) of Theorem 1.4 more explicit. Indeed, in [5], Nart and Ritzenthaler gave the list of q-Weil numbers of degree 6. We derive from it the following proposition (see Section 5).

Proposition 1.5. *If* $p(t)$ *is the characteristic polynomial of a supersingular abelian variety of dimension* 3 *then one of the following conditions holds*:

(1) $(a_1, a_2, a_3) = (q^{1/2}, q, q^{3/2})$ *or* $(-q^{1/2}, q, -q^{3/2})$, q *is a square and* $7 \nmid (p^3 - 1)$,
(2) $(a_1, a_2, a_3) = (0, 0, q^{3/2})$ *or* $(0, 0, -q^{3/2})$, q *is a square and* $3 \nmid (p - 1)$,
(3) $(a_1, a_2, a_3) = (\sqrt{pq}, 3q, q\sqrt{pq})$ *or* $(-\sqrt{pq}, 3q, -q\sqrt{pq})$, $p = 7$ *and* q *is not a square*,
(4) $(a_1, a_2, a_3) = (0, 0, q\sqrt{pq})$ *or* $(0, 0, -q\sqrt{pq})$, $p = 3$ *and* q *is not a square.*

2. The coefficients of Weil polynomials of degree 6

In this section, we prove Theorem 1.1. It is clear that a Weil polynomial with a real root must have the form

$$\left(t^2 - q\right)^2\left(t^2 + \beta t + q\right)$$

where $\beta \in \mathbb{Z}$ and $|\beta| < 2\sqrt{q}$. Conversely, these polynomials are Weil polynomials.

To deal with Weil polynomials with no real root, we use Robinson's method (described by Smyth in [7, §2, Lemma]). Fixing a polynomial of degree 3 and doing an explicit calculation we get the following lemma:

Lemma 2.1. *Let* $f(t) = t^3 + r_1 t^2 + r_2 t + r_3$ *be a monic polynomial of degree* 3 *with real coefficients. Then* $f(t)$ *has all real positive roots if and only if the following conditions hold*:

(1) $r_1 < 0$,
(2) $0 < r_2 < \frac{r_1^2}{3}$,
(3) $\frac{r_1 r_2}{3} - \frac{2r_1^3}{27} - \frac{2}{27}(r_1^2 - 3r_2)^{3/2} \leqslant r_3 \leqslant \frac{r_1 r_2}{3} - \frac{2r_1^3}{27} + \frac{2}{27}(r_1^2 - 3r_2)^{3/2}$ *and* $r_3 < 0$.

Proof. If $f(t)$ has all real positive roots, so do all its derivates. Thus condition (1) is obvious. Let $f_0'(t)$ be the primitive of $f''(t)$ vanishing at 0; if we add a constant to $f_0'(t)$ so that all its roots are real and positive, we obtain (2). Repeating this process with a primitive of $f'(t)$ vanishing at 0, we obtain (3). □

Let $x = (x_1, x_2, x_3) \in \mathbb{C}^3$ and set

$$p_x(t) = \prod_{i=1}^{3}\left(t^2 + x_i t + q\right),$$

$$f_x(t) = \prod_{i=1}^{3}\left(t - (2\sqrt{q} + x_i)\right) \quad \text{and} \quad \tilde{f}_x(t) = \prod_{i=1}^{3}\left(t - (2\sqrt{q} - x_i)\right). \tag{1}$$

If $p_x(t)$ is a Weil polynomial with no real root (thus $x_i = -(\omega_i + \overline{\omega_i})$, where $\omega_1, \overline{\omega_1}, \ldots, \omega_g, \overline{\omega_g}$ are the roots of $p_x(t)$) then the roots of $f_x(t)$ and $\tilde{f}_x(t)$ are real and positive. Conversely, suppose that the roots of $f_x(t)$ and $\tilde{f}_x(t)$ are real and positive and that $p_x(t)$ has integer coefficients. Then $p_x(t)$ is a Weil polynomial.

For $i = 1, 2, 3$, let a_i denote the coefficient associated to $p_x(t)$ in Theorem 1.1, s_i the ith symmetric function of the x_i's and r_i and $\tilde{r}_i$ the respective ith coefficients of $f_x(t)$ and $\tilde{f}_x(t)$.

Expanding the expression of $p_x(t)$ in (1), we find

$$a_1 = s_1,$$
$$a_2 = s_2 + 3q,$$
$$a_3 = s_3 + 2qs_1.$$

In the same way, expanding the expressions of $f_x(t)$ and $\tilde{f}_x(t)$, we find

$$\begin{aligned} r_1 &= -6\sqrt{q} - s_1, \\ r_2 &= 12q + 4\sqrt{q}s_1 + s_2, \\ r_3 &= -8q\sqrt{q} - 4qs_1 - 2\sqrt{q}s_2 - s_3, \end{aligned} \quad \text{and} \quad \begin{aligned} \tilde{r}_1 &= -6\sqrt{q} + s_1, \\ \tilde{r}_2 &= 12q - 4\sqrt{q}s_1 + s_2, \\ \tilde{r}_3 &= -8q\sqrt{q} + 4qs_1 - 2\sqrt{q}s_2 + s_3. \end{aligned}$$

Therefore we have

$$\begin{aligned} r_1 &= -6\sqrt{q} - a_1, \\ r_2 &= 9q + 4\sqrt{q}a_1 + a_2, \\ r_3 &= -2q\sqrt{q} - 2qa_1 - 2\sqrt{q}a_2 - a_3, \end{aligned} \quad \text{and} \quad \begin{aligned} \tilde{r}_1 &= -6\sqrt{q} + a_1, \\ \tilde{r}_2 &= 9q - 4\sqrt{q}a_1 + a_2, \\ \tilde{r}_3 &= -2q\sqrt{q} + 2qa_1 - 2\sqrt{q}a_2 + a_3. \end{aligned}$$

The polynomials $f_x(t)$ and $\tilde{f}_x(t)$ satisfy condition (1) of Lemma 2.1 if and only if

$$|a_1| < 6\sqrt{q}.$$

The polynomials $f_x(t)$ and $\tilde{f}_x(t)$ satisfy condition (2) of Lemma 2.1 if and only if

$$4\sqrt{q}|a_1| - 9q < a_2 \leqslant \frac{a_1^2}{3} + 3q.$$

We find that the first inequality in condition (3) of Lemma 2.1 holds for $f_x(t)$ if and only if it holds for $\tilde{f}_x(t)$ if and only if

$$-\frac{2a_1^3}{27} + \frac{a_1a_2}{3} + qa_1 - \frac{2}{27}\left(a_1^2 - 3a_2 + 9q\right)^{3/2} \leqslant a_3 \leqslant -\frac{2a_1^3}{27} + \frac{a_1a_2}{3} + qa_1 + \frac{2}{27}\left(a_1^2 - 3a_2 + 9q\right)^{3/2}.$$

Finally, $f_x(t)$ and $\tilde{f}_x(t)$ satisfy the second inequality in condition (3) of Lemma 2.1 if and only if

$$-2qa_1 - 2\sqrt{q}a_2 - 2q\sqrt{q} < a_3 < -2qa_1 + 2\sqrt{q}a_2 + 2q\sqrt{q}.$$

Hence Theorem 1.1 is proved.

3. Irreducible Weil polynomials

Given a Weil polynomial $p(t) = \prod_{i=1}^{g}(t^2 + x_it + q)$, we consider its real Weil polynomial $f(t) = \prod_{i=1}^{g}(t + x_i)$.

Proposition 3.1. *Suppose that $g \geqslant 2$ and $p(t) \neq (t-\sqrt{q})^2(t+\sqrt{q})^2$. Then $p(t)$ is irreducible over $\mathbb{Q}$ if and only if $f(t)$ is irreducible over $\mathbb{Q}$.*

Proof. Suppose that $p(t)$ is reducible. It is sufficient to prove that $p(t)$ factors as the product of two Weil polynomials (then $f(t)$ will be the product of its associated polynomials). The polynomial $p(t)$ decomposes as $p(t) = (t-\sqrt{q})^{2k}(t+\sqrt{q})^{2\ell}h(t)$ where $h(t)$ has no real root. If $k \neq \ell$ then $\sqrt{q} \in \mathbb{Q}$ and $p(t)$ factors obviously. The same conclusion holds when $k = \ell \neq 0$ and $h(t) \neq 1$. If $k = \ell > 1$ and $h(t) = 1$, we have the decomposition $p(t) = [(t-\sqrt{q})^2(t+\sqrt{q})^2][(t-\sqrt{q})^{2k-2}(t+\sqrt{q})^{2\ell-2}]$. Finally, if $k = \ell = 0$, by hypothesis $h(t)$ is the product of two monic non-constant polynomials which are obviously Weil polynomials.

Conversely, if $f(t)$ is reducible, we can assume (possibly changing labels of the x_i's) that there exists an integer k between 1 and $(g-1)$ such that the polynomials $\prod_{i=1}^{k}(t+x_i)$ and $\prod_{i=k+1}^{g}(t+x_i)$ have integer coefficients. Thus $\prod_{i=1}^{k}(t^2+x_it+q)$ and $\prod_{i=k+1}^{g}(t^2+x_it+q)$ have integer coefficients and their product is $p(t)$. $\square$

Now we focus on the case $g = 3$. In order to know if $p(t)$ is irreducible, it is sufficient to check if $f(t)$ (a polynomial of degree 3 with all real roots) is irreducible. To do this, we use Cardan's method. Let us recall quickly what it is.

Fixing a polynomial $h(t) = t^3 + rt + s$, we set $\Delta = s^2 - \frac{4}{27}r^3$. If $h(t)$ has all real roots, we have $\Delta \leqslant 0$. Moreover, $\Delta = 0$ if and only if $h(t)$ has a double root. When $\Delta < 0$, we set $u = \frac{-s+\sqrt{\Delta}}{2}$. The roots of $h(t)$ are in the form $(v + \bar{v})$ where v is a cube root of u.

We apply this to $f(t) = t^3 + a_1t^2 + (a_2 - 3q)t + (a_3 - 2qa_1)$:

Proof of Proposition 1.3. We set $h(t) = t^3 + rt + s$ so that $f(t) = h(t + \frac{a_1}{3})$. The polynomial $f(t)$ is reducible if and only if it has a root in $\mathbb{Q}$ if and only if $h(t)$ has a root in $\mathbb{Q}$.

If $\Delta = 0$, $f(t)$ is reducible. Suppose that $\Delta < 0$. If u is the cube of a certain $v \in \mathbb{Q}(\sqrt{\Delta})$, we have obviously $(v + \bar{v}) \in \mathbb{Q}$. Conversely, if $h(t)$ has a root in $\mathbb{Q}$ then u has a cube root $v = a + ib$ with $a \in \mathbb{Q}$ and we have

$$u = v^3 = \left(a^3 - 3ab^2\right) + ib\left(3a^2b - b^2\right).$$

If $a \neq 0$, identifying real parts in the last equality, we see that $b^2 \in \mathbb{Q}$, then, identifying imaginary parts, $b \in \mathbb{Q}(\sqrt{-\Delta})$. Therefore $v \in \mathbb{Q}(\sqrt{\Delta})$. If $a = 0$, then $s = 0$ and $\Delta = \frac{4}{27}r^3 = (\frac{2}{3}r)^2\frac{r}{3}$. Thus $u = \frac{1}{2}\sqrt{\frac{4}{27}r^3} = (\sqrt{\frac{r}{3}})^3$ is a cube in $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{\frac{r}{3}})$. $\square$

4. Newton polygons

Let $p(t)$ be an irreducible Weil polynomial of degree 6 and e the least common denominator of $v_p(f(0))/n$ where $f(t)$ runs through the irreducible factors of $p(t)$ over $\mathbb{Q}_p$ (the field of p-adic numbers). By [4], $p(t)^e$ is the characteristic polynomial of a simple abelian variety. Thus $p(t)$ is the characteristic polynomial of an abelian variety of dimension 3 if and only if e is equal to 1 that is, $v_p(f(0))/n$ are integers. One way to obtain information about p-adic valuations of the roots of $p(t)$ is to study its Newton polygon (see [9]). The condition "$v_p(f(0))/n$ are integers" implies that the projection onto the x-axis of an edge of the Newton polygon having a slope $\ell n/k$ (with $\mathrm{pgcd}(\ell, k) = 1$) has length a multiple of k. We graph the Newton polygons satisfying this condition and in each case, we give a necessary and sufficient condition to have $e = 1$. The obtained results are summarized in Theorem 1.4.

Ordinary case: $\boldsymbol{v_p(a_3) = 0}$. The Newton polygon of $p(t)$ is represented in Fig. 1 and we always have $e = 1$.

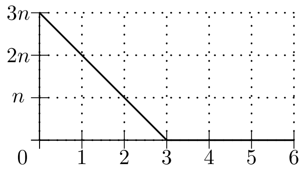

Fig. 1. Ordinary case.

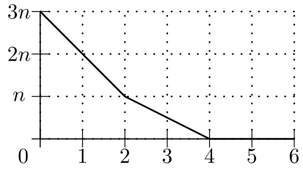

Fig. 2. p-rank 2 case.

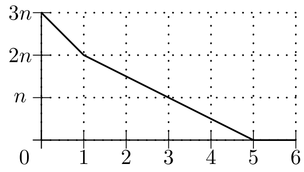

Fig. 3. p-rank 1 case.

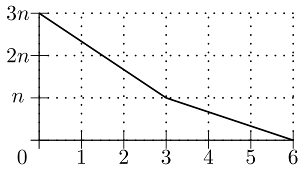

Fig. 4. Type 1/3 case.

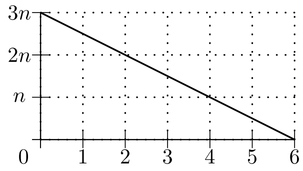

Fig. 5. Supersingular case.

***p*-rank 2 case: $v_p(a_3) > 0$ and $v_p(a_2) = 0$.** The only Newton polygon for which $e = 1$ is represented in Fig. 2.

This is the Newton polygon of $p(t)$ if and only if $v_p(a_3) \geqslant n/2$. If this condition holds, $p(t)$ has a factor in $\mathbb{Q}_p$ of degree 2 with roots of valuation $n/2$ and thus $e = 1$ if and only if this factor is irreducible, that is, if and only if $p(t)$ has no root of valuation $n/2$ in $\mathbb{Q}_p$ (note that when n is odd, this last condition always holds).

***p*-rank 1 case: $v_p(a_3) > 0$, $v_p(a_2) > 0$ and $v_p(a_1) = 0$.** The only Newton polygon for which $e = 1$ is represented in Fig. 3.

This is the Newton polygon of $p(t)$ if and only if $v_p(a_2) \geqslant n/2$ and $v_p(a_3) \geqslant n$. If these conditions hold, $p(t)$ has a factor in $\mathbb{Q}_p$ of degree 4 with roots of valuation $n/2$ and thus $e = 1$ if and only if this factor has no root in $\mathbb{Q}_p$, that is, if and only if $p(t)$ has no root of valuation $n/2$ in $\mathbb{Q}_p$.

***p*-rank 0 case: $v_p(a_3) > 0$, $v_p(a_2) > 0$ and $v_p(a_1) > 0$.** There are two Newton polygons for which $e = 1$. One is represented in Fig. 4.

This is the Newton polygon of $p(t)$ if and only if $v_p(a_1) \geqslant n/3$, $v_p(a_2) \geqslant 2n/3$ and $v_p(a_3) = n$. If these conditions hold, $p(t)$ has two factors in $\mathbb{Q}_p$ of degree 3, one with roots of valuation $2n/3$ and the other with roots of valuation $n/3$; $e = 1$ if and only if those factors are irreducible in $\mathbb{Q}_p$, that is, if and only if $p(t)$ has no root in $\mathbb{Q}_p$.

The other Newton polygon is represented in Fig. 5; the corresponding abelian varieties are supersingular.

This is the Newton polygon of $p(t)$ if and only if $v_p(a_1) \geqslant n/2$, $v_p(a_2) \geqslant n$ and $v_p(a_3) \geqslant 3n/2$. If these conditions hold, $e = 1$ if and only if $p(t)$ has no root nor factor of degree 3 in $\mathbb{Q}_p$.

5. Supersingular case

Nart and Ritzenthaler [5] proved that the only supersingular q-Weil numbers of degree six are

$$\begin{array}{ll} \pm\sqrt{q}\zeta_7, \quad \pm\sqrt{q}\zeta_9, & \text{if } q \text{ is a square,} \\ \sqrt{q}\zeta_{28}\ (p=7), \quad \sqrt{q}\zeta_{36}\ (p=3), & \text{if } q \text{ is not a square,} \end{array}$$

where ζ_n is a primitive nth root of unity.

We will use this result to obtain a list of possible supersingular characteristic polynomials as stated in Proposition 1.5. We will have to calculate the minimal polynomial of some algebraic integers; in order to do this, we will often use the (trivial) fact that if α is a root of $f(t) = \sum_{i=0}^{n} b_i t^{n-i}$ and $a \in \mathbb{C}$ then $a\alpha$ is a root of $f_a(t) = \sum_{i=0}^{n} b_i a^i t^{n-i}$. We denote by $\phi_n(t)$ the nth cyclotomic polynomial.

• If q is a square, as $\phi_7(t)=t^6+t^5+t^4+t^3+t^2+t+1$, the minimal polynomial of $\sqrt{q}\zeta_7$ (respectively $-\sqrt{q}\zeta_7$) is $p(t)=t^6+q^{1/2}t^5+qt^4+q^{3/2}t^3+q^2t^2+q^{5/2}t+q^3$ (respectively $p(t)=t^6-q^{1/2}t^5+qt^4-q^{3/2}t^3+q^2t^2-q^{5/2}t+q^3$). If $p\neq 7$, $p(t)$ has no factor of degree 1 and 3 over $\mathbb{Q}_p$ if and only if $\mathbb{Q}_p$ and its cubic extensions do not contain a 7th primitive root of unity; this is equivalent (see [1, Proposition 2.4.1, p. 53]) to

$$7\nmid\left(p^3-1\right).$$

In the same way, $\phi_9(t)=t^6+t^3+1$ and the minimal polynomial of $\sqrt{q}\zeta_9$ (respectively $-\sqrt{q}\zeta_9$) is $p(t)=t^6+q^{3/2}t^3+q^3$ (respectively $p(t)=t^6-q^{3/2}t^3+q^3$). If $p\neq 3$, $p(t)$ have no factor of degree 1 and 3 over $\mathbb{Q}_p$ if and only if

$$3\nmid(p-1).$$

If $p=7$ in the first case or $p=3$ in the second case, $p(t)$ is irreducible over $\mathbb{Q}_p$ (apply Eisenstein's criterion to $p(t+1)$).

• Suppose that q is not a square. When $p=7$, as $\phi_{28}(t)=t^{12}-t^{10}+t^8-t^6+t^4-t^2+1$, the monic polynomial with roots $\sqrt{q}\zeta_{28}$ is $t^{12}-qt^{10}+q^2t^8-q^3t^6+q^4t^4-q^5t^2+q^6$ which is the product of

$$t^6+\sqrt{pq}t^5+3qt^4+q\sqrt{pq}t^3+3q^2t^2+q^2\sqrt{pq}t+q^3$$

and

$$t^6-\sqrt{pq}t^5+3qt^4-q\sqrt{pq}t^3+3q^2t^2-q^2\sqrt{pq}t+q^3.$$

When $p=3$, as $\phi_{36}(t)=t^{12}-t^6+1$, the monic polynomial with roots $\sqrt{q}\zeta_{36}$ is $t^{12}-q^3t^6+q^6$ which is the product of

$$t^6+q\sqrt{pq}t^3+q^3$$

and

$$t^6-q\sqrt{pq}t^3+q^3.$$

The resulting polynomials are characteristic polynomials of abelian varieties of dimension 3 (see [5]).

Acknowledgments

I would like to thank Christophe Ritzenthaler for suggesting this work and for helpful discussions. I would also like to thank my thesis advisor, Yves Aubry, for his helpful comments and Hamish Ivey-Law for his careful reading of this paper.

References

[1] Y. Amice, Les nombres p-adiques, P.U.F., 1975.
[2] J. González, On the p-rank of an abelian variety and its endomorphism algebra, Publ. Math. 42 (1998) 119–130.
[3] D. Maisner, E. Nart, Abelian surfaces over finite fields as jacobians, Experiment. Math. 11 (2002) 321–337, appendix of E.W. Howe.
[4] J. Milne, W. Waterhouse, Abelian varieties over finite fields, in: 1969 Number Theory Institute, in: Proc. Sympos. Pure Math., vol. XX, Amer. Math. Soc., Providence, RI, 1971, pp. 53–64; vol. 76, 1990, pp. 351–366.
[5] E. Nart, C. Ritzenthaler, Jacobians in isogeny classes of supersingular threefolds in characteristic 2, Finite Fields Appl. 14 (2008) 676–702.

[6] H.G. Rück, Abelian surfaces and Jacobian varieties over finite fields, Compos. Math. 76 (1990) 351–366.
[7] C. Smyth, Totally positive algebraic integers of small trace, Ann. Inst. Fourrier 33 (1973) 285–302.
[8] W. Waterhouse, Abelian varieties over finite fields, Ann. Sci. Ecole Norm. Sup. (4) 2 (1969) 521–560.
[9] E. Weiss, Algebraic Number Theory, McGraw, New York, 1963.
[10] C.P. Xing, The characteristic polynomials of abelian varieties of dimension three and four over finite fields, Sci. China 37 (3) (1994) 147–150.