Can. J. Math. Vol. **47** (3), 1995 pp. 655–672.

A FAMILY OF REAL p^n-TIC FIELDS

YUAN-YUAN SHEN AND LAWRENCE C. WASHINGTON

ABSTRACT. Let $q = p$ if p is an odd prime, $q = 4$ if $p = 2$. Let ζ_q be any primitive q-th root of unity, and let $O = \mathbf{Z}[\zeta_q + \zeta_q^{-1}]$. We study the family of polynomials

$$P_n(X; a) = R_n(X) - \frac{a}{p^n} S_n(X),$$

where $R_n(X)$ and $S_n(X)$ are the polynomials in the expansion

$$(X - \zeta_q)^{p^n} = R_n(X) - \zeta_q S_n(X), \quad \text{with } R_n(X), S_n(X) \in O[X].$$

We show that for fixed n, $P_n(X; a)$ is irreducible for all but finitely many $a \in O$, and for $p = 3$, we show that it is irreducible for all $a \in O$. The roots are all real and are permuted cyclically by a linear fractional transformation defined over the real p^n-th cyclotomic field. From the roots we obtain a non-maximal set of independent units for the splitting field. In the last section we briefly treat extensions of our methods to composite p.

1. **Introduction.** The so-called "simplest" fields of degrees 2, 3, 4, 6 can be constructed using appropriate elements of $\mathrm{PGL}_2(\mathbf{Q})$. In [7], we used elements of $\mathrm{PGL}_2(\mathbf{R})$ to construct families of fields of degree 2^n for each $n > 0$. In the present paper we generalize this construction to obtain one-parameter families of polynomials of degree p^n, where p is prime. However, the polynomials now have coefficients in the p-th real cyclotomic field $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$. Using Faltings' theorem, we show that for each n these polynomials are irreducible except for finitely many values of the parameter. In the case $p = 3$, the polynomials have rational integral coefficients and can be regarded as generalizations of the "simplest" cubic polynomials of D. Shanks [6]. By determining all solutions of $Y^2 = X^3 - 48$ in $\mathbf{Z}[1/3]$, we are able to deduce that all of these 3^n-tic polynomials are irreducible.

One of the principal motivations for studying the simplest fields has been to produce number fields with explicit units. In the present case, the roots of our polynomials yield large sets of independent units in the splitting fields, and in certain cases we can augment this set with units from subfields. However, the fact that our polynomials are not in general Galois prevents us from obtaining a set of units of maximal rank.

In the last section, we indicate how our methods can be modified to allow p to be composite, and thus we obtain families of fields of degree p over $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$.

2. **Construction of the p^n-tic polynomials.** Let $q = p$ if p is an odd prime, $q = 4$ if $p = 2$. Let ζ_q be any primitive q-th root of unity, and let $O = \mathbf{Z}[\zeta_q + \zeta_q^{-1}]$. Write the

Received by the editors August 4, 1993.
AMS subject classification: Primary: 11R21; secondary: 11R09, 11R16, 11R18, 11R27.
Key words and phrases: p^n-tic fields, units.

https://doi.org/10.4153/CJM-1995-034-4 Published online by Cambridge University Press

polynomial $(X-\zeta_q)^{p^n}$ as a linear combination of 1 and ζ_q, say

$$(1)\qquad (X-\zeta_q)^{p^n} = R_n(X) - \zeta_q S_n(X), \quad \text{with } R_n(X), S_n(X) \in O[X].$$

Then $R_0(X) = X$, and $S_0(X) = 1$. Since we can express each ζ_q^i as a linear combination of 1 and ζ_q over the ring O, we have

$$\zeta_q^i = r_i - s_i\zeta_q \quad \text{for some } r_i, s_i \in O.$$

Therefore

$$\begin{aligned} R_n(X) - \zeta_q S_n(X) &= (X-\zeta_q)^{p^n} \\ &= \big((X-\zeta_q)^{p^{n-1}}\big)^p \\ &= \big(R_{n-1}(X) - \zeta_q S_{n-1}(X)\big)^p \\ &= \sum_{i=0}^{p}(-1)^i \binom{p}{i} r_i R_{n-1}^{p-i}(X) S_{n-1}^i(X) \\ &\quad -\zeta_q \sum_{i=0}^{p}(-1)^i \binom{p}{i} s_i R_{n-1}^{p-i}(X) S_{n-1}^i(X). \end{aligned}$$

We obtain the following recursion formulas:

$$(2)\qquad R_n(X) = \sum_{i=0}^{p}(-1)^i \binom{p}{i} r_i R_{n-1}^{p-i}(X) S_{n-1}^i(X),$$

$$(3)\qquad S_n(X) = \sum_{i=0}^{p}(-1)^i \binom{p}{i} s_i R_{n-1}^{p-i}(X) S_{n-1}^i(X).$$

Clearly, $s_0 = s_p = 0$ and $\binom{p}{i}/p \in \mathbf{Z}$ for $1 \le i < p$. Thus (3) becomes

$$S_n(X) = pR_{n-1}(X)S_{n-1}(X)\sum_{i=1}^{p-1}(-1)^i \left[\binom{p}{i}\Big/p\right] s_i R_{n-1}^{p-1-i}(X) S_{n-1}^{i-1}(X),$$

and hence by induction we obtain

$$(4)\qquad S_n(X) = p^n \prod_{j=0}^{n-1}\left(R_j(X)\sum_{i=1}^{p-1}(-1)^i \left[\binom{p}{i}\Big/p\right] s_i R_j^{p-1-i}(X) S_j^{i-1}(X)\right).$$

Thus we have the following lemma.

LEMMA 1. *The polynomials $R_j(X)$, $0 \le j < n$ divide the polynomial $S_n(X)$.*

REMARK. One easy way to obtain $R_n(X)$ and $S_n(X)$ in equation (1) is as follows: We may embed the q-th cyclotomic field $\mathbf{Q}(\zeta_q) = \mathbf{Q}(\zeta_q + \zeta_q^{-1})(\zeta_q)$ into $M_2\big(\mathbf{Q}(\zeta_q + \zeta_q^{-1})\big)$ by the ring homomorphism

$$a + b\zeta_q \longmapsto \begin{pmatrix} a & -b \\ b & a + b(\zeta_q + \zeta_q^{-1}) \end{pmatrix}, \quad \text{where } a, b \in \mathbf{Q}(\zeta_q + \zeta_q^{-1}).$$

https://doi.org/10.4153/CJM-1995-034-4 Published online by Cambridge University Press

So now, $X-\zeta_q$ corresponds to the matrix

$$\begin{pmatrix} X & 1 \\ -1 & X-(\zeta_q+\zeta_q^{-1}) \end{pmatrix},$$

and therefore $(X-\zeta_q)^{p^n}$ corresponds to the matrix

$$\begin{pmatrix} X & 1 \\ -1 & X-(\zeta_q+\zeta_q^{-1}) \end{pmatrix}^{p^n} = \begin{pmatrix} R_n(X) & S_n(X) \\ -S_n(X) & \star \end{pmatrix}.$$

The above matrix multiplication can be done by most of the mathematics software packages.

We define our p^n-tic polynomial to be

$$P_n(X;a) = R_n(X) - \frac{a}{p^n}S_n(X), \quad \text{where } a \in O. \tag{5}$$

From (4), $P_n(X;a) \in O[X]$, and hence the roots are all algebraic integers.

3. Basic properties of the p^n-tic polynomials

THEOREM 1. *(a) For $a \in O$, the p^n-tic polynomial $P_n(X;a)$ has p^n distinct real roots. In particular, $R_n(X) = P_n(X;0)$ has p^n distinct real roots.*

(b) Let ϵ be any root of $R_{n-1}(X)$. The matrix $M = \begin{pmatrix} \epsilon & -1 \\ 1 & \epsilon-(\zeta_q+\zeta_q^{-1}) \end{pmatrix}$ has order p^n in PGL$_2$(**R**). *The transformation*

$$\theta \longmapsto \frac{\epsilon\theta-1}{\theta+\epsilon-(\zeta_q+\zeta_q^{-1})}$$

permutes cyclically the roots of $P_n(X;a)$.

PROOF. We first show that $P_n(X;a)$ has at least one real root. This is obvious if p is odd, since the degree is odd. If $p=2$, the same result holds by an induction argument, see [7]. In particular, $R_{n-1}(X) = P_n(X;0)$ has a real root, say ϵ. Suppose θ is any real root of $P_n(X;a)$ and let $\alpha = \theta-\zeta_q$, $\beta = M\theta-\zeta_q$. Then

$$\beta = \alpha \cdot \frac{\epsilon-\zeta_q}{\theta+\epsilon-(\zeta_q+\zeta_q^{-1})}.$$

Note that $(\epsilon-\zeta_q)^{p^n} = R_n(\epsilon)-\zeta_q S_n(\epsilon) = R_n(\epsilon)$, because $R_{n-1}(X)$ divides $S_n(X)$ by Lemma 1. Therefore $(\epsilon-\zeta_q)^{p^n}$ is real, and so is the number

$$c = \left(\frac{\epsilon-\zeta_q}{\theta+\epsilon-(\zeta_q+\zeta_q^{-1})}\right)^{p^n}.$$

We have

$$\begin{aligned} R_n(M\theta)-\zeta_q S_n(M\theta) &= (M\theta-\zeta_q)^{p^n} \\ &= \beta^{p^n} \\ &= c\alpha^{p^n} \\ &= c(\theta-\zeta_q)^{p^n} \\ &= cR_n(\theta)-\zeta_q\big(cS_n(\theta)\big), \end{aligned}$$

https://doi.org/10.4153/CJM-1995-034-4 Published online by Cambridge University Press

and hence

$$R_n(M\theta) = cR_n(\theta) \quad \text{and} \quad S_n(M\theta) = cS_n(\theta).$$

As a consequence, $M\theta$ is also a root of $P_n(X; a)$, since

$$P_n(M\theta; a) = c \cdot P_n(\theta; a) = 0.$$

Therefore the transformation M permutes the roots.

Since M has two distinct eigenvalues $\epsilon - \zeta_q$ and $\epsilon - \zeta_q^{-1}$, it must be similar to the diagonal matrix

$$D = \begin{pmatrix} \epsilon - \zeta_q & 0 \\ 0 & \epsilon - \zeta_q^{-1} \end{pmatrix}.$$

Because the matrices M and D have the same order, it suffices to show that D is of order p^n. Now for any z

$$Dz = \frac{\epsilon - \zeta_q}{\epsilon - \zeta_q^{-1}} z = \zeta z,$$

where $\zeta = \frac{\epsilon - \zeta_q}{\epsilon - \zeta_q^{-1}}$. Note that ϵ is real and $R_{n-1}(\epsilon) = 0$. Therefore

$$(\epsilon - \zeta_q)^{p^{n-1}} = R_{n-1}(\epsilon) - \zeta_q S_{n-1}(\epsilon) = -\zeta_q S_{n-1}(\epsilon),$$

and hence

$$(\epsilon - \overline{\zeta_q})^{p^{n-1}} = -\overline{\zeta_q} S_{n-1}(\epsilon) = -\zeta_q^{-1} S_{n-1}(\epsilon).$$

Clearly $S_{n-1}(\epsilon) \neq 0$, since $\epsilon \neq \zeta_q$. All these yield

$$\zeta^{p^{n-1}} = \left(\frac{\epsilon - \zeta_q}{\epsilon - \overline{\zeta_q}}\right)^{p^{n-1}} = \frac{-\zeta_q S_{n-1}(\epsilon)}{-\zeta_q^{-1} S_{n-1}(\epsilon)} = \zeta_q^2, \tag{6}$$

and thus ζ is of order p^n. But $Dz = \zeta z$, so D is of order p^n and the only fixed points of a non-trivial power of D are 0 and ∞. Therefore a non-trivial power of M can have only two fixed points, namely ζ_q and ζ_q^{-1}, both of which are complex. If θ is a root, the numbers $M^k\theta$, $0 \leq k < p^n$, must be distinct roots of $P_n(X; a)$. This proves the theorem.

REMARK. From the proof of the above theorem, we know that if ϵ is a root of $R_{n-1}(X)$ then the element $(\epsilon - \zeta_q)/(\epsilon - \zeta_q^{-1})$ is a primitive p^n-th root of unity.

PROPOSITION 1. *If ϵ is the largest root of $R_{n-1}(X)$ and if $\xi = e^{\frac{(p+1)\pi i}{p}}$, then*

$$\frac{\epsilon - \xi}{\epsilon - \xi^{-1}} = \exp\left(\frac{2\pi i}{p^n}\right).$$

PROOF. Among the $(p-1)p^{n-1}$ primitive p^n-th roots of unity,

$$\exp\Big(\frac{2\pi i}{p^n}\Big) = \cos\Big(\frac{2\pi}{p^n}\Big) + i\sin\Big(\frac{2\pi}{p^n}\Big) \quad \text{and its inverse}$$

have the largest real part. We have

$$\Big\{\frac{\epsilon-\xi}{\epsilon-\xi^{-1}} \;\Big|\; \epsilon = \text{ root of } R_{n-1}(X)\Big\} = \Big\{\exp\Big(\frac{2k\pi i}{p^n}\Big) \;\Big|\; k \not\equiv 0 \pmod{p}\Big\}$$

(the left side is contained in the right side, and both have $(p-1)p^{n-1}$ elements) and $\Re(\frac{\epsilon-\xi}{\epsilon-\xi^{-1}}) = 1 - \frac{1-\cos\frac{2\pi}{p}}{\epsilon^2+2\epsilon\cos\frac{\pi}{p}+1}$ is the largest if ϵ is the largest root of $R_{n-1}(X)$. Since the product of the roots of $R_{n-1}(X)$ is 1, and the number of roots is odd, ϵ must be positive. Therefore $\Im(\frac{\epsilon-\xi}{\epsilon-\xi^{-1}}) = \frac{2\epsilon\sin\frac{\pi}{p}+\sin\frac{2\pi}{p}}{\epsilon^2+2\epsilon\cos\frac{\pi}{p}+1} > 0$. This proves the proposition.

For each natural number n, we let ϵ_n be the largest root of the polynomial $R_n(X)$. The case $p = 2$ was discussed in the 2^n-tic paper [7], so let p be an odd prime. We know that for $p = 3$,

$$\epsilon_0 = 0, \quad \epsilon_1 = 2\cos\Big(\frac{\pi}{9}\Big), \quad \epsilon_2 = 2\cos\Big(\frac{\pi}{27}\Big) + 2\cos\Big(\frac{3\pi}{27}\Big) + 2\cos\Big(\frac{5\pi}{27}\Big) + 2\cos\Big(\frac{7\pi}{27}\Big).$$

How are these ϵ_n's related in general? From the above proposition,

$$\frac{\epsilon_{n-1}-\xi}{\epsilon_{n-1}-\xi^{-1}} = \zeta_{p^n},$$

where $\zeta_{p^n} = \exp(2\pi i/p^n)$ and $\xi = \exp\big(\frac{(p+1)\pi i}{p}\big)$. Solving this equation for ϵ_{n-1}, and denoting the primitive p-th root of unity $\exp(\frac{2\pi i}{p})$ by ζ_p, we get (note that the following argument is not valid for $p = 2$)

$$\begin{aligned}
\epsilon_{n-1} &= \xi^{-1}\frac{\xi^2-\zeta_{p^n}}{1-\zeta_{p^n}} \\
&= -\zeta_{p^n}^{(\frac{p-1}{2})p^{n-1}}\frac{\zeta_{p^n}(\zeta_{p^n}^{p^{n-1}-1}-1)}{\zeta_{p^n}-1} \\
&= -\zeta_{p^n}^{(\frac{p-1}{2})p^{n-1}}\sum_{j=1}^{p^{n-1}-1}\zeta_{p^n}^{j} \\
&= -\sum_{j=1}^{p^{n-1}-1}\zeta_{p^n}^{j+(\frac{p-1}{2})p^{n-1}} \\
&= -\sum_{j=1}^{\frac{1}{2}(p^{n-1}-1)} 2\cos\Big(\frac{2\pi j+\pi(p^n-p^{n-1})}{p^n}\Big) \\
&= \sum_{j=1}^{\frac{1}{2}(p^{n-1}-1)} 2\cos\Big(\frac{p^{n-1}-2j}{p^n}\pi\Big) \\
&= \sum_{j=1}^{\frac{1}{2}(p^{n-1}-1)} 2\cos\Big(\frac{(2j-1)\pi}{p^n}\Big).
\end{aligned}$$

https://doi.org/10.4153/CJM-1995-034-4 Published online by Cambridge University Press

We have proved the next proposition (for the case $p = 2$, see [7]).

PROPOSITION 2. *Let ϵ_n be the largest root of the polynomial $R_n(X)$. Then*

$$\epsilon_n = \begin{cases} \cot\left(\frac{\pi}{2^{n+1}}\right) & \text{if } p = 2, \\ \sum_{j=1}^{\frac{1}{2}(p^n-1)} 2\cos\left(\frac{(2j-1)\pi}{p^{n+1}}\right) & \text{if } p \text{ is an odd prime.} \end{cases}$$

PROPOSITION 3. *Let $n \geq 2$ and let ϵ be any root of $R_{n-1}(X)$. Then*

$$\mathbf{Q}(\epsilon) = \mathbf{Q}(\zeta_{p^n})^+.$$

PROOF. Since $(\epsilon - \zeta_q)/(\epsilon - \zeta_q^{-1}) = \zeta$, for some primitive p^n-th root of unity ζ, we have $\epsilon = \zeta_q^{-1}\frac{\zeta_q^2-\zeta}{1-\zeta}$. Let $\sigma\colon \zeta \longmapsto \zeta^d$ be an automorphism of $\mathbf{Q}(\zeta)$ that fixes the element ϵ. Then

$$\zeta_q^{-d}\frac{\zeta_q^{2d} - \zeta^d}{1 - \zeta^d} = \zeta_q^{-1}\frac{\zeta_q^2 - \zeta}{1 - \zeta}.$$

We may write this relation in the following form

$$(\zeta_q^d - \zeta_q) + \zeta(\zeta_q^{-1} - \zeta_q^d) + \zeta^d(\zeta_q - \zeta_q^{-d}) + \zeta^{d+1}(\zeta_q^{-d} - \zeta_q^{-1}) = 0. \tag{7}$$

Applying $\zeta \longmapsto \zeta^{1+pj}$, for $j = 1, 2, 3$ to the relation (7), we obtain three more equations. Together with (7), they form a system of four linear equations in four unknowns

$$x_1 = \zeta_q^d - \zeta_q, \quad x_2 = \zeta_q^{-1} - \zeta_q^d, \quad x_3 = \zeta_q - \zeta_q^{-d}, \quad x_4 = \zeta_q^{-d} - \zeta_q^{-1}.$$

Writing this system in matrix form, we have

$$\begin{pmatrix} 1 & \zeta & \zeta^d & \zeta^{d+1} \\ 1 & \zeta\zeta^p & \zeta^d(\zeta^d)^p & \zeta^{d+1}(\zeta^{d+1})^p \\ 1 & \zeta\zeta^{2p} & \zeta^d(\zeta^d)^{2p} & \zeta^{d+1}(\zeta^{d+1})^{2p} \\ 1 & \zeta\zeta^{3p} & \zeta^d(\zeta^d)^{3p} & \zeta^{d+1}(\zeta^{d+1})^{3p} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

The determinant of the coefficient matrix is equal to

$$\zeta^{2(d+1)} \cdot \det\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \zeta^p & \zeta^{dp} & \zeta^{(d+1)p} \\ 1 & (\zeta^p)^2 & (\zeta^{dp})^2 & (\zeta^{(d+1)p})^2 \\ 1 & (\zeta^p)^3 & (\zeta^{dp})^3 & (\zeta^{(d+1)p})^3 \end{pmatrix}.$$

Clearly, our system has nontrivial solution and hence the above Vandermonde determinant is equal to 0. Therefore, the four numbers $1, \zeta^p, \zeta^{dp}$, and $\zeta^{(d+1)p}$ are not distinct. Only two cases arise:

CASE 1. $\zeta^{(d+1)p} = 1 \Rightarrow p|(d+1) \Rightarrow \zeta_q^{d+1} = 1 \Rightarrow \zeta_q^d = \zeta_q^{-1}$.

CASE 2. $\zeta^{dp} = \zeta^p \Rightarrow p|(d-1) \Rightarrow \zeta_q^{d-1} = 1 \Rightarrow \zeta_q^d = \zeta_q$.

From (7), the first case tells us that $\zeta^d = \zeta^{-1}$ and hence

$$\sigma \in \mathrm{Gal}\big(\mathbf{Q}(\zeta)/\mathbf{Q}(\zeta)^+\big).$$

The second case implies that $\zeta^d = \zeta$ and therefore $\sigma = \mathrm{id}$. Since the element $\zeta_q^{-1}\frac{\zeta_q^2-\zeta}{1-\zeta} \in \mathbf{Q}(\zeta)^+$ is only fixed by $\{\mathrm{id}, \sigma_{-1}\}$, the proposition is proved.

https://doi.org/10.4153/CJM-1995-034-4 Published online by Cambridge University Press

4. Irreducibility of the p^n-tic polynomials.

THEOREM 2. *Fix $n \geq 1$. Let $a \in \mathbf{Z}[\zeta_q+\zeta_q^{-1}]$. Then $P_n(X;a)$ is irreducible over the real q-th cyclotomic field $\mathbf{Q}(\zeta_q)^+$ except for finitely many values of a. When $p = 3$, $P_n(X;a)$ is irreducible for all $a \in \mathbf{Z}[\zeta_q+\zeta_q^{-1}]$.*

PROOF. If θ is a root of $P_n(X;a)$, then the p^n roots are

$$\{M^j\theta \mid 0 \leq j < p^n\},$$

where $M = \begin{pmatrix} \epsilon & -1 \\ 1 & \epsilon-(\zeta_q+\zeta_q^{-1}) \end{pmatrix}$ and $\frac{\epsilon-\zeta_q}{\epsilon-\zeta_q^{-1}} = \zeta_{p^n}$. We know that

$$M = A^{-1}DA,$$

where $D = \begin{pmatrix} \epsilon-\zeta_q & 0 \\ 0 & \epsilon-\zeta_q^{-1} \end{pmatrix}$, and one choice for A is $\begin{pmatrix} 1 & -\zeta_q \\ 1 & -\zeta_q^{-1} \end{pmatrix}$. Thus $M^j = A^{-1}D^jA$, and hence $AM^j = D^jA$. Let $\alpha = A\theta = \frac{\theta-\zeta_q}{\theta-\zeta_q^{-1}}$, and let $\beta = \alpha^{p^n}$. Calculation shows $\beta \in \mathbf{Q}(\zeta_q)$ as follows: (note $P_n(\theta;a) = R_n(\theta) - \frac{a}{p^n}S_n(\theta) = 0$)

$$\beta = \alpha^{p^n} = \frac{(\theta-\zeta_q)^{p^n}}{(\theta-\zeta_q^{-1})^{p^n}} = \frac{R_n(\theta)-\zeta_qS_n(\theta)}{R_n(\theta)-\zeta_q^{-1}S_n(\theta)} = \frac{a-p^n\zeta_q}{a-p^n\zeta_q^{-1}} \in \mathbf{Q}(\zeta_q).$$

We have the following: (see Lang's Algebra Section VIII, 9, Theorem 16 [5])

$$\mathbf{Q}(\zeta_{p^n},\theta) = \mathbf{Q}(\zeta_{p^n}, \sqrt[p^n]{\beta}) \text{ is of degree } p^n \text{ over } \mathbf{Q}(\zeta_{p^n}) \iff \beta \notin \mathbf{Q}(\zeta_{p^n})^p.$$

Suppose β is a p-th power in $\mathbf{Q}(\zeta_{p^n})$. Then $\mathbf{Q}(\zeta_q) \subset \mathbf{Q}(\zeta_q)(\sqrt[p]{\beta}) \subset \mathbf{Q}(\zeta_{p^n})$, and therefore we have

$$\mathbf{Q}(\zeta_q)(\sqrt[p]{\beta}) = \mathbf{Q}(\zeta_q) \quad \text{or} \quad \mathbf{Q}(\zeta_{qp}). \tag{8}$$

CASE I: $p = 2$. Then $q = 4$ and $a \in \mathbf{Z}$. This is the hard case and we proved in [7] that $P_n(X;a)$ is irreducible over $\mathbf{Q}$ if and only if a^2+4^n is not a square in $\mathbf{Z}$. Obviously, $a^2+4^n = b^2$ has only $2n-1$ solutions for $a \in \mathbf{Z}$. So the theorem is true for $p = 2$.

CASE II: $p > 3$ IS AN ODD PRIME. Then $q = p$. The result in (8) implies that

$$\beta = \zeta_p^x\gamma^p, \quad \text{for some } x \in \mathbf{Z} \text{ and } \gamma \in \mathbf{Q}(\zeta_p).$$

Let $\mathcal{P}$ be a prime ideal of $\mathbf{Z}[\zeta_p]$. Suppose $\mathcal{P}$ divides both $a-p^n\zeta_p$ and $a-p^n\zeta_p^{-1}$. Then $\mathcal{P}$ divides $p^n(\zeta_p-\zeta_p^{-1})$, so we have $\mathcal{P} = (1-\zeta_p)$. Therefore

$$(a-p^n\zeta_p) = (1-\zeta_p)^yI^p, \quad I = \text{ an ideal of } \mathbf{Q}(\zeta_p),\ y \in \mathbf{Z}.$$

Taking norms to $\mathbf{Q}(\zeta_p)^+$, we obtain

$$\left(a^2-p^n(\zeta_p+\zeta_p^{-1})a+p^{2n}\right) = (2-\zeta_p-\zeta_p^{-1})^y(I\bar{I})^p.$$

https://doi.org/10.4153/CJM-1995-034-4 Published online by Cambridge University Press

Let $I_1, \ldots, I_h$ be representatives for the elements of order p in the ideal class group of $\mathbf{Q}(\zeta_p)^+$. Then $\bar{I}I = \alpha I_i$, some i, some $\alpha \in \mathbf{Q}(\zeta_p)^+$. Let $I_i^p = (\delta_i)$. Putting everything together, we have

$$a^2 - p^n(\zeta_p + \zeta_p^{-1})a + p^{2n} = (\text{unit})(2 - \zeta_p - \zeta_p^{-1})^y \alpha^p \delta_i.$$

We need only to consider $y \in \{0, 1, 2, \ldots, p-1\}$, since we can adjust α^p. Because there are only finitely many numbers δ_i and finitely many classes of units modulo p-th powers, we have equations of the form (p, n fixed)

$$(9) \qquad a^2 - p^n(\zeta_p + \zeta_p^{-1})a + p^{2n} = cb^p, \quad a, b \in \mathbf{Q}(\zeta_p)^+,$$

where $c \neq 0$, $c \in$ finite set. When $p > 3$, such an equation in a, b represents a curve of genus > 1, so Faltings' theorem implies that there are only finitely many pairs (a, b) from $\mathbf{Q}(\zeta_p)^+$ which satisfy such an equation. Since there are only finitely many such equations, there are only finitely many values of $a \in \mathbf{Z}[\zeta_p]^+$ for which $\beta = p$-th power. This proves the theorem for $p > 3$.

CASE III: $p = 3$. Then $q = 3$ and $a \in \mathbf{Z}$. Since $(a - 3^n\zeta_3, a - 3^n\zeta_3^{-1})$ is a power of $\sqrt{-3}$, equation (8) gives us

$$a - 3^n\zeta_3 = \zeta_3^w \gamma^3 (\sqrt{-3})^m \quad \text{with } w \in \mathbf{Z},\ m = 0, 1, 2.$$

Let $R = \mathbf{Z}[\frac{1}{3}]$ and let $a_1 = a/3^n \in R$. We have

$$a_1 - \zeta_3 = \zeta_3^w \gamma_1^3 (\sqrt{-3})^{m'} \quad \text{with } \beta_1 \in R[\zeta_3], \text{ and } m' = 0, 1, 2.$$

Taking norms yields $a_1^2 + a_1 + 1 = 3^{m'}N^3$ with $N = \pm\,\mathrm{Norm}\,\beta_1 \in R$, therefore

$$(10) \qquad (2a_1 + 1)^2 = 4 \cdot 3^{m'}N^3 - 3.$$

(i) If $m' = 0$, equation (10) can be transformed to

$$(8a_1 + 4)^2 = (4N)^3 - 48.$$

We show below in Proposition 4 that the only R-valued points on the curve $y^2 = x^3 - 48$ are $(4, \pm 4)$, $(28, \pm 148)$, and $(73/9, \pm 595/27)$. Since y is even in our case, we can ignore the last pair. The first two yields $a_1 = 0, -1, 18, -19$.

(ii) If $m' = 1$, equation (10) becomes

$$(24a_1 + 12)^2 = (12N)^3 - 432.$$

The only rational points on the curve $y^2 = x^3 - 432$ are the point at infinity and $(12, \pm 36)$ (this is the curve A1 of conductor 27 in [1]). We obtain $a_1 = 1, -2$.

(iii) If $m' = 2$, equation (10) becomes

$$(72a_1 + 36)^2 = (36N)^3 - 3888.$$

https://doi.org/10.4153/CJM-1995-034-4 Published online by Cambridge University Press

The only rational point on the curve $y^2 = x^3 - 3888$ is the point at infinity (this is the curve B2 of conductor 243 in [1]).

For the values $a_1 = 0, -1, 18, -19, 1, -2$, we find that

$$(a - 3^n\zeta_3)/(a - 3^n\zeta_3^{-1})$$

takes on the values ζ_3^2, ζ_3, $\zeta_3^2(3+\zeta_3)^3/(3+\zeta_3^{-1})^3$, $\zeta_3(3+\zeta_3^{-1})^3/(3+\zeta_3)^3$, $-\zeta_3$, $-\zeta_3^2$, respectively.

For $a_1 = 0, \pm 1, -2$, we therefore have that

$$\mathbf{Q}(\zeta_{3^n}, \theta) = \mathbf{Q}(\zeta_{3^n}, \sqrt[3^n]{\pm\zeta_3^{\pm 1}}) = \mathbf{Q}(\zeta_{3^{n+1}}).$$

Since $\mathrm{Gal}\big(\mathbf{Q}(\zeta_{3^{n+1}})/\mathbf{Q}\big)$ is cyclic of order $2 \cdot 3^n$, and since the above implies that θ is not fixed by the subgroup of order 3, we must have $[\mathbf{Q}(\theta) : \mathbf{Q}] \geq 3^n$. Therefore $P_n(X; a)$ is irreducible.

Now consider $a_1 = 18, -19$. First, we claim that $(3+\zeta_3)/(3+\zeta_3^{-1})$ is not a cube in $\mathbf{Q}(\zeta_{3^m})$, for any $m \geq 1$. Otherwise its cube root generates a subextension of $\mathbf{Q}(\zeta_{3^m})/\mathbf{Q}(\zeta_3)$, hence equals a power of ζ_3 times a cube in $\mathbf{Q}(\zeta_3)$. Since $3+\zeta_3$ and $3+\zeta_3^{-1}$ are non-associated primes in $\mathbf{Z}[\zeta_3]$, this is impossible. Therefore

$$[\mathbf{Q}(\zeta_{3^{n+1}}, \theta) : \mathbf{Q}] = \Big[\mathbf{Q}\Big(\zeta_{3^{n+1}}, \sqrt[3^{n-1}]{(3+\zeta_3)/(3+\zeta_3^{-1})}\Big) : \mathbf{Q}(\zeta_{3^{n+1}})\Big] = 3^{n-1}.$$

Let $P = a^2 + 3^n a + 9^n$ and let $A = \frac{1}{3}\arctan\big(\frac{3^n+2a}{3^n\sqrt{3}}\big)$. Then over the field $\mathbf{Q}(\zeta_{3^{n+1}})$, we have the factorization

$$P_n(X; a) = P_{n-1}(X; 3^{n-1}\alpha_1)P_{n-1}(X; 3^{n-1}\alpha_2)P_{n-1}(X; 3^{n-1}\alpha_3), \tag{11}$$

where $\alpha_1, \alpha_3 = \frac{a+\sqrt{P}\sin A \pm \sqrt{3P}\cos A}{3^n}$, and $\alpha_2 = \frac{a-2\sqrt{P}\sin A}{3^n}$.

CLAIM. *These three factors are conjugate via* $\mathrm{Gal}\big(\mathbf{Q}(\zeta_{3^{n+1}})/\mathbf{Q}\big)$.

PROOF. Since we are in the cases $a_1 = 18, -19$, we have

$$P = 9^n(a_1^2 + a_1 + 1) = 9^n \cdot 7^3, \quad \text{and} \quad A = \frac{1}{3}\arctan\Big(\frac{\pm 37}{\sqrt{3}}\Big).$$

We'll look at the case for $a_1 = 18$ only, because the other one is similar. Calculation shows that $\alpha_1 = 18 + 7\sqrt{7}\sin A + 7\sqrt{21}\cos A \sim 55.0360$, $\alpha_2 = 18 - 14\sqrt{7}\sin A \sim -0.0178465$, and $\alpha_3 = 18 + 7\sqrt{7}\sin A - 7\sqrt{21}\cos A \sim -1.01816$. Note that $\alpha_1, \alpha_2, \alpha_3$ are independent of n, since A is independent of n.

Let $\beta = \cos(2\pi/9)$. Then β is a root of $8X^3 - 6X + 1$ and its conjugates are $\beta_1 = \beta$, $\beta_2 = \cos(8\pi/9)$, and $\beta_3 = \cos(4\pi/9)$. Calculation shows

$$\alpha_1 = -10 + 42\beta + 56\beta^2 = f(\beta),$$
$$\alpha_2 = 60 - 14\beta - 84\beta^2 = g(\beta),$$
$$\alpha_3 = 4 - 28\beta + 28\beta^2 = h(\beta).$$

https://doi.org/10.4153/CJM-1995-034-4 Published online by Cambridge University Press

Also, we have

$$f(\beta_1) = g(\beta_3) = h(\beta_2),$$
$$f(\beta_2) = g(\beta_1) = h(\beta_3),$$
$$f(\beta_3) = g(\beta_2) = h(\beta_1).$$

The result follows. Note that once we have found this factorization, it can be checked easily using (2) and (3).

In the factorization (11), one factor has θ as a root, hence is irreducible. Since the factors are conjugate via $\mathrm{Gal}\big(\mathbf{Q}(\zeta_{3^{n+1}})/\mathbf{Q}\big)$. All three factors are irreducible over $\mathbf{Q}(\zeta_{3^{n+1}})$. Since they are not in $\mathbf{Q}[X]$, it follows that $P_n(X;a)$ is irreducible over $\mathbf{Q}$. This completes the proof of the irreducibility theorem.

PROPOSITION 4. *Let $R = \mathbf{Z}[\frac{1}{3}]$. The R-valued solutions of $y^2 + 48 = x^3$ are*

$$(4, \pm 4), \quad (28, \pm 148), \quad \textit{and} \quad (73/9, \pm 595/27).$$

PROOF. Suppose $x, y \in R$, but not in $\mathbf{Z}$.

CASE I: y IS EVEN. Then $2|x \Rightarrow 8|y^2 \Rightarrow 4|y \Rightarrow 4|x$. Write $x = 4x_1$, $y = 4y_1$. The equation becomes $y_1^2 + 3 = 4x_1^3$. This implies y_1 is odd and so

$$\frac{y_1 + \sqrt{-3}}{2} \cdot \frac{y_1 - \sqrt{-3}}{2} = x_1^3.$$

Clearly $\frac{y_1+\sqrt{-3}}{2}$ and $\frac{y_1-\sqrt{-3}}{2}$ are relatively prime in the UFD $R[\zeta_3]$. Therefore

$$\frac{y_1 + \sqrt{-3}}{2} = \zeta_3^u(\sqrt{-3})^v\left(\frac{a + b\sqrt{-3}}{2}\right)^3, \quad a, b \in R. \tag{12}$$

Since $x_1 \notin \mathbf{Z}$ and $y_1 \notin \mathbf{Z}$, we have $v_3(y_1) \equiv 0 \pmod 3$, where v_3 is the 3-adic valuation, and so $v \equiv 0 \pmod 3$. Therefore, we may assume $v = 0$.

(i) $u = 0$: Equation (12) becomes

$$4(y_1 + \sqrt{-3}) = a^3 + 3a^2b\sqrt{-3} - 9ab^2 - 3b^3\sqrt{-3}.$$

Hence $4 = 3b(a^2 - b^2)$. If b is odd, then a must be odd. But then $a^2 - b^2 \equiv 0 \pmod 8$, a contradiction. Therefore b is even. If a is even then $3b(a^2 - b^2) \equiv 0 \pmod 8$, so a is odd. Therefore $4y_1 = a^3 - 9ab^2$ is odd, a contradiction.

(ii) $u = 1$: Equation (12) becomes

$$8(y_1 + \sqrt{-3}) = (-1 + \sqrt{-3})(a + b\sqrt{-3})^3.$$

Hence $8 = a^3 - 3a^2b - 9ab^2 + 3b^3$. Let $l = v_3(a)$, $m = v_3(b)$. Since $y_1 \notin \mathbf{Z}$, at least one of l, m is < 0. The 3-adic valuations of the terms on the right are $3l$, $1 + 2l + m$, $2 + l + 2m$, $1 + 3m$, respectively. We claim there is a unique smallest one: If $l \geq 1 + m$ then $1 + 3m$ is smallest, while if $l \leq m$ then $3l$ is smallest. Therefore either $3l$ or $1 + 3m$ is the unique smallest valuation. Since at least one of l, m is negative, the right hand side has negative valuation, hence cannot equal 8.

(iii) $u = 2$: The automorphism $\sqrt{-3} \longmapsto -\sqrt{-3}$, plus appropriate adjustment of signs, reduces this case to case (ii).

https://doi.org/10.4153/CJM-1995-034-4 Published online by Cambridge University Press

CASE II: y IS ODD. $(y+4\sqrt{-3})(y-4\sqrt{-3}) = x^3$. Since $y+4\sqrt{-3}$ and $y-4\sqrt{-3}$ are relatively prime in $R[\zeta_3]$, we have

$$(13) \qquad y+4\sqrt{-3} = \zeta_3^u(\sqrt{-3})^v\left(\frac{a+b\sqrt{-3}}{2}\right)^3, \quad a,b \in R.$$

As before, we may assume $v = 0$.

(i) $u = 0$: Equation (13) becomes

$$8(y+4\sqrt{-3}) = a^3 + 3a^2b\sqrt{-3} - 9ab^2 - 3b^3\sqrt{-3}.$$

Hence $32 = 3b(a+b)(a-b)$. If $a+b$ is odd, then so is $a-b$. Therefore

$$b = \pm 32\cdot 3^r, \quad a+b = \pm 3^s, \quad a-b = \pm 3^t,$$

and hence $\pm 64\cdot 3^r = 2b = \pm 3^s \pm 3^t$, so $64 = \pm 3^{s-r} \pm 3^{t-r}$, which is impossible. Therefore $a+b$ is even, and so is $a-b$. Suppose b is odd. Then $a+b \not\equiv a-b \pmod 4$, so

$$2^4 \| a+b \text{ and } 2^1 \| a-b, \quad \text{or} \quad 2^1 \| a+b \text{ and } 2^4 \| a-b.$$

Changing the sign of b if necessary, we may assume the first possibility. Then

$$b = \pm 3^r, \quad a+b = \pm 16\cdot 3^s, \quad a-b = \pm 2\cdot 3^t, \quad r+s+t = -1.$$

We obtain $\pm 2\cdot 3^r = \pm 16\cdot 3^s \pm 2\cdot 3^t$, so $8 = \pm 3^{r-s} \pm 3^{s-t}$. This implies $\{r-s, t-s\} = \{0, 2\}$ (in some order). Therefore $-1 = r+s+t = (r-s)+(t-s)+3s = 2+3s$, so $s = -1$ and $\{r,t\} = \{-1,1\}$. This yields finitely many possibilities which may be checked individually. The solutions are $(a,b) = (\pm 7/3, \pm 3)$ and $(\mp 17/3, \pm 1/3)$. All of these yield $x = (a^2+3b^2)/4 = 73/9$ and hence $y = \pm 595/27$.

Now suppose b is even. Since $a+b$ is even, so is a. Write $a = 2a_1$, $b = 2b_1$. Then $4 = 3b_1(a_1+b_1)(a_1-b_1)$. It is easy to see that b_1 must be even and a_1 must be odd. Therefore

$$b_1 = \pm 4\cdot 3^r, \quad a_1+b_1 = \pm 3^s, \quad a_1-b_1 = \pm 3^t, \quad r+s+t = -1.$$

Subtracting, we obtain $\pm 8\cdot 3^r = 2b_1 = \pm 3^s \pm 3^t$, so $8 = \pm 3^{s-r} \pm 3^{t-r}$. Therefore $\{s-r, t-r\} = \{0,2\}$, and $-1 = r+s+t = 2+3r$. It follows that $r = -1$ and $\{s,t\} = \{-1,1\}$. The finitely many cases may be checked individually, and yield $(a,b) = (\pm 10/3, \pm 8/3)$. These yield $x = (a^2+3b^2)/4 = 73/9$, which is the same as above.

(ii) $u = 1$: Equation (13) becomes

$$16(y+4\sqrt{-3}) = (-1+\sqrt{-3})(a+b\sqrt{-3})^3.$$

Hence $64 = a^3 - 3a^2b - 9ab^2 + 3b^3$. An analysis of 3-adic valuations, as in the case where y is even and $u = 1$, shows that this equation is impossible.

(iii) $u = 2$: The automorphism $\sqrt{-3} \longmapsto -\sqrt{-3}$ reduces this to the case $u = 1$.

Therefore the only solutions of $y^2+48=x^3$ with $x,y\in R$ are

$$(x,y)=(73/9,\pm 595/27)$$

and the integral solutions. From [4], the integral solutions are $(4,\pm 4)$, and $(28,\pm 148)$. The result could also be deduced from the data in Table 4 in *Modular Functions of One Variable IV* (ed. by B. J. Birch and W. Kuyk), Springer Lecture Notes in Math. 476, Springer-Verlag, 1975. This completes the proof of the proposition.

5. **Units and roots of the p^n-tic polynomial.** Since $p=2$ was treated in [7], we assume p is odd. Fix a root θ of $P_n(X;a)$, and therefore the roots are of the form

$$M^k\theta,\quad 0\le k<p^n,$$

where $M=\begin{pmatrix}\epsilon & -1\\ 1 & \epsilon-(\zeta_q+\zeta_q^{-1})\end{pmatrix}$ and $\epsilon=\zeta_q^{-1}(\zeta_q^2-\zeta_{p^n})/(1-\zeta_{p^n})$. Let $K=\mathbf{Q}(\epsilon)=\mathbf{Q}(\zeta_{p^n})^+$. Throughout this section, we assume $P_n(X;a)$ is irreducible over K. As shown in Theorem 2, this excludes only finitely many a. Then it is easy to see that $K(\theta)$ is the Galois closure of $\mathbf{Q}(\theta)$, and the Galois group $\mathrm{Gal}\big(K(\theta)/K\big)=\langle\sigma\rangle$ is cyclic of order p^n, where

$$\sigma^k(\theta)=M^k\theta,\quad 0\le k<p^n.$$

Since the constant term of $P_n(X;a)$ is -1, these $\sigma^k(\theta)$ are units in the ring of integers of $K(\theta)$. Obviously, these p^n units are not independent. For instance, we have the following lemma.

LEMMA 2. *For odd primes p, we have $\prod_{j=0}^{p-1}\sigma^{jp^{n-1}}(\theta)=1$.*

PROOF. We have

$$M_n=\lambda_nA^{-1}D_nA,$$

where $\lambda_n=\epsilon_{n-1}-\zeta_q^{-1}$, $D_n=\begin{pmatrix}\frac{\epsilon_{n-1}-\zeta_q}{\epsilon_{n-1}-\zeta_q^{-1}} & 0\\ 0 & 1\end{pmatrix}$, and $A=\begin{pmatrix}1 & -\zeta_q\\ 1 & -\zeta_q^{-1}\end{pmatrix}$.
Since $D_n^{p^{n-1}}=\begin{pmatrix}\zeta_q^2 & 0\\ 0 & 1\end{pmatrix}$ and $M_1=\lambda_1A^{-1}\begin{pmatrix}\frac{0-\zeta_q}{0-\zeta_q^{-1}} & 0\\ 0 & 1\end{pmatrix}A$, we have

$$M_n^{p^{n-1}}=M_1\quad\text{in }\ \mathrm{PGL}_2(\mathbf{R}).$$

CLAIM. $\prod_{j=0}^{p-1}M_1^j(X)=1$, *for all X.*

PROOF OF THE CLAIM. Let $Y=AX$. Then

$$M_1^j(X)=A^{-1}D_1^jY=A^{-1}(\zeta_q^{2j}Y)=\zeta_q\frac{1-\zeta_q^{2j-2}Y}{1-\zeta_q^{2j}Y}.$$

The product clearly equals 1, and hence the claim is true. The lemma follows immediately from the claim.

THEOREM 3. *The $(p-1)p^{n-1}$ elements*

$$\{\sigma^{k-1}(\theta)\mid 1\le k\le(p-1)p^{n-1}\}$$

are independent units in the ring $O_{K(\theta)}$ of integers of the field $K(\theta)$, where $K=\mathbf{Q}(\epsilon)=\mathbf{Q}(\zeta_{p^n})^+$.

https://doi.org/10.4153/CJM-1995-034-4 Published online by Cambridge University Press

PROOF. Let $\theta_k = \sigma^{k-1}(\theta)$, $1 \le k \le p^n$ and let $m = p^{n-1}$. Then

$$\theta_{k+(p-1)m} = \prod_{j=0}^{p-2} \theta_{k+jm}^{-1}, \quad \text{for } 1 \le k \le p^{n-1}. \tag{14}$$

Suppose we have $b_1, b_2, b_3, \ldots, b_{(p-1)m} \in \mathbf{Z}$ such that

$$\prod_{k=1}^{(p-1)m} \theta_k^{b_k} = 1. \tag{15}$$

Applying $\sigma, \ldots, \sigma^{(p-1)m-1}$ to equation (15) and simplifying by using formula (14), we obtain $(p-1)m$ equations. Taking absolute values followed by taking logarithms of these $(p-1)m$ equations, we have a system of $(p-1)m$ linear equations in $(p-1)m$ unknowns $x_k = \log|\theta_k|$, $1 \le k \le (p-1)m$. If B is the coefficient matrix, then $\det(B) = 0$.

LEMMA 3. *The determinant of the* $(p-1)m \times (p-1)m$ *matrix* B *is*

$$\det(B) = \prod_{\substack{\zeta=\text{primitive}\\ p^n\text{-th root of } 1}} \sum_{k=1}^{(p-1)m} b_k \zeta^{k-1}.$$

PROOF. The first row of the matrix B is $(b_1, \ldots, b_{(p-1)m})$. If $(c_1, \ldots, c_{(p-1)m})$ is the j-th row, the $(j+1)$-st row is

$$(0, c_1, c_2, \ldots, c_{(p-1)m-1}) - c_{(p-1)m}(1, 0, \ldots, 1, 0, \ldots),$$

where the 1's are in positions $1, 1+m, 1+2m, \ldots, 1+(p-2)m$.

Let ζ be any primitive p^n-th root of unity and let $\lambda = \sum_{k=1}^{(p-1)m} b_k \zeta^{k-1}$. Then we claim

$$\vec{\zeta} = \begin{pmatrix} 1 \\ \zeta \\ \vdots \\ \zeta^{(p-1)m-1} \end{pmatrix}$$

is an eigenvector of B with eigenvalue λ. Clearly, the first row times $\vec{\zeta}$ yields λ. Assume the j-th row times $\vec{\zeta}$ is $\lambda\zeta^{j-1}$. Then the $(j+1)$-st row times $\vec{\zeta}$ is

$$\begin{aligned} c_1\zeta + c_2\zeta^2 + \cdots + c_{(p-1)m-1}\zeta^{(p-1)m-1} &- c_{(p-1)m}(1 + \zeta^m + \cdots + \zeta^{(p-2)m}) \\ &= \zeta(c_1 + c_2\zeta + \cdots + c_{(p-1)m-1}\zeta^{(p-1)m-2}) - c_{(p-1)m}(-\zeta^{(p-1)m}) \\ &= \zeta(\lambda\zeta^{j-1} - c_{(p-1)m}\zeta^{(p-1)m-1}) + c_{(p-1)m}\zeta^{(p-1)m} \\ &= \lambda\zeta^j. \end{aligned}$$

Therefore $\vec{\zeta}$ is an eigenvector with eigenvalue λ. Since ζ can take on $(p-1)m$ different values, we have a full set of eigenvectors. The determinant is the product of the eigenvalues.

By the lemma, we have $\sum_{k=1}^{(p-1)m} b_k\zeta^{k-1} = 0$, for some primitive p^n-th root of unity ζ. Since $\phi(p^n) = (p-1)m$, the set $\{1, \zeta, \ldots, \zeta^{(p-1)m-1}\}$ is linearly independent over the rationals, and hence $b_1 = b_2 = \cdots = b_{(p-1)m} = 0$. Therefore the $(p-1)p^{n-1}$ units $\{\sigma^{k-1}(\theta) \mid 1 \le k \le (p-1)p^{n-1}\}$ are independent. This completes the proof of the theorem.

https://doi.org/10.4153/CJM-1995-034-4 Published online by Cambridge University Press

REMARK. So far we have $(p-1)p^{n-1}$ independent units, all of which are roots of $P_n(X;a)$. If the field $\mathbf{Q}(\theta)$ is Galois over the rationals, then the rank of the unit group is p^n-1 and we need only $p^{n-1}-1$ more units in order to get a set of units which is close to being a system of fundamental units. We can reach this goal by the method described in the next section. Unfortunately, the field $\mathbf{Q}(\theta)$ is not Galois in general. We know that $K(\theta)$ is the Galois closure of $\mathbf{Q}(\theta)$ so that the rank of the full unit group is $(p-1)p^{2n-1}-1$ and we need many more units to reach the same goal. Although the set of the cyclotomic units in $K=\mathbf{Q}(\zeta_{p^n})^+=\mathbf{Q}(\epsilon)$ will be part of them, it doesn't help us enough. In the next section we show how to obtain additional units from subfields of $K(\theta)$, though we still do not obtain a maximal set of independent units.

6. **A set of p^n-1 independent units.** Define a sequence (u_j) of real numbers as follows:

$$u_0=\theta \text{ and } u_j=\frac{R_1(u_{j-1})}{S_1(u_{j-1})} \quad \text{for } 1\leq j\leq n.$$

For convenience, we denote the field $\mathbf{Q}(u_j)$ by K_j for $1\leq j\leq n$. Obviously, we have the following lemma.

LEMMA 4. *The element u_{j-1} satisfies the polynomial*

$$P_1(X;pu_j), \quad \textit{for } 1\leq j\leq n.$$

LEMMA 5. *We have the following identities:*

$$u_{m+j}=\frac{R_j(u_m)}{S_j(u_m)}, \quad \textit{for } 0\leq m+j\leq n.$$

In particular, $u_n=\frac{a}{p^n}$, and therefore $K_n=\mathbf{Q}$.

PROOF. From (2) and (3), we have, for $1\leq j\leq n$

$$\frac{R_j(X)}{S_j(X)}=\frac{R_1\left(\frac{R_{j-1}(X)}{S_{j-1}(X)}\right)}{S_1\left(\frac{R_{j-1}(X)}{S_{j-1}(X)}\right)}. \tag{16}$$

For $j=0$ the lemma is trivial, since $R_0(X)/S_0(X)=X$. Assuming it is true for $j-1$, we easily find from (16) that it is true for j. Letting $j=n$ in the lemma, and using the fact that $P_n(\theta;a)=0$, we find that

$$u_n=\frac{R_n(\theta)}{S_n(\theta)}=\frac{a}{p^n}.$$

Therefore $K_n=\mathbf{Q}$. This completes the proof of the lemma.

THEOREM 4. *The element u_j satisfies the polynomial*

$$P_{n-j}(X;a/p^j), \quad \textit{for } 1\leq j\leq n.$$

Furthermore, the field K_j is a simplest p^{n-j}-tic field, if p^j divides a. In this case, the element u_j is also a unit in the ring $O_{K(\theta)}$ of the integers of $K(\theta)$.

https://doi.org/10.4153/CJM-1995-034-4 Published online by Cambridge University Press

PROOF. Lemma 5 tells us that the element u_j satisfies the polynomial

$$R_{n-j}(X) - \frac{a}{p^n} S_{n-j}(X),$$

which is in fact the polynomial

$$R_{n-j}(X) - \frac{a/p^j}{p^{n-j}} S_{n-j}(X) = P_{n-j}(X; \frac{a}{p^j}).$$

This completes the proof of the theorem.

REMARK. More generally, we see that u_m is a root of $P_j(X; p^j u_{m+j})$, so each intermediate extension K_m / K_{m+j} could be regarded as being "of simplest type."

From the previous theorem, we have for each $0 \leq j < n$ that the element u_j is a unit in the ring $O_{K(\theta)}$ if p^j divides a. Theorem 3 gives us $(p-1)p^{n-j-1}$ independent units, namely

$$\{\sigma^{p^j(k-1)}(u_j) \mid 1 \leq k \leq (p-1)^{n-j-1}\}$$

in the ring $O_{K(u_j)}$ of integers of the field $K(u_j)$. Putting all these units together, we have in total

$$(p-1)p^{n-1} + (p-1)p^{n-2} + \cdots + (p-1)p^2 + (p-1)p^1 + (p-1)p^0 = p^n - 1$$

units in the field $K(\theta)$. Are these units independent? The answer is yes, and we will prove this in the following theorem.

THEOREM 5. *Let $a \in \mathbf{Z}[\zeta_q + \zeta_q^{-1}]$ and let $p^n | a$. Then the $p^n - 1$ elements*

$$\{\sigma^{p^j(k-1)}(u_j) \mid 1 \leq k \leq (p-1)p^{n-j-1} \text{ and } 0 \leq j < n\}$$

are independent units in the ring $O_{K(\theta)}$ of algebraic integers of the field $K(\theta)$, where $K = \mathbf{Q}(\epsilon) = \mathbf{Q}(\zeta_{p^n})^+$.

PROOF. We will prove the theorem by induction on n. The result is trivial for $n = 1$. Assume the theorem is true for $n - 1$. If there is a relation, then we have rational integers $b_{k,j}$ such that

$$\eta = \prod_{k=1}^{(p-1)p^{n-1}} \left(\sigma^{k-1}(u_0)\right)^{b_{k,0}} = \prod_{j=1}^{n-1} \prod_{k=1}^{(p-1)p^{n-j-1}} \left(\sigma^{p^j(k-1)}(u_j)\right)^{b_{k,j}}. \tag{17}$$

The right side is in $K(u_1)$. Since the field $K(u_1)$ is fixed by the automorphisms

$$\{\sigma^{jp^{n-1}}; 0 \leq j < p\},$$

the element η is invariant under these automorphisms. Therefore, we have

$$\prod_{k=1}^{(p-1)p^{n-1}} \sigma^{jp^{n-1}} \left(\sigma^{k-1}(u_0)\right)^{b_{k,0}} = \eta,$$

https://doi.org/10.4153/CJM-1995-034-4 Published online by Cambridge University Press

and hence

$$\begin{aligned}\eta^p &= \prod_{j=0}^{p-1} \prod_{k=1}^{(p-1)p^{n-1}} \sigma^{jp^{n-1}} \left(\sigma^{k-1}(u_0)\right)^{b_{k,0}} \\ &= \prod_{k=1}^{(p-1)p^{n-1}} \sigma^{k-1} \left(\prod_{j=0}^{p-1} \sigma^{jp^{n-1}} (u_0) \right)^{b_{k,0}}.\end{aligned}$$

From Lemma 2, the above gives us $\eta^p = 1$ and so $\eta = 1$. We have

$$\prod_{k=1}^{(p-1)p^{n-1}} \left(\sigma^{k-1}(u_0)\right)^{b_{k,0}} = 1.$$

Theorem 3 tells us that $b_{k,0} = 0$, for all k. Now, the relation in (17) becomes

$$\prod_{j=1}^{n-1} \prod_{k=1}^{p^{n-j-1}} \left(\sigma^{p^j(k-1)}(u_j)\right)^{b_{k,j}} = 1.$$

From the induction hypothesis, the $p^{n-1} - 1$ units

$$\{\sigma^{p^j(k-1)}(u_j) \mid 1 \leq k \leq p^{n-j-1} \text{ and } 1 \leq j < n\}$$

are independent, and so

$$b_{k,j} = 0, \quad \text{for } 1 \leq k \leq p^{n-j-1} \text{ and } 1 \leq j < n.$$

Therefore all $b_{k,j}$ are 0, and this completes the proof of the theorem.

7. **Fields of composite degree.** To conclude our study of the real fields arising from matrices in $\mathrm{PGL}_2(\mathbf{R})$, we make a brief observation on the fields of composite degree but not a prime power. Real cyclic sextic fields are studied in [2] and [3] by M.-N. Gras. The corresponding matrix is $\begin{pmatrix} 1 & -1 \\ 1 & 2 \end{pmatrix}$. Fields of degree 10 and 12 have been studied by C. Levesque. We can obtain these fields by a slight variation of our methods used above.

In Section 2, our p was restricted to be a prime integer and n could be any positive integer. Now, we let $n = 1$ and consider an even integer $p > 2$. It is easy to see the matrix $M_p = \begin{pmatrix} 0 & -1 \\ 1 & \zeta_p + \zeta_p^{-1} \end{pmatrix}$ is similar to $D_p = \begin{pmatrix} \zeta_p & 0 \\ 0 & \zeta_p^{-1} \end{pmatrix}$, and hence is of order $p/2$ in $\mathrm{PGL}_2\big(\mathbf{Q}(\zeta_p)\big)$. Therefore, what we want is a square root M_{2p} of M_p so that M_{2p} has the correct order. One way to do this is as follows: We know that

$$M_p = A^{-1} D_p A, \quad \text{for } A = \begin{pmatrix} 1 & \zeta_p \\ 1 & \zeta_p^{-1} \end{pmatrix}.$$

Replacing the matrix D_p by the matrix $D_{2p} = \begin{pmatrix} \zeta_{2p} & 0 \\ 0 & \zeta_{2p}^{-1} \end{pmatrix}$ gives us a square root of M_p. Let $M_{2p} = A^{-1} D_{2p} A$. Then

$$M_{2p} = \frac{1}{\zeta_{2p} + \zeta_{2p}^{-1}} \begin{pmatrix} 1 & -1 \\ 1 & 1 + \zeta_p + \zeta_p^{-1} \end{pmatrix}.$$

This turns out to be a good choice. Firstly, when $p = 6$ the matrix M_{2p} is the matrix of M.-N. Gras. Secondly, as we show below, a result similar to Theorem 1 remains true.

As before, we consider the polynomial $(X+\zeta_p)^p$ and write it in the form

$$(X+\zeta_p)^p = R(X) + \zeta_p S(X),$$

where $R(X)$ and $S(X)$ are polynomials over the ring $O = \mathbf{Z}[\zeta_p + \zeta_p^{-1}]$. The polynomials in which we are interested are

$$P(X;a) = R(X) - \frac{a}{p}S(X), \quad \text{where } a \in O.$$

LEMMA 6. *For even $p > 2$, the number $(1+\zeta_p)^{p/2}$ is purely imaginary, and $(1+\zeta_p)^p$ is real and negative. Moreover, $(1+\zeta_p)^p = R(1) < 0$.*

PROOF. We have

$$(1+\zeta_p)^{p/2} = \zeta_{2p}^{p/2}(\zeta_{2p}^{-1} + \zeta_{2p})^{p/2}.$$

Since $\zeta_{2p}^{p/2} = i$ and $\zeta_{2p}^{-1} + \zeta_{2p}$ is real, the first and second statements hold. Since $(1+\zeta_p)^p = R(1) + \zeta_p S(1)$, we must have $S(1) = 0$ and $R(1) = (1+\zeta_p)^p$.

THEOREM 6. *For $a \in \mathbf{Z}[\zeta_p + \zeta_p^{-1}]$, the polynomial $P(X;a)$ has p distinct real roots. Moreover, the matrix*

$$M = \begin{pmatrix} 1 & -1 \\ 1 & 1+\zeta_p+\zeta_p^{-1} \end{pmatrix}$$

has order p in $\mathrm{PGL}_2(\mathbf{R})$, and the transformation

$$\theta \longmapsto \frac{\epsilon\theta - 1}{\theta + \epsilon - (\zeta_p + \zeta_p^{-1})}$$

permutes cyclically the roots of $P(X;a)$.

PROOF. The polynomial $P(X;a)$ has at least one real root, since Lemma 6 gives us $P(1;a) = R(1) < 0$ and it is easy to see $P(0;a) = R(0) = 1 > 0$. Suppose θ is any root of $P(X;a)$ and let $\alpha = \theta + \zeta_p$, $\beta = M\theta + \zeta_p$. Then

$$\beta = \alpha \cdot \frac{1+\zeta_p}{\theta + 1 + \zeta_p + \zeta_p^{-1}}.$$

Lemma 6 implies that the number $(1+\zeta_p)^p$ is real and so is the number

$$c = \Big(\frac{1+\zeta_p}{\theta + 1 + \zeta_p + \zeta_p^{-1}}\Big)^p.$$

As in the proof of Theorem 1, we have

$$R(M\theta) = cR(\theta) \quad \text{and} \quad S(M\theta) = cS(\theta).$$

Therefore, the transformation M permutes the roots.

https://doi.org/10.4153/CJM-1995-034-4 Published online by Cambridge University Press

Since M has two distinct eigenvalues $1+\zeta_p$ and $1+\zeta_p^{-1}$, it must be similar to the diagonal matrix

$$D = \begin{pmatrix} 1+\zeta_p & 0 \\ 0 & 1+\zeta_p^{-1} \end{pmatrix}.$$

Because the matrices M and D have the same order, it suffices to show that D is of order p. Now for any z

$$Dz = \frac{1+\zeta_p}{1+\zeta_p^{-1}} z = \zeta_p z,$$

and so D is of order p and this completes the proof as in Theorem 1.

References

1. J. E. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge University Press, New York, 1992.
2. Marie-Nicole Gras, *Special units in real cyclic sextic fields*, Math. Comp. **48**(1987), 179–182.
3. ———, *Familles d'unités dans les extensions cycliques réelles de degré* 6 *de* **Q**, Publ. Math. Besançon, 1984/1985–1985/86.
4. O. Hemer, *Notes on the Diophantine equation* $y^2 - k = x^3$, Ark. Mat. **3**(1954), 67–77.
5. Serge Lang, *Algebra*, Addison-Wesley, Reading, Massachusetts, 1965.
6. D. Shanks, *The simplest cubic fields*, Math. Comp. **28**(1974), 1137–1152.
7. Y.-Y. Shen and L. C. Washington, *A family of real* 2^n*-tic fields*, to appear.

Department of Mathematics
Tunghai University
Taichung, Taiwan 40704
R.O.C.

Department of Mathematics
University of Maryland
College Park, Maryland 20742
U.S.A.

https://doi.org/10.4153/CJM-1995-034-4 Published online by Cambridge University Press