ACTA ARITHMETICA
LI (1988)

A generalization of Schinzel's theorem on radical extensions of fields and an application

by

WILLIAM YSLAS VÉLEZ (Tucson, Ariz.)

The theorem due to Schinzel to which the title alludes characterizes when $F(\sqrt[m]{a})$, $F(\sqrt[m]{b})$ are F-isomorphic, where x^m-a, x^m-b are irreducible over F and $\operatorname{char} F \nmid m$.

In order to state this characterization we need to develop some notation. First of all we shall make the firm convention throughout this paper that all extensions are separable, this will obviate the need for stating that $\operatorname{char} F \nmid m$.

By ζ_m we shall mean a primitive mth root of unity and

$$\eta_{2^t} = \zeta_{2^t} + \zeta_{2^t}^{-1}.$$

Given F, let $N = \infty$ if $\eta_{2^t} \in F$ for all t, otherwise let $N = \max\{t\colon \eta_{2^t} \in F\}$. Observe that if $\eta_{2^t} \in F$ then $\eta_{2^k} \in F$ for all $k \leqslant t$ since $\eta_{2^t}^2 = 2 + \eta_{2^{t-1}}$.

Let F^* denote the multiplicative group of non-zero elements and F^k the multiplicative group of kth powers of F^*. We shall write $a = b(F^k)$ to mean that $ab^{-1} \in F^k$. We can now state Schinzel's theorem.

THEOREM A. *Let x^m-a, x^m-b be irreducible over F. Then $F(\sqrt[m]{a})$, $F(\sqrt[m]{b})$ are F-isomorphic iff either*

(i) $a = b^i(F^m)$, *for some i prime to m, or*

(ii) $N < \infty$, $2^{N+1} \mid m$, $-a$, $-b \in F^2$ *and* $a = b^i(2+\eta_{2^N})^{m/2}(F^m)$, *for some i prime to m.*

In his 1975 paper [8], Schinzel characterized when

$$[F(\alpha_1, \ldots, \alpha_k)\colon F] = n_1 \ldots n_k, \qquad \text{where } \alpha_i^{n_i} \in F^*.$$

As a corollary to these studies Schinzel obtained the above result. In a 1982 paper [1], Acosta de Orozco and Vélez studied the lattice of subfields of $F(\sqrt[m]{a})$ over F, where x^m-a is irreducible over F, and obtained A as a corollary.

Recently [10], by using several elementary results dealing with radical

extensions we have been able to give a more direct proof of Schinzel's theorem. In this paper we shall generalize Schinzel's theorem in the following fashion. We shall characterize when the two algebras

$$F[x]/(x^m-a), \qquad F[x]/(x^m-b)$$

are F-isomorphic, that is, we shall generalize Schinzel's theorem by deleting the condition on irreducibility.

The generalization, besides being of interest in its own right, has some immediate applications. Gerst [4], Jacobson and Vélez [6] have shown that $Q(\sqrt[m]{a})$, $Q(\sqrt[m]{b})$ are arithmetically equivalent iff either (i) $a = b^i(Q^m)$, $(i, m) = 1$ or (ii) $8|m$ and $a = b^i 2^{m/2}(Q^m)$, $(i, m) = 1$, where of course x^m-a, x^m-b are irreducible over Q. Jacobson and Vélez then went on to determine when $Q(\sqrt[m]{a})$, $Q(\sqrt[m]{b})$ had isomorphic adèle rings. By using a result of Iwasawa (Lemma 7 of [5]), $Q(\sqrt[m]{a})$, $Q(\sqrt[m]{b})$ have isomorphic adèle rings iff

$$Q(\sqrt[m]{a}) \otimes_Q Q_p \cong Q(\sqrt[m]{b}) \otimes_Q Q_p,$$

for all primes p.

However, Jacobson and Vélez showed (Theorem 2.2 of [6]) that the above tensor product holds for all odd primes p given that $Q(\sqrt[m]{a})$, $Q(\sqrt[m]{b})$ are arithmetically equivalent.

Thus the two fields in question have isomorphic adèle rings iff

$$Q(\sqrt[m]{a}) \otimes_Q Q_2 \cong Q(\sqrt[m]{b}) \otimes_Q Q_2.$$

However this isomorphism is equivalent to determining when the two algebras

$$Q_2[x]/(x^m-a), \qquad Q_2[x]/(x^m-b)$$

are Q_2-isomorphic. This was accomplished in [6] but the analysis was very detailed and used quite a bit of arithmetic information. As the reader can now see, the generalization of Schinzel's theorem can now be applied to answer this question.

A word now about the organization of this paper. In Section 1 we shall collect together the results that we shall need from the theory of radical extensions. In Section 2 we shall prove the generalization of Schinzel's theorem and in Section 3 we shall apply these results to the study of adèle rings.

Finally a word of thanks. It was Professor Peter Roquette who encouraged me to find a more direct proof of Schinzel's theorem (this appears in [10]) and he also mentioned that a generalization of Schinzel's theorem was preferable and more natural to the very detailed analysis that appeared in [6].

1. Statement of results on radical extensions. Let K/F be an algebraic extension. If $\alpha \in K$, $o_F(\alpha) = o(\alpha)$ shall denote the order of αF^* in the quotient group K^*/F^*. By $\deg_F(\alpha) = \deg(\alpha)$ we shall mean the degree of the field extension $F(\alpha)/F$, $T(K/F)$ shall denote the torsion subgroup of K^*/F^*, and $T_p(K^*/F^*)$ the elements of $T(K/F)$ of order a power of p.

PROPOSITION 1.1. *Let $o(\alpha) = m = 2^e n$, n odd, $e > 0$ and $a = \alpha^m$.*

(i) *$\zeta_4 \in F(\alpha)\setminus F$ iff $-a \in F^2$ iff $F(\zeta_4) = F(\alpha^{m/2})$. Further, if $\deg(\alpha^n) < 2^e$ then $\zeta_4 \in F(\alpha)\setminus F$.*

(ii) *If $p^s || m$ ($p^s | m$, $p^{s+1} \nmid m$) and $\zeta_{2p} \notin F(\alpha)\setminus F$ then $p^s = \deg(\alpha^{m/p^s})$.*

(iii) *If $\zeta_p \notin F$ and there exists an element $\delta \in F(\alpha)$ with $o(\delta) = p^t$ and $p^t \nmid o(\alpha)$ then $\zeta_{p^t} \in F(\alpha)$.*

Proof. For x^m-a irreducible, the first part of (i) is part (a) of Theorem 1.8 of [3], however the reducible case is similiar. The second part of (i) is Lemma 2.2 of [9]. Part (ii) is a special case of Lemma 1.5 of [3]. For part (iii) if x^m-a is irreducible, then this result can be derived from Theorem A of [3], while for the reducible part we would use Theorem 5.1 of [2].

PROPOSITION 1.2. *Let $\zeta_4 \notin F$ and $K = F(\zeta_4)$.*

(i) *If $N = \infty$ then $T_2(K/F) = \langle \zeta_{2^n} F^* : \text{for all } n \rangle \cong \boldsymbol{Z}_{2^\infty}$.*

(ii) *If $N < \infty$ then $T_2(K/F) = \langle (1+\zeta_{2^N}) F^* \rangle \cong \boldsymbol{Z}_{2^N}$.*

(iii) *If p is odd then $T_p(K/F) = \langle \zeta_{p^s} F^* : \zeta_{p^s} \in F(\zeta_4) \rangle$.*

Proof. (i) and (ii) are a special case of Theorem A of [3], however a short proof can also be found in Lemma 1 of [7]. Part (iii) is a special case of Corollary 1.4 of [3].

Notation: Let $o(\alpha) = m = 2^e n$, n odd. Then set $\alpha_E = \alpha^n$ and $\alpha_O = \alpha^{2^e}$, where E, O denote even and odd respectively. Since n and 2^e are relatively prime there are integers x, y for which $nx + 2^e y = 1$ and $\alpha = \alpha_E^x \alpha_O^y$.

2. Proof of the main theorem. It will be convenient to first prove a slight generalization of A (Theorem 2.2). However, we will begin with the following lemma.

LEMMA 2.1. *Let x^m-a, x^m-b be irreducible over F and $\zeta_4 \in F$. Then $F(\sqrt[m]{a})$, $F(\sqrt[m]{b})$ are F-isomorphic iff $a = b^i(F^m)$, $(i, m) = 1$.*

Proof. From A we have that the two fields are F-isomorphic iff either (i) or (ii) hold. Now (ii) states that $N < \infty$, $2^{N+1} | m$, $-a$, $-b \in F^2$ and

$$a = b^i(2+\eta_{2^N})^{m/2}(F^m), \qquad (i, m) = 1.$$

Since $\zeta_4 \in F$, $-1 \in F^2$, and $-a \in F^2$ implies $a \in F^2$, contradicting the irreducibility of x^m-a if a is even. Thus (ii) cannot hold, so therefore (i) holds and we have that $a = b^i(F^m)$, $(i, m) = 1$.

THEOREM 2.2. *Suppose that* $a, b \notin F^p$ *for all* p *dividing* m *and let* $m = 2^e n$, n *odd.*

Then the following statements are equivalent:

(a) *There are roots* $\alpha^m = a$, $\beta^m = b$ *such that* $F(\alpha)$, $F(\beta)$ *are* F*-isomorphic.*

(b) *Either* (i) $a = b^i (F^m)$, $(i, m) = 1$ *or* (ii) $N < \infty$, $2^{N+1} | m$, $-a$, $-b \in F^2$, *and* $a = b^i (2+\eta_{2^N})^{m/2} (F^m)$.

(c) *The algebras* $F[x]/(x^m - a)$, $F[x]/(x^m - b)$ *are* F*-isomorphic.*

Proof. It is obvious that (c) implies (a).

Suppose (a) holds and further, without loss of generality, we may assume that $F(\alpha) = F(\beta)$. Let p be odd, then since $a \notin F^p$ we have that $x^{p^s} - a$ is irreducible for all s. From this it follows that

$$n = \deg \alpha_O = o(\alpha_O) = \deg \beta_O = o(\beta_O).$$

Thus $\deg \alpha = \deg \beta = 2^f n$, $f \leqslant e$. If $f = e$ then $x^m - a$, $x^m - b$ are irreducible and we may apply A. Thus we may assume that $f < e$. From 1.1(i) we then have that $\zeta_4 \in F(\alpha) \setminus F$, $F(\zeta_4) = F(\alpha^{m/2}) = F(\beta^{m/2})$ and $-a$, $-b \in F^2$. Clearly $\deg \alpha = \deg(\alpha_E) \cdot \deg(\alpha_O)$. Further, if $o_{F(\zeta_4)}(\alpha_E) = 2^k$, then by 1.1(ii), $\deg_{F(\zeta_4)}(\alpha_E) = 2^k$, thus $\deg \alpha = 2^{k+1} = 2^f$, and $k = f-1$. So $o_{F(\zeta_4)}(\alpha_E) = o_{F(\zeta_4)}(\beta_E) = 2^{f-1}$.

From the above we see that both α, β satisfy irreducible binomials of degree $2^{f-1} n$ over $F(\zeta_4)$. Thus by 2.1 we have that

$$\alpha^{2^{f-1} n} = (\beta^{2^{f-1} n})^i \big(F(\zeta_4)^{2^{f-1} n}\big), \quad (i, 2^{f-1} n) = 1.$$

So we have that

$$\alpha^{2^{f-1} n} = (\beta^{2^{f-1} n})^i \gamma^{2^{f-1} n}, \quad \gamma \in F(\zeta_4).$$

Further $\gamma^m \in F$ since α^m, $\beta^m \in F$. By 1.2 we have that $\gamma = \gamma_E \zeta_k c$, where $\gamma_E F^* \in T_2(F(\zeta_4)/F)$, $k | n$ and $c \in F$. Thus we have that

$$\alpha^{2^{f-1} n} = (\beta^{2^{f-1} n})^i (\gamma_E c)^{2^{f-1} n}, \quad (i, 2^{f-1} n) = 1, \ c \in F,$$

and thus

$$a = \alpha^m = b^i \gamma_E^m c^m, \quad (i, 2^{f-1} n) = 1.$$

Further, $\gamma_E^{2^e} \in F$, so $\gamma_E^m \in F^n$, thus $a = b^i c_1^n$, for some $c_1 \in F$, so $\alpha_O = \beta_O^i c_1 \zeta_n^k$, $(i, n) = 1$ for some k. (Recall the notation of Section 1.)

If $f = 1$, then $F(\alpha_E) = F(\beta_E) = F(\zeta_4)$. However the elements of order 2^e in $T_2(F(\zeta_4)/F)$ form a cyclic group, thus $\alpha_E = \beta_E^j c_2$, $(j, 2) = 1$. Then we have that, with $nx + 2^e y = 1$,

$$\alpha = \alpha_E^x \alpha_O^y = \beta_E^{jx} \beta_O^{iy} c_1 c_2 \zeta_n^k = \beta^{jnx + i2^e y} c_1 c_2 \zeta_n^k \quad \text{and} \quad (jnx + i2^e y, 2^e n) = 1$$

and by raising the above to the mth power we have condition (b) of the theorem. Thus we may assume in the following that $f > 1$, so $(i, m) = 1$

If $\gamma_E^{2^e} = -c_1^2$, then $a = -b^i c_1^{2n} c^m$. However, $-b \in F^2$ (as noted in the first paragraph) and i odd yields that $a \in F^2$, a contradiction (recall that $a \notin F^p$ for all $p | m$). Thus $-\gamma_E^{2^e} \notin F^2$.

If $N = \infty$ then $\gamma_E = \zeta_{2^{e+1}}^j c_2$ and $\gamma_E^{2^e} = (-1)^j c_2^{2^e}$. Thus j must be even and $a = b^i (c_2 c)^m$, $(i, m) = 1$.

If $N < \infty$, then $\gamma_E = (1+\zeta_{2^N})^j c_2$ and $\gamma_E^{2^e} = \big(\zeta_{2^N}(2+\eta_{2^N})\big)^{j 2^{e-1}} c_2^{2^e}$. Thus $\zeta_{2^N}^{j 2^{e-1}} \in F$ and in fact it must be 1 since $-\gamma_E^{2^e} \notin F^2$. Thus, if $e \leqslant N$, then j must be even, so $j = 2j'$ and

$$a = b^i \big(\zeta_{2^N}(2+\eta_{2^N})\big)^{2^e n j'} (c_2 c)^m = b^i \big((2+\eta_{2^N})^{j'} c_2 c\big)^m.$$

If $e > N$ then

$$\zeta_{2^N}^{2^e} = 1 \quad \text{and} \quad a = b^i (2+\eta_{2^N})^{jm/2} c^m, \quad (i, m) = 1.$$

It is then easy to check that if j is even then we have condition (i) and if j is odd we have condition (ii). Thus (a) implies (b).

Finally we want to prove that (b) implies (c).

If $a = b^i c^m$, $(i, m) = 1$, $c \in F$ then it is obvious that the two algebras $F[x]/(x^m - a)$, $F[x]/(x^m - b)$ are F-isomorphic. Thus suppose that $N < \infty$, $2^{N+1} | m$, $-a$, $-b \in F^2$ and $a = b^i (2+\eta_{2^N})^{m/2} c^m$. Let β denote a fixed root of $x^m - b$. Since $-b \in F^2$ and $b \notin F^2$ we have that $F(\zeta_4) = F(\zeta_{2^N}) = F(\beta^{m/2})$, thus $\zeta_{2^N} \in F(\beta)$. Now $(1+\zeta_{2^N})^2 = \zeta_{2^N}(2+\eta_{2^N})$, so $\zeta_{2^{N+1}} \sqrt{2+\eta_{2^N}} \in F(\beta)$. Since $2^{N+1} | m$, we have that $\zeta_{2^{N+1}} = \zeta_m^j$, for some j. Thus

$$\beta^i \zeta_{2^{N+1}} \sqrt{2+\eta_{2^N}}\, c = \beta^i \sqrt{2+\eta_{2^N}}\, \zeta_m^j c \in F(\beta).$$

However,

$$(\beta^i \sqrt{2+\eta_{2^N}}\, \zeta_m^j c)^m = b^i (2+\eta_{2^N})^{m/2} c^m = a$$

is a root of $x^m - a$, so let $\alpha = \beta^i \zeta_{2^{N+1}} \sqrt{2+\eta_{2^N}} \in F(\beta)$.

Since $-a$ is also in F^2 we have that $\zeta_{2^{N+1}} \sqrt{2+\eta_{2^N}} \in F(\alpha)$, thus $\beta^i \in F(\alpha)$ and since $(i, m) = 1$, this implies that $F(\alpha) = F(\beta)$. So we have two roots $\alpha^m = a$, $\beta^m = b$ with $F(\alpha) = F(\beta)$ and

$$\alpha = \beta^i \zeta_m^j \sqrt{2+\eta_{2^N}}\, c.$$

If we multiply this equation by ζ_m^k, and let k run from 1 to m we have that

$$F(\zeta_m^k \alpha) = F(\zeta_m^k \beta^i \zeta_{2^{N+1}} \sqrt{2+\eta_{2^N}}) = F(\zeta_m^k \beta^i).$$

This last equality holds for the following reason. Recall that

$$\zeta_{2^{N+1}}\sqrt{2+\eta_{2^N}} = \pm(1+\zeta_{2^N}), \quad F\left((\beta^i\zeta_m^k)^{m/2}\right) = F(\beta^{m/2}) = F(\zeta_4) = F(\zeta_{2^N}).$$

Thus

$$\zeta_{2^{N+1}}\sqrt{2+\eta_{2^N}} \in F(\beta^i\zeta_m^k), \quad \text{so} \quad F(\zeta_m^k\beta^i\zeta_{2^{N+1}}\sqrt{2+\eta_{2^N}}) \subset F(\beta^i\zeta_m^k).$$

However,

$$F(\zeta_m^k\beta^i\zeta_{2^{N+1}}\sqrt{2+\eta_{2^N}})^{m/2} = F\left((\beta^i)^{m/2}(1+\zeta_{2^N})^{m/2}\right) = F(\beta^{m/2})$$

since we are assuming that $2^{N+1}|m$ thus $2^N|m/2$ and $(1+\zeta_{2^N})^{2^N}\in F$, so

$$\zeta_{2^{N+1}}\sqrt{2+\eta_{2^N}} \in F(\zeta_m^k\beta^i\zeta_{2^{N+1}}\sqrt{2+\eta_{2^N}}),$$

thus $\zeta_m^k\beta^i$ is also in this field, so equality holds.

Let $z\in\mathbf{Z}$ be such that $zi\equiv 1 \pmod m$ (recall that $(i, m) = 1$), then

$$F(\zeta_m^k\alpha) = F(\zeta_m^k\beta^i) = F(\zeta_m^{kz}\beta),$$

so the mapping $\zeta_m^k\alpha$ into $\zeta_m^{kz}\beta$ gives a bijection between the roots of x^m-a and x^m-b such that corresponding fields are equal, thus $F[x]/(x^m-a)$, $F[x]/(x^m-b)$ are F-isomorphic.

Before proving the main theorem we have to do some preliminary work and set up some notation.

Given x^m-a with distinct roots $\alpha_1, \ldots, \alpha_m$, let $\alpha=\alpha_1$ be such that $o(\alpha)\leqslant o(\alpha_i)$ for $i=1, \ldots, m$. Let $o(\alpha)=r$, $\alpha^r=a'$ and $m=rm'$. Then $\alpha^m=a=(\alpha^r)^{m'}=(a')^{m'}$. Thus $a\in F^{m'}$, further it is obvious that $m'=\max\{t\colon t|m \text{ and } a\in F^t\}$.

LEMMA 2.3. *Let $r=2^e n$, n odd. Then x^n-a' is irreducible over F. Further, if $2^{e+1}|m$ then $-a'\notin F^2$ and x^r-a' is irreducible over F.*

Proof. Since n is odd, x^n-a' is irreducible over F iff $a'\notin F^p$, for all p dividing n. So let $p|n$ and set $\gamma=\alpha^{r/p}$. Then γ is a root of the binomial x^p-a' and $\gamma\notin F$ since $o(\gamma)=p$. If $a'=c^p$ then $\gamma=c\zeta_p$. If $p^s\|n$ then from $\gamma=c\zeta_p$ we obtain that $\alpha=\zeta_{p^s}\sqrt[p^s]{c}$. However, since $p^s|m$ we have that $\zeta_{p^s}^{-1}\alpha=\sqrt[p^s]{c}$ is also a root of x^m-a, yet $o(\sqrt[p^s]{c})<r$, contradicting the minimality of the order of α. Thus $a'\notin F^p$ and x^n-a' is irreducible.

Suppose that $2^{e+1}|m$ and let $\alpha_E=\alpha^n$. If $-a'\in F^2$ then $\sqrt{-a}\in F$. Since $2^{e+1}|m$, we have that $\alpha\zeta_{2^{e+1}}$ is also a root of x^m-a. However

$$(\alpha\zeta_{2^{e+1}})^{r/2} = \sqrt{a'}\,\zeta_4 = \sqrt{-a'}\in F, \quad \text{so} \quad o(\alpha\zeta_{2^{e+1}})\leqslant r/2,$$

contradicting the minimality of the order of α.

Thus we can conclude that $-a'\notin F^2$.

However, if $\deg(\alpha_E)<2^e$ then by 1.1(i) we have that $-a'\in F^2$, a contradiction. Thus $\deg(\alpha_E)=2^e$ so x^r-a' is irreducible over F.

LEMMA 2.4. *Let G be a torsion abelian group, H a finite subgroup of G and $g\in G$. Let $b\in Hg$ be such that $o(b)\leqslant o(hg)$ for all $h\in H$. Then $o(b)|o(hg)$, for all $h\in H$.*

Proof. Let $G_1=\langle H, g\rangle$. If G_1 is a p-group then the assertion is obvious. Thus let $G_1=\prod_{i=1}^{k} G_{p_i}$, $(p_i, p_j)=1$ if $i\neq j$ and each G_{p_i} is a p_i-group, p_i prime. Let $H=\prod_{i=1}^{k} H_{p_i}$ and $g=(g_1, \ldots, g_k)$. Then it is obvious that

$$Hg = H_{p_1}g_1\times\ldots\times H_{p_k}g_k.$$

Further, if $b_i\in H_{p_i}g_i$ is chosen to have minimal order then in that case it is clear that $\prod_{i=1}^{k} o(b_i)|o(hg)$, for all $h\in H$. However, $b=(b_1, \ldots, b_k)\in Hg$ so b has minimal order in Hg and $o(b)|o(hg)$ for all $h\in H$.

THEOREM 2.5. *With the preceding notation in force we have that*

$$o(\alpha)|o(\alpha_i) \quad \text{and} \quad \deg(\alpha)|\deg(\alpha_i), \quad i=1, \ldots, m.$$

Proof. To prove the first assertion let

$$G = T\left(F(\alpha, \zeta_m)^*/F^*\right), \quad H=\langle\zeta_m F^*\rangle, \quad g=\langle\alpha F^*\rangle$$

and apply 2.4.

Let $p^s\|n$, p odd. Since x^n-a' is irreducible over F, $p^s\|\deg(\alpha)$. We wish to show that $p^s|\deg(\alpha_i)$, for all i. By the first part of the theorem p^s also divides $o(\alpha_i)$, for all i. If $\zeta_p\in F$ then this implies by 1.1(ii) that $p^s|\deg(\alpha_i)$. So let us assume that $\zeta_p\notin F$.

Let us write α_i in the form $\zeta_h\zeta_{p^t}(\alpha')^c(\alpha'')^d$, where $(h, p)=1$, $hp^t|m$, $\alpha'=\alpha^{r/p^s}$, $\alpha''=\alpha^{p^s}$ and $c(r/p^s)+dp^s=1$. Thus $F(\alpha_i)=F(\alpha''\zeta_h, \alpha'\zeta_{p^t})$.

If $t\leqslant s$ then $\alpha'\zeta_{p^t}$ is a root of $x^{p^s}-a'$, which is irreducible, thus $p^s|\deg(\alpha_i)$. So we may assume that $t>s$. Then it is clear that $\zeta_p\in F(\alpha'\zeta_{p^t})$ since $(\alpha')^{p^{t-1}}\in F$. Let $p^j=o_{F(\zeta_p)}(\alpha'\zeta_{p^t})$. If $j<s$ this implies that $(\alpha'\zeta_{p^t})^{p^j}=(\alpha')^{p^j}\zeta_{p^{t-j}}\in F(\zeta_p)$, so $(\alpha')^{p^j}\in F(\zeta_{p^{t-j}})$, which in turn yields, since $j<s$, that $\sqrt[p]{a'}\in F(\zeta_{p^{t-j}})$. However, $F(\zeta_{p^{t-j}})/F$ is abelian, so $F(\sqrt[p]{a'})/F$ is also abelian. Since $\zeta_p\notin F$ this is a contradiction. Thus we have that $j\geqslant s$ and thus $p^j=\deg_{F(\zeta_p)}(\alpha'\zeta_{p^t})$ by 1.1 (ii), so $p^s|\deg(\alpha_i)$.

Since p was an arbitrary prime divisor of n, this implies that $n|\deg(\alpha_i)$.

Now let us consider the case of 2. Let us write α_i in the form

$$\alpha_i = \zeta_h\zeta_{2^t}\alpha_E^x\alpha_O^y, \quad \text{where } (h, 2)=1,\ h2^t|m \text{ and } nx+2^e y=1.$$

Thus

$$F(\alpha_i) = F(\alpha_O \zeta_h, \alpha_E \zeta_{2^t}).$$

If $t \leqslant e$ then $\alpha_E \zeta_{2^t}$ is a root of $x^{2^e} - a'$, so $\deg(\alpha_E) | \deg(\alpha_i)$.

If $t > e$ then by 2.3, $-a' \notin F^2$ and $2^e = \deg(\alpha_E)$. Thus we only have to prove that $2^e | \deg(\alpha_E \zeta_{2^t})$.

From the first part of this theorem we have that $2^e | o(\alpha_i)$. If $\zeta_4 \notin F(\alpha) \setminus F$ then by 1.1(ii), $2^e | \deg(\alpha_i)$. Thus we may assume that $\zeta_4 \in F(\zeta_{2^t} \alpha_E) \setminus F$.

If $t = e+1$ then $(\alpha_E \zeta_{2^{e+1}})^{2^{e-1}} = \sqrt{-a'} \notin F$ and $(\alpha_E \zeta_{2^{e+1}})^{2^e} = -a'$, so $o(\alpha_E \zeta_{2^{e+1}}) = 2^e$. However, $\zeta_4 \in F(\alpha_E \zeta_{2^{e+1}}) \setminus F$ iff $-(-a') \in F^2$, which is a contradiction. So $t > e+1$. Since $t - e \geqslant 2$, we have that $F(\alpha_E \zeta_{2^t})$ contains $F(a' \zeta_{2^{t-e}})$, which in turn contains $F(\zeta_4)$.

Let $2^s = o_{F(\zeta_4)}(\alpha_E \zeta_{2^t})$. Then by 1.1(ii) we have that $2^s = \deg_{F(\zeta_4)}(\alpha_E \zeta_{2^t})$, so $2^{s+1} = \deg(\alpha_E \zeta_{2^t})$.

If $s+1 \geqslant e$ then $2^e | \deg(\alpha_i)$. Thus we may assume that $s+1 < e$. Since $(\alpha_E \zeta_{2^t})^{2^s} \in F(\zeta_4)$, we have that $(\alpha_E)^{2^s} \in F(\zeta_4, \zeta_{2^{t-s}})$. However, $s \leqslant e-2$, so we have that $\sqrt[4]{a'} \in F(\zeta_4, \zeta_{2^{t-s}})$, thus $F(\sqrt[4]{a'})/F$ is an abelian extension, so $F(\zeta_4) = F(\sqrt{a'})$ by 1.1(i), thus $-a' \in F^2$, but this is a contradiction (recall that $2^{e+1} | m$ implies that $-a' \notin F^2$).

We can now prove the main theorem.

THEOREM 2.6. *Let $m' = \max\{k: k|m \text{ and } a \in F^k\}$, $m'' = \max\{k: k|m \text{ and } b \in F^k\}$, $m = rm'$. Then $F[x]/(x^m - a)$, $F[x]/(x^m - b)$ are F-isomorphic iff $m' = m''$ and there exists $a', b' \in F$ with $(a')^{m'} = a$, $(b')^{m'} = b$ and $F[x]/(x^r - a')$, $F[x]/(x^r - b')$ are F-isomorphic.*

Proof. Let α, β denote roots of $x^m - a$, $x^m - b$ respectively with minimal order. Then by 2.5 $\deg(\alpha) = \min\{\deg(\alpha_i),\ i = 1, \ldots, m\}$ and $\deg(\beta) = \min\{\deg(\beta_i),\ i = 1, \ldots, m\}$.

Suppose that $F[x]/(x^m - a)$, $F[x]/(x^m - b)$ are F-isomorphic. Then clearly $\deg(\alpha) = \deg(\beta) =$ a power of 2 times n. So with $o(\alpha) = 2^e n$ we have that $o(\beta) = 2^f n$.

Since the two algebras are F-isomorphic there exists a root β_i of $x^m - b$ with $F(\alpha)$, $F(\beta_i)$ F-isomorphic. Without loss of generality we may assume that $F(\alpha) = F(\beta_i)$.

Thus $\deg(\alpha) = \deg(\beta_i)$. Let $o(\beta_i) = 2^{f'} q$, q odd, where $f \leqslant f'$ and $n | q$, by 2.5.

Let us first consider the case where $2^{e+1} | m$. Then by 2.3 we have that $\deg(\alpha) = 2^e n$ and $\zeta_4 \notin F(\alpha) \setminus F$, so $-a' \notin F^2$, where $\alpha^{2^e n} = a'$. This implies that $e \leqslant f$.

Since $\zeta_4 \notin F(\beta_i) \setminus F$ (recall that $F(\alpha) = F(\beta_i)$), we have that $2^{f'} = \deg(\beta_i^q)$. So $2^{f'} | \deg(\beta)$ and $\deg(\beta) | 2^f n$, so $f' \leqslant f$. Thus $f = f'$ and from this we see that $2^f n = \deg(\beta) = \deg(\alpha) = 2^e n$, so $f = e$.

So we have shown that if $2^{e+1} | m$ then $2^e \| o(\beta_i)$.

Next let us assume that $2^{e+1} \nmid m$. Since the roles of α and β are interchangeable we may also assume that $2^{f+1} \nmid m$. So $2^e \| m$, $2^f \| m$ and $e = f$. Further, since $o(\beta) = 2^e n | o(\beta_i)$ for all i, we have that $2^e \| o(\beta_i)$.

Thus in all cases we have that $2^e \| o(\beta_i)$.

Let us write β_i in the form

$$\beta_i = \zeta_k \beta_E^x \zeta_h \zeta_{h'} \beta_O^y$$

where k is a power of 2, hh' is odd and divides m, $(h, h') = 1$ and if $p | h'$ then $\zeta_p \in F$. From what we have just shown we have that $o(\zeta_k \beta_E^y) = 2^e$.

Let $p^s \| n$ and $p^t \| o(\beta_i)$, where $s \leqslant t$ by 2.5. If $\zeta_p \in F$ then by 1.1(ii), $p^t | \deg(\beta_i)$, and $p^s \| \deg(\beta_i)$, so $s = t$. From this we see that $h' | n$.

Let us now consider the case where $\zeta_p \notin F$ and $s < t$. Since $p^s \| (\beta_O^y)$, we see that $p^t \| h$. At this point we have to use a little muscle. We have that $F(\alpha) = F(\beta_i)$, where $p^s \| o(\alpha)$ and there is an element in $F(\alpha)$ whose order is p^t, $s < t$. By 1.1(iii) we have that $\zeta_{p^t} \in F(\alpha) = F(\beta_i)$.

Let us write $\zeta_h = \zeta_{h_1} \zeta_{h_2}$, where $(h_1, h_2) = 1$ and $h_1 | n$. Thus we see that $p^t \| h_2$, and by the preceding paragraph, we have that $\zeta_{h_2} \in F(\alpha)$. Thus $\zeta_{h_1} \zeta_{h'} \beta_O^y \in F(\alpha)$ and $h_1 h' | n$. Further $o(\zeta_k \beta_E^x \zeta_{h_1} \zeta_{h'} \beta_O^y) = 2^e n$ and it is a root of $x^m - b$. Thus if we set $\beta_j = \beta \zeta_k \zeta_{h_1} \zeta_h$ then we have that $F(\alpha) = F(\beta_j)$ and $o(\beta_j) = o(\alpha) = 2^e n$. Let $\beta_j^{2^e n} = b'$, then it is clear that a', $b' \notin F^p$ for all $p | r$, $(a')^{m'} = a$, $(b')^{m'} = b$ and there are roots $\alpha^r = a'$, $\beta_j^r = b'$ with $F(\alpha) = F(\beta_j)$. So by 2.2

$$F[x]/(x^r - a'), \qquad F[x]/(x^r - b')$$

are F-isomorphic.

Conversely suppose that there are a', $b' \in F$ with $(a')^{m'} = a$, $(b')^{m'} = b$, a', $b' \in F^p$ for all p dividing r and $F[x]/(x^r - a')$, $F[x]/(x^r - b')$ are F-isomorphic.

Then either (i) $a = b^i c^r$ with $(i, r) = 1$ or (ii) $N < \infty$, $2^{N+1} | r$, $-a'$, $-b' \in F^2$ and $a = b^i (2 + \eta_{2^N})^{r/2} c^r$, with $(i, r) = 1$. Write m in the form $m = m_1 m_2$ where $(m_1, m_2) = 1$ and m_2 is the maximal divisor of m which is relatively prime to r. Thus any mth root of unity may be written in the form $\zeta_{k_1} \zeta_{k_2}$, where $k_i | m_i$, $i = 1, 2$.

If (i) then $\alpha = \beta^i c$, so $\zeta_{k_1} \zeta_{k_2} \alpha = \zeta_{k_1} \zeta_{k_2} \beta^i c$ and thus

$$F(\zeta_{k_1} \zeta_{k_2} \alpha) = F(\zeta_{k_2}, \zeta_{k_1} \beta^i).$$

Let $zi \equiv 1 \pmod r$, then $F(\zeta_{k_1} \beta^i) = F(\zeta_{k_1}^z \beta^i)$ so

$$F(\zeta_{k_1} \zeta_{k_2} \alpha) = F(\zeta_{k_2}, \zeta_{k_1}^z \beta) = F(\zeta_{k_2} \zeta_{k_1}^z \beta).$$

Hence the correspondence, $\zeta_{k_2}\zeta_{k_1}\alpha$ into $\zeta_{k_2}\zeta_{k_1}^{r}\beta c$ gives a one-to-one correspondence between the roots of x^m-a, x^m-b respectively such that corresponding roots give the same fields, which implies that

$$F[x]/(x^m-a), \qquad F[x]/(x^m-b)$$

are F-isomorphic.

In case (ii) we use the same idea as was used in the proof of 2.2, together with the decomposition of m used above.

On combining 2.2 and 2.6 we have the following:

THEOREM 2.7. *The algebras $F[x]/(x^m-a)$, $F[x]/(x^m-b)$ are F-isomorphic iff there exist a', $b'\in F$ with $(a')^{m'}=a$, $(b')^{m'}=b$, $m=rm'$ such that a', $b'\notin F^p$ for all $p|r$ and either* (i) $a'=(b')^i(F^r)$, $(i,r)=1$ *or* (ii) $N<\infty$, $2^{N+1}|r$, $-a'$, $-b'\in F^2$ *and* $a'=(b')^i\,(2+\eta_{2^N})^{r/2}(F^r)$, *where* $(i,r)=1$.

With such an explicit characterization the following result follows easily.

COROLLARY 2.8. *The algebras $F[x]/(x^m-a)$, $F[x]/(x^m-b)$ are F-isomorphic iff for every prime p dividing m with $p^s\|m$, $F[x]/(x^{p^s}-a)$, $F[x]/(x^{p^s}-b)$ are F-isomorphic.*

3. The adèle rings of $Q(\sqrt[m]{a})$, $Q(\sqrt[m]{b})$. As pointed out in the introduction, $Q(\sqrt[m]{a})$, $Q(\sqrt[m]{b})$ are arithmetically equivalent (that is they have the same zeta function) iff either $a=b^i \pmod{Q^m}$ or $8|m$ and $a=b^i 2^{m/2} \pmod{Q^m}$, where i is prime to m in both cases.

If $Q(\sqrt[m]{a})$, $Q(\sqrt[m]{b})$ are arithmetically equivalent then we can ask when they have isomorphic adèle rings. This reduces to the question as to when the two algebras

$$Q_2[x]/(x^m-a), \qquad Q_2[x]/(x^m-b)$$

are Q_2-isomorphic. We will now apply the results in Section 2 to answer this question.

In the following theorem we shall assume that a is even. If a is odd then we replace a by $a2^m$.

THEOREM 3.1. *Let x^m-a, x^m-b be irreducible over Q with $a=2^t a_1$, $(a_1,2)=1$, $0\leqslant t\leqslant m$* (recall the convention about a above), *$m=2^e n$, $t=2^r t_1$, $(nt_1,2)=1$, $0\leqslant r\leqslant e$. Then $Q(\sqrt[m]{a})$, $Q(\sqrt[m]{b})$ have isomorphic adèle rings iff either* (i) $a\equiv b^i \pmod{Q^m}$, *for some $(i,m)=1$ or* (ii) $8|m$ *and* $b^i\equiv a2^{m/2} \pmod{Q^m}$, *for some $(i,m)=1$, and either* (A) $a_1\equiv -1 \pmod 8$ *or* (B) *if* $a_1\equiv 1 \pmod 8$, *then $r\leqslant e-2$ and $a_1\in Q^{2^{r+1}}$ (that is, $a_1\equiv 1 \pmod{2^{r+3}}$).*

Proof. In case $a\equiv b^i \pmod{Q^m}$, then clearly the adèle rings are isomorphic since $Q(\sqrt[m]{a})$, $Q(\sqrt[m]{b})$ are Q-isomorphic. Thus we may assume that

$b^i\equiv a2^{m/2} \pmod{Q^m}$. Further, by replacing b by $b^i(Q(\sqrt[m]{b}))\cong Q(\sqrt[m]{b^i})$ since $(i,m)=1$ we may take $i=1$ and $b=a2^{m/2}$. So $b\equiv a2^{m/2}\equiv a \pmod{Q^n}$, thus $Q_2[x]/(x^n-a)$, $Q_2[x]/(x^n-b)$ are Q_2-isomorphic.

Hence we have by 2.7 that

(*) $\quad Q_2[x]/(x^m-a)$, $Q_2[x]/(x^m-b)$ are Q_2-isomorphic iff

(**) $\quad Q_2[x]/(x^{2^e}-a)$, $Q_2[x]/(x^{2^e}-b)$ are Q_2-isomorphic.

So we only have to characterize when (**) holds for the case that $b=a2^{2^{e-1}}$. Further, without loss of generality, since we are dealing with (**), we may assume that $a=2^{2^r}a_1$, where $0\leqslant r\leqslant e$ and $e\geqslant 3$.

If $a_1\equiv 3, 5, 7 \pmod 8$ then $a_1\notin Q_2^2$. If $a_1\equiv -1 \pmod 8$, then by 2.2, (**) holds. If $a_1\equiv 3$ or $5 \pmod 8$, then $-a\notin Q_2^2$ so (**) holds iff there is an j prime to 2 satisfying $b\equiv a^j \pmod{Q_2^{2^e}}$, which becomes

$$2^{2^{e-1}}2^{2^r}a_1\equiv(2^{2^r}a_1)^j \pmod{Q_2^{2^e}},$$

so $2^{e-1}+2^r\equiv 2^r j \pmod{2^e}$, thus $j\equiv 1+2^{e-r-1} \pmod{2^{e-r}}$. Thus if we take $j=1+2^{e-r-1}$, then we also need $a_1\equiv a_1^{1+2^{e-r-1}} \pmod{Q_2^{2^e}}$, so $a_1^{2^{e-r-1}}\equiv 1 \pmod{Q_2^{2^e}}$ and since $a_1\equiv 3$ or $5 \pmod 8$, $a_1^{2^{e-r-1}}\not\equiv 1 \pmod{Q_2^{2^e}}$.

Thus, if $a_1\not\equiv 1 \pmod 8$, then (**) holds iff $a\equiv -1 \pmod 8$.

Now, let us assume that $a_1\equiv 1 \pmod 8$, so $a_1\in Q_2^2$. Thus define l by $a_1\in Q_2^{2^l}$, $l\leqslant e$ and l is maximal with this property. Thus we have that $a_1=(a_1')^{2^l}$, where if $l<e$, then $a_1'\equiv\pm 3 \pmod 8$ (since $\pm a_1'\notin Q_2^2$).

Case 1. $r=e$. If $l=e$, then $a\in Q_2^{2^e}$, yet $b=a2^{e-1}\notin Q_2^{2^e}$, so (**) does not hold. Thus we may assume that $l<e$ (so $a_1\equiv\pm 3 \pmod 8$). Then $a=(2^{2^{e-l}}a_1')^{2^l}$, $b=(2^{2^{e-l-1}}2^{2^{e-l}}a_1')^{2^l}$.

Thus, (**) holds iff

$$Q_2[x]/(x^{2^{e-l}}-\varepsilon_1 2^{2^{e-l}}a_1'), \qquad Q_2[x]/(x^{2^{e-l}}-\varepsilon_2 2^{2^{e-l-1}}2^{2^{e-l}}a_1')$$

are Q_2-isomorphic for some choice of ε_1, $\varepsilon_2\in\{\pm 1\}$. However, since $a_1\equiv\pm 3 \pmod 8$, there cannot exist such an isomorphism by 2.2. So (**) cannot hold in this case.

Case 2. $r=e-1$. Then $b=2^{2^{e-1}}2^{2^{e-1}}a_1=2^{2^e}a_1$, thus we may interchange a and b and return to case 1. Thus (**) cannot hold in this case.

So in the following we may assume that $r\leqslant e-2$.

If $l\geqslant r+1$, then $a=(2(a_1')^{2^{l-r}})^{2^r}$, $b=(2^{2^{e-r-1}}2(a_1')^{2^{e-r}})^{2^r}$ and by choosing $j=1+2^{e-r-1}$ one obtains that

$$(2(a_1')^{2^{l-r}})^j\equiv 2^{2^{e-r-1}}2(a_1')^{2^{l-r}} \pmod{Q_2^{2^{e-r}}},$$

so by 2.6, (**) holds.

Thus we are left with the case where $r \leqslant e-2$ and $l \leqslant r$.

Since $l \leqslant r \leqslant e-2$, $l < e$, so $a_1 \equiv \pm 3 \pmod 8$ and using this and applying 2.2 and 2.6 we see that (**) cannot hold in this case.

References

[1] Maria Acosta de Orozco and William Yslas Vélez, *The lattice of subfields of a radical extension*, J. Number Theory 15 (1982), 388–405.

[2] — — *The torsion group of a field defined by radicals*, ibid. 19 (1984), 283–294.

[3] David Gay and William Yslas Vélez, *The torsion group of a radical extension*, Pacific J. Math. 92 (1981), 317–327.

[4] Irving Gerst, *On the theory of n-th power residues and a theorem of Kronecker*, Acta Arith. 17 (1970), 121–139.

[5] Kenkichi Iwasawa, *On the ring of valuation vectors*, Ann. of Math. 57 (1953), 331–356.

[6] Eliot Jacobson and William Yslas Vélez, *On the adèle rings of radical extensions of the rationals*, Archiv der Mathematik 45 (1985), 12–20.

[7] Warren May, *Fields with free multiplicative groups modulo torsion*, Rocky Mountain J. Math. 10 (1980), 599–604.

[8] Andrzej Schinzel, *On linear dependence of roots*, Acta Arith. 28 (1975), 161–175.

[9] William Yslas Vélez, *On normal binomials*, ibid. 36 (1980), 113–124.

[10] — *Several results on radical extensions*, Archiv der Mathematik 45 (1985), 342–349.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF ARIZONA
Tucson, Arizona 85721

Received on 21.5.1986 (1640)

ACTA ARITHMETICA
LI (1988)

An arithmetic problem on the sums of three squares

by

A. Arenas (Barcelona)

Introduction. As is well known, any positive integer $n \neq 4^a(8b+7)$ can be expressed as a sum of three integer squares. In general, given a decomposition of n, $n = x_1^2 + x_2^2 + x_3^2$, very little is known about the integers x_i. C. F. Gauss proved that n admits a primitive representation as a sum of three squares if and only if $n \not\equiv 0, 4, 7 \pmod 8$ (cf. [5], Art. 291). Catalan showed that if $n = 3^v$, the three summands could be chosen to be prime to 3 (cf. [3]).

Special representations of integers as a sum of three squares have recently appeared in connection with the determination of some Stiefel–Whitney classes (see [11]). Let ξ_n be the real bundle over the classifying space BA_n associated to the standard representation of the alternating group A_n into $SO_n(\boldsymbol{R})$. Let $w^*(\xi_n) \in H^*(BA_n, \boldsymbol{Z}/2\boldsymbol{Z}) = H^*(A_n, \boldsymbol{Z}/2\boldsymbol{Z})$ be its Stiefel–Whitney class. Since $w^1(\xi_n) = 0$, $w^2(\xi_n)$ is the nontrivial element of $H^2(A_n, \boldsymbol{Z}/2\boldsymbol{Z}) = \boldsymbol{Z}/2\boldsymbol{Z}$. It is shown in [11] (cf. also [7]), that if $n \equiv 3 \pmod 8$ admits a representation as a sum of three integer squares with $(x_1, n) = 1$ and $x_1^2 \leqslant (n+1)/3$, then there exists a continuous surjective representation ϱ: $\mathrm{Gal}(\overline{\boldsymbol{Q}(T)}/\boldsymbol{Q}(T)) \to A_n$ of the absolute Galois group of $\boldsymbol{Q}(T)$ such that its second Stiefel–Whitney class $\varrho^* w^2(\xi_n)$ is trivial.

Given an integer n, we consider in this paper the maximum value $l = l(n)$ such that n can be written as a sum of three integer squares with l summands prime to n. We call $l(n)$ the level of n.

Obviously, all integers having level 3 satisfy the preceding condition.

The problem of the determination of the level of an integer leads to compare numbers of representations of this integer by different ternary quadratic forms of a very special type.

Since the number of representation $r(n, f)$ of a given positive integer by a quadratic form cannot be determined in general, we approximate this number by the average value $r(n, \mathrm{gen}\, f)$, where $\mathrm{gen}\, f$ stands for the genus of f. By means of Siegel's Hauptsatz (see [9]) this average value can be calculated using p-adic densities.

For the forms we are dealing with, we have that $r(n, \mathrm{gen}\, f) = r(n, \mathrm{spn}\, f)$, where $\mathrm{spn}\, f$ denotes the spinorial genus of f.