PACIFIC JOURNAL OF MATHEMATICS
Vol. 92, No. 2, 1981

THE TORSION GROUP OF A RADICAL EXTENSION

DAVID GAY AND WILLIAM YSLAS VÉLEZ

The torsion group of a radical field extension is defined and its structure determined using a theorem of Kneser. In the case of a number field, a representation theorem is proved characterizing all abelian groups that can appear as torsion groups of a radical extension.

Let F be a field with multiplicative group F^*. Let K be an extension of F and let $T(K^*/F^*)$ be the torsion subgroup of K^*/F^*. In this paper we will determine the structure of the group $T(K^*/F^*)$ in case $K = F(\alpha)$ where α is a root of irreducible $x^m - a \in F[x]$ and char $F \nmid m$. In particular, we shall prove the following:

THEOREM A. *For a positive integer q, let ζ_q denote a primitive qth root of unity. Let $x^m - a \in F[x]$ be irreducible with root α and $m = 2^n m_0$ with m_0 odd. For p a prime let T_p denote the p-torsion of $T = T(F(\alpha)^*/F^*)$. Let $\eta_{2^n} = \zeta_{2^n} + \zeta_{2^n}^{-1}$. Define N to be the largest integer, if such exists, so that $\eta_{2^N} \in F$; otherwise, let $N = \infty$. Then*

$$T = \langle \alpha^{2^n} F^* \rangle \times T_2 \times H$$

where

(a) $H = \langle \{\zeta_k \in F(\alpha)$: *if p is prime and $p \mid k$, then* $\zeta_p \in F\} F^* \rangle$;

(b) *If* $\zeta_4 \notin F(\alpha) \backslash F$, *then* $T_2 = \langle \alpha^{m_0} F^* \rangle$;

(c) *If* $\zeta_4 \in F(\alpha) \backslash F$, *then*

(i) *if* $N = \infty$, $T_2 = \langle \alpha^{m_0} \zeta_{2^{n+1}} F^* \rangle \times \langle \{\zeta_{2^t}$: *all* $t\} F^* \rangle \cong \boldsymbol{Z}_{2^{n-1}} \times \boldsymbol{Z}_{2^\infty}$;

(ii) *if* $n \leqq N < \infty$, $T_2 = \langle \alpha^{m_0}(1 + \zeta_{2^N})^{2^{N-n}} F^* \rangle \times \langle (1 + \zeta_{2^N}) F^* \rangle \cong \boldsymbol{Z}_{2^{n-1}} \times \boldsymbol{Z}_{2^N}$;

(iii) *if* $N < n$, $T_2 = \langle \alpha^{m_0} F^* \rangle \times \langle \alpha^{m_0 2^{n-N}}(1 + \zeta_{2^N}) F^* \rangle \cong \boldsymbol{Z}_{2^n} \times \boldsymbol{Z}_{2^{N-1}}$.

The following questions concerning the group $T(K^*/F^*)$ have already been examined for various extensions K/F:

(1) Let M be a subgroup of T containing F^* such that M/F^* is finite. When is it the case that $[M: F^*] = [F(M): F]$? Kummer theory [6, p. 218] says that this equation holds when the exponent of M/F^* is m and a primitive mth root of unity ζ_m is an element of F. Besicovitch [1], Mordell [9], and Siegel [13] found necessary and sufficient conditions for this equation to hold in case the only roots of unity in $F(M)$ are ± 1. Kneser [5] has generalized all of these results by proving the

THEOREM. *The equation $[M: F^*] = [F(M): F]$ holds iff, for every*

prime p, $\zeta_p \in M$ *implies* $\zeta_p \in F$ *and* $1 + \zeta_4 \in M$ *implies* $\zeta_4 \in F$.

(2) *Let* $\theta \in T$. *What is the general relationship between* $[\theta F^*: F^*]$ *and* $[F(\theta): F]$? (*The former is called the order of* θ *over* F; *the latter, the degree of* θ *over* F.) *Risman* [11] *has shown the*

THEOREM. *There exist integers* n *and* t *so that* $nt = [\theta F^*: F^*]$, $n \mid [F(\theta): F]$, $(n, t) = 1$ *and, if* p *is prime with* $p \mid t$, *then* $\zeta_{2p} \in F(\theta) \backslash F$.

(3) *Suppose* $\zeta_4 \notin F$. *Then what is the two-torsion* T_2 *of* $T(F(\zeta_4)^*/F^*)$? *May* [8] *has answered this with*

THEOREM. *Suppose* $\zeta_4 \notin F$ *and* char $F \neq 2$. *Then* $N = \infty$ *implies* $T_2 = \langle \{\zeta_{2^m}: \text{all } m\} F^* \rangle \cong \boldsymbol{Z}_{2^\infty}$; $N < \infty$ *implies* $T_2 = \langle (1 + \zeta_{2^N}) F^* \rangle \cong \boldsymbol{Z}_{2^N}$.

The remainder of this paper is organized as follows. In § 1 we prove Theorem A using the theorem of Kneser above. Along the way, we will also characterize $T_p(F(\zeta_{2p})^*/F^*)$ and obtain some results relating $[\alpha F^*: F^*]$ with $[F(\alpha): F]$. Moreover, we will give a new proof of the exact version of Kneser's theorem that we need here. This should make § 1 relatively self-contained.

In the final section (§ 2), we will characterize for a given algebraic number field F those abelian groups that can arise as $T(F(\alpha)^*/F^*)$ for α a root of irreducible $x^m - \alpha \in F[x]$.

1. Kneser's theorem and proof of Theorem A. We assume the notation of the introduction. In addition, for $\alpha \in K$ we denote $o(\alpha) = o_F(\alpha) = [\alpha F^*: F^*]$. For p a prime, we recall that $T_p(K^*/F^*)$ denotes the p-primary subgroup of $T(K^*/F^*)$.

Both Kneser's theorem and Risman's theorem suggest that special things happen when $\zeta_{2p} \in F(\alpha)/F$. Accordingly, our first results are concerned with the group $T_p(F(\zeta_{2p})^*/F^*)$. This group plays a major role in the final determination of the torsion group of a radical extension.

LEMMA 1.1. (a) *Suppose* p *is odd,* $\zeta_p \notin F$ *and* $\alpha \in F(\zeta_p)$ *with* $o(\alpha) = p^r$. *Then* $\alpha \in \zeta_{p^r} F^*$.

(b) *Suppose* $\zeta_4 \notin F$ *and* $\alpha \in F(\zeta_4)$ *with* $o(\alpha) = 2^r$. *Then* $r = 1$ *implies* $\alpha \in \zeta_4 F^*$ *and* $r \geqq 2$ *implies* $\zeta_{2^r} \in F(\zeta_4)$ *and* $\alpha \in (1 + \zeta_{2^r}) F^*$.

Proof. (a) We prove this by induction on r. For $r = 1$, α is a root of $x^p - \alpha^p \in F[x]$ which must be reducible since $([F(\zeta_p): F], p) = 1$. Thus $\alpha = \zeta_p b$, for some $b \in F$. If $r > 1$, then $o(\alpha^p) = p^{r-1}$ and by the inductive hypothesis $\alpha^p = \zeta_{p^{r-1}} c$ for some $c \in F$. Let σ be a generating

automorphism of the Galois group $G(F(\zeta_p)/F)$. Then $(\alpha/\sigma(\alpha))^p = (\zeta_{p^r}/\sigma(\zeta_{p^r}))^p$ so that $\alpha/\sigma(\alpha) = \zeta_p(\zeta_{p^r}/\sigma(\zeta_{p^r}))$. Since there exists a primitive pth root of unity ζ'_p such that $\zeta'_p/\sigma(\zeta'_p) = \zeta_p$, we have $\alpha/\sigma(\alpha) = \zeta'_{p^r}/\sigma(\zeta'_{p^r})$ for some primitive p^rth root of unity ζ'_{p^r}. Thus $\alpha \in \zeta'_{p^r}F^*$.

(b) Suppose $r = 1$. Then α is a root of irreducible $x^2 - \alpha^2 \in F[x]$. Thus $F(\alpha) = F(\zeta_4)$ so that $\alpha \in \zeta_4 F^*$.

For $r \geqq 2$, we prove this by induction. In case $r = 2$, $o(\alpha) = 4$ and α is a root of the new reducible polynomial $x^4 - \alpha^4 \in F[x]$.

Thus by Capelli's theorem ([4], p. 60f), $\alpha^4 = -4b^4$ for some $b \in F$ or $\alpha = \zeta_8\sqrt{2}\,b \in (1 + \zeta_4)F^*$. For $r > 2$, $\alpha^2 = (1 + \zeta_{2^{r-1}})c$, for some $c \in F$, by the inductive hypothesis. Thus, if σ is complex conjugation (where $\sigma(\zeta_{2^{r-1}})\cdot\zeta_{2^{r-1}} = 1$), we have $(\alpha/\sigma(\alpha))^2 = (1 + \zeta_{2^{r-1}})/\sigma(1 + \zeta_{2^{r-1}}) = \zeta_{2^{r-1}}$. Therefore $\alpha/\sigma(\alpha) = \zeta_{2^r} = (1 + \zeta_{2^r})/\sigma(1 + \zeta_{2^r})$ and consequently $\alpha \in (1 + \zeta_{2^r})F^*$. □

As an immediate consequence of this lemma we have the following result characterizing the structure of $T_p(F(\zeta_{2p})^*/F^*)$.

COROLLARY 1.2. *Let* $T_p = T_p(F(\zeta_{2p})^*/F^*)$ *and suppose* $\zeta_{2p} \notin F$. *Then*

(a) T_p *is infinite iff* $T_p = \langle\{\zeta_{p^r}: r > 0\}F^*\rangle$, *in which case* $T_p \cong \boldsymbol{Z}_p^\infty$;

(b) *if* T_p *is finite and* R *is largest such that* $\zeta_{p^R} \in F(\zeta_{2p})$, *then*

(i) p *odd implies* $T_p = \langle\zeta_{p^R}F^*\rangle \cong \boldsymbol{Z}_{p^R}$ *and*

(ii) $p = 2$ *implies*

$$T_2 = \begin{cases} \langle(1 + \zeta_{2^{R-1}})F^*\rangle \cong \boldsymbol{Z}_{2^{R-1}}, & \eta_{2^R} \notin F \\ \langle(1 + \zeta_{2^R})F^*\rangle \cong \boldsymbol{Z}_{2^R}, & \eta_{2^R} \in F. \end{cases}$$

Proof. The proof is obvious from Lemma 1.1 except for (b)(ii). The proof of the latter follows from $(1 + \zeta_{2^R})^2 = \zeta_{2^R}(\eta_{2^R} + 2)$ and from the fact that $\eta_{2^{R-1}} \in F$. □

The next result tells the complete story about the relationship between the order of an element and its degree in the extreme case when the two numbers are relatively prime. We will use the following result.

1.3 (Norris-Vélez, [3] or [10]). Suppose $\alpha \in K$ and $o(\alpha) = [\alpha F^*: F^*] = m$. Let $k = \max\{n: n \mid m \text{ and } \zeta_n \in F(\alpha)\}$ and suppose $F(\alpha) \supseteqq L \supseteqq F(\zeta_k)$ with $l = [F(\alpha): L]$. Then $L = F(\alpha^l)$.

COROLLARY 1.4. *Suppose* $(o(\alpha), [F(\alpha): F]) = 1$. *Then* $\alpha \in \zeta_{o(\alpha)}F^*$, i.e., α *is "essentially" a root of unity.*

Proof. Let $m = o(\alpha)$ and $n = [F(\alpha): F]$. We claim that $(n, m) = 1$

entails m odd. For if m were even, then n would also be even contracting $(n, m) = 1$. Thus m must be odd.

We will prove the corollary by induction on the number of distinct primes dividing m. If $m = p^k$, then it follows from 1.3 that $F(\alpha) = F(\zeta_{p^l})$ for some $l \leqq k$. Since $[F(\zeta_{p^l}): F] \mid (p-1)p^{l-1}$ and $([F(\alpha): F], p) = 1$, it follows that $F(\zeta_{p^l}) = F(\zeta_p)$. The lemma then implies the truth of the corollary in this case.

Now suppose $m = m_0 p^k$ with $(m_0, p) = 1$. By what we have just seen $\alpha^{m_0} = c\zeta_{p^k}$ for some $c \in F$. Let ζ'_{p^k} be a primitive p^kth root of 1 as well as an m_0th root of ζ_{p^k}. Then $(\alpha/\zeta'_{p^k})^{m_0} = c$ and $o(\alpha/\zeta'_{p^k}) = m_0$. Thus by the inductive hypothesis $\alpha/\zeta'_{p^k} = \zeta_{m_0} b$ for some $b \in F$ so that $\alpha = \zeta'_{p^k}\zeta_{m_0} b$. □

We begin the proof of Kneser's theorem by deriving another result concerning the relationship between the order of an element and its degree. This is a sufficient condition for the two numbers to be equal, a result at the opposite extreme from the one just proved.

LEMMA 1.5. *For every prime p dividing $o(\alpha)$ suppose that $\zeta_{2p} \notin F(\alpha)\backslash F$. Then $[F(\alpha): F] = o(\alpha)$.*

Proof. It is sufficient to prove this in case $o(\alpha) = p^k$ for some prime p.

Suppose p is odd. If $[F(\alpha^{p^{k-1}}): F] < p$, then $F(\alpha^{p^{k-1}}) = F(\zeta_p)$, contradicting $\zeta_{2p} \notin F(\alpha)\backslash F$. Thus $x^p - \alpha^{p^k}$ is irreducible and consequently so is $x^{p^k} - \alpha^{p^k}$. Hence $[F(\alpha): F] = o(\alpha)$.

Let $p = 2$. If $k = 1$, then the conclusion is immediate. Assume $k \geqq 2$. Then $x^{2^k} - \alpha^{2^k}$ is reducible iff $x^4 - \alpha^{2^k}$ is reducible iff $\alpha^{2^k} = -4b^4$ for some $b \in F$ by Capelli (*loc. cit.*) iff $\alpha^{2^{k-2}} = \pm(1 \pm i)b$, contradicting either $o(\alpha) = 2^k$ or $i = \zeta_4 \notin F(\alpha)\backslash F$. Thus $x^{2^k} - \alpha^{2^k}$ must be irreducible and $[F(\alpha): F] = o(\alpha)$. □

The next result is of a more general nature; under certain conditions it characterizes the p-torsion group of an extension given by adjoining radicals. The proof is a modification of Kneser's [5].

LEMMA 1.6. *Let p be a prime, K an extension of F and N a subgroup of K^* such that $F^* \subseteq N$ and N/F^* is a finite p-group. Suppose that $\zeta_{2p} \notin F(N)\backslash F$. Then*

$$[F(N): F] = [N: F^*] \quad \text{and} \quad T_p(F(N)^*/F^*) = N/F^* .$$

Proof. Let $\mathscr{N} \subseteq F(N)^*$ so that $\mathscr{N}/F^* = T_p(F(N)^*/F^*)$. Since

$\mathscr{N}\backslash F^*$ is an abelian p-group, there exists a sequence of subgroups $F^* = N_0 \subseteqq N_1 \subseteqq \cdots \subseteqq \mathscr{N}$ such that $[N_i\colon N_{i-1}] = p$. Consequently, for every i, there exists $\beta_i \in N_i\backslash N_{i-1}$ such that $\beta_i^p \in N_{i-1}$.

We claim that for all n, $[F(N_n)\colon F] = p^n$ and $T_p(F(N_n)^*/F^*) = N_n/F$. We prove this by induction on n. In case $n = 0$ this is obvious. Assume that $[F(N_{k-1})\colon F] = p^{k-1}$ and $T_p(F(N_{k-1})^*/F^*) = N_{k-1}/F^*$.

To prove the claim in case $n = k$, we first show that $\beta_k \notin F(N_{k-1})$. For otherwise, since $o(\beta_k)$ is also a power or p, we would have $\beta_k F^* \in T_p(F(N_{k-1})^*/F^*) = N_{k-1}/F^*$, a contradiction. Thus $\beta_k \notin F(N_{k-1})$ and, by Lemma 1.5, $[F(N_k)\colon F(N_{k-1})] = p$. Hence $[F(N_k)\colon F] = [F(N_k)\colon F(N_{k-1})]\cdot[F(N_{k-1})\colon F] = p^k$.

To prove the remainder of the claim, let $\beta F^* \in T_p(F(N_k)^*/F^*)$. By Lemma 1.5 either $\beta \notin F(N_{k-1})$ and $\beta^p \in F(N_{k-1})$ or $\beta \in F(N_{k-1})$. We claim that in either case $\beta = \beta_k^j\gamma$ for some $\gamma \in F(N_{k-1})$. This is certainly true in the latter case with $j = p$. To show it so in case $\beta \notin F(N_{k-1})$ and $\beta^p \in F(N_{k-1})$, let σ be an isomorphism of $F(N_k)$ into an extension field of $F(N_{k-1})$ fixingeve ry element of $F(N_{k-1})$ but not β_k. Since $[F(N_k)\colon F(N_{k-1})] = p$, it follows that $F(N_{k-1}) = \{\delta \in F(N_k)\colon \sigma(\delta) = \delta\}$. Thus $\sigma(\beta) \neq \beta$, $\sigma(\beta_k) = \zeta_p\beta_k$, $\sigma(\beta^p) = \beta^p$ and $\sigma(\beta) = \zeta_p^j\beta$ for some $(j, p) = 1$. Thus $\sigma(\beta^{-1}\beta_k^j) = \beta^{-1}\beta_k^j$ so that $\beta = \beta_k^j\gamma$ for some $\gamma \in F(N_{k-1})$. Because $o(\beta)$ and $o(\beta_k^j)$ are p-powers, it follows that $\gamma F^* \in T_p(F(N_{k-1})^*/F^*) = N_{k-1}/F^*$. Thus $\beta F^* \in N_k/F^*$. This completes the induction and the proof of the original claim.

Since $F(N_i) \subseteqq F(N)$ for all i and $[F(N)\colon N] < \infty$, it follows that the chain $N_0 \subseteqq N_1 \subseteqq \cdots \subseteqq \mathscr{N}$ is finite. Thus $N_k = \mathscr{N}$ for some k. Hence

$$T_p(F(N)^*/F^*) = T_p(F(\mathscr{N})^*/F^*) = \mathscr{N}/F^*$$

and $[F(\mathscr{N})\colon F] = [\mathscr{N}\colon F^*]$. Consequently, $[F(N)\colon F] = [F(\mathscr{N})\colon F] = [\mathscr{N}\colon F^*] \geqq [N\colon F^*]$. But since $[N\colon F^*] \geqq [F(N)\colon F]$ in all cases, we have $[F(N)\colon F] = [N\colon F^*]$ and $T_p(F(N)^*/F^*) = N/F^*$. The proof is complete. □

Just as Lemma 1.6 considered the p-torsion group, so does the following theorem consider the whole torsion group.

THEOREM 1.7. *Let K be an extension of F and M a subgroup of K^* satisfying $F^* \subseteqq M$ and $[M\colon K^*] < \infty$. If, for all primes p, $\zeta_{2p} \notin F(M)\backslash F$, then $[F(M)\colon F] = [M\colon F^*]$ and $T(F(M)^*/F^*) = M/F^*$.*

Proof. Let p be a prime and suppose $p^t \| [M\colon F^*]$. Let $T_p(M/F^*) = M_p/F^*$. Then by Lemma 1.6, $[M_p\colon F^*] = p^t = [F(M_p)\colon F]$. Thus $p^t | [F(M)\colon F]$ and therefore $[M\colon F^*] | [F(M)\colon F]$. Since we have in general (with no hypothesis) $[M\colon F^*] \geqq [F(M)\colon F]$, it follows that

$[M: F^*] = [F(M): F]$.

To prove the second part of the theorem, we show that $T_p(F(M)^*/F^*) = T_p(M/F^*)$. Thus, let $\beta F^* \in T_p(F(M)^*/F^*)$. As a consequence of the equality proved in the preceeding paragraph, we have

$$p^t = [M_p: F^*] \leqq [\langle \beta, M_p \rangle: F^*] = [F(M_p, \beta): F] \leqq p^t$$

thus $[M_p: F^*] \leqq [\langle \beta, M_p \rangle: K^*]$ and hence $\beta F^* \in M_p/F^*$. □

We now apply these results to the determination of $T(F(M)^*/F^*)$ in case $M = \alpha F^*$ where $x^m - \alpha^m$ is irreducible in $F[x]$. It is clear that Theorem 1.7 implies Theorem A for the case $\zeta_{2p} \notin F(\alpha)\backslash F$ for all primes p. Thus we turn to an examination of the case when $\zeta_{2p} \in F(\alpha)\backslash F$ for some prime p.

THEOREM 1.8. *Let $m = m_0 p^k$ with $(m_0, p) = 1$ and suppose $\zeta_{2p} \in F(\alpha)$. Then*

(a) $F(\alpha^{m_0 2^{k-1}}) = F(\zeta_4) = F(\sqrt{a})$ *in case* $p = 2$ *and* $k \geqq 1$;

(b) $T_p(F(\alpha)^*/F^*) = \langle \alpha^{m_0} F^*, T_p(F(\zeta_{2p})^*/F^*) \rangle$;

(c) $\langle \alpha^{m_0} F^* \rangle \cap T_p(F(\zeta_{2p})^*/F^*) = F^*$ *if* p *is odd*;

(d) $\langle \alpha^{m_0} F^* \rangle \cap T_2(F(\zeta_4)^*/F^*) = \langle \zeta_4 F^* \rangle$ *if* $p = 2$ *and* $k \geqq 1$.

Proof. (a) Let $m = 2^k m_0$ with m_0 odd. If $\zeta_4 \in F(\alpha)\backslash F$, then $x^{2^k} - a$ is reducible over $F(\zeta_4)$. The latter is true iff $x^4 - a$ is reducible over $F(\zeta_4)$ iff $a = -4b^4$ for some $b \in F(\zeta_4)$. Thus $a = (2b^2\zeta_4)^2$ and $\alpha^{2^{k-1} m_0} = c\zeta_4$ for some $c \in F(\zeta_4)$. Since the square of $\alpha^{2^{k-1} m_0}$ is in F, it follows that $c \in F$.

(b) First we claim that $p^k \| [F(\zeta_{2p}, \alpha^{m_0}): F]$. Indeed, in case p is odd, this follows from the facts that $([F(\zeta_{2p}): F], [F(\alpha^{m_0}): F]) = 1$, $F(\zeta_{2p})/F$ is Galois and $p^k = [F(\alpha^{m_0}): F]$. In case $p = 2$, we have seen from (a) that $F(\zeta_4) \subseteqq F(\alpha^{m_0})$; furthermore $[F(\alpha^{m_0}): F] = 2^k$.

Now let $\beta F^* \in T_p(F(\alpha)^*/F^*)$. We claim that $\beta \in F(\zeta_{2p}, \alpha^{m_0})$. Otherwise, we would have $[\beta F(\zeta_{2p}, \alpha^{m_0})^*: F(\zeta_{2p}, \alpha^{m_0})^*] = p^l$, $l \geqq 1$. Thus from Lemma 1.5 it would follow that $[F(\zeta_{2p}, \alpha^{m_0}, \beta): F(\zeta_{2p}, \alpha^{m_0})] = p^l$, implying $p^{l+k} | [F(\alpha): F]$, a contradiction. So $\beta \in F(\zeta_{2p}, \alpha^{m_0})$ and consequently

$$\beta F(\zeta_{2p})^* \in T_p(F(\zeta_{2p}, \alpha^{m_0})^*/F(\zeta_{2p})^*) .$$

By Theorem 1.7, $T_p(F(\zeta_{2p}, \alpha^{m_0})^*/F(\zeta_{2p})^*) = \langle \alpha^{m_0} F(\zeta_{2p})^* \rangle$. Thus $\beta = \gamma(\alpha^{m_0})^j$ for some $j \in \boldsymbol{Z}$ and $\gamma \in F(\zeta_{2p})$. Hence $\gamma F^* \in T_p(F(\zeta_{2p})^*/F^*)$ and (b) follows.

(c) If p is odd, then the degrees $[F(\alpha^{m_0}): F]$ and $[F(\zeta_{2p}): F]$ are relatively prime implying that $\langle \alpha^{m_0} F^* \rangle \cap T_p(F(\zeta_{2p})^*/F^*) = F^*$.

(d) From (a), $F(\alpha^{m_0 2^{k-1}}) = F(\zeta_4)$. Thus $\alpha^{m_0 2^{k-1}} = \zeta_4 c$ for some $c \in F$.

The conclusion then follows from the fact that $[\alpha F(\zeta_4)^*: F(\zeta_4)^*] = 2^{k-1}$. □

An immediate consequence of this theorem is

COROLLARY 1.9. *Let* $m = m_0 2^k$ *where* m_0 *is odd. Then* $T_2(F(\alpha)^*/F^*) = T_2(F(\alpha^{m_0})^*/F^*)$.

We also have the following bonus.

COROLLARY 1.10. *Suppose* p *is odd and* $\zeta_p, \zeta_{p^s} \in F(\alpha)\backslash F$. *Then* $\zeta_{p^s} \in F(\zeta_p)$.

Proof. Since $\zeta_{p^s} \in T_p(F(\alpha)^*/F^*)$, Corollary 1.2 and part (b) of the theorem imply $\zeta_{p^s} = (\alpha^{m_0})^{jp^l}\zeta_{p^r}b$ for some $b \in F^*$ and integers j, l, r such that $(j, p) = 1$ and $\zeta_{p^r} \in F(\zeta_{2p})$. Thus $(\alpha^{m_0})^{jp^l} = \zeta_{p^s}\zeta_{p^r}^{-1}b^{-1} = \zeta_{p^q}b^{-1}$ where $q = k - l$. By 1.8(c), we have $\langle \alpha^{m_0}F^* \rangle \cap T_p(F(\zeta_p)^*/F^*) = F^*$ implying $j = 0$ and $\zeta_{p^s} \in F(\zeta_p)$. □

The proof of Theorem A will be complete once we determine the structure of $T_2(F(\alpha^{m_0})^*/F^*)$ ($m = 2^k m_0$, m_0 odd). This we accomplish in the following technical lemma.

LEMMA 1.11. (a) *Let* G *be a group with* $G = \langle \rho \rangle \times \langle \sigma \rangle$, $\langle \rho \rangle \cong \boldsymbol{Z}_{2^a}$, $\langle \sigma \rangle \cong \boldsymbol{Z}_{2^b}$, $b \geqq a \geqq 1$. *Let* $H = \langle (\rho^{2^{a-1}}, \sigma^{2^{b-1}}) \rangle$ *and* $\bar{\rho}$, $\bar{\sigma}$ *the images of* ρ, σ *respectively in* G/H. *Then* $G/H = \langle \bar{\rho}\bar{\sigma}^{2^{b-a}} \rangle \times \langle \bar{\sigma} \rangle$, $\langle \bar{\rho}\bar{\sigma}^{2^{b-a}} \rangle \cong \boldsymbol{Z}_{2^{a-1}}$, *and* $\langle \bar{\sigma} \rangle \cong \boldsymbol{Z}_{2^b}$.

(b) *Let* $G = \langle \rho \rangle \times \boldsymbol{Z}_{2^\infty}$ *where* $\langle \rho \rangle \cong \boldsymbol{Z}_{2^n}$. *Let* $\sigma \in Z_{2^\infty}$ *be the unique element of order* 2^n. *Then* $G = \langle \rho\sigma \rangle \times \boldsymbol{Z}_{2^\infty}$. *Let* $H = \langle (\rho^{2^{n-1}}, \sigma^{2^{n-1}}) \rangle$. *Let* $\bar{\rho}$, $\bar{\sigma}$, $\bar{\boldsymbol{Z}}_{2^\infty}$ *be images of* ρ, σ, $\boldsymbol{Z}_{2^\infty}$ *respectively in* G/H. *Then* $G/H = \langle \bar{\rho}\bar{\sigma} \rangle \times \bar{\boldsymbol{Z}}_{2^\infty}$ *where* $\langle \bar{\rho}\bar{\sigma} \rangle \cong \bar{\boldsymbol{Z}}_{2^{n-1}}$ *and* $\bar{\boldsymbol{Z}}_{2^\infty} \cong \boldsymbol{Z}_{2^\infty}$.

Proof. (a) The element $(\rho, \sigma^{2^{b-a}})$ is of order 2^a in G. Also $(\rho, \sigma^{2^{b-a}})^{2^{a-1}} = (\rho^{2^{a-1}}, \sigma^{2^{b-1}})$. It is easy to see that $(\rho, \sigma^{2^{b-a}})$ and $(1, \sigma)$ generate G and that $\langle (\rho, \sigma^{2^{b-a}}) \rangle \cap \langle (1, \sigma) \rangle = 1$. Thus $G = \langle (\rho, \sigma^{2^{b-a}}) \rangle \times \langle (1, \sigma) \rangle$.

(b) Analogous to (a) since $H < \langle \rho\sigma \rangle$. □

Proof of Theorem A. We only need to prove (c). If $N < \infty$, let $b = \max(n, N)$, $a = \min(n, N)$. Then (ii) and (iii) follow from Lemma 1.11 (a) and Theorem 1.8 (d).

If $N = \infty$, then (i) follows from Lemma 1.11 (b) and Theorem 1.8 (d) with $\langle \rho \rangle = \langle \alpha^{m_0}F^* \rangle$ and $\boldsymbol{Z}_{2^\infty} = \{\zeta_{2^t}F^* : \text{all } t\}$. □

2. **A characterization of H for algebraic number fields.** As

in the previous sections let $x^m - a \in F[x]$ be irreducible with root α and $\text{char } F \nmid m$. Let $\mathscr{P} = \{p: p \text{ prime and } \zeta_p \in F\}$. For an integer n let $\mathscr{P}(n)$ be the set of primes dividing n.

In general, the group $H = \langle\{\zeta_q \in F(\alpha): \mathscr{P}(q) \cap \mathscr{P} = \phi\}F^*\rangle$ of Theorem A can be quite large. For example, if F is the field of real numbers and $\alpha = \zeta_4$, then $H = \langle\{\zeta_q: q \text{ odd}\}F^*\rangle$. However, if F is an algebraic number field, then H is a finite cyclic group. Henceforth, we assume F is an algebraic number field. Thus we have $H = \langle\zeta_q F^*\rangle$ for some q satisfying $\mathscr{P}(q) \cap \mathscr{P} = \phi$. In fact, $H \cong \boldsymbol{Z}_q$. We can show more: Let S denote the set defined by $q \in S$ iff

(1) $\mathscr{P}(q) \cap \mathscr{P} = \phi$;

(2) $F(\zeta_q)$ (respectively, $F(\zeta_{4q})$) is the splitting field of an irreducible binomial;

(3) if $\zeta_r \in F(\zeta_q)$ (respectively, $\zeta_r \in F(\zeta_{4q})$) and $\mathscr{P}(r) \cap \mathscr{P} = \phi$, then $r \mid q$.

Then we can prove the following.

THEOREM B. *Let $H = \langle\zeta_q F^*\rangle$ be the group of Theorem* A *with $\mathscr{P}(q) \cap \mathscr{P} = \phi$. Then $q \in S$.*

Theorem B is an immediate consequence of the following.

LEMMA 2.1. *Let K/F be abelian with $F(\alpha) \supseteq K \supseteq F$ and $n = [K: F]$.*

(a) *If $\zeta_4 \notin F(\alpha)\backslash F$, then K is the splitting field of $x^n - a$.*

(b) *If $\zeta_4 \in F(\alpha)\backslash F$, then $K(\zeta_4)$ is the splitting field of $x^n - a$ or $x^{2n} - a$.*

Proof. (a) Let $k = \max\{l: l \mid m \text{ and } \zeta_l \in F(\alpha)\}$. By 1.3, $K(\zeta_k)$ is the splitting field of $x^l - a$ where $l = [K(\zeta_k): F]$. The group of $x^l - a$ is abelian so that, by a theorem of Schnizel ([12], Theorem 2) and the fact that $\zeta_4 \notin F(\alpha)\backslash F$, its Galois group is also cyclic. Thus K is the splitting field of $x^n - a$.

(b) By Theorem 1.8 (a), $F(\zeta_4) = F(\sqrt{a})$ and α is a root of the irreducible binomial $x^{m/2} - \sqrt{a}$ over $F(\zeta_4)$. Let $n' = [K(\zeta_4): F(\zeta_4)]$. By (a) $K(\zeta_4)$ is the splitting field of $x^{n'} - \sqrt{a}$ over $F(\zeta_4)$. Thus $K(\zeta_4)$ is the splitting field of $x^{2n'} - a$ over F. It is easy to see that $2n' = n$ or $2n$. □

If $q \in S$ and $F(\zeta_q)$ is the splitting field of irreducible $x^n - b$, then call $x^n - b$ an *associated binomial* for q. If $F(\zeta_{4q})$ is the splitting field of an irreducible binomial $x^{n'} - c$ and $\zeta_r \in F(_{4q})$ with $\mathscr{P}(r) \cap \mathscr{P} = \phi$ implying $r \mid q$, then call $x^{n'} - c$ an *associated binomial* for q. Then we have the following converse to Theorem B.

THEOREM C. *Let $q \in S$ with $x^n - b$ an associated binomial for q. Let K be the splitting field of $x^n - b$. For any positive integer s, there exists $c \in F$ so that*

(i) *$x^{sn} - bc^n$ is irreducible;*

(ii) *the group H of Theorem A for $x^{sn} - bc^n$ is equal to $\langle \zeta_q F^* \rangle$;*

(iii) *$\zeta_4 \notin F(\alpha) \backslash K$.*

Theorem C is an immediate consequence of the following more general result.

LEMMA 2.2. *As above, assume F is an algebraic number field. Let $x^n - b \in F[x]$ be irreducible with root β. Then for any integer s there exists $c \in F$ so that (1) $x^{ns} - bc^n$ is irreducible; (2) if γ is a root of the latter with $\gamma^s = \beta c$, then $F(\beta) \subseteq F(\gamma)$ and $\zeta_k \in F(\gamma)$ implies $\zeta_k \in F(\beta)$.*

Proof. Let s be an integer, $s > 1$. For every rational prime p, the binomial $x^s - p$ is irreducible over $\boldsymbol{Q}$. Moreover, for distinct primes $p_1, \cdots, p_k$, $[\boldsymbol{Q}(\sqrt[s]{p_1}, \cdots, \sqrt[s]{p_k}) : \boldsymbol{Q}] = s^k$ by [1]. Thus, if F is an algebraic number field, there are infinitely many primes so that $x^s - p$ is irreducible over F.

Now, if η is an algebraic number with $[F(\eta, \beta) : F(\beta)] = s$ and $\zeta_k \in F(\eta)$, then $[F(\beta, \zeta_k) : F(\beta)] \mid s$. Thus let $\mathscr{S} = \{\zeta_k : [F(\zeta_k, \beta) : F(\beta)] \mid s\}$ and consider the field $L = F(\beta, \mathscr{S})$. Because the number of solutions to $\phi(x) \leqq x_0$ for fixed x_0 is finite, the set $\mathscr{S}$ is finite and thus L is an algebraic number field. (ϕ is Euler's ϕ-function.)

Choose p to be a prime so that $x^s - p$ is irreducible over $L(\sqrt[s]{\beta})$. Then we claim that $x^{sn} - bp^n$ is irreducible over F. We will prove the claim by showing that the degree of a root is sn. Let γ be a root with $\gamma^s = \beta p$. Then γ is also a root of $x^s - \beta p$ over $L(\sqrt[s]{\beta})$. Furthermore, there exists a root $\hat{\gamma}$ of $x^s - p$ so that $L(\sqrt[s]{\beta}, \gamma) = L(\sqrt[s]{\beta}, \hat{\gamma})$. Thus $[L(\sqrt[s]{\beta}, \gamma) : L(\sqrt[s]{\beta})] = s$, $x^s - \beta p$ is irreducible over L, and hence $[L(\gamma) : L] = [F(\gamma) : F(\beta)] = s$. Since $[F(\beta) : F] = n$, the degree of γ over F is sn. This proves the claim.

Now let $\zeta_k \in F(\gamma)$. Then by the definition of L, $\zeta_k \in L$. But by the fact that $[L(\gamma) : L] = [F(\gamma) : F(\beta)]$, it follows that $F(\gamma) \cap L = F(\beta)$. Thus $\zeta_k \in F(\beta)$. This completes the proof of the lemma. □

Our final result is a characterization of the set S.

PROPOSITION 2.3.

(1) *If $r, s \in S$ and $\mathscr{P}(r) = \mathscr{P}(s)$, then $r = s$.*

(2) *$|S| < \infty$.*

Proof. (1) follows from the fact that if $q \in S$ and $p \in \mathscr{P}(q)$,

then $p^t \| q$ implies (by Corollary 1.8) $\zeta_{p^t} \in F(\zeta_p)$ and $\zeta_{p^{t+1}} \notin F(\zeta_p)$.

(2) Let $\mathscr{P}(S) = \{p: p \in \mathscr{P}(q) \text{ for some } q \in S\}$. By Lemma 2.1, $p \in \mathscr{P}(S)$ implies that either $F(\zeta_p)$ or $F(\zeta_{4p})$ is the splitting field of an irreducible binomial. We can show that $F(\zeta_{4p})$ is always the splitting field of an irreducible binomial. For, suppose $x^n - b$ is irreducible, has splitting field $F(\zeta_p)$ and that $\zeta_4 \notin F(\zeta_p)$. Since $F(\zeta_p)$ is abelian, $x^n - b$ must be a normal polynomial. Hence $\zeta_n \in F(\zeta_p)$ and thus $4 \nmid n$. If n is odd, then $x^{2n} + b^2$ is irreducible with splitting field $F(\zeta_{4p})$. If $2 \| n$, then $x^{2n} + 2^n b^2$ is irreducible with splitting field $F(\zeta_{4p})$. Thus

$$\mathscr{P}(S) = \{p: p \text{ prime}, p \notin \mathscr{P}, F(\zeta_{4p}) \text{ is the splitting field of an irreducible binomial}\}.$$

We claim that $\mathscr{P}(S)$ is finite. This and (1) would show $|S| < \infty$.

To prove this claim, let n be the number of roots of unity in $F(\zeta_4)$. By the argument in the proof of Lemma 2.2, the set $\{p: p \text{ prime } [F(\zeta_{4p}): F(\zeta_4)] \leqq n\}$ is finite. Thus let $p \in \mathscr{P}(S)$ so that $[F(\zeta_{4p}): F(\zeta_4)] = m > n$. Therefore $F(\zeta_{4p})$ is the splitting field of an irreducible and abelian binomial $x^m - b$ for some $b \in F$. Thus $\zeta_m \in F(\zeta_{4p})$ and, by [3; Proposition 1], $\mathscr{P}(m) \subseteqq \mathscr{P} \subseteqq \mathscr{P}(n)$. Hence, since $m > n$, we have $F(\zeta_m) \cap F(\zeta_{n^2}) \supsetneqq F(\zeta_4)$. Thus also $F(\zeta_{4p}) \cap F(\zeta_{n^2}) \supsetneqq F(\zeta_4)$. But the number of primes p so that the latter occurs must be finite since $[F(\zeta_{n^2}): \boldsymbol{Q}] < \infty$. Thus $\mathscr{P}(S)$ is finite. □

REMARK. The set S is closely related to the set $N = \{n: \text{there exist } b \in F \text{ so that } x^n - b \text{ normal}\}$. In fact, if $n \in N$, then there exist n_0, q_0 with $n = n_0 q_0$, $\mathscr{P}(n_0) \subseteqq \mathscr{P}$, $q_0 | q$ for some $q \in S$.

More precisely, suppose $\zeta_4 \in F$. If $p \in \mathscr{P}$, define $A(p) \geqq 1$ by $\zeta_{p^{A(p)}} \in F$, $\zeta_{p^{A(p)+1}} \notin F$. For $q \in S$, $p \in \mathscr{P}$, define $B(p, q)$, $a(p, q)$ by $\zeta_{p^{B(p,q)}} \in F(\zeta_q)$, $\zeta_{p^{B(p,q)+1}} \notin F(\zeta_q)$ and $p^{a(p,q)} \| [F(\zeta_q): F]$. Let $\mathscr{P}_q = \mathscr{P}(\prod_{p \in \mathscr{P}} p^{A(p)-B(q,p)}[F(\zeta_q): F])$ and $m(q) = \prod_{p \in \mathscr{P}} p^{B(p,q)-a(p,q)}$. Then a typical element of N is of the form

$$q_0[F(\zeta_q): F]m_1(q)m_2(q)$$

where $q \in S$, $q_0 | q$ with $F(\zeta_{q_0}) = F(\zeta_q)$, $\mathscr{P}(m_1(q)) \subseteqq \mathscr{P} \backslash \mathscr{P}_q$ and $m_2(q) | m(q)$. The case $\zeta_4 \notin F$ is similar (modulo 2!). See [2] for details and proof.

We conclude with some examples of the set S for various algebraic number fields:

(1) $F = \boldsymbol{Q}$, $S = \{1, 3\}$ (see [7]);

(2) $F = \boldsymbol{Q}(\zeta_4)$, $S = \{1, 3, 5\}$ (see [14]);

(3) $F = \boldsymbol{Q}(\zeta_3)$, $S = \{1, 7\}$ (see [2]);

(4) $F = \boldsymbol{Q}(\sqrt{(5 + \sqrt{5})/2})$. Since $\boldsymbol{Q}(\zeta_5) = \boldsymbol{Q}(\zeta_4\sqrt{(5 + \sqrt{5})/2})$, it

follows that $F(\zeta_4) = F(\zeta_5)$. Thus $x^4 + 36$ is irreducible with splitting field $F(\zeta_{60}) = F(\zeta_{15})$. Hence $S = \{1, 3, 5, 15\}$.

REFERENCES

1. A. S. Besicovitch, *On the linear independence of fractional powers of integers,* J. London Math. Soc., **15** (1940), 3-6.
2. D. Gay, *Normal binomials over algebraic number fields,* J. Number Theory, Vol. 12, No. 3 (1980), 311-326.
3. D. Gay and W. Yslas Vélez, *On the degree of the splitting field of an irreducible binomial,* Pacific J. Math., **78** (1978), 117-120.
4. I. Kaplansky, *Fields and Rings,* The University of Chicago Press, 1972,
5. M. Kneser, *Lineare abhängigkeit von Wurzeln,* Acta Arithmetica, **24** (1975), 307-308.
6. S. Lang, *Algebra,* Addison-Wisley, 1965.
7. H. Mann and W. Yslas Vélez, *On normal radical extensions of the rationals,* J. Linear and Multilinear Algebra, **3** (1975), 73-80.
8. W. May, *Fields with free multiplicative groups modulo torsion,* submitted.
9. L. J. Mordell, *On the linear independence of algebraic numbers,* Pacific J. Math., **3** (1953), 625-630.
10. M. J. Norris and W. Yslas Vélez, *Structure theorems for radical extensions of fields,* Acta Arithmetica, to appear.
11. L. J. Risman, *On the order and degree of solutions to pure equations,* P.A.M.S., **55** (1976), 261-266.
12. A. Schinzel, *Abelian binomials, power residues, and exponential congruences,* Acta Arithmetica, **32** (1976/77), 245-274.
13. C. L. Siegel, *Algebraische Abhängigkeit von Wurzeln,* Acta Arithmetica, **21** (1972), 59-64.
14. W. Yslas Vélez, *On normal binomials,* Acta Arithmetica, **36** (1980), 113-124.

Received September 26, 1979.

THE UNIVERSITY OF ARIZONA
TUCSON, AZ 85721