Pacific Journal of Mathematics

EXPLICIT CONSTRUCTION OF CERTAIN SPLIT EXTENSIONS OF NUMBER FIELDS AND CONSTRUCTING CYCLIC CLASSFIELDS

STANLEY JOSEPH GURAK

Volume 157 No. 2 February 1993

PACIFIC JOURNAL OF MATHEMATICS
Vol. 157, No. 2, 1993

EXPLICIT CONSTRUCTION OF CERTAIN SPLIT EXTENSIONS OF NUMBER FIELDS AND CONSTRUCTING CYCLIC CLASSFIELDS

S. GURAK

The problem of explicitly constructing classfields (Hilbert's Twelfth problem) is largely unresolved, except when a classfield is absolutely abelian or abelian over an imaginary quadratic number field. Here an explicit construction of certain split extensions of number fields is given, which maintains control over the primes which ramify. This naturally leads to the construction of cyclic classifields over a given number field. An algorithm is provided to obtain the minimal polynomials for the generating elements of the extension constructed. The methods employed here rely heavily on classfield theory and the properties of Lagrange resolvents and group determinants.

1. Introduction. The principal goal of this research is to obtain an explicit construction of certain split algebraic extension fields over a given number field F. The characterization of such fields is given for dihedral extensions of degree 6, 8 and 12 over Q in a previous work [**6**]. Those constructions rely on the arithmetic of quadratic fields and explicit formulas such as Cardano's. The constructions given here rely on classfield theory and the properties of Lagrange resolvents. There is a natural extension of the construction for similar extensions over function fields which will be treated in a subsequent paper.

To be more precise about the extensions we seek to construct, let Z_n denote the ring of residues modulo n, for some integer $n > 1$, with unit group Z_n^*. Consider a polynomial $p(x) = x^n + a_1x^{n-1} + \cdots + a_0$, irreducible over F, with Galois group G of the form $V \cdot T$, where T is cyclic of order n with $T \trianglelefteq G$ and V is isomorphic to a subgroup of Z_n^* (that is, G is a semi-direct product of T by V). Let K be the splitting field of $p(x)$ so $G(K/F) = G$, and let k and R be the subfields fixed by T and V respectively. We wish to give an explicit general construction for the extension K/F (or K/k) in terms of the arithmetic of $k(\zeta)$, where $\zeta = \exp(2\pi i/n)$. Since $K = k \cdot R$, the problem of determining K primarily is one of finding explicit generators for the field R (or a conjugate field). Of course, R is generated by some root of $p(x)$, but actually finding roots of $p(x)$

in terms of radicals is generally quite tedious. The strategy here is to replace $p(x)$ by a collection of irreducible polynomials of prime power degrees, each of whose roots are explicitly found in terms of radicals. The collection is so chosen that R is generated by a certain choice of roots, one from each polynomial in the collection.

To carry out this approach, first note that the multiplication in G is explicitly given in terms of a generator σ of T via

$$\tau\sigma\tau^{-1} = \sigma^{\theta(\tau)} \qquad (\tau \in V), \tag{1}$$

for some homomorphism $\theta\colon V \to Z_n^*$. (The map θ is independent of the choice of generator σ, and in fact, a monomorphism since K is the splitting field of R.) Write $n = n_1 n_2 \cdots n_t$ as a product of distinct prime powers, and let π_i denote the natural projection of Z_n^* onto $Z_{n_i}^*$ $(1 \le i \le t)$. Set $\theta_i = \pi_i \circ \theta$ with

$$\ker\theta_i = \{\tau \in V | \theta(\tau) \equiv 1 \pmod{n_i}\} \qquad (1 \le i \le t). \tag{2}$$

and put $T_i = \langle \sigma^{n_i} \rangle$ for $1 \le i \le t$. The subgroups $(\ker\theta_i)\ T_i$ $(1 \le i \le t)$ are easily seen to be normal in G. Let K_i, R_i and k_i be the subfields of K fixed by $(\ker\theta_i)T_i$, $V \cdot T_i$ and $(\ker\theta_i)T$ respectively $(1 \le i \le t)$. Then one has the following correspondence from Galois theory

$$\begin{tikzcd}
 & K_i \arrow[dl, dash] \arrow[ddr, dash] \arrow[rrr, leftrightarrow] & & & 1 \arrow[dl, dash] \arrow[ddr, dash] & \\
R_i \arrow[ddr, dash] & & & V_i \arrow[ddr, dash] & & \\
 & & k_i \arrow[dl, dash] & & & T/T_i \arrow[dl, dash] \\
 & F \arrow[rrr, leftrightarrow] & & & G_i &
\end{tikzcd} \tag{3}$$

where $V_i = V/(\ker\theta_i)$ and $G_i = V_i \cdot T/(T_i)$ $(1 \le i \le t)$. Since $\bigcap \ker\theta_i = 1$, and $\bigcap T_i = 1$, we find that $K = \prod K_i$, $R = \prod R_i$ and $k = \prod k_i$. In particular, $\deg(R_i/F) = n_i$ and $\deg(k_i/F) = [V\colon \ker\theta_i]$. We have shown

Proposition 1. *To construct the splitting field K, it suffices to find generating elements α_i for the fields R_i and γ_i for the abelian extensions k_i over F.*

We note that the subfields k_i can be exhibited explicitly from the arithmetic of k in a straightforward manner using Galois theory (for instance, by taking appropriate norms or traces). Thus the above result reduces the construction of R to that of finding explicit generators for each of the subfields R_i of prime power degree over F. Our strategy to construct such a given subfield is to exhibit a particular generator, which is explicitly given in terms of radicals over a suitable resolvent field, together with its minimal polynomial of prime power degree. A general algorithm for this construction is given in §3 with explicit examples appearing later in §4.

2. Characterization of the resolvent field. Recall the situation just described with $n = n_1 \cdots n_t$ as a product of distinct prime powers. The extension K is the splitting field of some irreducible polynomial of degree n over F whose Galois group $G = V \cdot T$ is a semi-direct product of a cyclic group T of order n by a group V isomorphic to a subgroup of Z_n^*. The subfields k and R are those fixed by T and V respectively in the Galois correspondence. The mapping $\theta\colon V \to Z_n^*$ in (1) can be determined from classfield theory, without explicitly determining K, using only arithmetic in the abelian extension k/F. Indeed, K/k is classfield to a certain ideal group $\mathbf{J}$ defined for a suitable k-modulus $\mathscr{M}$. So if $\mathbf{I}$ is the group of fractional k-ideals prime to $\mathscr{M}$, the quotient $\mathbf{I}/\mathbf{J} \cong G(K/k) = T$ through Artin reciprocity. We shall indicate the Artin map of K/k by

$$[\sigma] \to \sigma \quad \text{for } \sigma \text{ in } T, \tag{4}$$

where $[\sigma]$ represents the coset of $\mathbf{I}/\mathbf{J}$ which maps to σ in T. Since $T \trianglelefteq G$ we have $\tau(\mathbf{J}) = \mathbf{J}$, so $\tau([\sigma]) = [\tau\sigma\tau^{-1}] = [\sigma^{\theta(\tau)}]$ from properties of the Artin map. To actually determine θ one needs only to find a prime ideal $\mathfrak{p}$ in the coset $[\sigma]$, then compute the coset to which $\tau(\mathfrak{p})$ belongs for each τ in V. For a given generator α for R/F of zero trace and fixed generator σ of T, form the Lagrange resolvents

$$\omega_\nu = \omega_\nu(\alpha) = \alpha + \zeta^{-\nu}\sigma(\alpha) + \cdots + \zeta^{-(n-1)\nu}\sigma^{n-1}(\alpha) \qquad (\nu \in Z_n). \tag{5}$$

Set

$$\alpha_\mu = \frac{1}{n}\sum_{\nu=1}^{n-1} \zeta^{\mu\nu}\omega_\nu \qquad (\mu \in Z_n) \tag{6}$$

where $\zeta = \zeta_n = \exp(2\pi i/n)$, so that for $0 \le \lambda < n$,

$$\sigma^\lambda(\alpha_\mu) = \alpha_{\mu+\lambda} \qquad (\mu \in Z_n). \tag{7}$$

The elements α_μ is (6) are the distinct zeros of an irreducible polynomial

$$p(x) = x^n + a_1 x^{n-1} + \cdots + a_n \tag{8}$$

of degree n, with $a_1 = 0$, whose splitting field is K. By replacing α by a suitable conjugate, we may assume that $\omega_1 \neq 0$.

It is known that the elements $\beta_\nu = \omega_\nu^n$ $(\nu \in Z_n)$ lie in $k(\zeta)$. (This follows readily from the proof of Lemma 1 below.) The β_ν actually lie in some subfield k' called the *resolvent field* for $p(x)$ over F, which can be described in terms of Galois theory in the following manner.

Label each element ϕ of $G(k(\zeta)/F)$ by $\phi = \phi_{\tau,s}$, where τ is the unique map in V which coincides with ϕ on k, and s in Z_n^* is determined by the action $\phi(\zeta) = \zeta^s$. The resolvent field k' is that which is fixed by the subgroup $W = \{\phi_{\tau,s} | s \equiv \theta(\tau) \bmod n\}$. Since $\phi_{1,1}$ is the only map in W that fixes k, one finds that $k'(\zeta) = k(\zeta) = k'k$. That k' contains the β_ν $(0 \leq \nu < n)$ is immediate from the next lemma.

LEMMA 1. *For each $\phi = \phi_{\tau,s}$ in $G(k(\zeta)/F)$ and integer ν, $\phi_{\tau,s}(\beta_\nu) = \beta_{\nu s\theta(\tau^{-1})}$.*

Proof. Let $\tilde{\phi}$ be any extension of ϕ to $K(\zeta)$, say with $\tilde{\phi}|_K = \tau\sigma^t$ in G for some integer t, $0 \leq t < n$. First note that from (1) and (7),

$$\tilde{\phi}(\alpha_\mu) = \tau\sigma^t(\alpha_\mu) = \tau\sigma^{t+\mu}(\alpha) = \sigma^{(t+\mu)\theta(\tau)}\tau(\alpha) = \alpha_{(t+\mu)\theta(\tau)}.$$

Thus, from (4), we have

$$\begin{aligned}\tilde{\phi}(\omega_\nu) &= \sum_{\mu\in Z_n} \zeta^{-\mu\nu s}\alpha_{(t+\mu)\theta(\tau)} = \sum_{\mu\in Z_n} \zeta^{-\nu s(\mu\theta(\tau^{-1})-t)}\alpha_\mu \\ &= \zeta^{ts\nu} \sum_{\mu\in Z_n} \zeta^{-\nu s\mu\theta(\tau^{-1})}\alpha_\mu = \zeta^{ts\nu}\omega_{s\theta(\tau^{-1})\nu},\end{aligned}$$

upon replacing μ by $\mu\theta(\tau^{-1})-t$ in the first summation. In particular, $\phi(\beta_\nu) = \beta_{s\theta(\tau^{-1})\nu}$.

The resolvent field k' has a convenient characterization in terms of class field theory. Suppose k/F has conductor $\mathscr{f}$ and put $\mathscr{m} = \mathrm{LCM}(nO_F, \mathscr{f})$, where O_F is the ring of integers of F. Let $\mathscr{C}$ denote the group of fractional F-ideals prime to $\mathscr{m}$ and $\mathscr{A}$ be the subgroup of $\mathscr{C}$ which corresponds to the classfield k over F. The Artin map of k/F induces an isomorphism of $\mathscr{C}/\mathscr{A}$ with V, which we shall indicate by

$$[\tau] \to \tau. \tag{9}$$

(Here $[\tau]$ represents the coset of $\mathscr{C}/\mathscr{A}$ which maps to $\tau|_k$ in $G(k/F)$ via the Artin map.) In a similar way, let $[\phi]$ represent the coset of fractional F-ideals in $\mathscr{C}$ which are sent to ϕ in $G(k(\zeta)/F)$ by the Artin map of $k(\zeta)/F$. In addition, let $\mathscr{N} = \mathscr{N}_{F/Q}$ denote the absolute ideal norm mapping from F to Q. It follows from the properties of the Artin map that for $\phi = \phi_{\tau,s}$ in $G(k(\zeta)/F)$,

$$[\phi_{\tau,s}] = \{\mathfrak{a} \in [\tau] | \mathscr{N}\mathfrak{a} \equiv s \pmod{n}\}. \tag{10}$$

The resolvent field k'/F corresponds through classfield theory to the group

$$\mathscr{B} = \bigcup_{\phi \in W} [\phi]. \tag{11}$$

To aid in the computation of k', we mention the following result.

PROPOSITION 1. *Let $h(x)$ be any irreducible polynomial of degree $[k : F]$ over F with splitting field k. Select a zero λ of $h(x)$ and label its conjugates*

$$\tau(\lambda) = \lambda_{\theta(\tau)} \qquad (\tau \in V). \tag{12}$$

Then the elements $E_\mu = \sum_{\tau \in V} \zeta^{-\mu\theta(\tau)} \lambda_{\theta(\tau)}$ $(0 \le \mu < n)$ all lie in the resolvent field k'.

Proof. Since $E_\mu = k(\zeta)$, it suffices to show that each map in W fixes E_μ. But, for any $\phi = \phi_{\tau',\theta(\tau')}$ in W and $0 \le \mu < n$,

$$\phi(E_\mu) = \sum_{\tau \in V} \zeta^{-\mu\theta(\tau)\theta(\tau')} \lambda_{\theta(\tau)\theta(\tau')} = E_\mu \quad \text{from (12)}.$$

If $K \cap Q(\zeta) = Q$ then

$$G(k(\zeta)/F) = \{\phi_{\tau,s} | \tau \in V,\, s \in Z_n^*\} \quad \text{and}$$
$$G(k(\zeta)/k) = \{\phi_{1,s} | s \in Z_n^*\}.$$

In particular, we have

PROPOSITION 2. *Suppose $K \cap Q(\zeta) = Q$. Then $G(k(\zeta)/k) \cong G(k'/F)$ and $k \cap k' = F$.*

Proof. The action $\phi_{1,s} \to \phi_{1,s}W$ $(s \in Z_n^*)$ yields a monomorphism of $G(k(\zeta)/k)$ into $G(k'/F)$ since $k'k = k(\zeta)$. Also $\phi_{\tau,s} = \phi_{1,s\theta(\tau^{-1})} \circ \phi_{\tau,\theta(\tau)}$ here for any $\tau \in V$ and $s \in Z_n^*$, so the map is clearly surjective. Hence $G(k(\zeta)/k) \cong G(k'/F)$ and $k \cap k' = F$.

EXAMPLE 1. To illustrate the preceding theory with $n = 5$ and $F = Q$, consider the complex quartic abelian field $k = Q(\Lambda)$, where $\Lambda = \zeta_{16}+\zeta_{16}^7$, of conductor $\mathscr{f} = 16$ and class number $h = 1$ [**13**]. The ring of integers of k has fundamental unit $E = 1 + \sqrt{2}$ and integral basis $\{1, \sqrt{2}, \Lambda, \sqrt{2}\Lambda\}$. The field k over Q corresponds through classfield theory to the subgroup $\mathscr{A} = \{(x) | x \equiv 1, 7, 17, 23, 33, 39, 49, 71 \pmod{80}, x > 0\}$ defined with $m = 80$. It admits an ideal group J defined modulo $\mathscr{M} = (5^2)$ consisting of principal ideals generated by elements γ prime to $\mathscr{M}$ and of the form $\gamma = \alpha \cdot \beta$ for some $\alpha \in (k^x)^5$ and $\beta \equiv 1 + 5(\delta + a(1 + 2\sqrt{2})\Lambda) \bmod \mathscr{M}$ with $a \in Z$, $\delta \in Q(\sqrt{2})$. The ideal group J corresponds to a classfield K which is normal over Q with $[K : k] = 5$. The Galois group $G = G(K/Q)$ is a semi-direct product of the form $V \cdot T$ as we have been discussing, say with $T = G(K/k)$ generated by an element σ for which $[\sigma] = (1+5\sqrt{2}\Lambda)J$ in (4). Incidentally, we find $[\sigma^j] = (1 + 5j\sqrt{2}\Lambda)J \quad (0 \le j \le 4)$. Also, if $\tau \in V \cong G(k/Q)$ is given by the action $\Lambda \to \overline{\Lambda} = \zeta_{16}^{11} + \zeta_{16}^{13} = -(\sqrt{2} + 1)\Lambda$, then $\tau[\sigma] = (1 - 5\sqrt{2}\Lambda)J = (1 + 5(2 + \sqrt{2})\Lambda)J = (1 + 10\sqrt{2}\Lambda)J$. Thus $\theta(\tau) = 2$ in (1). Further, we find $\theta(\tau^2) = 4$, $\theta(\tau^3) = 3$ and $\theta(1) = 1$.

Suppose α is a generator for the field R fixed by V, so chosen that the Lagrange resolvents (5) satisfy $\omega_\nu = 0$ for $(\nu, 5) > 1$. To determine the resolvent field k' for its minimal polynomial $p(x)$ in (8), we find the corresponding subgroup $\mathscr{B}$ of $\mathscr{C}$ from (11). Noting that

$$[\tau] = \{(x) | x > 0,\ x \equiv 11, 13, 27, 29, 43, 59, 61, 77 \pmod{80}\},$$
$$[\tau^2] = \{(x) | x > 0,\ x \equiv 9, 31, 41, 47, 57, 63, 73, 79 \pmod{80}\}$$
and
$$[\tau^3] = \{(x) | x > 0,\ x \equiv 3, 19, 21, 37, 51, 53, 67, 69 \pmod{80}\}$$

in (9), we find the sets $[\phi]$ in (11) are

$$[\phi_{1,1}] = \{(x) | x > 0,\ x \equiv 1, 71 \pmod{80}\},$$
$$[\phi_{\tau,2}] = \{(x) | x > 0,\ x \equiv 27, 77 \pmod{80}\},$$
$$[\phi_{\tau^2,4}] = \{(x) | x > 0,\ x \equiv 9, 79 \pmod{80}\}, \qquad \text{and}$$
$$[\phi_{\tau^3,3}] = \{(x) | x > 0,\ x \equiv 3, 53 \pmod{80}\}.$$

Thus, we have $\mathscr{B} = \{(x) | x > 0, x \equiv 1, 3, 9, 27, 53, 71, 77, 79 \pmod{80}\}$ with corresponding field $k' = Q(\sqrt{10 + 3\sqrt{10}})$ from classfield theory.

Alternatively, we could use Proposition 1, choosing $\lambda = \Lambda$, to find that

$$\begin{aligned} E_{-1}^2 &= [\zeta\Lambda + \zeta^2\overline{\Lambda} + \zeta^3(-\overline{\Lambda}) + \zeta^4(-\Lambda)]^2 = [(\zeta - \zeta^4)\Lambda + (\zeta^2 - \zeta^3)\overline{\Lambda}]^2 \\ &= \tfrac{1}{2}(-5 - \sqrt{5})(-2 + \sqrt{2})[1 + \tfrac{1}{2}(1 - \sqrt{5})(1 + \sqrt{2})]^2 \\ &= 10 - 3\sqrt{10}. \end{aligned}$$

Hence $k' = Q(\sqrt{10 + 3\sqrt{10}})$.

EXAMPLE 2. Now consider $F = Q(\gamma)$ of narrow class number $h^+ = 1$, where $\gamma = \gamma_1$ is the positive zero of $r(x) = x^3 - x - 1$ and γ_2 and γ_3 denote the complex ones. The group U_F^+ of totally positive units is seen to be generated by γ. Choose square roots $\gamma_1^{1/2}$, $\gamma_2^{1/2}$, $\gamma_3^{1/2}$ with $\gamma_2^{1/2} \cdot \gamma_3^{1/2} = \gamma_1^{-1/2} > 0$. The extension $K = Q(\gamma_1^{1/2}, \gamma_2^{1/2}, \gamma_3^{1/2})$ has dihedral Galois group $G = D_4$ over F generated by automorphisms σ and τ in (1) satisfying

$$\begin{aligned} &\sigma\colon\ \gamma_1^{1/2} \to -\gamma_1^{1/2}, \quad \gamma_2^{1/2} \to \gamma_3^{1/2}, \quad \gamma_3^{1/2} \to -\gamma_2^{1/2} \qquad \text{and} \\ &\tau\colon\ \gamma_1^{1/2} \to \gamma_1^{1/2}, \quad \gamma_2^{1/2} \to \gamma_3^{1/2}, \quad \gamma_3^{1/2} \to \gamma_2^{1/2}. \end{aligned}$$

The field fixed by $\langle\tau\rangle$ is $R = F(\gamma_1^{1/2}, \gamma_2^{1/2} + \gamma_3^{1/2})$ that by $\langle\sigma\rangle$ is $k = F(\gamma_1^{1/2}(\gamma_2 - \gamma_3))$. The element $\alpha = \gamma_2^{1/2} + \gamma_3^{1/2}$ satisfies the minimal polynomial $p(x) = x^4 + 2\gamma x^2 + (4 - 3\gamma^2)$ in (8) with splitting field K over F. Choosing $\lambda = \gamma_1^{1/2}(\gamma_2 - \gamma_3)$ in Proposition 1, we deduce that the resolvent field for $p(x)$ is $k' = F(i\gamma_1^{1/2}(\gamma_2 - \gamma_3))$. Direct computation of β_1 and β_{-1} from the Lagrange resolvents $\omega_1(\alpha)$ and $\omega_{-1}(\alpha)$ in (5) yields

$$\beta_{\pm 1} = 64(7\gamma^2 - 8 \pm 4i(\gamma_2 - \gamma_3)/\gamma_1^{1/2}).$$

The extension k/F is of conductor $\mathfrak{f} = 4(\gamma_2 - \gamma_3)^2 = 4(4 - 3\gamma^2)$, where $4 - 3\gamma^2$ generates the unique unramified prime above 23 in F. To determine the resolvent field k' from classfield theory using (11), let χ and ψ be the quadratic numerical characters of F realized modulo $4(4 - 3\gamma^2)$ which are induced by extending the Kronecker symbols $(\frac{\gamma}{\mathfrak{p}})$ and $(\frac{4-3\gamma^2}{\mathfrak{p}})$, and setting

$$\chi(\eta) = \left(\frac{\gamma}{(\eta)}\right) \quad \text{and} \quad \psi(\eta) = \left(\frac{4 - 3\gamma^2}{(\eta)}\right) \quad \text{for } \eta > 0.$$

Since χ and ψ annihilate U_F^+ and $h^+ = 1$, it follows from classfield theory (chiefly Theorem 3 [4]) that

$$[1] = \{(\eta) | \chi \circ \psi(\eta) = 1\,, \eta > 0\} \quad \text{and}$$
$$[\tau] = \{(\eta) | \chi \circ \psi(\eta) \neq 1\,, n > 0\}$$

in (9) where $\mathscr{m} = (4(4-3\gamma^2))$. Let ρ be the quadratic numerical character of F, realized modulo 4, satisfying $\rho(\eta) \equiv N_{F/Q}\eta \pmod 4$. Then we find the sets $[\phi]$ in (11) are

$$[\phi_{1,1}] = \{(\eta) | \chi \circ \psi(\eta) = 1\,,\ \rho(\eta) = 1 \text{ and } \eta > 0\} \quad \text{and}$$
$$[\phi_{\tau,-1}] = \{(\eta) | \chi \circ \psi(\eta) \neq 1\,,\ \rho(\eta) \neq 1 \text{ and } \eta > 0\}.$$

In particular, we have $\mathscr{B} = \{(\eta) | \chi \circ \psi \circ \rho(\eta) = 1\,,\ \eta > 0\}$ with corresponding classfield $k' = F(i\gamma_1^{1/2}(\gamma_2 - \gamma_3))$ since $\rho(\eta) = (-1/(\eta))$ for $n > 0$.

The resolvent field k' for $p(x)$ over F can be expressed as a compositum of resolvent fields (one for each of the splitting fields K_i $(1 \le i \le t)$ in (3)) in a manner consistent with the decomposition $k = \prod k_i$. To see this, let $W_i = \{\phi_{t,s} | s \equiv \theta(\tau) \mod n_i\}$ with fixed field k_i' $(1 \le i \le t)$. Now each $k_i' \subset k_i(\zeta^{n/n_i})$ since $k_i(\zeta^{n/n_i})$ corresponds through Galois theory to the subgroup $\{\phi_{\tau,1} | \theta(\tau) \equiv 1 \pmod{n_i}\}$ $(1 \le i \le t)$. Suppose $\alpha^{(i)}$ is a generator for R_i/F (and thus for K_i/k_i) of zero trace in (5), and form the resolvents

$$\omega_\nu^{(i)} = \alpha^{(i)} + \zeta^{-\nu n/n_i}\sigma(\alpha^{(i)}) + \cdots + \zeta^{-\nu(n_i-1)n/n_i}\sigma^{(n_i-1)}(\alpha^{(i)}) \qquad (\nu \in Z). \tag{13}$$

Set $\beta_\nu^{(i)} = (\omega_\nu^{(i)})^{n_i}$ for $\nu \in Z$, and

$$\alpha_\mu^{(i)} = \frac{1}{n_i}\sum_{\nu=1}^{n_i-1} \zeta^{\mu\nu n/n_i}\omega_\nu^{(i)} = \sigma^\mu(\alpha^{(i)}) \qquad (\mu \in Z_{n_i}), \tag{14}$$

for $1 \le i \le t$. Using an argument analogous to that in the proof of Lemma 1, one finds the $\beta_\nu^{(i)}$ are fixed by each $\phi_{\tau,s}$ in W_i and thus lie in k_i' $(1 \le i \le t)$). The minimal polynomial $p_i(x)$ over F for $\alpha^{(i)}$ has splitting field K_i and resolvent field k_i' over F. Since $W = \bigcap W_i$, the resolvent field k' is the compositum $\prod_{i=1}^t k_i'$. In addition, $\alpha = \prod \alpha^{(i)}$ is a generator for R/F of zero trace.

In the next section we take up the construction of the fields R_i, determining suitable generators $\alpha^{(i)}$ and computing their minimal polynomial $p_i(x)$ over F.

3. Construction of $K = k \cdot R$ when $[R : F]$ is a prime power. Here we retain the notation and setup of the previous sections, but with $n = l^u$ a prime power. In this section we shall describe how to construct arbitrary extensions $K = k \cdot R$ with $K \cap Q(\zeta) = Q$ and Galois group G satisfying (1). (The methods can be adapted to construct such extensions K where $K \cap Q(\zeta) \neq Q$, but require more delicate treatment.) Under the assumption $K \cap Q(\zeta) = Q$, one recalls that $G(k(\zeta)/F) = \{\phi_{\tau,s} | \tau \in V,\ s \in Z_n^*\}$, so that the values $\sum_{\nu \in Z_n^*} \zeta^{\mu\nu} \beta_\nu$ $(0 \leq \mu < n)$ are readily seen to all lie in k. In addition, we have

$$\sigma^\lambda(\omega_\nu) = \zeta^{\nu\lambda}\omega_\nu \qquad (\nu \in Z) \tag{15}$$

in (5). We may further assume that $\omega_\nu = 0$ for $(\nu, n) > 1$ by replacing α with $\alpha - \frac{1}{l}(\alpha_0 + \alpha_{l^{u-1}} + \cdots + \alpha_{(l-1)l^{u-1}})$ if necessary in (5), since

$$\begin{aligned}\omega_\nu\left(\alpha - \tfrac{1}{l}\sum_{t=0}^{l-1}\alpha_{tl^{u-1}}\right) &= \omega_\nu\left(\alpha - \frac{1}{l}\sum_{t=0}^{l-1}\sigma^{tl^{u-1}}(\alpha))\right) \\ &= \omega_\nu(\alpha) - \omega_\nu(\alpha)\left[\tfrac{1}{l}\sum_{t=0}^{l-1}\zeta^{\nu t l^{u-1}}\right]\end{aligned}$$

equals $\omega_\nu(\alpha)$ if $l \nmid \nu$ else zero when $l | \nu$ from (6) and (15). We shall henceforth assume that this normalization has been made. Finally we note that if $\tilde{\phi}$ is any extension of $\phi_{\tau,s}$ to $K(\zeta)$ which fixes R, then $\tilde{\phi}(\omega_\nu) = \omega_{\nu s\theta(\tau^{-1})}$ from the proof of Lemma 1. Thus we find that $\tilde{\alpha} = \frac{1}{n}\sum_{\nu \in Z_n^*} \omega_\nu^r$ lies in R; in fact, $R = F(\tilde{\alpha})$ if $(r, n) = 1$.

We now describe how to construct arbitrary extensions $K = k \cdot R$ as above with $K \cap Q(\zeta) = Q$ and Galois group G satisfying (1). Explicit examples will be constructed later in §4.

First choose an irreducible polynomial $q(x)$ of degree $\phi(n)$ over F with Galois group isomorphic to $H = Z_n^*$ and splitting field k'. Consider an explicit isomorphism

$$\psi\colon G(k'/F) \cong H, \tag{16}$$

and label the element ρ_r of $G(k'/F)$ so that $\phi(\rho_r) = r$. Choose a zero ε of $q(x)$, and label its conjugates

$$\varepsilon_r = \rho_r(\varepsilon) \qquad (r \in H). \tag{17}$$

Assume the ε_r satisfy the condition

$$\prod_{t\in H} \varepsilon_t^{r_t} \text{ is an } n\text{th power in } k' \text{ only if the } r_t \text{ are all congruent modulo } n, \tag{18}$$
$$\text{or } \sum_{t\in H} tr_t \equiv 0 \pmod{n} \text{ when } n = l.$$

Finally, fix an ordering for the elements of $H = Z_n^*$. Select a function $f: H \to Z$ which sends a given residue class to some specified integer representing that class, and for which the group matrix

$$A = (a_{s,t}) \qquad (s, t \in H), \tag{19}$$

with $a_{s,t} = f(st^{-1})$, has an inverse, say B. (We note that it is easy to find such functions f.) Set

$$\beta_\nu = \prod_{t\in H} \varepsilon_t^{a_{\nu,t}} \qquad (\nu \in H). \tag{20}$$

For this choice, note that $\rho_r(\beta_\nu) = \beta_{\nu r}$ for ν and r in H, since

$$\rho_r(\beta_\nu) = \prod_{t\in H} \rho_r(\varepsilon_t)^{a_{\nu,t}} = \prod_{t\in H} \varepsilon_{rt}^{a_{\nu,t}} = \prod_{t\in H} \varepsilon_{rt}^{a_{\nu r,tr}} = \prod_{t\in H} \varepsilon_t^{a_{\nu r,t}}.$$

With the above choices we have

Proposition 3. *Suppose the elements β_ν $(\nu \in H)$ are selected as in (20), where the ε_t satisfy condition* (18). *Then the extension $k'(\zeta, \beta_\nu^{1/n} | \nu \in H)$ is cyclic of degree n over $k'(\zeta)$.*

Proof. Note that $\prod_{\nu\in H} \beta_\nu^{r_\nu}$ is an nth power in k'
if and only if $\prod_{\nu\in H}\prod_{t\in H} \varepsilon_t^{a_{\nu,t}^{r_\nu}}$ is an nth power in k'
if and only if $\prod_{t\in H} \varepsilon_t^{\sum_{\nu\in H} a_{\nu,t} r_\nu}$ is an nth power in k'.
Since $\sum_{\nu\in H} a_{\nu,t} r_\nu \equiv \sum_{\nu\in H} \nu t^* r_\nu \equiv t^* \sum_{\nu\in H} \nu r_\nu \pmod{n}$ for $t \in H$ from (19), it follows from (18) and (20) that $\prod_{\nu\in H} \beta_\nu^{r_\nu}$ is an nth power in k' if and only if

$$\sum_{\nu\in H} \nu r_\nu \equiv 0 \pmod{n}. \tag{21}$$

It follows from (21) that for a given $\nu \in H$,

$$\beta_\nu = \beta_1^\nu \cdot \gamma^n \tag{22}$$

for some γ in k'. Also $\beta_1^{r_1}$ lies in $(k')^n$ if and only if $r_1 \equiv 0 \pmod{n}$. In particular, $k'(\zeta, \beta_\nu^{1/n} | \nu \in H) = k'(\zeta, \beta_1^{1/n})$, and the conclusion of the proposition follows.

To proceed with the construction, fix a generator σ for $k'(\zeta, \beta_\nu^{1/n}|\nu \in H)$ over $k'(\zeta)$. It follows from the proposition above that $\beta_t^{1/n}$ generates $k'(\zeta, \beta_\nu^{1/n}|\nu \in H)$ over $k'(\zeta)$ for any t in H. Choose particular nth roots $\beta_t^{1/n}$ so that $\sigma(\beta_t^{1/n}) = \zeta^t \beta_t^{1/n}$ $(t \in H)$, and set

$$\alpha_\mu = \frac{1}{n} \sum_{\substack{t=1 \\ (t,n)=1}} \zeta^{\mu t} \beta_t^{1/n} \qquad (\mu \in Z). \tag{23}$$

The values α_μ in (23) are distinct and comprise a complete set of conjugates over F. In particular $\alpha = \alpha_0$ generates an extension R over F of degree n with Lagrange resolvents (5) satisfying

$$\omega_\nu = \begin{cases} \beta_\nu^{1/n} & \text{if } l \nmid \nu, \\ 0 & \text{if } l|\nu. \end{cases} \tag{24}$$

The minimal polynomial $p(x)$ for α has splitting field K, which we assert is the compositum $k \cdot R$ for a certain abelian extension k/F. We shall determine the abelian extension k from classfield theory. Suppose k'/F has conductor $\mathscr{f}'$ and $\mathscr{m} = LCM(\mathscr{f}', nO_F)$. If $\mathscr{C}$ is the group of fractional F-ideals prime to $\mathscr{m}$, then k'/F corresponds through classfield theory to a subgroup $\mathscr{B}$ of index $\phi(n)$ in $\mathscr{C}$. In particular, $\mathscr{C}/\mathscr{B} \cong G(k'/F)$ via the Artin map

$$[r] \to \rho_r \qquad (r \in H), \tag{25}$$

where $[r]$ denotes the coset of $\mathscr{C}/\mathscr{B}$ set to ρ_r in $G(k'/F)$. We assume that the isomorphism ψ in (16) is chosen so that the sets

$$\mathscr{B}_r = \{\alpha \in [r] | \mathscr{N}\mathscr{a} \equiv r \mod n\} \neq \varnothing \tag{26}$$

for each r in H. (Note that this can always be arranged; in the extreme case $k' = F(\zeta)$, the map ψ is the inverse of the Artin map of $F(\zeta)/F$. The following result specifies how to obtain k and determine $G = G(K/F)$.

THEOREM 1. *The set* $\mathscr{A} = \bigcup_{r \in H} \mathscr{B}_r$ *is a subgroup of* $\mathscr{C}$ *with corresponding classfield* k/F. *The splitting field* $K = k \cdot R$ *with Galois group* G, *a semi-direct product of* T *by* V, *where* $T = \langle \sigma|_K \rangle$ *has fixed field* k *and* $V = G(K/R)$ *is isomorphic to a subgroup of* Z_n^*. *Furthermore, the group* G *satisfies* (1), *where for any* τ *in* V, *the value* $\theta(\tau)$ *is the unique* s *in* H *for which* $[\phi_{\tau,s}] \subset B$ *in* (11)

Proof. Evidently $\mathscr{A}$ is a subgroup of $\mathscr{C}$, and thus corresponds through classfield theory to an abelian extension k/F. In addition,

$\mathscr{A} \cap \mathscr{B} = \mathscr{B}_1 = [\phi_{1,1}]$ so the corresponding classfields $k \cdot k' = k'(\zeta) = k(\zeta)$. Since $\mathscr{A}\mathscr{B} = \mathscr{C}$ we have the following diagram of subfields of $k(\zeta)$ and corresponding subgroups of $\mathscr{C}$:

$$(3) \qquad \begin{tikzcd}[column sep=small] & k(\zeta) \arrow[dl, dash] \arrow[dr, dash] & & \longleftrightarrow & & \mathscr{B}_1 \arrow[dl, dash] \arrow[dr, dash] & \\ k \arrow[dr, dash] & & k' \arrow[dl, dash] & & \mathscr{A} \arrow[dr, dash] & & \mathscr{B} \arrow[dl, dash] \\ & F & & \longleftrightarrow & & \mathscr{C} & \end{tikzcd}$$

In particular, $[k(\zeta) : k] = [\mathscr{A} : \mathscr{B}_1] = \phi(n)$ so $k \cap F(\zeta) = F$ and $G(k/F) \cong G(k'(\zeta)/k') \cong \mathscr{B}/\mathscr{B}_1$. Since $\mathscr{B}_r \neq \varnothing$ and $[r] \to \rho_r$ via the Artin map of k'/F, there exists an extension $\overline{\rho}_r$ of ρ_r to $k'(\zeta) = k(\zeta)$, in fact to $K(\zeta)$, which maps

$$(27) \qquad \zeta \to \zeta^r \quad \text{and} \quad \omega_\nu \to \omega_{\nu r} \qquad (r \in H).$$

Now K is the field fixed by the $\overline{\rho}_r$ $(r \in H)$. But since the $\overline{\rho}_r$ fix k, it follows that $k \subset K$, in fact, with $G(K/k) = \langle \sigma|_K \rangle$. Also $K \cap F(\zeta) = F$. In particular, we have the following correspondence from Galois theory

$$(3) \qquad \begin{tikzcd}[column sep=small] & K \arrow[dl, dash] \arrow[dr, dash] & & \longleftrightarrow & & 1 \arrow[dl, dash] \arrow[dr, dash] & \\ k \arrow[dr, dash] & & R \arrow[dl, dash] & & T = \langle \sigma|_K \rangle \arrow[dr, dash] & & V \arrow[dl, dash] \\ & F & & \longleftrightarrow & & G & \end{tikzcd}$$

Since no $\sigma|_K \neq 1$ fixes R, we find that $K = k \cdot R$ and $V = G(K/R) \cong G(k/F)$. It follows that G is a semi-direct product of T by V, so that the relation

$$\tau\sigma|_K\tau^{-1} = \sigma|_K^{\theta(\tau)} \qquad (\tau \in V)$$

defines a homomorphism $\theta \colon V \to Z_n^*$ as in (1). The map θ is injective since K is the splitting field for R; thus V is isomorphic to some subgroup of Z_n^*.

To complete the proof of the theorem it remains to specify the range of θ. Recall from (11) how $\mathscr{B}$ is constructed from certain cosets $[\phi]$ in $\mathscr{C}$. It follows from (10) that for a given τ in V, the set $[\tau] \cap \mathscr{B}$ coincides with exactly one of the cosets $[\phi_{\tau,s}]$ $(s \in H)$; namely, that for which $s = \theta(\tau)$.

To aid in the computation of k, we introduce the following corollary.

COROLLARY 1. *Let $h(x)$ be any irreducible polynomial of degree $\phi(n)$ over F with splitting field k'. Select a zero δ of $h(x)$ and label its conjugates*

$$\delta_r = \rho_r(\delta) \qquad (r \in H) \tag{28}$$

as in (17). *Then the elements $N_\nu = \sum_{\mu\in H} \zeta^{\mu\nu}\delta_\mu$ $(\nu \in H)$ all lie in the classfield k.*

Proof. Since $N_\nu \in k(\zeta)$ it suffices to show that each map $\overline{\rho}_r$ $(r \in H)$, described by (27), fixes N_ν. But $\overline{\rho}_r(N_\nu) = \sum_{\mu\in H} \zeta^{\mu\nu r}\delta_{\mu r} = \sum_{\mu\in H} \zeta^{\mu\nu}\delta_\mu$ for any r, ν in H.

To compute the minimal polynomial

$$p(x) = x^n + a_2x^{n-2} + \cdots + a_n \tag{29}$$

for $\alpha = \alpha_0$ in (6), we introduce a counting function

$$N(x_1, \ldots, x_t) = \sum\nolimits' \zeta^{x_1u_1+\cdots+x_tu_t} \tag{30}$$

for non-negative integers $x_1, \ldots, x_t$. The primed sum is taken over all t-tuples $(u_1, \ldots, u_t)$ with integral components u_i $(1 \le i \le t)$ pairwise mutually distinct and in the range $[0, n)$. The counting function (30) has the following iterative property.

PROPOSITION 4.

$$N(x_1) = \begin{cases} n & \textit{if } x_1 \equiv 0 \pmod{n}, \\ 0 & \textit{if } x_1 \not\equiv 0 \pmod{n}. \end{cases} \tag{31}$$

For $t > 1$,

$$N(x_1, \ldots, x_t) = \begin{cases} (n-t+1)N(x_1, \ldots, x_{t-1}) & \\ \qquad\qquad\qquad\qquad \textit{if } x_t \equiv 0 \pmod{n}, & \\ -N(x_1 + x_t, \ldots, x_{t-1}) & \\ -\cdots - N(x_1, \ldots, x_{t-1} + x_t) \quad \textit{otherwise}. & \end{cases} \tag{32}$$

Proof. Formula (31) is obvious. To verify (32) when $x_t \equiv 0 \pmod{n}$, we first note that there are $n - t + 1$ choices for the value u_t in any tuple $(u_1, u_2, \ldots, u_t)$ in the primed sum, once the first $t-1$ components have been selected. Since $\zeta^{x_1u_1+\cdots+x_{t-1}u_{t-1}} = \zeta^{x_1u_1+\cdots+x_tu_t}$ in this case, evidently $N(x_1, \ldots, x_t) = (n-t+1)N(x_1, \ldots, x_{t-1})$. Now if $x_t \neq 0 \pmod{n}$ then $\sum_{u=0}^{n-1} \zeta^{ux_t} = 0$. Since $\sum' \zeta^{u_1x_1+\cdots+u_tx_t}$ equals

$$\sum{}' \zeta^{u_1x_1+\cdots+u_{t-1}x_{t-1}} \left(\sum \zeta^{u_tx_t}\right) - \sum{}' \zeta^{u_1(x_1+x_t)+\cdots+u_{t-1}x_{t-1}} \\ - \cdots - \sum{}' \zeta^{u_1x_1+\cdots+u_{t-1}(x_{t-1}+x_t)}$$

we find that (32) holds when $x_t \not\equiv 0 \pmod{n}$.

Corollary 2. (i) *If* $x_1 + \cdots + x_t \not\equiv 0 \pmod{n}$ *then* $N(x_1, \ldots, x_t) = 0$.

(ii) *If* $x_1 + \cdots + x_t$ *sums to zero* $(\mathrm{mod}\ n)$ *but no smaller subset sums to zero* $(\mathrm{mod}\ n)$ *then* $N(x_1, \ldots, x_t) = (-1)^{t-1}(t-1)!n$ *for* $t \geq 1$.

We shall omit the proof of the corollary since both (i) and (ii) follow easily from (31) and (32) by using induction on t.

We are ready to determine the coefficient of $p(x)$.

Theorem 2. *The coefficient* a_m $(2 \leq m \leq n)$ *for the term* x^{n-m} *is a sum of all terms of the form*

$$\frac{(-1)^m}{n^m} \beta_{t_1}^{c_1/n} \cdots \beta_{t_e}^{c_e/n} N(\underbrace{t_1, \ldots, t_1}_{c_1 \text{ times}}, \ldots, \underbrace{t_e, \ldots, t_e}_{c_e \text{ times}})/(c_1! \cdots c_e!) \tag{33}$$

where $t_i \in H$, $1 \leq c_i \leq m$ *for* $1 \leq i \leq e$ *with* $\sum_{i=1}^{e} c_i = m$ *and* $\sum_{i=1}^{e} c_it_i \equiv 0 \pmod{n}$. *Each term* $\beta_{t_1}^{c_1/n} \cdots \beta_{t_e}^{c_e/n}$ *which appears is a product of the elements* ε_r.

Proof. Now

$$p(x) = \prod_{\mu=0}^{n-1}(x - \alpha_\mu) = \prod_{\mu=0}^{n-1}\left(x - \frac{1}{n}\sum \zeta^{\mu t}\beta_t^{1/n}\right),$$

where the sum is over t in H. Expanding the product, we find that each term that appears in the expressions for a_m is of the form $\beta_{t_1}^{c_1/n} \cdots \beta_{t_e}^{c_e/n}$, where $c_1 + \cdots + c_e = m$, with multiplier

$$\frac{(-1)^m}{n^m} \sum{}' \zeta^{(u_{1,1}+\cdots+u_{1,c_1})t_1+\cdots+(u_{e,1}+\cdots+u_{e,c_e})t_e}. \tag{34}$$

Here the primed sum is over m-tuples $(u_{1,1}, \ldots, u_{e,c_e})$ in $[0, n)^m$ with mutually distinct components and ordered so

$$u_{1,1} < u_{1,2} < \cdots < u_{1,c_1}, \ldots, u_{e,1} < u_{e,2} < \cdots < u_{e,c_e}.$$

But (34) equals the multiplier of $\beta_{t_1}^{c_1/n} \cdots \beta_{t_e}^{c_e/n}$ in (33) above, and the terms for which $\sum_{i=1}^{e} c_i t_i \not\equiv 0 \pmod{n}$ have multiplier equal zero by Corollary 2. The terms with $\sum_{i=1}^{e} c_i t_i \equiv 0 \pmod{n}$ satisfy

$$\beta_{t_1}^{c_1/n} \cdots \beta_{t_e}^{c_e/n} = \prod_{i=1}^{e} \prod_{\nu \in H} \varepsilon_\nu^{a_{t_i,\nu} c_i/n} = \prod_{\nu \in H} \varepsilon_\nu^{r_\nu}, \tag{35}$$

where

$$r_\nu = \frac{1}{n} \sum_{i=1}^{e} a_{t_i,\nu} c_i . \tag{36}$$

But $a_{t_i,\nu} \equiv t_i \nu^* \pmod{n}$ so $\sum_{i=1}^{e} a_{t_i,\nu} c_i \equiv \nu^* \sum_{i=1}^{e} t_i c_i \equiv 0 \pmod{n}$; hence the r_ν are integers in (35). (Here ν^* is the multiplicative inverse of $\nu \pmod{n}$).

For $n = 3, 4, 5, 7$ and 8 and indicated choice of matrix A in (19), we obtain the following expressions for the coefficients of $p(x)$. (Here N and Tr denote the norm and trace from k' to F respectively.)

(37) $n = 3$:

$$A = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}, \quad B = \frac{1}{3} \begin{bmatrix} -1 & 2 \\ 2 & -1 \end{bmatrix},$$
$$a_2 = -(N\varepsilon)/3, \quad a_3 = -(N\varepsilon)(\mathrm{Tr}\,\varepsilon)/27;$$

(38) $n = 4$:

$$A = \begin{bmatrix} 1 & 3 \\ 3 & 1 \end{bmatrix}, \quad B = \frac{1}{8} \begin{bmatrix} -1 & 3 \\ 3 & -1 \end{bmatrix},$$
$$a_2 = -(N\varepsilon)/4, \quad a_3 = 0, \quad a_4 = (2N\varepsilon^2 - \mathrm{Tr}\,\beta)/64;$$

(39) $n = 5$:

$$A = \begin{bmatrix} 1 & 3 & -1 & 2 \\ 2 & 1 & 3 & -1 \\ -1 & 2 & 1 & 3 \\ 3 & -1 & 2 & 1 \end{bmatrix}, \quad B = \frac{1}{5} \begin{bmatrix} 1 & 0 & -1 & 1 \\ 1 & 1 & 0 & -1 \\ -1 & 1 & 1 & 0 \\ 0 & -1 & 1 & 1 \end{bmatrix},$$

$$\begin{aligned} a_2 &= -(\varepsilon_1\varepsilon_4 + \varepsilon_2\varepsilon_3)/5, \quad a_3 = -\mathrm{Tr}(\varepsilon_1\varepsilon_2\varepsilon_3)/25, \\ a_4 &= -(\mathrm{Tr}(\varepsilon_1\varepsilon_2^2\varepsilon_3) + N\varepsilon - (\varepsilon_1^2\varepsilon_4^2 + \varepsilon_2^2\varepsilon_3^2))/125, \\ a_5 &= -(\mathrm{Tr}(\beta - 5\varepsilon_1\varepsilon_2^2\varepsilon_3^2) + 5(N\varepsilon)\cdot\mathrm{Tr}\,\varepsilon)/3125; \end{aligned}$$

(40) $n=7$:

$$A=\begin{bmatrix} 1 & -2 & 4 & -1 & 2 & 3 \\ 3 & 1 & -2 & 4 & -1 & 2 \\ 2 & 3 & 1 & -2 & 4 & -1 \\ u-1 & 2 & 3 & 1 & -2 & 4 \\ 4 & -1 & 2 & 3 & 1 & -2 \\ -2 & 4 & -1 & 2 & 3 & 1 \end{bmatrix},$$

$$B=\frac{1}{7}\begin{bmatrix} 0 & 1 & 1 & 0 & 0 & -1 \\ -1 & 0 & 1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 1 & 1 & 0 \\ 0 & 0 & -1 & 0 & 1 & 1 \\ 1 & 0 & 0 & -1 & 0 & 1 \\ 1 & 1 & 0 & 0 & -1 & 0 \end{bmatrix},$$

$$\begin{aligned}
a_2 &= -(\varepsilon_1\varepsilon_6+\varepsilon_2\varepsilon_5+\varepsilon_3\varepsilon_4)/7,\\
a_3 &= -[2(\varepsilon_1\varepsilon_2\varepsilon_4+\varepsilon_3\varepsilon_5\varepsilon_6)+\mathrm{Tr}(\varepsilon_2\varepsilon_4\varepsilon_5)]/49,\\
a_4 &= -[-(\varepsilon_2\varepsilon_3\varepsilon_4\varepsilon_5+\varepsilon_1\varepsilon_2\varepsilon_5\varepsilon_6+\varepsilon_1\varepsilon_3\varepsilon_4\varepsilon_6)\\
&\qquad +\mathrm{Tr}(\varepsilon_1\varepsilon_4\varepsilon_5\varepsilon_2^2/\varepsilon_3+3\varepsilon_1\varepsilon_2\varepsilon_4\varepsilon_5)-2(\varepsilon_2^2\varepsilon_5^2+\varepsilon_1^2\varepsilon_6^2+\varepsilon_3^2\varepsilon_4^2)]/343,\\
a_5 &= -[\mathrm{Tr}(\varepsilon_1\varepsilon_4\varepsilon_5^2\varepsilon_2^2/\varepsilon_3+2\varepsilon_1\varepsilon_2^2\varepsilon_4^2\varepsilon_5/\varepsilon_6\\
&\qquad -3\varepsilon_2^2\varepsilon_4\varepsilon_5^2-\varepsilon_1\varepsilon_5^2\varepsilon_2\varepsilon_6-2\varepsilon_1\varepsilon_2^2\varepsilon_4\varepsilon_5)+5(N\varepsilon)\,\mathrm{Tr}(\varepsilon^{-1})]/2401,\\
a_6 &= -7^{-5}[\mathrm{Tr}(\varepsilon_1\varepsilon_4^2\varepsilon_5^2\varepsilon_2^3/\varepsilon_3\varepsilon_6-\varepsilon_2^2\varepsilon_5^2\varepsilon_4^2-2\varepsilon_1\varepsilon_4\varepsilon_5^2\varepsilon_2^3/\varepsilon_3+3\varepsilon_1\varepsilon_2\varepsilon_5^2\varepsilon_4\varepsilon_6\\
&\qquad +3\varepsilon_1^2\varepsilon_2^2\varepsilon_4\varepsilon_5\varepsilon_6/\varepsilon_3-\varepsilon_1\varepsilon_2^2\varepsilon_4\varepsilon_5^2-\varepsilon_1\varepsilon_2^2\varepsilon_5\varepsilon_4^2\\
&\qquad +2\varepsilon_1\varepsilon_2\varepsilon_3\varepsilon_4^2\varepsilon_5-5\varepsilon_1^2\varepsilon_2\varepsilon_4\varepsilon_5\varepsilon_6)\\
&\qquad +(\varepsilon_2^3\varepsilon_5^3+\varepsilon_1^3\varepsilon_6^3+\varepsilon_3^3\varepsilon_4^3)+(\varepsilon_1^2\varepsilon_2^2\varepsilon_4^2+\varepsilon_3^2\varepsilon_5^2\varepsilon_6^2)\\
&\qquad +2(\varepsilon_1\varepsilon_2^2\varepsilon_5^2\varepsilon_6+\varepsilon_2\varepsilon_3^2\varepsilon_4^2\varepsilon_5+\varepsilon_3\varepsilon_1^2\varepsilon_6^2\varepsilon_4)\\
&\qquad -5(\varepsilon_2^2\varepsilon_3\varepsilon_4\varepsilon_5^2+\varepsilon_1^2\varepsilon_2\varepsilon_5\varepsilon_6^2+\varepsilon_3^2\varepsilon_1\varepsilon_6\varepsilon_4^2)+15(N\varepsilon)],\\
a_7 &= 7^{-7}[\mathrm{Tr}(-\beta+7\varepsilon_1\varepsilon_5^3\varepsilon_4\varepsilon_2^3/\varepsilon_3+7\varepsilon_1\varepsilon_4^2\varepsilon_5^2\varepsilon_2^3/\varepsilon_3-14\varepsilon_1\varepsilon_2^2\varepsilon_5^2\varepsilon_4^2\\
&\qquad -7\varepsilon_1\varepsilon_2^3\varepsilon_4^2\varepsilon_5^2/\varepsilon_6-7\varepsilon_1^2\varepsilon_2^2\varepsilon_4\varepsilon_5^2\varepsilon_6/\varepsilon_3-7\varepsilon_1^2\varepsilon_2^3\varepsilon_4^2\varepsilon_5/\varepsilon_3\\
&\qquad -7\varepsilon_2^3\varepsilon_4\varepsilon_5^3-7\varepsilon_1\varepsilon_2^2\varepsilon_4\varepsilon_5^2\varepsilon_6+21\varepsilon_1^2\varepsilon_2^2\varepsilon_4^2\varepsilon_5+21\varepsilon_2^2\varepsilon_5^2\varepsilon_4^2\varepsilon_3\\
&\qquad +21\varepsilon_1\varepsilon_2^3\varepsilon_4\varepsilon_5^2+7\varepsilon_1\varepsilon_2^2\varepsilon_3\varepsilon_4^3\varepsilon_5/\varepsilon_6+7\varepsilon_1^2\varepsilon_2\varepsilon_4\varepsilon_5^2\varepsilon_6\\
&\qquad -14\varepsilon_1\varepsilon_2^2\varepsilon_5^3\varepsilon_6-14\varepsilon_1\varepsilon_2^2\varepsilon_4^2\varepsilon_5\varepsilon_6\\
&\qquad -35\varepsilon_1\varepsilon_2^2\varepsilon_3\varepsilon_4^2\varepsilon_5+7\varepsilon_1\varepsilon_2^2\varepsilon_3\varepsilon_4\varepsilon_5^2)\\
&\qquad +14(N\varepsilon)\,\mathrm{Tr}\,\varepsilon];
\end{aligned}$$

(41) $n = 8$:

$$A = \begin{bmatrix} 9 & -3 & -1 & 3 \\ -3 & 9 & 3 & -1 \\ -1 & 3 & 9 & -3 \\ 3 & -1 & -3 & 9 \end{bmatrix}, \quad B = \frac{1}{64}\begin{bmatrix} 9 & 3 & -1 & -3 \\ 3 & 9 & -3 & -1 \\ -1 & -3 & 9 & 3 \\ -3 & -1 & 3 & 9 \end{bmatrix},$$

$$\begin{aligned}
a_2 &= -(\varepsilon_1\varepsilon_7 + \varepsilon_3\varepsilon_5)/8, \quad a_3 = a_5 = a_7 = 0, \\
a_4 &= (-2\operatorname{Tr}(\varepsilon_1^3\varepsilon_3) + 5(\varepsilon_1^2\varepsilon_7^2 + \varepsilon_3^2\varepsilon_5^2) \\
&\qquad - 3(\varepsilon_1^3\varepsilon_3^3/\varepsilon_5\varepsilon_7 + \varepsilon_5^3\varepsilon_7^3/\varepsilon_1\varepsilon_3) + 4N\varepsilon)/1024, \\
a_6 &= 8^{-5}[\operatorname{Tr}(-\varepsilon_1^6\varepsilon_3^3/\varepsilon_5^2\varepsilon_7 + 3\varepsilon_1\varepsilon_5\varepsilon_7^4 - 2\varepsilon_1^2\varepsilon_7\varepsilon_3^3 + 2\varepsilon_1^4\varepsilon_3^3/\varepsilon_5) \\
&\qquad - 2(N\varepsilon)(\varepsilon_1\varepsilon_7 + \varepsilon_3\varepsilon_5) - 2(\varepsilon_1^3\varepsilon_7^3 + \varepsilon_3^3\varepsilon_5^3)], \\
a_8 &= 8^{-8}[\operatorname{Tr}(-\beta - 20\varepsilon_1^5\varepsilon_7\varepsilon_3^3/\varepsilon_5 - 8\varepsilon_1^5\varepsilon_7^2\varepsilon_3 - 8\varepsilon_1^6\varepsilon_3^4/\varepsilon_5\varepsilon_7 + 16\varepsilon_1^3\varepsilon_7^2\varepsilon_3^3 \\
&\qquad + 8\varepsilon_1^7\varepsilon_3^3/\varepsilon_5^2 + 4\varepsilon_1^6\varepsilon_3^2) \\
&\qquad + 2(\varepsilon_1^4\varepsilon_7^4 + \varepsilon_3^4\varepsilon_5^4) + 2(\varepsilon_1^6\varepsilon_3^6/\varepsilon_5^2\varepsilon_7^2 + \varepsilon_5^6\varepsilon_7^6/\varepsilon_1^2\varepsilon_3^2) \\
&\qquad - 56(N\varepsilon^2) + 32(N\varepsilon)(\varepsilon_1^2\varepsilon_7^2 + \varepsilon_3^2\varepsilon_5^2) \\
&\qquad + 32(N\varepsilon)(\varepsilon_1^3\varepsilon_3^3/\varepsilon_5\varepsilon_7 + \varepsilon_5^3\varepsilon_7^3/\varepsilon_1\varepsilon_3) - 8(N\varepsilon)\operatorname{Tr}\varepsilon_1^3\varepsilon_3 \\
&\qquad - 6(N\varepsilon)(\varepsilon_3^2\varepsilon_7^2 + \varepsilon_1^2\varepsilon_5^2)].
\end{aligned}$$

It is natural to ask how general is the above construction. In particular, suppose we are given an extension $K = k \cdot R$ of the kind under consideration and a generator α for R over F normalized so that the Lagrange resolvents (5) satisfy $\omega_\nu = 0$ for $(\nu, n) > 1$. Does the construction actually yield the generator $\alpha = \frac{1}{n}\sum_{\nu=1;(\nu,n)=1}^{n} \omega_\nu$ for a suitable choice of elements ε_r in (17)? If not, to what extent can this be done?

We assert that a generator $\tilde{\alpha} = \frac{1}{n}\sum_{\nu=1;(\nu,n)=1}^{n}(\omega_\nu(\alpha))^r$ for R over F is obtainable provided the inverse B for the matrix A in (19) has

(42) $$\operatorname{den} B = r \cdot n \quad \text{with } (r, n) = 1.$$

(Here $\operatorname{den} B$ denotes the least common denominator of the entries of B when written in reduced form.)

Indeed, suppose f is chosen so that the inverse matrix $B = (b_{s,t})$ has $\operatorname{den} B = rn$ with $(r, n) = 1$. Set

(43) $$\tilde{\varepsilon}_\mu = \prod_{t \in H} \omega_t^{rnb_{\mu,t}} \qquad (\mu \in H).$$

It follows from the proof of Lemma 1 and (15), (19) and (42) that the $\tilde{\varepsilon}_\mu$ are fixed by σ and W, so lie in k'. Now, using (43) to obtain values $\tilde{\beta}_\nu$ from (20); that is

$$\tilde{\beta}_\nu = \prod_{\mu\in H} \tilde{\varepsilon}_\mu^{a_{\nu,\mu}} \qquad (\nu \in H). \tag{44}$$

we find that

$$\tilde{\beta}_\nu = \prod_{t\in H}\cdot\prod_{\mu\in H} \omega_t^{rna_{\nu,\mu}b_{\mu,t}} = \prod_{t\in H} \omega_t^{rn(\sum_{\mu\in H} a_{\nu,\mu}b_{\mu,t})} = \omega_\nu^{rn} = \beta_\nu^r$$

for any ν in H. Thus the construction yields a generator $\tilde{\alpha} = \frac{1}{n}\sum \omega_\nu^r$ as claimed. In particular, the original generator α is obtained if the inverse matrix B had den $B = n$. For these cases, the construction yields all generators α for R normalized so $\omega_\nu = 0$ for $(\nu, n) \neq 1$ in (5).

The author has shown that condition (42) can be achieved if and only if $n = l^u$ is odd; moreover, that den $B = n$ can be obtained at least for $n = 3, 5, 7, 9$ and 11, but not for $n = 13$. The proofs of these results involve long, tedious computations with group determinants and will appear elsewhere. (We note that the matrices A in (37), (39) and (40) are so chosen that den $B = n$ holds.)

Before concluding this section, some remarks on constructing extensions with prescribed ramification, e.g., classfields, are in order. For this purpose we require some results from local classfield theory. Let L be any finite abelian extension of a number field M. Fix a prime ideal $\mathfrak{p}$ of M, and choose a prime $\mathfrak{P}$ lying above $\mathfrak{p}$ in L. Let $L_\mathfrak{P}$ and $M_\mathfrak{p}$ be the local extensions at $\mathfrak{P}$ and $\mathfrak{p}$ respectively, and denote the corresponding unit groups by $U_\mathfrak{P}$ and $U_\mathfrak{p}$. It is known [**1, 10, 11**] from local classfield theory that the Galois group $G(L_\mathfrak{P}/M_\mathfrak{p})$ is isomorphic to $M_\mathfrak{p}^\times/N_{L_\mathfrak{P}/M_\mathfrak{p}}(L_\mathfrak{P}^\times)$, where $N_{L_\mathfrak{P}/M_\mathfrak{p}}$ is the local norm map from $L_\mathfrak{P}$ to $M_\mathfrak{p}$. In addition, the inertia group $I(L_\mathfrak{P}/M_\mathfrak{p})$ is isomorphic to $U_\mathfrak{p}/N_{L_\mathfrak{P}/M_\mathfrak{p}}(U_\mathfrak{P})$, say of order $e(\mathfrak{P}:\mathfrak{p})$.

The construction detailed at the beginning of this section yields a generator α for a cyclic extension K over k of degree n which is normal over F and linearly disjoint from $Q(\zeta)$. Any nth root $\beta_\nu^{1/n}$ generates $K(\zeta)$ over $k(\zeta)$. The idea here is to relate the ramification in K/k to that in the Kummer extension $K(\zeta)/k(\zeta)$ where it is easy to determine. For convenience we state the relevant result of Kummer [**10**].

PROPOSITION 5 (*Kummer's criteria*). *Let $L = M(\beta^{1/n})$ for some number field M which contains ζ. Suppose $\mathfrak{p}$ is a prime ideal of M,* *say with uniformizing parameter* π *in* $M_{\wp}$. *Write* $\beta = \gamma \cdot \pi^{v}$ *with* $(\gamma, \pi) = 1$ *in* $M_{\wp}$.

(i) *If* $(\wp, \beta) = (\wp, n) = 1$, *then* $\wp$ *is unramified in* L.

(ii) *If* $(\wp, \beta) > 1$ *but* $(\wp, n) = 1$, *then* $\wp$ *ramifies in* L *if and only if* $n | v$.

(iii) *If* $(\wp, n) > 1$ *but* $(\wp, \beta) = 1$, *then* $\wp$ *ramifies in* L *if and only if* $\beta \notin U_{\wp}^{n}$.

(*Note that determining whether* β *lies in* $U_{\wp}^{n}$ *in statement* (iii) *amounts to checking whether* β *is an* n*th power modulo a suitable power of* $\wp$.)

Now fix a rational prime p and choose a prime ideal $\widetilde{\mathscr{B}}$ lying above p in $K(\zeta)$. Consider the following Hasse diagram of local extensions.

$$\begin{tikzcd}
& K(\zeta)_{\widetilde{\mathscr{B}}} \arrow[dl, dash] \arrow[dr, dash] & \\
k(\zeta)_{\tilde{\wp}} \arrow[dr, dash] & & K_{\mathscr{B}} \arrow[dl, dash] \\
& k_{\wp} \arrow[d, dash] & \\
& Q_p &
\end{tikzcd}$$

Here $\mathscr{B} = \widetilde{\mathscr{B}} \cap K$, $\tilde{\wp} = \widetilde{\mathscr{B}} \cap k(\zeta)$ and $\wp = \widetilde{\mathscr{B}} \cap k$. Consider the homomorphism Ψ from unit quotient groups $U_{\tilde{\wp}} / N_{K(\zeta)_{\widetilde{\mathscr{B}}} / k(\zeta)_{\tilde{\wp}}} U_{\widetilde{\mathscr{B}}}$ to $U_{\wp} / N_{K_{\mathscr{B}} / k_{\wp}} U_{\mathscr{B}}$ given by

$$x \longrightarrow N_{k(\zeta)_{\tilde{\wp}} / k_{\wp}} x \cdot N_{K_{\mathscr{B}} / k_{\wp}} U_{\mathscr{B}}. \tag{45}$$

The map Ψ is injective. Indeed, $N_{k(\zeta)_{\tilde{\wp}} / k_{\wp}} x \in N_{K_{\mathscr{B}} / k_{\wp}} U_{\mathscr{B}}$ if and only if $x \in N^{-1}_{k(\zeta)_{\tilde{\wp}} / k_{\wp}} (N_{K_{\mathscr{B}} / k_{\wp}} U_{\mathscr{B}})$. But, since $K \cap k(\zeta) = k$, this last group $N^{-1}_{k(\zeta)_{\tilde{\wp}} / k_{\wp}} (N_{K_{\mathscr{B}} / k_{\wp}} U_{\mathscr{B}})$ is readily seen, using the translation theorem of local classfield theory **[11]**, to be norm group $N_{K(\zeta)_{\widetilde{\mathscr{B}}} / k(\zeta)_{\tilde{\wp}}} U_{\widetilde{\mathscr{B}}}$. In particular, the ramification index $e(\widetilde{\mathscr{B}} : \tilde{\wp})$ divides $e(\mathscr{B} : \wp)$. In order for Ψ to be onto, it is necessary that

$$N_{k(\zeta)_{\tilde{\wp}} / k_{\wp}} U_{\tilde{\wp}} \cdot N_{K_{\mathscr{B}} / k_{\wp}} U_{\mathscr{B}} = U_{\wp}. \tag{46}$$

In any case,

$$e(\mathscr{B} : \wp) = e(\widetilde{\mathscr{B}} : \tilde{\wp}) \cdot [U_{\wp} : N_{k(\zeta)_{\tilde{\wp}} / k_{\wp}} U_{\tilde{\wp}} \cdot N_{K_{\mathscr{B}} / k_{\wp}} U_{\mathscr{B}}]. \tag{47}$$

For the situation at hand we have

PROPOSITION 6. *If $p \nmid l$ or $p = n = l$, then* $U_{\tilde{\mathfrak{p}}}/(N_{K(\zeta)_{\tilde{\mathscr{B}}}/k(\zeta)_{\tilde{\mathfrak{p}}}} U_{\tilde{\mathscr{B}}}) \cong U_{\mathfrak{p}}/N_{K_{\mathscr{B}}/k_{\mathfrak{p}}} U_{\mathscr{B}}$.

Proof. If $p \nmid l$ then $N_{k(\zeta)_{\tilde{\mathfrak{p}}}/k_{\mathfrak{p}}} U_{\tilde{\mathfrak{p}}} = U_{\mathfrak{p}}$ since $k(\zeta)/k$ is unramified at $\mathfrak{p}$. If $p = n = l$ then $([K : k], [k(\zeta) : k]) = 1$ so $e(\widetilde{\mathscr{B}} : \mathfrak{p}) = e(\mathscr{B} : \mathfrak{p}) e(\tilde{\mathfrak{p}} : \mathfrak{p})$. But $e(\widetilde{\mathscr{B}} : \mathfrak{p}) = e(\widetilde{\mathscr{B}} : \tilde{\mathfrak{p}}) e(\tilde{\mathfrak{p}} : \mathfrak{p})$; hence $e(\widetilde{\mathscr{B}} : \tilde{\mathfrak{p}}) = e(\mathscr{B} : \mathfrak{p})$ so (46) holds. In either case, Ψ is an isomorphism.

It is clear from the above proposition that the problem to construct K/k with specific ramification at $\mathfrak{p}$ is more one of finding β_ν in (20) (actually the ε_r in (17)) so that $k(\zeta, \beta_\nu^{1/n})/k(\zeta)$ has the same ramification at $\tilde{\mathfrak{p}}$ by virtue of Kummer's criteria. Specifying the ramification at $\mathfrak{p}$ in the exceptional case $p = l$ and $n = l^u$ for $u > 1$, requires more careful selection of β. We shall apply these ideas to construct some specific classfields among the examples given in the next section.

4. Some examples. Several examples are given now to exhibit the construction detailed in the previous section.

EXAMPLE 3. Next we wish to apply the construction to find a generator α and minimal polynomial for the unique cyclic field K, which is totally ramified at 7, unramified elsewhere, and of degree 7 over Q. Here $k' = Q(\zeta)$ from Proposition 2 since $k = Q$. Selecting $\varepsilon = \varepsilon_1 = \zeta^{-1}$ in (17) yields $\beta_\nu = \zeta^\nu$ in (20). The element $\beta = \beta_1 = \zeta$ is a unit of $Q(\zeta)$, but not a seventh power in the completion of $Q(\zeta)$ at $(1 - \zeta)$. Thus the extension $Q(\zeta, \beta^{1/7})/Q(\zeta)$ is totally ramified at $(1 - \zeta)$ and unramified elsewhere by Kummer's criteria. Since $e(\widetilde{\mathscr{B}} : \tilde{\mathfrak{p}}) = e(\mathscr{B} : \mathfrak{p}) = 7$ here, it follows that K is generated by

$$7\alpha = \zeta_{49} + \zeta_{49}^{-19} + \zeta_{49}^{-18} + \zeta_{49}^{18} + \zeta_{49}^{19} + \zeta_{49}^{-1}, \qquad \text{where } \zeta = \exp(2\pi i/49),$$

with minimal polynomial $p(x) = x^7 - 21x^5 - 21x^4 + 91x^3 + 112x^2 - 84x - 97$ from (40). Here the particular choice of 7th roots $\beta_\nu^{1/7}$ in (23) is determined by the automorphism σ of $K(\zeta)$ which sends $\zeta_{49} \to \zeta_{49}^8$.

EXAMPLE 4. Here we wish to construct the classfield K/k, where $k = Q(\zeta_{16} + \zeta_{16}^7)$, that was described in Example 1 of the previous section. Since K/k is ramified only at 5, we seek an element β in $k' = Q(\sqrt{10 + 3\sqrt{10}})$ for which $k(\zeta, \beta^{1/5})/k(\zeta)$ is ramified only at the prime $(1 - \zeta)$.

Let ρ be the element of $G(k'/Q)$ sending $\lambda = \sqrt{10+3\sqrt{10}}$ to $\bar{\lambda} = \sqrt{10-3\sqrt{10}}$. Choose ψ in (16) so that $\rho_1 = 1$, $\rho_2 = \rho$, $\rho_3 = \rho^3$ and $\rho_4 = \rho^2$. (One can check that this choice yields the correct field k here from Theorem 1 or its corollary.) Select $\varepsilon = \lambda + 2$ a zero of the polynomial $q(x) = x^4 + 8x^3 + 4x^2 - 48x - 54$. A straightforward calculation shows that the ideal $(\lambda + 2) = \mathfrak{p}_1\mathfrak{p}_1^2\mathfrak{q}$ as a product of primes in k', where $(3) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$ and $(2) = \mathfrak{q}^4$. The primes above 3 are labelled so that $\bar{\rho}_r(\mathfrak{p}_i) = \mathfrak{p}_{ir \pmod 5}$, consistent with that of the ε_r in (17). The element

$$\beta = \beta_1 = -148 + 32\sqrt{10} + \lambda(-686 + 214\sqrt{10}),$$

obtained in (20), generates the ideal $\mathfrak{q}^5\mathfrak{p}_1^5\mathfrak{p}_2^5\mathfrak{p}_4^5$, but is not a fifth power in a completion of $k(\zeta)$ at $(1-\zeta)$. It follows from Kummer's criteria that β may be a suitable choice. By Theorem 1, we find that $\alpha = \frac{1}{5}(\beta_1^{1/5} + \beta_2^{1/5} + \beta_3^{1/5} + \beta_4^{1/5})$ generates some classfield of k of degree 5, and has minimal polynomial $p(x) = x^5 + 12x^3/5 + 48x^2/25 + 282x/125 + 7792/3125$ from (39). Moreover, the Galois group $G = G(k/Q)$ satisfies (1) with $\theta(\tau) = 2$. (Here τ is that generator of V mapping $\zeta_{16} + \zeta_{16}^7$ to $\zeta_{16}^{11} + \zeta_{16}^{13}$ as in Example 1.)

It remains to verify that $k(\alpha) = K$, the desired classfield. However, a straightforward, albeit tedious, computation shows that there are only three admissible ideal groups of k which have conductor divisible only by 5, are invariant under $G(k/Q)$, and have corresponding classfields of degree 5. They are

$$J_1 = \{(\gamma) | \gamma = \alpha \cdot \beta \text{ where } 5 \nmid \alpha\beta,\ \alpha \in (k^x)^5 \text{ and }$$
$$\beta \equiv 1 + 5(\delta + a(1+\sqrt{2})\Lambda) \pmod{5^2}$$
$$\text{for some integer } \delta \in Q(\sqrt{2}) \text{ with } a \in \mathbf{Z}\},$$

$$J_2 = \{(\gamma) | \gamma = \alpha \cdot \beta \text{ where } 5 \nmid \alpha\beta,\ \alpha \in (k^x)^5 \text{ and }$$
$$\beta \equiv 1 + 5(a\sqrt{2} + \delta\Lambda) \pmod{5^2}$$
$$\text{for some integer } \delta \in Q(\sqrt{2}) \text{ with } a \in \mathbf{Z}\} \text{ and}$$

$$J_3 = J = \{(\gamma) | \gamma = \alpha \cdot \beta \text{ where } 5 \nmid \alpha\beta,\ \alpha \in (k^x)^5 \text{ and }$$
$$\beta \equiv 1 + 5(\delta + a(1+2\sqrt{2})\Lambda) \pmod{5^2}$$
$$\text{for some integer } \delta \in Q(\sqrt{2}) \text{ with } \alpha \in \mathbf{Z}\}.$$

The classfield corresponding to J_2 is seen to be $k(\zeta_{25}+\zeta_{25}^7+\zeta_{25}^{-7}+\zeta_{25}^{-1})$, which is actually abelian over Q.

Now the norm $\eta = N_{K/k}(\Lambda - 5\alpha) = \Lambda^5 + 60\Lambda^2 + 240\Lambda^2 + 1410\Lambda + 7792 \equiv 12 - 10\sqrt{2} + \Lambda(-4 + 6\sqrt{2}) \mod 25$. Multiplying by the fifth power $\mu = [-7 - 7\sqrt{2} + \Lambda(-9 + 6\sqrt{2})]^5 \equiv -7 + 7\sqrt{2} + 9\Lambda \mod 25$, yields $\eta\mu \equiv 1 + 5[1 + 2\sqrt{2} - (1 + 2\sqrt{2})\Lambda] \bmod 25$. Since (η) lies in J, it follows that $k(\alpha) = K$.

EXAMPLE 5. The quadratic field $k = Q(\sqrt{-47})$ has class number $h = 5$, and hence admits an unramified extension K of degree 5 which is normal over Q, with dihedral Galois group D_5. It is easy to determine that k' is generated by $(\zeta - \zeta^4)\sqrt{-47} = \sqrt{47\eta\sqrt{5}}$, where $\eta = (1 + \sqrt{5})/2$, upon choosing $\lambda = \sqrt{-47}$ in Proposition 1. To construct K/k we seek, in view of Proposition 5, an element $\beta = \beta_1$ in k' for which $k(\zeta, \beta^{1/5})$ is unramified everywhere over $k(\zeta)$. Select $\varepsilon = \varepsilon_1 = -\frac{1}{4}[47 - 5\sqrt{5} + (-5 + \sqrt{5})\sqrt{47\eta\sqrt{5}}]$, a unit in k'. The element ε has minimal polynomial $q(x) = x^4 + 47x^3 + 519x^2 - 47x + 1$ and conjugates

$$\begin{aligned}
\varepsilon_2 &= -\tfrac{1}{4}[47 + 5\sqrt{5} - (5 + \sqrt{5})\sqrt{-47\bar{\eta}\sqrt{5}}],\\
\varepsilon_3 &= -\tfrac{1}{4}[47 + 5\sqrt{5} + (5 + \sqrt{5})\sqrt{-47\bar{\eta}\sqrt{5}}],\\
\varepsilon_4 &= -\tfrac{1}{4}[47 - 5\sqrt{5} - (-5 + \sqrt{5})\sqrt{47\eta\sqrt{5}}]
\end{aligned}$$

in (17). The corresponding β from (20) and (39) are

$$\begin{aligned}
\beta_1 &= \tfrac{1}{4}[9353 + 4225\sqrt{5} - (715 + 325\sqrt{5})\sqrt{47\eta\sqrt{5}}],\\
\beta_2 &= \tfrac{1}{4}[9353 - 4225\sqrt{5} + (715 - 325\sqrt{5})\sqrt{-47\bar{\eta}\sqrt{5}}],\\
\beta_3 &= \tfrac{1}{4}[9353 - 4225\sqrt{5} - (715 - 325\sqrt{5})\sqrt{-47\bar{\eta}\sqrt{5}}],\\
\beta_4 &= \tfrac{1}{4}[9353 + 4225\sqrt{5} + (715 + 325\sqrt{5})\sqrt{47\eta\sqrt{5}}].
\end{aligned}$$

Since β is a unit in $k(\zeta)$, and also a fifth power in the completion at $(1 - \zeta)$, we find that $k(\zeta, \beta^{1/5})$ is unramified over $k(\zeta)$. Thus the element $\alpha = \frac{1}{5}(\beta_1^{1/5} + \beta_2^{1/5} + \beta_3^{1/5} + \beta_4^{1/5})$ generates K/k and has minimal polynomial $p(x) = x^5 + 2x^3/5 - 47x^2/25 + 522x/125 - 9353/3125$ from (39). (This is essentially the construction of H. Hasse **[9]** for the Hilbert classfield of $Q(\sqrt{-47})$.)

EXAMPLE 6. Here we wish to use the construction to find a generator α and its minimal polynomial for the unique cyclic field K, which is totally ramified at 11, unramified elsewhere, and of degree 5 over Q. Here $k' = Q(\zeta)$ as in Example 5. Set $\lambda = \zeta - \zeta^4 = \sqrt{-\sqrt{5}\eta}$ and $\lambda = \zeta^2 - \zeta^3 = -\bar{\eta}\sqrt{-\sqrt{5}\eta}$ in $Q(\zeta)$, where $\eta = (1 + \sqrt{5})/2$. Selecting ψ in

(16) to be the inverse of the Artin map of $Q(\zeta)/Q$ and $\varepsilon = (5+\eta\lambda)/2$ in (17), yields $\beta = \beta_1 = \frac{1}{44}(90 - 17\sqrt{5})(50+\lambda(-5+19\sqrt{5}))$ in (20). The element β is a fifth power in the completion of $Q(\zeta)$ at $(1-\zeta)$, but not a global fifth power, and has norm 55^5. Using Kummer's criteria, $Q(\zeta, \beta^{1/5})/Q(\zeta)$ is found to be totally ramified at each prime lying above 11, but unramified elsewhere. Hence it follows that K is generated by $\alpha = \frac{1}{5}(\beta_1^{1/5}+\beta_2^{1/5}+\beta_3^{1/5}+\beta_4^{1/5})$ with minimal polynomial $p(x) = x^5 - 3x^3 - 3x^2 - x - 1/11$ from (29). The zeros of $p(x)$ can be expressed solely in terms of real numbers. It is easy to check that the zeros are just the conjugates of $(\zeta_{11} + \zeta_{11}^{-1} - 1)/(2 - \zeta_{11} - \zeta_{11}^{-1})$.

EXAMPLE 7. To illustrate the construction of classfields for which $F \neq Q$, consider the extension $k = Q(\sqrt[4]{2})$ of $F = Q(\sqrt{2})$. One finds that k has narrow class number one (so does F), that $\{1+\sqrt[4]{2}, 1-\sqrt[4]{2}\}$ is a fundamental system for the units of k and that $\{1, \sqrt[4]{2}, \sqrt{2}, \sqrt[4]{8}\}$ is an integral basis. The totally positive units of k are generated by $1+\sqrt{2}$ and $(1+\sqrt[4]{2})^2$. In addition, k/F is seen to correspond through classfield theory to the congruence group

$$(48)\quad \{(x) | x > 0,\ x \equiv 1, 3, \pm 1 - \sqrt{2}, \pm 3 + \sqrt{2}, \\ 3 + 2\sqrt{2},\ 1 + 2\sqrt{2} \bmod 4\sqrt{2}\}$$

of conductor $\mathscr{f} = (4\sqrt{2})$. (The set (48) contains precisely those ideals for which the extended Kronecker symbol $(\sqrt{2}/\mathscr{a}) = 1$.)

The field k admits an ideal group J defined modulo $\mathscr{M} = (5^2)$ consisting of principal ideals generated by elements γ prime to $\mathscr{M}$ and of the form $\gamma = \alpha \cdot \beta$ for some $\alpha \in (k^x)^5$ and $\beta \equiv 1 + 5(a + b\sqrt{2} + c\sqrt[4]{8}) \bmod \mathscr{M}$ with $a, b, c \in Z$. The ideal group J corresponds to a classfield K which is normal over F with $[K : k] = 5$. The Galois group $G = G(K/F)$ is a semi-direct product of the form (1), say with generator σ for $T = G(K/k)$ for which $[\sigma^j] = (1+5j\sqrt{2})J$ $(0 \leq j \leq 4)$ in (4). Also, since $\tau(\sqrt[4]{2}) = -\sqrt[4]{2}$, we have $\tau[\sigma^j] = [\sigma^{-j}]$ so G is dihedral. (A straightforward, but tedious, computation shows that J is the only admissible ideal group of k which has conductor divisible only by 5, is invariant under $G(k/F)$ and has corresponding classified K with $G(K/F) = D_5$.)

To determine the resolvent field k', we choose $\lambda = \sqrt[4]{2}$ in Proposition 1 to find $E_{-1}^2 = [(\zeta - \zeta^4)\sqrt[4]{2}]^2 = -\eta\sqrt{10}$ where $\eta = (1+\sqrt{5})/2$. Hence $k' = F(i\sqrt{\sqrt{10}\eta})$. Realizing (48) modulo $\mathscr{m} = 20\sqrt{2}$, we find the sets $[\phi]$ in (11) are

$$\begin{aligned}[\phi_{1,1}] = \{(x)|x>0,\ x \equiv 1, 9, 11, 19, \pm 1 - 5\sqrt{2}, 1 + 10\sqrt{2},\\ 3 \pm 2\sqrt{2}, \pm 3 - 3\sqrt{2}, \pm 3 - 7\sqrt{2}, 3 \pm 8\sqrt{2},\\ \pm 7 + 3\sqrt{2}, \pm 7 + 7\sqrt{2}, -7 \pm 8\sqrt{2}, 7 \pm 2\sqrt{2}, 9 + 10\sqrt{2},\\ \pm 9 - 5\sqrt{2}, \pm 11 + 5\sqrt{2}, 11 + 10\sqrt{2}, -13 \pm 2\sqrt{2},\\ \pm 13 - 3\sqrt{2}, \pm 13 - 7\sqrt{2}, -13 \pm 8\sqrt{2},\\ 17 \pm 2\sqrt{2}, \pm 17 + 3\sqrt{2}, 17 \pm 8\sqrt{2}, \pm 17 + 7\sqrt{2},\\ \pm 19 + 5\sqrt{2}, 19 + 10\sqrt{2} \bmod 20\sqrt{2}\}\end{aligned}$$

and

$$\begin{aligned}[\phi_{\tau,-1}] = \{(x)|x>0,\ x \equiv -3, 7, 13, -17, -1 \pm 4\sqrt{2},\\ -1 \pm 6\sqrt{2}, \pm 1 + 9\sqrt{2}, \pm 1 + \sqrt{2}, \pm 3 - 5\sqrt{2}, -3 - 10\sqrt{2},\\ \pm 7 + 5\sqrt{2}, 7 - 10\sqrt{2}, \pm 9 + \sqrt{2}, -9 \pm 4\sqrt{2}, \pm 9 + 9\sqrt{2},\\ -9 \pm 6\sqrt{2}, \pm 11 - \sqrt{2}, \pm 11 + 4\sqrt{2}, -11 + 6\sqrt{2},\\ \pm 11 - 9\sqrt{2}, 13 - 10\sqrt{2}, \pm 13 - 5\sqrt{2}, \pm 17 + 5\sqrt{2},\\ -17 - 10\sqrt{2}, \pm 19 - 6\sqrt{2}, -19 \pm 6\sqrt{2}, -19 \pm 4\sqrt{2},\\ \pm 19 - 9\sqrt{2} \bmod 20\sqrt{2}\}.\end{aligned}$$

The classfield corresponding to $\mathscr{B} = [\phi_{1,1}] \cup [\phi_{\tau,-1}]$ must be $k' = F(i\sqrt{\sqrt{10}\eta})$.

Now to construct K/k we seek a suitable element β in k' for which $k(\zeta, \beta^{1/5})/k(\zeta)$ is ramified only at the prime $(1-\zeta)$ lying above 5. Let ρ be the element of $G(k'/F)$ sending $\Lambda = i\sqrt{\sqrt{10}\eta}$ to $\overline{\Lambda} = \frac{i}{\eta}\sqrt{\sqrt{10}\eta}$ and choose ψ in (16) so that $\rho_1 = 1$, $\rho_2 = \rho$, $\rho_3 = \rho^3$ and $\rho_4 = \rho^2$. (This choice of ψ yields the correct field k in Theorem 1 or its corollary.) Select $\varepsilon = \varepsilon_1 = \sqrt{2} - \sqrt{5}\eta + 2\Lambda$, a unit of k' and zero of the irreducible polynomial $q(x) = x^4 + (10 - 4\sqrt{2})x^3 + (47 + 10\sqrt{2})x^2 + (30 + 2\sqrt{2})x + (99 + 70\sqrt{2})$. Its conjugates in (17) are $\varepsilon_2 = \sqrt{2} - \sqrt{5}\overline{\eta} + 2\Lambda/\eta$, $\varepsilon_3 = \sqrt{2} - \sqrt{5}\overline{\eta} - 2\Lambda/\eta$, and $\varepsilon_4 = \sqrt{2} - \sqrt{5}\eta - 2\Lambda$. The corresponding $\beta = \beta_1$, from (20) and (39) is

$$\begin{aligned}&\tfrac{1}{2}((-89325 + 64303\sqrt{2}) + \sqrt{5}(40007 - 28715\sqrt{2}))\\ &\quad + \Lambda((32737 - 22440\sqrt{2}) + \sqrt{5}(-14651 + 10028\sqrt{2})).\end{aligned}$$

Since β is not a fifth power in the completion of $k(\zeta)$ at $(1-\zeta)$, we find from Theorem 1 that $\alpha = \frac{1}{5}(\beta_1^{1/5} + \beta_2^{1/5} + \beta_3^{1/5} + \beta_4^{1/5})$ generates some classfield of k of degree 5. This classfield must be K in view of the parenthetical remark made about J. From (39), α has minimal polynomial

$$\begin{aligned} p(x) = x^5 - (19 + 10\sqrt{2})/5x^3 + (30 + 2\sqrt{2})/25x^2 \\ + (38 + 20\sqrt{2})/125x + (179900 - 127256\sqrt{2})/3125. \end{aligned}$$

Example 8. In this final illustration, we wish to apply the construction to find a generator α and minimal polynomial for the real subfield K of $Q(\zeta_{17})$. Again $k' = Q(\zeta)$ since $k = Q$. Selecting $\varepsilon_r = 2 + \zeta^r$ in (41) yields

$$\begin{aligned} \beta = \beta_1 &= (4 + i)^2(3 + 2i\sqrt{2})^4(4 + i + 2\sqrt{2} + 2i\sqrt{2})^4/17^3, \\ \beta_2 &= (4 - i)^2(3 + 2i\sqrt{2})^4(4 - i - 2\sqrt{2} + 2i\sqrt{2})^4/17^3, \\ \beta_3 &= (4 + i)^2(3 - 2i\sqrt{2})^4(4 + i - 2\sqrt{2} - 2i\sqrt{2})^4/17^3, \\ \beta_4 &= (4 - i)^2(3 - 2i\sqrt{2})^4(4 - i + 2\sqrt{2} - 2i\sqrt{2})^4/17^3 \end{aligned}$$

in (20). Now it follows from Proposition 5 that $Q(\zeta, \beta^{1/8})/Q(\zeta)$ is totally ramified at each $Q(\zeta)$-prime lying above 17, and unramified at other primes except possibly at $(1 + \zeta)$ lying above 2. Hcwever, it can be checked that β is an eighth power in the completion of $Q(\zeta)$ at $(1 + \zeta)$. For any $Q(\zeta)$-prime $\mathfrak{p}$ lying above 17, we have $e(\tilde{\mathfrak{p}} : \mathfrak{p}) = 8$, so (46) holds. As K is the unique cyclic field with such ramification, it is generated by $\alpha = \frac{1}{8}(\beta_1^{1/8} + \beta_3^{1/8} + \beta_5^{1/8} + \beta_7^{1/8})$ for our construction. The minimal polynomial for α is $p(x) = x^8 - 20x^6/(2^4) + 1986x^4/(2^8 \cdot 17) - 50256x^2/(2^{12} \cdot 17^2) + 300304/(2^{16} \cdot 17^3)$ from (41), and has zeros

$$\pm \frac{1}{4\sqrt{17}} \sqrt{(85 \pm \sqrt{17}) \mp \sqrt{4777 + 409\sqrt{17}}}$$

expressed solely in terms of real numbers.

References

[1] E. Artin and J. Tate, *Classfield Theory*, Benjamin, New York, 1968.

[2] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York, 1966.

[3] L. E. Dickson, *Elementary Theory of Equations*, Wiley, New York.

[4] S. Gurak, *Ideal-theoretic characterization of the relative genus field*, J. Reine Angew. Math., **296** (1977), 119–125.

[5] ——, *On the representation theory for full decomposable forms*, J. Number Theory, **13**, no. 4 (1981), 421–442.

[6] ——, *Cubic and Biquadratic Pseudoprimes of Lucas Type*, in Number Theory (edited by J. M. De Koninck & C. Levesque), Walter de Gruyter, Berlin, 1989.
[7] ——, *Minimal polynomials for circular numbers*, Pacific J. Math., **112**, no. 2 (1984), 313–331.
[8] ——, *Pseudoprimes for higher order linear recurrence sequences*, Math. Comp., **55**, no. 192 (1990), 783–813.
[9] H. Hasse, *Uber den Klassenkorper zum quadratischen Zahlkorper mit diskriminante* -47, Acta. Arith., **9** (1964), 419–434.
[10] S. Iyanaga, *Class-Field Theory Notes*, Univ. of Chicago, 1961.
[11] G. Janusz, *Algebraic Number Fields*, Academic Press, New York, 1973.
[12] J. Rotman, *The Theory of Groups*, Allyn & Bacon, Boston, 1970.
[13] B. Setzer, *The determination of all imaginary quartic Abelian number fields with class number* 1, Math. Comp., **35**, no. 152 (1980), 1383–1386.
[14] B. L. van der Waerden, *Modern Algebra*, vol. I, Unger, New York, 1949.

Received August 5, 1991 and in revised form October 1, 1991.

University of San Diego
San Diego, CA 92110-2492

PACIFIC JOURNAL OF MATHEMATICS

Founded by

E. F. BECKENBACH (1906–1982) F. WOLF (1904–1989)

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be in typed form or offset-reproduced (not dittoed), double spaced with large margins. Please do not use built up fractions in the text of the manuscript. However, you may use them in the displayed equations. Underline Greek letters in red, German in green, and script in blue. The first paragraph must be capable of being used separately as a synopsis of the entire paper. In particular it should contain no bibliographic references. Please propose a heading for the odd numbered pages of less than 35 characters. Manuscripts, in triplicate, may be sent to any one of the editors. Please classify according to the 1991 *Mathematics Subject Classification* scheme which can be found in the December index volumes of *Mathematical Reviews.* Supply name and address of author to whom proofs should be sent. All other communications should be addressed to the managing editor, or Julie Speckart, University of California, Los Angeles, California 90024-1555.

There are page-charges associated with articles appearing in the Pacific Journal of Mathematics. These charges are expected to be paid by the author's University, Government Agency or Company. If the author or authors do not have access to such Institutional support these charges are waived. Single authors will receive 50 free reprints; joint authors will receive a total of 100 free reprints. Additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* (ISSN 0030-8730) is published monthly except for July and August. Regular subscription rate: $190.00 a year (10 issues). Special rate: $95.00 a year to individual members of supporting institutions.

Subscriptions, orders for numbers issued in the last three calendar years, and changes of address should be sent to Pacific Journal of Mathematics, P.O. Box 969, Carmel Valley, CA 93924, U.S.A. Old back numbers obtainable from Kraus Periodicals Co., Route 100, Millwood, NY 10546.

The Pacific Journal of Mathematics at P.O. Box 969, Carmel Valley, CA 93924 (ISSN 0030-8730) is published monthly except for July and August. Second-class postage paid at Carmel Valley, California 93924, and additional mailing offices. Postmaster: send address changes to Pacific Journal of Mathematics, P.O. Box 969, Carmel Valley, CA 93924.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

PACIFIC JOURNAL OF MATHEMATICS

Volume 157 No. 2 February 1993