ILLINOIS JOURNAL OF MATHEMATICS
Volume 33, Number 4, Winter 1989

GENERALIZED CYCLOTOMIC FIELDS

BY

STEPHEN BEALE AND D.K. HARRISON

This note examines the splitting field $K \subseteq \mathbf{C}$ over $\mathbf{Q}$ of the set of polynomials of the form $X^n - b$, with $n \in \mathbf{N}^*$ and $b \in \mathbf{Q}$. We obtain the Galois group $\mathrm{Aut}_{\mathbf{Q}}(K)$ as a natural subgroup of a semidirect product of the Pontryagin dual of a quotient of the divisible hull of the positive rationals and the automorphism group of the maximal abelian extension of the rationals.

Section 1

Let R denote the Pontryagin dual $\mathrm{Hom}(\mathbf{Q}/\mathbf{Z}, \mathbf{Q}/\mathbf{Z})$ of $\mathbf{Q}/\mathbf{Z}$. For each $n \in \mathbf{N}^*$ and $r \in R$ there is an integer k, uniquely determined modulo $n\mathbf{Z}$, such that

$$r\left(\frac{1}{n} + \mathbf{Z}\right) = \frac{k}{n} + \mathbf{Z}.$$

We denote the class of k mod $n\mathbf{Z}$ by $j_n(r)$ and observe that $r \mapsto j_n(r)$ is a ring homomorphism of R onto $\mathbf{Z}/n\mathbf{Z}$ with kernel nR. If we write $\bar{j}_n$ for the induced $R/nR \to \mathbf{Z}/n\mathbf{Z}$, then these maps interact properly with the natural epimorphisms $R/nR \to R/mR$ and $\mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z}$ when m divides n (i.e., the diagram

$$\begin{array}{ccc} R/nR & \xrightarrow{\bar{j}_n} & \mathbf{Z}/n\mathbf{Z} \\ \downarrow & & \downarrow \\ R/mR & \xrightarrow{\bar{j}_m} & \mathbf{Z}/m\mathbf{Z} \end{array}$$

commutes), allowing us to identify the corresponding projective limits R and $\hat{\mathbf{Z}}$ (= the Prüfer ring $\varprojlim_n \mathbf{Z}/n\mathbf{Z}$). With the Krull topology (for which the sets $N_A = \{f \in R \mid f(a) = 0, \forall a \in A\}$ form a basis of neighborhoods of the identity when A ranges over finite subsets of $\mathbf{Q}/\mathbf{Z}$), R is a profinite group. The units $U(R) = \mathrm{Aut}(\mathbf{Q}/\mathbf{Z})$ of R form a closed subspace of R in which multiplication and inversion are continuous (in the relative topology) and hence $U(R)$

Received December 21, 1987.

is itself a profinite group. We also have the map

$$\alpha \mapsto e^{2\pi i\alpha}$$

of $\mathbf{Q}$ into $\mathbf{C}$ with kernel $\mathbf{Z}$; we write C for its image and ζ_n for the image of $1/n$, and we denote by ω the inverse of the induced isomorphism $\mathbf{Q}/\mathbf{Z} \to C$.

For B a discrete abelian group, there is a natural isomorphism

$$\operatorname{Hom}(B \otimes \mathbf{Q}/\mathbf{Z}, \mathbf{Q}/\mathbf{Z}) \to \operatorname{Hom}(B, R);$$

we give $\operatorname{Hom}(B, R)$ the strongest topology making this map continuous; here we take $B \otimes \mathbf{Q}/\mathbf{Z}$ to be discrete and we let $\operatorname{Hom}(B \otimes \mathbf{Q}/\mathbf{Z}, \mathbf{Q}/\mathbf{Z})$ have the Krull topology so that $\operatorname{Hom}(B \otimes \mathbf{Q}/\mathbf{Z}, \mathbf{Q}/\mathbf{Z})$ and hence $\operatorname{Hom}(B, R)$ are profinite groups. We note that $U(R)$ acts on $\operatorname{Hom}(B, R)$ by

$$(r, f) \to r \circ f$$

and that this action is continuous as a map from $U(R) \times \operatorname{Hom}(B, R)$ into $\operatorname{Hom}(B, R)$. It follows that with the product topology the semidirect product $\operatorname{Hom}(B, R) \rtimes U(R)$ is a topological group; the multiplication is given by

$$(f, r)(g, s) = (f + r \cdot g, rs),$$

for all $f, g \in \operatorname{Hom}(B, R)$, $r, s \in U(R)$. Furthermore since both $\operatorname{Hom}(B, R)$ and $U(R)$ are compact, Hausdorff, and totally disconnected, so is their product, and therefore the semidirect product is a profinite group.

When B is free abelian we have a surjection

$$\eta_*\colon \operatorname{Hom}(B, R) \to \operatorname{Hom}(B, R/2R)$$

induced by the projection $\eta\colon R \to R/2R$, and we give $\operatorname{Hom}(B, R/2R)$ the strongest topology making η_* continuous. Assume B is so and let $\lambda\colon U(R) \to \operatorname{Hom}(B, R/2R)$ be a continuous group homomorphism. We define B_λ to be the subset

$$B_\lambda = \{(f, r) \in \operatorname{Hom}(B, R) \rtimes U(R) | \lambda(r) = \eta_*(f)\}$$

of $\operatorname{Hom}(B, R) \rtimes U(R)$. Bearing in mind that the class modulo $2R$ of an element $r \in R$ is determined completely by its restriction to $\frac{1}{2}\mathbf{Z}/\mathbf{Z}$ and that if r is a unit of R, $r|_{\frac{1}{2}\mathbf{Z}\setminus\mathbf{Z}}$ must be the identity, one checks that the continuous map

$$(f, r) \mapsto \lambda(r) - \eta_*(f)$$

of $\operatorname{Hom}(B, R) \rtimes U(R)$ into $\operatorname{Hom}(B, R/2R)$ is in fact a group homomorphism. As the kernel of this map, B_λ is a closed subgroup of $\operatorname{Hom}(B, R) \rtimes U(R)$ and hence is a profinite group.

Section 2

Let E be the maximal abelian extension in $\mathbf{C}$ of $\mathbf{Q}$; this is the smallest subfield of $\mathbf{C}$ containing the roots of all polynomials of the form $X^n - 1$ with $n \in \mathbf{N}^*$. Write B for the multiplicative group of positive rational numbers; this is a free abelian group with basis the set S of prime numbers. For each $n \in \mathbf{N}^*$, $k \in \mathbf{Z}$, and $b \in B$, the polynomial $X^n - b^k$ has exactly one positive real root; we denote this root by $b^{k/n}$ and we write $\mathscr{D}$ for the set of all such roots, F for the field $\mathbf{Q}[\mathscr{D}]$, and K for $E[\mathscr{D}] = E \cdot F$. K is the splitting field of the set of polynomials $x^n - b$, $n \in \mathbf{N}^*$, $b \in B$. Denote its Galois group over $\mathbf{Q}$ by Γ.

For p a prime number and k a unit of $\mathbf{Z}/p\mathbf{Z}$ we define the symbol (k/p) in $R/2R$ to be 0 if k is a square in $\mathbf{Z}/p\mathbf{Z}$ and to be 1 otherwise; $k \mapsto (k/p)$ is then a group homomorphism from $U(\mathbf{Z}/p\mathbf{Z})$ to $R/2R$. For $r \in U(R)$ we define $\lambda(r) \in \mathrm{Hom}(B, R/2R)$ on elements of the basis S of B by

$$\lambda(r)(p) = \begin{cases} 0 & \text{if } p = 2 \text{ and } j_8(r) = \pm 1 + 8\mathbf{Z}, \\ 1 & \text{if } p = 2 \text{ and } j_8(r) = \pm 3 + 8\mathbf{Z}, \\ \left(\dfrac{j_p(r)}{p}\right) & \text{if } p \equiv 1 \pmod 4, \\ & \text{or if } p \equiv 3 \pmod 4 \text{ and } j_4(r) = 1 + 4\mathbf{Z}, \\ 1 + \left(\dfrac{j_p(r)}{p}\right) & \text{if } p \equiv 3 \pmod 4 \text{ and } j_4(r) = 3 + 4\mathbf{Z}, \end{cases}$$

where $j_n\colon R \to \mathbf{Z}/n\mathbf{Z}$ is the map defined in §1. One checks with little difficulty that $\lambda\colon r \mapsto \lambda(r)$ is a continuous group homomorphism of $U(R)$ into $\mathrm{Hom}(B, R/2R)$. It is B_λ that we are after.

THEOREM 2.1. *With B and λ defined as above*, $\Gamma \cong B_\lambda$.

Proof. For $\sigma \in \Gamma$, $b \in B$, and $\alpha \in \mathbf{Q}$, the number $\sigma(b^\alpha)/b^\alpha$ is a root of unity which depends only on the class of α modulo $\mathbf{Z}$; b^α is to be interpreted as the unique positive real root of $x^n - b^k$, where $\alpha = k/n$, $k \in \mathbf{Z}$, $n \in \mathbf{N}^*$. Define $\mu\colon \Gamma \to \mathrm{Hom}(B, R)$ by'

$$\sigma \mapsto \left(b \mapsto \left(\alpha + \mathbf{Z} \mapsto \omega\left(\sigma(b^\alpha)/b^\alpha\right)\right)\right),$$

and $\nu\colon \Gamma \to U(R)$ by

$$\sigma \mapsto \omega\sigma|_C\omega^{-1}.$$

It is straightforward to check that ν is a continuous group epimorphism and that μ is a well defined continuous map satisfying

$$\mu(\tau\sigma) = \mu(\tau) + \nu(\tau)\mu(\sigma), \quad \forall \tau, \sigma \in \Gamma$$

(i.e., μ is a derivation when $\mathrm{Hom}(B, R)$ is considered a Γ-module through ν). One notes that this is exactly what is needed to insure that $\varphi\colon \Gamma \to \mathrm{Hom}(B, R) \rtimes U(R)$ defined by

$$\sigma \mapsto (\mu(\sigma), \nu(\sigma))$$

is a group homomorphism. One checks that the kernel of φ is trivial, and with the aid of the quadratic Gauss sums

$$\sqrt{p} = \begin{cases} \zeta_8 + \zeta_8^7 & \text{if } p = 2, \\ \sum_{i=1}^{p-1} \left(\frac{i}{p}\right) \zeta_p^i & \text{if } p \equiv 1 \pmod 4, \\ \sum_{i=1}^{p-1} \left(\frac{i}{p}\right) \zeta_{4p}^{4i+3p} & \text{if } p \equiv 3 \pmod 4) \end{cases}$$

(see [1], pp. 70–75; here (i/p) is the ordinary Legendre symbol with values in $U(\mathbf{Z}) = \{\pm 1\}$), one sees that the diagram

$$\begin{array}{ccc} \Gamma & \xrightarrow{\nu} & U(R) \\ {\scriptstyle \mu}\downarrow & & \downarrow{\scriptstyle \lambda} \\ \mathrm{Hom}(B, R) & \xrightarrow[\eta_*]{} & \mathrm{Hom}(B, R/2R) \end{array}$$

commutes; it follows immediately that φ has its image in B_λ. In order to show that its image is all of B_λ, we will identify K with a quotient of the group algebra $E(D)$ over E of the divisible hull $D = B \otimes \mathbf{Q}$ of B. The $\mathbf{Q}$ here is the additive group of rationals. D is an abelian group which we write multiplicatively, and for $d \in D$ we let u_d denote the basis element of $E(D)$ corresponding to d. Since B is free abelian, the inclusions $\mathbf{Z} \to \mathbf{Q}$ and $\frac{1}{2}\mathbf{Z} \to \mathbf{Q}$ induce injections

$$B \cong B \otimes \mathbf{Z} \to D \quad \text{and} \quad B \otimes \tfrac{1}{2}\mathbf{Z} \to D$$

which we use to identify B and $B_1 = B \otimes \frac{1}{2}\mathbf{Z}$ with subgroups of D.

For $b \in B$ and $\alpha \in \mathbf{Q}$ we have defined above the element $b^\alpha \in F$; the map

$$(b, \alpha) \mapsto b^\alpha$$

is $\mathbf{Z}$-bilinear from $B \times \mathbf{Q}$ into the units of K and so induces a group homomorphism $D \to U(K)$ which in turn determines a surjective E-algebra homomorphism

$$\theta\colon E(D) \to K = EF.$$

Note that $\theta(\{u_d | d \in B_1\}) \subseteq E \cap F$ so $\theta(u_d)u_1 \in E(D)$ when $d \in B_1$. We will show that the kernel of this map is the ideal $\mathfrak{a}$ of $E(D)$ generated by the set

$$T = \{u_d - \theta(u_d)u_1 | d \in B_1\}$$

and thereby obtain an isomorphism $\bar{\theta}\colon E(D)/\mathfrak{a} \to K$.

We note that D/B_1 is a torsion abelian group and hence is the union of its finite subgroups; from this it follows that $E(D)$ is the union of its subalgebras $E(H)$ where H ranges over subgroups of D containing B_1 as a subgroup of finite index (one uses here the fact that the set of such H is directed by inclusion). Hence to show that $\mathfrak{a}$ is the kernel of θ it will be enough to show that for any such H the kernel of $\theta_H = \theta|_{E(H)}$ is $E(H) \cdot T$. So let H be a subgroup of D with $B_1 \leq H$ and with $\{h_1, \dots, h_t\}$ a set of B_1-coset representatives in H. Then in the terminology of [2], the field $L = E[\theta(h_1), \dots, \theta(h_i)]$ is a pure, separable, and coseparable extension of E and hence Cogalois over E. If $\theta(h_i)$ and $\theta(h_j)$ represent the same element of the Cogalois group $\mathrm{Cog}(L|E) =$ torsion subgroup of $U(L)/U(E)$, then h_i and h_j represent the same coset of B_1 (one checks) which implies that $i = j$. It follows that $\theta(h_1)U(E), \dots, \theta(h_t)U(E)$ are distinct elements of $\mathrm{Cog}(L|E)$ and hence that $\theta(h_1), \dots, \theta(h_t)$ are linearly independent over E. This implies $\dim_E(L) \geq t$.

We next observe that vectors $u_{h_1} + E(H) \cdot T, \dots, u_{h_t} + E(H) \cdot T$ span $E(H)/E(H) \cdot T$ as a vector space over E, and hence

$$\dim_E(E(H)/E(H) \cdot T) \leq t.$$

Now since T and hence $E(H) \cdot (T)$ are included in the kernel of θ_H, and since $L \cong E(H)/\mathrm{Ker}(\theta_h)$, we have

$$t \leq \dim_E(L) = \det_E(E(H)/\mathrm{Ker}(\theta_H)) \leq \det_E(E(H)/E(H) \cdot T) \leq t,$$

which implies $E(H) \cdot T = \mathrm{Ker}(\theta_H)$. This shows that $\mathfrak{a}$ is the kernel of θ and gives us the isomorphism

$$\bar{\theta}\colon E(D)/\mathfrak{a} \to K.$$

We now complete the proof of the theorem by showing that φ maps Γ onto B_λ. Let $(f, r) \in B_\lambda$. The map

$$(b, \alpha) \mapsto \omega^{-1}(f(b)(\alpha + \mathbf{Z}))u_{b \otimes \alpha}$$

of $B \times \mathbf{Q}$ into the units of $E(D)$ is $\mathbf{Z}$-bilinear so induces a group homomorphism

$$D = B \otimes \mathbf{Q} \to U(E(D))$$

which induces an E-algebra homomorphism

$$\hat{\sigma}: E(D) \to E(D).$$

Since $\tau \mapsto \tau|_C$ is an isomorphism of $\mathrm{Aut}(E)$ onto $\mathrm{Aut}(C)$, there is a unique element $\bar{r} \in \mathrm{Aut}(E)$ extending $\omega^{-1}r\omega \in \mathrm{Aut}(C)$. Define $\tilde{\sigma}$: $E(D) \to E(D)$ by

$$\sum e_d u_d \mapsto \sum \bar{r}(e_d)\hat{\sigma}(u_d).$$

One uses quadratic Gauss sums as above to check that $\tilde{\sigma}$ maps T (and hence $\mathfrak{a}$) into $\mathfrak{a}$. Thus we get an E-algebra homomorphism (taking 1 to 1) $\bar{\sigma}$: $E(D)/\mathfrak{a} \to E(D)/\mathfrak{a}$, and since $E(D)/\mathfrak{a} \cong K$ is a field, $\bar{\sigma}$ is an automorphism. Finally we let $\sigma_{f,r}$ be the composition $\bar{\theta}\bar{\sigma}\bar{\theta}^{-1}$ and check that $\mu(\sigma_{f,r}) = f$ and $\nu(\sigma_{f,r}) = r$ to complete the proof. □

Section 3

We turn now to a consideration of subfields of K which are finite dimensional over the rationals, focusing on a family of these fields with the property that every such subfield is included in some one in our family.

We call a positive integer n *indicial* and write $n \in \mathrm{Ind}$ if 8 divides n whenever n has a prime divisor congruent to 2 or 3 mod 4. These will be cofinal in an upcoming inverse limit. For n indicial we write $S(n)$ for the set of prime divisors of n and $s(n)$ for the cardinality of $S(n)$. We define the nth indicial polynomial to be

$$\Omega_n = \prod_{p \in S(n)} (X^n - p)$$

and let K_n denote the splitting field in K of Ω_n over $\mathbf{Q}$ and Γ_n the Galois group of K_n over $\mathbf{Q}$. We also set $E_n = \mathbf{Q}[\zeta_n]$ and $F_n = \mathbf{Q}[S(n)^{1/n}]$, where $S(n)^{1/n} = \{p^{1/n} | p \in S(n)\}$, and we observe that $K_n = E_n F_n$ and that $E = \bigcup_{n \in \mathrm{Ind}} E_n$, that $F = \bigcup_{n \in \mathrm{Ind}} 1 F_n$, and that $K = \bigcup_{n \in \mathrm{Ind}} K_n$. Furthermore if n, m are indicial then so is their least common multiple $[n, m]$, and $E_n E_m = E_{[n,m]}$, $F_n F_m \subseteq F_{[n,m]}$, and $K_n K_m \subseteq K_{[n,m]}$. Thus the family $\{K_n | n \in \mathrm{Ind}\}$ is cofinal (in the sense of the last paragraph) in the set of all finite dimensional extensions of $\mathbf{Q}$ in K.

Let n be indicial. Write d_n for the greatest common divisor of 2 and n, U_n for the units of $\mathbf{Z}/n\mathbf{Z}$, and M_n for $\mathrm{Map}(S(n), \mathbf{Z}/n\mathbf{Z})$. M_n is an abelian group under pointwise addition of maps, and U_n acts on M_n by pointwise multiplication; $M_n \rtimes U_n$ will denote their semidirect product with respect to this action.

For k, j positive integers with $j|k$, π_{kj} will denote the canonical map $\mathbf{Z}/k\mathbf{Z} \to \mathbf{Z}/j\mathbf{Z}$. The assignment $f \mapsto \pi_{n,d_n} \circ f$ maps M_n onto $\mathrm{Map}(S(n), \mathbf{Z}/d_n\mathbf{Z})$ with kernel $d_n M_n$; we will use the induced isomorphism to identify $M_n/d_n M_n$ with $\mathrm{Map}(S(n), \mathbf{Z}/d_n\mathbf{Z})$. Note that this group is trivial when n is odd.

Let η_n: $M_n \to M_n/d_n M_n$ be the natural projection, and define λ_n: $U_n \to M_n/d_n M_n$ by

$$\lambda_n^{(u)}(p) = \begin{cases} \dfrac{a^2-1}{8} + d_n\mathbf{Z}, & p = 2, \\ \left[\dfrac{u}{p}\right], & p \equiv 1 \bmod 4, \\ \left[\dfrac{u}{p}\right] + \dfrac{a-1}{2} + d_n\mathbf{Z}, & p \equiv 3 \bmod 4, \end{cases}$$

where $u = a + n\mathbf{Z} \in U_n$ and $p \in S(n)$, and where $[u/p]$ is defined to be $0 \in \mathbf{Z}/d_n\mathbf{Z}$ if u is a square in U_n and $1 \in \mathbf{Z}/d_n\mathbf{Z}$ otherwise; it is straightforward to check that λ_n is a well defined group homomorphism.

We let

$$V_n = \begin{cases} (U_n)^2 \cdot \{1, -1\} & \text{if } n \text{ is even} \\ U_n & \text{if } n \text{ is odd.} \end{cases}$$

PROPOSITION 3.1. *λ_n maps U_n onto $M_n/d_n M_n$ and V_n is its kernel.*

Proof. This clear when n is odd, so assume that n is even and hence that $8|n$. It is easily seen that V_n is included in the kernel. Suppose that $u \in U_n$ is in the kernel, with $u = a + n\mathbf{Z}$, a relatively prime to n. Then u is a square in U_n if and only if $a \equiv 1 \bmod 8$ and $[u/p] = 0$ for every odd prime p dividing n. Now if $a \equiv 1 \bmod 8$ then $\frac{1}{2}(a-1) \equiv 0 \bmod 2$, so for $p|n$ with $p \equiv 3 \bmod 4$,

$$\left[\frac{u}{p}\right] = \left[\frac{u}{p}\right] + \left(\frac{a-1}{2} + 2\mathbf{Z}\right) = \lambda_n(u)(p) = 0.$$

Since $[u/p] = \lambda_n(u)(p) = 0$ for $p|n$ with $p \equiv 1 \bmod 4$ as well, we have $u \in U_n^2$ if $a \equiv 1 \bmod 8$. Thus since

$$\frac{a^2-1}{8} + 2\mathbf{Z} = \lambda_n(u)(2) = 0$$

implies $a \equiv \pm 1 \bmod 8$, u fails to be a square in U_n only if $a \equiv -1 \bmod 8$. In this case $-a \equiv 1 \bmod 8$,

$$\left[\frac{-u}{p}\right] = \left[\frac{u}{p}\right] + \left[\frac{-1}{p}\right] = 0$$

for $p | n$ with $p \equiv 1 \bmod 4$, and for $p | n$ with $p \equiv 3 \bmod 4$,

$$\begin{aligned}\left[\frac{-u}{p}\right] &= \left[\frac{u}{p}\right] + \left[\frac{-1}{p}\right] = \left[\frac{u}{p}\right] + 1\\ &= \left[\frac{u}{p}\right] + \left(\frac{a-1}{2} + 2\mathbf{Z}\right) = \lambda_n(u)(p) = 0,\end{aligned}$$

and hence $-u \in U_n^2$ and $u \in V_n$. Thus $\operatorname{Ker}(\lambda_n) = V_n$.

Still assuming that n is even, we note that $-1 \notin U_n^2$ and hence that $|V_n| = 2|U_n^2|$. By decomposing U_n into a product of groups of units mod prime powers we find that

$$[U_n \colon U_n^2] = 2^{s(n)+1}$$

and hence that

$$|V_n| = 2\varphi^{(n)}/2^{s(n)+1} = \varphi^{(n)}/2^{s(n)}.$$

It follows that the image of λ_n has cardinality $2^{s(n)} = [M_n \colon 2M_n]$, which shows the map is surjective. □

Let $G_n = \{(f, u) \in M_n \rtimes U_n | \eta_n(f) = \lambda_n(u)\}$. Define g_n to be the order of G_n and note that since

$$(f, u) \mapsto \eta_n(f) - \lambda_n(u)$$

is a group homomorphism (as one easily checks) of $M_n \rtimes U_n$ onto M_n/d_nM_n with kernel G_n, G_n is a group and

$$gn = \frac{|M_n \rtimes U_n|}{|M_n/2M_n|} = \left(\frac{n}{d_n}\right)^{s(n)} \varphi(n),$$

where φ is the Euler function.

Write C_n for the subgroup $\langle \zeta_n \rangle$ of C and ω_n for the unique group isomorphism $C_n \to \mathbf{Z}/n\mathbf{Z}$ satisfying $\omega_n(\zeta_n) = 1 + n\mathbf{Z}$. Define $\nu_n \colon \Gamma_n \to U_n$ by

$$\sigma \mapsto \omega_n(\sigma(\zeta_n));$$

ν_n has its image in U_n since $\sigma(\tau_n)$ is a primitive nth root of unity, and one easily checks that ν_n is a group homomorphism. For each $\sigma \in \Gamma_n$ and $p \in$

$S(n)$, $\sigma(p^{1/n})/p^{1/n}$ is an nth root of 1, so we can define a map $\mu_n\colon \Gamma_n \to M_n$ by

$$\sigma \mapsto \left(p \mapsto \omega_n\left(\sigma\left(p^{1/n}\right)/p^{1/n}\right)\right);$$

for $\sigma, \tau \in \Gamma_n$, this map satisfies

$$\mu_n(\sigma\tau) = \mu_n(\sigma) + \nu_n(\sigma)\mu_n(\tau).$$

Thus

$$\varphi_n\colon \sigma \mapsto \left(\mu_n(\sigma), \nu_n(\sigma)\right)$$

is a group homomorphism of Γ_n into $M_n \rtimes U_n$.

THEOREM 3.2. *φ_n maps Γ_n isomorphically onto G_n.*

Proof. One checks that φ_n is injective and uses quadratic Gauss sums as in 2 to see that its image lies in G_n. We take advantage of the finiteness of Γ_n and G_n in showing that the image of φ_n is all of G_n. The following lemma enables us to count the relevant dimensions.

LEMMA 3.3. *F_n and $E_n \cap F_n$ are cogalois extensions (see [2]) of $\mathbf{Q}$ with cogalois groups isomorphic, respectively, to M_n and M_n/d_nM_n.*

Proof. Write L for $E_n \cap F_n$ and $\mathbf{Q}^*$ for the units of $\mathbf{Q}$. By [2], F_n is cogalois over $\mathbf{Q}$ and hence the subextension $L|\mathbf{Q}$ is also cogalois, and $\mathrm{Cog}(L|\mathbf{Q}) \leq \mathrm{Cog}(F_n|\mathbf{Q})$. Let t be a positive integer dividing n. For a prime $p \in S(n)$ and an integer a, $p^{a/t}$ is an element of F_n whose coset modulo $\mathbf{Q}^*$ depends only on p and the class u of a modulo $t\mathbf{Z}$, and we let $p^{u/t}\mathbf{Q}^*$ stand for this coset; it is an element of $\mathrm{Cog}(F_n|\mathbf{Q})$. It is straightforward to check that

$$f \mapsto \prod_{p \in S(n)} p^{f(p)/n}\mathbf{Q}^*$$

is a group isomorphism of M_n onto $\mathrm{Cog}(F_n|\mathbf{Q})$.

Using Gauss sums again, one notes that for every $p \in S(n)$, $p^{1/d_n} \in E_n$, and since $d_n|n$, $p^{1/d_n} \in F_n$ as well, so that $p^{a/d_n} \in L$ for every integer a. Hence

$$f \mapsto \prod_{p \in S(n)} p^{f(p)/d_n}\mathbf{Q}^*$$

defines a map from $\mathrm{Map}(S(n), \mathbf{Z}/d_n\mathbf{Z}) \cong M_n/2M_n$ into $\mathrm{Cog}(L|\mathbf{Q})$ which one checks is an injective group homomorphism. Its surjectivity follows (as one checks) from the fact, which we proceed to establish, that every element of $\mathrm{Cog}(L|\mathbf{Q})$ has order dividing d_n.

Let $y \in \mathrm{Cog}(L|\mathbf{Q})$ have order k. Note that $k|n$ since $\mathrm{Cog}(L|\mathbf{Q}) \leq \mathrm{Cog}(F_n|\mathbf{Q})$ and the latter has exponent n. Also, y is of the form $b\mathbf{Q}^*$ with $b \in L$ and $b^k \in \mathbf{Q}^*$; thus b is a root in L of $X^k - b^k \in \mathbf{Q}[x]$. The conjugates of b over $\mathbf{Q}$ all look like ζb with ζ a kth root of 1, and they all lie in L since L is a subfield of the abelian extension E_n. Thus if ζb is a conjugate of b, then $\zeta \in L_n \subseteq F_n \subseteq \mathbf{R}$ which implies that $\zeta = \pm 1$. It follows that all conjugates of b are in the set $\{b, -b\}$ and therefore that $b^2 \in \mathbf{Q}$ and $y^2 = 1$. Thus $k|2$, and since $k|n$ as well, we get $k|d_n$. This establishes the lemma.

We complete the proof of the theorem by observing that, as a consequence of the lemma,

$$[F_n\colon \mathbf{Q}] = |\mathrm{Cog}(F_n|\mathbf{Q})| = n^{s(n)}$$

and

$$[E_n \cap F_n\colon \mathbf{Q}] = |\mathrm{Cog}(E_n \cap F_n|\mathbf{Q})| = d_n^{s(n)},$$

and hence

$$\begin{aligned} |\Gamma_n| &= [K_n\colon \mathbf{Q}] = [E_n\colon \mathbf{Q}][F_n\colon \mathbf{Q}]/[E_n \cap F_n\colon \mathbf{Q}] \\ &= \varphi(n)\cdot \frac{n^{s(n)}}{d^{s(n)}} \\ &= g_n. \end{aligned}$$

□

The next result gives G_n as an extension of M_n/d_nM_n. Let

$$N_n = \mathrm{Map}(S(n), dn(\mathbf{Z}/n\mathbf{Z})) = d_nM_n.$$

The action of U_n on M_n restricts to an action of V_n on N_n, and the semidirect product $N_n \rtimes V_n$ with respect to this action is a subgroup of $M_n \rtimes U_n$. Since N_n is the kernel of $\eta_n\colon M_n \to M_n/d_nM_n$ and V_n is the kernel of $\lambda_n\colon U_n \to M_n/d_nM_n$, $N_n \rtimes V_n$ is actually a subgroup of G_n.

THEOREM 3.4. *There is an exact sequence*

$$1 \to N_n \rtimes V_n \to G_n \to M_n/N_n \to 1.$$

Proof. The map from G_n to M_n/M_n is given by $(f, u) \mapsto \lambda_n(u)$. All details are easy to check. □

We now give a criterion for deciding when an arbitrary number field is K_n for some indicial integer n. Let L be a finite extension of $\mathbf{Q}$. Write $r' = r'(L)$ for the cardinality of the group $\mu(L)$ of roots of unity in L. We note that r' is always even, and we set

$$r = r(L) = \begin{cases} r' & \text{if } 4 \mid r' \\ \frac{1}{2}r' & \text{if } 4 \nmid r'. \end{cases}$$

Recall that B denotes the multiplicative group of positive rationals, and set

$$A = A(K) = \{\alpha \in B \mid \exists a \in L \text{ with } a^r = \alpha\}.$$

LEMMA 3.5. *Assume n is an indicial integer. Then $r(K_n) = n$.*

Proof. Since $\zeta_n \in \mu(K_n)$, $n \mid r'$ and $\varphi^{(n)} \mid \varphi(r')$. Also $E_{r'} \cdot F_n \subseteq K_n$, so $[E_{r'} \cdot F_n \colon \mathbf{Q}]$ divides g_n. We note that Lemma 3.3 remains valid when E_n is replaced by any extension of E_n which is abelian over $\mathbf{Q}$, and hence $[E_{r'} \cap F_n\colon \mathbf{Q}] = d_n^{s(n)}$. It follows that

$$[E_{r'} \cdot F_n\colon \mathbf{Q}] = \varphi(r')n^{s(n)}/d_n^{s(n)},$$

and because this divides $g_n = \varphi(n)n^{s(n)}/d_n^{s(n)}$ we obtain $\varphi(r') = \varphi(n)$. If n is even then $n = r'$, and since $8 \mid n$ in this case, $8 \mid r'$, so $r = r' = n$. If n is odd then $\varphi^{(n)} = \varphi^{(r')}$ implies $r' = 2n$; in this case 4 does not divide r' and $r = \frac{1}{2}r' = n$. Thus in either case we conclude that $r = n$. □

COROLLARY 3.6. *If n and m are indicial and $K_n \subseteq K_m$, then $n \mid m$.*

THEOREM 3.7. *With L, r, and A as above, the following are equivalent*:
(1) $L = K_n$ *for some indicial integer* n;
(2) r *is indicial and* $L = K_r$;
(3) r *is indicial*, $S(r) \subseteq A$, *and* $[L\colon \mathbf{Q}] \leq g_r$;
(4) $\exists$ m *indicial with* $m \mid r$, $S(m) \subseteq A$, *and* $[L\colon \mathbf{Q}] \leq g_m$.

Proof. The implication (1) ⇒ (2) follows from the last lemma, and (2) ⇒ (3) ⇒ (4) is clear. If (4) holds then $\zeta_m \in L$ and $X^r - p$ has a root in L for every $p \mid m$. It follows that $X^m - p$ splits over L for each $p \mid m$, and hence that $K_m \subseteq L$. The condition $[L\colon \mathbf{Q}] \leq g_m$ then implies that $L = K_m$. □

Finally, we remark that for n indicial it can be shown that a prime number q ramifies in K_n if and only if q divides n. Furthermore, if p is a prime number which is indicial (i.e., if p is a prime congruent to 1 (mod 4) then p ramifies fully in K_p, and for q a prime different from p, q decomposes in K_p into a product of g primes each of inertial degree f, where f is the multiplicative order f_0 of $q \bmod p$ and $g = p(p-1)/f_0$ if $X^p - \bar{p} \in \mathbf{Z}/q\mathbf{Z}[x]$ has a root in $\mathbf{Z}/q\mathbf{Z}$ and $f = p \cdot f_0$ and $g = (p-1)/f_o$ if $X^p - \bar{p}$ has no root in $\mathbf{Z}/q\mathbf{Z}$.

Section 4

Let $K|k$ be a finite extension of fields and let $\mathrm{Sub}(K|k)$ be the lattice (with respect to inclusion) of field extensions of k in K. An inclusion reversing bijection θ of $\mathrm{Sub}(K|k)$ onto itself will be called a *duality* of $K|k$ if for all $L \in \mathrm{Sub}(K|k)$, $[K: L] = [\theta(L): k]$ holds. A field extension for which a duality exists will be called *semiabelian*. We make analogous definitions for a finite group G and its lattice of subgroups $\mathrm{Sub}(G)$, and note that a Galois field extension is semiabelian if and only if its Galois group is. We also point out that as a lattice antiisomorphism, a duality of $K|k$ takes intersections to composities and composites to intersections. A similar statement holds for groups.

Let G be a finite abelian group. By selecting an isomorphism of G onto its Pontryagin dual $\hat{G}$ and following the induced lattice isomorphism $\mathrm{Sub}(G) \to \mathrm{Sub}(\hat{G})$ with the lattice antiisomorphism

$$H \mapsto \{\sigma \in G | \chi(\sigma) = 1, \forall \chi \in H\}$$

of $\mathrm{Sub}(\hat{G})$ onto $\mathrm{Sub}(G)$, one obtains a duality of G. Thus finite abelian groups are semiabelian. The next two theorems follow easily from this observation.

THEOREM 4.1. *Every Cogalois field extension (see [2]) is semiabelian.*

THEOREM 4.2. *Every abelian field extension is semiabelian.*

Let n be an indicial integer. Let $m = m(n) = d_n \cdot \prod_{p \in S(n)} p$ and $k_n = E_{m(n)} = \mathbf{Q}[\zeta_{m(n)}]$. Note that k_n is a subfield of K_n.

THEOREM 4.3. *$K_n|k_n$ is a semiabelian field extension.*

Proof. Lemma 3.5 implies that $K|k$ is a pure extension. Since it is also separable and coseparable, theorem 1.5 of [2] implies it is Cogalois and hence semiabelian. □

The existence of a duality for a group imposes a symmetry on its lattice of subgroups which we exploit in the following application.

THEOREM 4.4. *Let $K|k$ be a semiabelian Galois field extension of finite degree g. Let*

$$g = p_1^{e_1} \cdots p_2^{e_s}$$

be the prime decomposition of g. Then for $i = 1, \dots, s$ there is a unique subextension L_i of degree $p_i^{e_i}$ over k, and

$$K \cong L_1 \otimes_k \cdots \otimes_k L_s$$

as k-algebras.

Proof. By theorem 7 of [3] semiabelian groups are nilpotent. Hence $G = \mathrm{Aut}_k(K)$ has unique Sylow subgroups. We choose a duality θ of G, and for each $i = 1, \dots, s$ we let H_i denote the p_i-Sylow subgroup of G. Then $\theta(H_i)$ has index $p_i^{e_i}$ in G, and since there is just one such subgroup in G, it is independent of the choice of θ. The Galois correspondence then gives a unique element L_i of $\mathrm{Sub}(K|k)$ with $[L_i\colon k] = p_i^{e_i}$.

To obtain the isomorphism of the theorem's second assertion, we note that multiplication induces a k-algebra homomorphism

$$L_1 \otimes_k \cdots \otimes_k L_s \to K$$

with image $L_1 \dots L_s$. The properties of θ imply that

$$\begin{aligned} L_1 \dots L_s &= K^{\theta(H_1) \cap \cdots \cap \theta(H_s)} \\ &= K^{\theta(\langle H_1, \dots, H_s \rangle)} \\ &= K^{\theta(G)} \\ &= K^{\{1\}} \\ &= K. \end{aligned}$$

Thus our map is surjective. Since both domain and codomain have dimension g over k, the map is also injective, and the theorem is proved. □

COROLLARY 4.5. *Let n be indicial and for each $p|n$ write e_p for the largest power of p dividing $g_n/\varphi_{(m(n))} = [K_n\colon k_n]$. Then for each such p there is a unique subextension $L_{(p,n)}$ of $K_n|k_n$ with $[L(p,n)\colon k_n] = p^{e_p}$, and K_n is isomorphic as a k_n-algebra to the tensor product over k_n of the $L_{(p,n)}$.*

REFERENCES

1. K. IRELAND and M. ROSEN, *A classical introduction to modern number theory*, Springer Verlag, New York, 1982.
2. C. GREITHER and D.K. HARRISON, *A Galois correspondence for radical extensions of fields*, J. Pure Appl. Algebra, **43** (1986), pp. 257–270.
3. M. SUZUKI, *Structure of a group and the structure of its lattice of subgroups*, Ergeb. Math. Grenzgeb., Springer, New York, 1956.

UNIVERSITY OF OREGON
EUGENE, OREGON