ILLINOIS JOURNAL OF MATHEMATICS
Volume 22, Number 4, December 1978

A MATRIX CRITERION FOR NORMAL INTEGRAL BASES

BY
DONALD MAURER

Let $K|F$ be a finite Galois extension of an algebraic number field F. In certain circumstances it is known that the ring of integers $\mathcal{O}_K$ has a normal integral basis. The uniqueness of such a basis has been studied in [2] and [3]. In this paper we give a characterization of the structure constants of an order, over an integral domain, having a normal integral basis. As an example these results are then applied to cyclic cubic extensions: we obtain an explicit characterization of the normal orders of such extensions in terms of their discriminants; and when F is the rational field $\mathbf{Q}$, we are able to characterize discriminants of tamely ramified cyclic cubic extensions, and explicitly construct all such fields having a given discriminant. It is known (e.g., class-field theory) that each cyclic extension of $\mathbf{Q}$ is determined by a complex-valued Dirichlet character χ with the property that for almost all primes p, $\chi(p) = 1$ if and only if p splits completely in the extension. For quadratic extensions the character is known explicitly in terms of the discriminant. For higher degree extensions the corresponding character is no longer determined by the discrimant, but there is still a very strong connection which our results make explicit.

Structure constants

Throughout this section R will denote an integral domain with an identity 1_R, and G a finite group of order n. If B: $RG \times RG \rightarrow R$ is an R-bilinear form on the group ring RG, the equation

$$x \circ y = \sum_{\tau \in G} B(\tau x, \tau y)\tau^{-1}, \quad x, y \in R, \tag{1}$$

defines a binary operation which, together with the ordinary R-module structure, makes RG into an R-algebra which we shall denote by $\Gamma = \Gamma_B$. In general this algebra is not necessarily commutative or associative; although, via the ordinary group ring multiplication, G acts as a group of R-automorphisms.

Suppose that $R = \mathcal{O}_F$ and $G = \text{Gal}\ (K|F)$. An R-order $\mathcal{O}$ in K is *normal* if it has a basis of the form $\{\sigma(\alpha)\}_{\sigma \in G}$ for some $\alpha \in \mathcal{O}$. A normal order is evidently isomorphic to RG as an RG-module. Now let $c^{\rho}_{\sigma,\tau} \in R$ be defined by the relations

$$\sigma(\alpha)\tau(\alpha) = \sum_{\sigma \in G} c^{\rho}_{\sigma,\tau}\rho(\alpha), \quad \sigma, \tau \in G;$$

Received June 24, 1977.

then for each $\upsilon \in G$, apply to both sides of the equation to obtain $c^{\upsilon}_{\sigma,\tau} = c^{1}_{\upsilon^{-1}\sigma,\upsilon^{-1}\tau}$. If we let B' denote the bilinear form on $\mathcal{O}$ determined by the conditions $B'(\sigma(\alpha), \sigma(\tau)) = c^{1}_{\sigma,\tau}$, then for all $x, y \in \mathcal{O}$ we have

$$xy = \sum_{\rho \in G} B'(\rho(x), \rho(y))\rho^{-1}(\alpha).$$

We can define a bilinear form B on RG by setting $B(\sigma, \tau) = B'(\sigma(\alpha), \tau(\alpha))$; then the RG-module isomorphism $\mathcal{O} \cong RG$ is extended to an algebra isomorphism $\phi\colon \mathcal{O} \cong \Gamma_B$ (note that $\phi(\sigma(x)) = \sigma \cdot \phi(x)$, where the multiplication indicated on the right hand side is the group ring multiplication). Conversely, if B has been chosen so that Γ_B is a commutative integral domain with identity, and K is its quotient field, then $K \mid F$ has Galois group G and Γ_B is a normal order in K. This establishes a bijection between normal R-orders in Galois extensions of F and forms B for which Γ_B is a commutative integral domain with identity. The purpose of this section will be to classify those B for which Γ_B is an integral domain with identity.

We fix an enumeration $1_G = \sigma_1, \sigma_2, \ldots, \sigma_n$ of the elements of G. Then each $\tau \in G$ defines a permutation $\tilde{\tau}$ by the equation $\sigma_{\tilde{\tau}(i)} = \tau\sigma_i$; we also define $v(i)$ by $\sigma_{v(i)} = \sigma_i^{-1}$. For each $\tau \in G$ we define the form $B^{\tau}(x, y) = B(\tau x, \tau y)$; and denote its matrix, relative to the normal basis $\sigma_1, \ldots, \sigma_n$, by $M^{\tau} = (m^{\tau}_{ij})$. It is a consequence of the Galois action that $m^{\tau}_{ij} = m_{\tilde{\tau}(i),\tilde{\tau}(j)}$ $(m_{ij} = m^{1_G}_{ij})$; thus there are at most n^2 distinct structure constants relative to the above basis and they occur as the entries of the matrix $M = (m_{ij})$. If Γ is commutative, then M is symmetric so that there are at most $n(n+1)/2$ distinct structure constants. These remarks hold for the matrices of B^{τ} relative to any basis of the form $\theta_1, \ldots, \theta_n$ where $\theta_i = \sigma_i\theta$ (the right side is multiplication in the group ring).

Suppose that θ' also generates a normal basis. If $\theta' = \sum w_i\theta_i$, then

$$\begin{pmatrix} \theta'_1 \\ \vdots \\ \theta'_n \end{pmatrix} = W \begin{pmatrix} \theta_1 \\ \vdots \\ \theta_n \end{pmatrix}$$

where the (i, j)th position of W contains $w_{u(i,j)}$, and $u(i, j)$ is defined by $\sigma_{u(i,j)} = \sigma_i^{-1}\sigma_j$. The matrix W is called a *group matrix* [3] for G; if the rows sum to one, we say W is *normalized.*

We now consider conditions under which Γ has an identity. Suppose 1_Γ is an identity and θ generates a normal basis. Then $\sigma 1_\Gamma = 1_\Gamma$ (all $\sigma \in G$) implies $1_\Gamma = rs(\theta)$, where $r \in R$, and $s(\theta) = \theta_1 + \cdots + \theta_n$. The condition $1_\Gamma \circ 1_\Gamma = 1_\Gamma$ implies that r is a unit so $\theta' = r\theta$ also generates a normal basis. Whence $1_\Gamma = s(\theta')$. Finally the conditions $\theta'_i \circ 1_\Gamma = \theta'_i$ $(1 \le i \le n)$ imply that

$$B_{\theta'}(\theta'_i, s(\theta')) = \begin{cases} 1 & \text{if } i = 1 \\ 0 & \text{if } i > 1 \end{cases} \tag{2}$$

where B_θ is the uniquely determined form satisfying

$$x \circ y = \sum_{i=1}^{n} B_\theta(x, y)\sigma_{v(i)}\theta.$$

Conversely if θ is any element which generates a normal basis and satisfies (2), then $s(\theta)$ is an identity for Γ. There is no loss in generality if we assume $\theta = 1_G$; then (2) can be expressed in matrix terms by

$$\text{(3)} \qquad \sum_{j=1}^{n} m_{ij} = \begin{cases} 1 & \text{if } i = 1 \\ 0 & \text{if } i > 1. \end{cases}$$

Now let $B^G = \sum_{\tau \in G} B^\tau$, with corresponding matrix $M^G = (m_{ij}^G)$. If we define, for $x \in RG$, trace $(x) = s(1_G)x$, then it is straightforward to see that $B^G(x, y) =$ trace $(x \circ y)$. The R-algebra Γ is *separable* if the trace-form B^G is nondegenerate (i.e., det $M^G \neq 0$). We will be concerned with separable algebras throughout. Note that (3) implies

$$\text{(4)} \qquad \sum_{j=1}^{n} m_{ij}^G = 1 \quad \text{for } 1 \leq i \leq n.$$

We now consider associativity and the existence of zero divisors. We say that Γ *splits completely* if $\Gamma \cong \Gamma_1 \oplus \cdots \oplus \Gamma_s$, where each $\Gamma_i \cong R$. If Γ splits completely it is evident that it is commutative, associative and semisimple (since R contains no nilpotent elements). Moreover it has an identity. Our next lemma characterizes complete splitting. Assume that Γ has an identity $1_\Gamma = s(1_G)$.

LEMMA. *Suppose R is a field. Then Γ splits completely if and only if*

(i) *the polynomial* $\Phi(x) = \det\,(M - xM^G)$ *factors into linear factors over R, and*

(ii) *the zeros $\zeta_1, \ldots, \zeta_n$ of Φ_M can be ordered so that*

$$M = {}^tW \begin{pmatrix} \zeta_1 & & \\ & \ddots & \\ & & \zeta_n \end{pmatrix} W \quad (\text{${}^tW$ denotes transpose of W})$$

where W^{-1} is the normalized group matrix whose first row is $\zeta_{\nu(1)}, \ldots, \zeta_{\nu(n)}$.

Proof. Suppose Γ splits completely. Then it is straightforward to show that $s = n$ and each $\Gamma_i = Re_i$ where e_1j $\ldots, e_n$ is a normal basis. Since $e_i \circ e_j = 0$ if $i \neq j$, we see that the matrices of B and B^G with respect to $e_1, \ldots, e_n$ are diagonal. If

$$\begin{pmatrix} \sigma_1 \\ \vdots \\ \sigma_n \end{pmatrix} = W \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix},$$

then W is a normalized group matrix, and we have

$$M^G = {}^tWW, \qquad M = {}^tW \operatorname{diag}(\zeta_1, \ldots, \zeta_n)W,$$

for some $\zeta_1, \ldots, \zeta_n \in R$. The first of these relations requires explanation. Since ${}^tW^{-1}M^GW^{-1}$ is the matrix of B^G with respect to $e_1, \ldots, e_n$, it must be diagonal.

Let $e = e_1$ so that $e_i = \sigma_i e$. Then we find that the form $B_e = \sum w_j B^{\sigma_j}$, where $w_1, \ldots, w_n$ is the first row of W. Hence $B_e^G = B^G$ (W is normalized). It follows that ${}^t W^{-1} M^G W^{-1}$ must satisfy (4), whence it must be I_n.

Since Γ is separable, Φ is of degree n, and evidently its zeros are just $\zeta_1, \ldots, \zeta_n$. This proves the necessity of (i).

Finally, $e_i = e_i \circ e_i$ implies

$$e_i = \sum_{\tau \in G} B(e_{\bar{\tau}(i)}, e_{\bar{\tau}(i)})\tau^{-1} = \sum_{\tau \in G} \zeta_{\bar{\tau}(i)} \tau^{-1},$$

and this proves the necessity of (ii).

Conversely (i) and (ii) imply that $e_1, \ldots, e_n$ as defined by the equations $e_i = \sum_{\tau \in G} \zeta_{\bar{\tau}(i)} \tau^{-1}$ give a system of orthogonal idempotents.

Remarks. When R is an algebraic number field there is an algorithm [5] for factoring polynomials in $R[x]$ which can be applied to Φ. Therefore there is an effective procedure for determining whether the conditions of the lemma are satisfied.

Suppose that $S \supset R$ is an integral domain and $1_S = 1_R$. We can define an S-algebra Γ_S on the group ring SG by (1); and there is a natural embedding $\Gamma \to \Gamma_S$. Therefore if Γ_S splits completely for some extension $S \supset R$, Γ is commutative, associative and has an identity. We can prove the converse. Let Γ be associative with an identity. Separability implies the existence of an element $\zeta \in \Gamma$ such that $B(x, y) = \text{trace}\,(\zeta \circ x \circ y)$. This leads to the factorizations

$$(5) \qquad M^G = {}^t W W, \qquad M = {}^t W \operatorname{diag}(\zeta_1, \ldots, \zeta_n) W \quad (\zeta_1 = \zeta),$$

where W^{-1} is the (normalized) group matrix whose first row is $\sigma_{\nu(1)}, \ldots, \sigma_{\nu(n)}$. Therefore, if we define a normal basis $w_1, \ldots, w_m$ by

$$\begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = W^{-1} \begin{pmatrix} \sigma_1 \\ \vdots \\ \sigma_n \end{pmatrix},$$

we have, for each $\tau \in G$, $B^\tau(w_i, w_j) = 0$ when $i \neq j$.

Now, the associative condition can be reduced to

$$1_G \circ (\alpha \circ \beta) = (1_G \circ \alpha) \circ \beta, \quad \text{for all } \alpha, \beta \in G.$$

If $M_w = (m_{ij}(w))$ is the matrix of B_w with respect to $w_1, \ldots, w_n$, this condition can be expressed as

$$(6) \qquad \sum_{\tau \in G} m_{\tau,\alpha} m_{\theta,\theta\tau^{-1}} = \sum_{\tau \in G} m_{\tau,\tau\alpha} m_{\theta\tau^{-1},\theta\beta}$$

for all $\alpha, \beta, \theta \in G$, where we have set $m_{\sigma_i,\sigma_j} = m_{ij}(w)$. In view of (5) we obtain

$$(7) \qquad \sum_{\alpha \in G} m_{\alpha\tau,\alpha\sigma} = \begin{cases} 1 & \text{if } \sigma = \tau \\ 0 & \text{if } \sigma \neq \tau. \end{cases}$$

Now sum (6) over all θ and use (7) to obtain $m_{\alpha,\beta} = m_{\beta^{-1},\beta^{-1}\alpha}$. Letting $\alpha = \beta$ we have $m_{\alpha,\alpha} = m_{\alpha-1,1}$. Since $m_{ij}(w) = 0$ if $i \neq j$, we now see that $m_{ii}(w) = 0$ if $i > 1$. Therefore $w_i \circ w_i = w_i$, so that $w_1, \ldots, w_n$ is a system of orthogonal idempotents for Γ_S.

Then if we take S to be any extension field of the quotient field of R containing the entries of W^{-1} we obtain the splitting $\Gamma_S = \Gamma_1 \oplus \cdots \oplus \Gamma_n$; $\Gamma_i \cong \Gamma w_i$. Consideration of dimensions gives $\Gamma_i \cong S$.

We now summarize our classification in:

THEOREM 1. *Let B be given. The R-algebra $\Gamma = \Gamma_B$ is separable, associative, commutative and has an identity if and only if there exist nonzero elements $\zeta_1, \ldots, \zeta_n$ (in some fixed algebraic closure of the quotient field F of R) such that*

$$M = {}^tW \begin{pmatrix} \zeta_1 & & \\ & \ddots & \\ & & \zeta_n \end{pmatrix} W \tag{8}$$

where W^{-1} exists and is the normalized group matrix whose first row is $\zeta_{\nu(1)}, \ldots, \zeta_{\nu(n)}$.

In this case $\zeta_1, \ldots, \zeta_n$ are the zeros of $\Phi(x)$; and if $\Phi = \Phi_1, \ldots, \Phi_r$ is the factorization of Φ over $F[x]$, then $\Gamma = \Gamma_1 \oplus \cdots \oplus \Gamma_S$ where Γ_i is an integral domain with identity whose quotient field is the splitting field of $\Phi_i = 0$.

Proof. We have just seen that if Γ is separable, associative and has an identity, then M has a factorization of the form (8).

Conversely, suppose we have such a factorization. Let $\xi_1, \ldots, \xi_n$ be given such that W is the normalized group matrix whose first row is $\xi_{\nu(1)}, \ldots, \xi_{\nu(n)}$. Then trace $(\zeta_i \circ \xi_j) = \delta_{ij}$. Since $m_{ij} =$ trace $(\zeta \circ \xi_i \circ \xi_j)$ (where $\zeta = \zeta_1$), we see that M satisfies condition (3) so Γ has an identity. Moreover, straightforward calculations show $M^G = {}^tWW$; therefore Γ is separable. Also, $\Phi(\zeta_i) = 0$ for all i. We may without loss of generality assume R to be a field and then apply the lemma.

Now suppose Φ is irreducible over $F[x]$. We show that Γ is an integral domain. Let K be the splitting field of Φ, so that Γ_K splits completely. Whence Γ is semisimple. Therefore if Γ has nontrivial zero divisors, there is a nontrivial decomposition $\Gamma = \Gamma_1 \oplus \Gamma_2$ as R-algebras. If e_{ij} ($j = 1, 2, \ldots$) is an R-basis for Γ_i, then $B^\tau(e_{1j}, e_{2K}) = 0$ for all $\tau \in G$ and j, k. So the matrices of B and B^G with respect to the basis $\{e_{ij}\}$ are in block diagonal form. Hence we obtain a nontrivial factorization $\Phi = \Phi_1\Phi_2$. It follows that Γ_F is a Galois extension of F with group G. By separability, there is a $\lambda \in \Gamma_F$ such that

$$m_{ij} = \text{trace } (\lambda \circ \xi_i \circ \xi_j) = \text{trace } (\zeta \circ \xi_i \circ \xi_j).$$

Thus $\lambda = \zeta \in \Gamma_F$. It follows that Γ_F is the splitting field of Φ. If

$$\Gamma = \Gamma_1 \oplus \cdots \oplus \Gamma_s$$

where Γ_i are indecomposable, then Γ_i are integral domains, and we have a corresponding factorization $\Phi = \Phi_1, \ldots, \Phi_s$. Now if Γ is an integral domain, then Φ is irreducible since G acts transitively on $\zeta_1, \ldots, \zeta_n$.

This completes the proof. Note that as in the comment following the lemma, the factorization of Φ can be determined if R is a ring of algebraic elements.

Remarks. (1) The factorization in (8) determines G uniquely, for if there is a factorization of M with $\zeta'_1, \ldots, \zeta'_n$ and a group G' then Γ and Γ' are isomorphic as R-algebras so $G = \mathrm{Aut}_R(\Gamma) = \mathrm{Aut}_R(\Gamma') = G'$.

(2) $\{\zeta_i\}$ and $\{\xi_i\}$ are dual bases with respect to the trace-form. So if $R = \mathcal{O}_F$ is the ring of integers in a number field F, and $\Gamma \cong \mathcal{O}_K$ then $\zeta_1, \ldots, \zeta_n$ is a basis for the inverse different of $K|F$ (e.g., this occurs if $F = \mathbf{Q}$ and $K|\mathbf{Q}$ is tamely ramified, abelian).

Cubic extensions

In this section we assume that R is an integral domain with characteristic different from 2 or 3. We apply the results of the preceeding section to the case $n = 3$. Then G is cyclic of order 3 and $\sigma_2^2 = \sigma_3$.

Suppose M is symmetric and satisfies (3), then Γ is an R-algebra with identity, and we have the relations

$$\begin{aligned} m_{12} &= \tfrac{1}{2}(1 - m_{11} - m_{22} + m_{33}), \\ m_{13} &= \tfrac{1}{2}(1 - m_{11} + m_{22} - m_{33}), \\ m_{23} &= \tfrac{1}{2}(-1 + m_{11} - m_{22} - m_{33}). \end{aligned}$$

Therefore, in view of (3), M is uniquely determined by m_{11}, m_{22} and m_{33}. If we set $x = m_{11} + m_{22} + m_{33}$, then

$$m_{ij}^G = \begin{cases} x & \text{if } i = j \\ \dfrac{1-x}{2} & \text{if } i \neq j, \end{cases}$$

and $D = \det M^G = (1 - 3p)^2$, where $x = 1 - 2p$.

In order to construct integral domains Γ we must choose M so that (8) holds, and Φ is irreducible. Since $D \neq 0$, Φ can be replaced by $\Psi = D^{-1}\Phi$. Then Ψ has the form

$$\Psi(x) = x^3 - x^2 + \frac{p'}{D}x - \frac{q'}{D}; \quad p', q' \in R.$$

Assume that a nonzero element $\Theta = 1 - 3p$ ($p \in R$) is given. We try to find an M satisfying these conditions and so that $D = \Theta^2$. Of course, we should not expect a unique solution.

If such an M exists, and $\zeta_1, \zeta_2, \zeta_3$ are the zeros of Ψ, then it is easy to see that $\det W^{-1} = 1 - 3p'/D$; and so we must have $\Theta = (1 - 3p'/D)^{-1}$, or

$$p' = -p\Theta. \tag{9}$$

Thus p' is determined by D. We must determine q' so that

$$M = {}^{t}W \begin{pmatrix} \zeta_1 & & \\ & \zeta_2 & \\ & & \zeta_3 \end{pmatrix} W, \quad \text{where} \quad W^{-1} = \begin{pmatrix} \zeta_1 & \zeta_3 & \zeta_2 \\ \zeta_2 & \zeta_1 & \zeta_3 \\ \zeta_3 & \zeta_2 & \zeta_1 \end{pmatrix},$$

is an R-matrix; and Ψ is irreducible. Evidently M is an R-matrix if and only if $m_{ii} \in R$ $(i = 2, 3)$. But a calculation shows that W is the normalized group matrix determined by $\Theta\zeta_i + p$ $(i = 1, 2, 3)$; and so we find

$$m_{22} + p = D(\zeta_1\zeta_3^2 + \zeta_2\zeta_1^2 + \zeta_3\zeta_2^2), \qquad m_{33} + p = D(\zeta_1\zeta_2^2 + \zeta_2\zeta_3^2 + \zeta_3\zeta_1^2).$$

This leads to the following equation for q':

$$27q'^2 + 2bq' + c = 0,$$

where $b = \Theta(3 - \Theta)$ and $c = A^2 - p^2(1 + p)\Theta$ for some $A \in R$. The solubility of this latter equation can be shown to be equivalent to the condition

$$(10) \qquad 4\Theta = 27A^2 + B^2, \quad A, B \in R.$$

For if 3 is a unit in R, this is a consequence of the quadratic formula, and

$$(11) \qquad q' = \tfrac{1}{27}(\pm B - b).$$

If 3 is not a unit, then we must further show that it is possible to choose the sign of B in (11) so that $q' \in R$. However, in determining the discriminant of the quadratic equation defining q', we see that $B^2 \equiv b^2 \pmod{27}$. Now if both $B - b$ and $B + b$ are divisible by 3, then $b \equiv 0 \pmod 3$. This cannot happen; therefore one of these factors is prime to 3 and so there is exactly one choice of sign so that $q' \in R$.

Suppose that the coefficients of Ψ have been determined as above. Then if Ψ factors, it factors completely. We must have a criterion for its irreducibility. For this we may assume R is a field. Let $R^* = R(\sqrt{3})$, so R^* contains the cube roots of 1_R. Then Ψ factors over R if and only if it factors over R^*. Let ρ be a primitive cube root of unity and let $(\rho, \zeta) = \zeta_1 + \rho\zeta_2 + \rho^2\zeta_3$ be the Lagrange resolvent. For A and B as defined in (10) we then set $\Theta(A, B) = (\rho, \zeta)^3$. A direct computation using our previous relations gives the formula

$$\Theta(A, B) = \frac{1}{2D}(B + 3A\sqrt{-3}),$$

and Ψ is irreducible if and only if $\Theta(A, B)$ is not a cube in R^*.

We now specialize to the case where R is a local or global number field. If v is a prime divisor of R and v^* a prime divisor of R^* dividing v $(v \neq v^*)$, then in terms of the cubic power residue symbol

$$\left(\frac{\Theta(A, B)}{v^*}\right)_3 = \left(\frac{\frac{1}{2}(B + 3A\sqrt{-3})}{v^*\bar{v}^*}\right)_3 \quad \text{if } v \nmid \Theta,$$

where $\bar{v}^*$ is the conjugate of v^*. Hence we have proved that if v is any prime not dividing 3Θ, then Ψ factors locally at R_v if and only if

$$\left(\frac{\frac{1}{2}(B +\text{-}3A\sqrt{-3}}{v}\right)_3 = 1.$$

We have:

THEOREM 2. *Let R be a ring of integers in a local or global number field. Then there is a normal cubic R-order Γ with discriminant Θ^2 if and only if $\Theta \in R$ satisfies the following:*

(i) $\Theta \equiv 1 \pmod 3$;
(ii) $4\Theta = 27A^2 + B^2$, $A, B \in R$;
(iii) $\frac{1}{2}(B + 3A\sqrt{-3})$ *is not a cube in* R^*.

Moreover, if these conditions are satisfied, then a normal basis is given by $\{\Theta\zeta_i + (1 - \Theta)/3\}_{i=1,2,3}$, *where* ζ_i *are the roots of* $\Phi = 0$.

Proof. Everything has been proved except the last statement. Since $(1 - \Theta)/3 = p$, we note that $\gamma_i = \Theta\zeta_i + (1 - \Theta)/3$ $(i = 1, 2, 3)$ is the first row of the matrix W. So if v_1, v_2, v_3 is the normal basis corresponding to M, trace $(v_i v_j) =$ trace $(\gamma_i \gamma_j)$ from which we see that $\gamma_i = v_i$ $(i = 1, 2, 3)$.

Remarks. (1) If R is global and $\Theta \in R$ is a unit satisfying the conditions of Theorem 2, then the class number of the quotient field of R is divisible by three.

(2) If $R = \mathbf{Z}$, then $\Theta > 0$; so if Θ were a unit then we would have $\Theta = +1$. But then $\Psi(x) = x^3 - x^2$, which is not irreducible. This shows that every cyclic cubic over $\mathbf{Q}$ must ramify because $\mathbf{Z}$ does not contain "enough" units.

Suppose that R is a number field. Then the normal basis theorem implies that any cyclic cubic extension of R is of the form Γ for some M. If Γ corresponds to the triple (Θ, A, B) we define a character χ on the free group generated by those primes which do not divide 3Θ by

$$\chi(m) = \left(\frac{\frac{1}{2}(B + 3A\sqrt{-3})}{m}\right)_3 \tag{12}$$

Our results imply that for almost all primes v, $\chi(v) = 1$ if and only if v splits (completely) in Γ. Since a normal extension is determined by the primes which split completely in it, χ is uniquely associated to Γ; and the number of distinct cubic cyclic fields corresponding to a given Θ is equal to the number of distinct triples (Θ, A, B), satisfying (ii) of Theorem 2, such that for any pair (Θ, A, B) and (Θ, A', B'),

$$(B + 3A\sqrt{-3})/(B' + 3A'\sqrt{-3}) \notin R^{*3}$$

Finally we consider tamely ramified cyclic cubic extensions of $\mathbf{Q}$. It is known that such extensions have a normal integral basis; and hence correspond to $\mathbf{Z}$-algebras for some M. We have:

THEOREM 3. *An integer D is the discriminant of a cyclic tamely ramified cubic number field if and only if it has the form $D = \Theta^2$, where Θ is square free, and $4\Theta = 27A^2 + B^2$ is soluable in integers. If D satisfies these conditions Θ is uniquely determined and the number of distinct extensions of discriminant D is given by $\frac{1}{2}r(\Theta)$, where $r(\Theta)$ is the number of distinct solutions of $4\Theta = 27A^2 + B^2$ in integers.*

Proof. It is clear that D must be of the stated form, and that Θ is uniquely determined. That Θ is square-free follows from the definition of tame ramification. Conversely these conditions imply Θ satisfies the hypotheses of Theorem 2, so we can find a normal $\mathbf{Z}$-order $\mathcal{O}$ with discriminant D. Let K be the quotient field of $\mathcal{O}$, it is necessary to show that $\mathcal{O}$ is the ring of integers in K. Since Θ is square-free we have the factorization

$$\tfrac{1}{2}(B + 3A\sqrt{-3}) = \pi_1, \dots, \pi_n \quad (\text{in } \mathbf{Q}^*)$$

where π_i are distinct primes. If $\mathcal{O}$ is a proper subring of the integers $\mathcal{O}_K$, then there exists a Θ' dividing Θ and such that $\mathcal{O}_K$ corresponds to some triple (Θ', A', B'). Our remarks concerning the character defined in (12) imply that

$$(B + 3A\sqrt{-3})/(B' + 3A'\sqrt{-3}) \in \mathbf{Q}^{*3};$$

therefore we have the factorization

$$\tfrac{1}{2}(B' + 3A'\sqrt{-3}) = \varepsilon\pi_1, \dots, \pi_n,$$

where ε is a unit. Since Θ is square-free, Norm $(\pi_i) \equiv 1 \pmod 3$ all i. That is, $\pi_i = \frac{1}{2}(x_i + 3y_i\sqrt{-3})$. Comparing both sides of the above equation, we see that $\varepsilon = 1$. Hence by the unique factorization, this is a contradiction unless $\Theta' = \Theta$, $A' = A$, and $B' = B$.

Finally we have seen that to each pair (A, B) satisfying (10) there is exactly one choice of $\pm B$ in (11) giving an integral q'. Thus, in view of the previous paragraph, there are $\frac{1}{2}r(\Theta)$ cyclic extensions with discriminant D.

We suppose that $K \mid \mathbf{Q}$ is a tamely ramified cyclic cubic extension with $\mathcal{O}_K$ corresponding to (Θ, A, B). It is easy now to generalize our results to give a characterization of the orders $\mathcal{O} \subset \mathcal{O}_K$ having a normal $\mathbf{Z}$-basis. They correspond to triples (Θ', A', B') satisfying the following conditions:

(i) $4\Theta' = 27A'^2 + B'^2$, $A', B' \in Z$,

(ii) $B' + 3A'\sqrt{-3} \equiv B + 3A\sqrt{-3} \pmod{\mathbf{Q}^{*3}}$.

Thus their determination is reduced to the calculation of cubic residues in Q^{*3}.

Summary and further remarks

The preceeding section has been devoted to an application of our results to constructions in the case $n = 3$. Although the arithmetic of cyclic cubic extensions has been treated elsewhere [1] in extensive detail, the methods presented here are more direct and apply, with obvious modifications, to general integral domains. Moreover, a consideration of the similarity between quadratic and cubic constructions lead to the conjecture that the discriminant (at least when G is cyclic) is essentially the norm of the nth power of a Lagrange resolvent of the zeros of Φ. This would provide the key to extending the constructive procedures discussed in this paper.

REFERENCES

1. A. CHATELET, *Arithmetique des corps abeliens du troisième degre*, Ann. Sci. Ecole Norm. Sup. (3), vol. 63 (1946), pp. 109–160 (1947).
2. M. NEUMAN AND O. TAUSSKY, *A generalization of the normal basis in abelian algebraic number fields*, Comm. Pure Appl. Math., vol. 9 (1956), pp. 85–91.
3. R. C. THOMPSON, *Normal matrices and the normal basis in abelian number fields*, Pacific J. Math., vol. 12 (1962), pp. 1115–1124.
4. ———, *Unimodular group matrices with rational integers as elements*, Pacific J. Math., vol. 14 (1964), pp. 719–726.
5. P. J. WEINBERGER AND L. P. ROTHSCHILD, *Factoring polynomials over algebraic number fields*, ACM Transactions on Mathematical Software, vol. 2 (1976), pp. 335–350.

CENTER FOR NAVAL ANALYSIS
ARLINGTON, VIRGINIA