

Integral Bases for Number Fields Arising from Circulant Matrices

Robert G. Underwood

Department of Mathematics
Auburn University Montgomery
Montgomery, AL 36124, USA
runderwo@mail.aum.edu

Abstract. In this paper we compute integral bases for some algebraic number fields.

Mathematics Subject Classification: 11R04, 11R09, 11S15

Keywords: finite extension, integral basis, Galois extension, circulant matrix

1. INTRODUCTION

Let K be a finite extension of \mathbb{Q} of degree $n = [K : \mathbb{Q}]$ and let R be the integral closure of \mathbb{Z} in K . Since R is a finitely generated torsion free \mathbb{Z} -module, R is a free \mathbb{Z} -module. Since $K = \mathbb{Q}R$, R contains a basis for K over \mathbb{Q} , called an *integral basis* for K over \mathbb{Q} . In this paper we compute integral bases for some given algebraic number fields.

We have the following standard facts about R . Most of these results can be found in [1, Chapters I, II] or [3]. An ideal J of R factors uniquely into a product of distinct prime ideals in R . Specifically, for each rational prime $p \in \mathbb{Z}$, the principal ideal pR factors as

$$pR = P_1^{e_1} P_2^{e_2} \cdots P_g^{e_g}$$

where e_i , $i = 1, 2, \dots, g$, are positive integers. For each i , the prime P_i is said to *lie above* p . Every non-zero prime ideal in R lies above a unique rational prime in \mathbb{Z} . Since the ring of integers R is a Dedekind domain, each ideal P_i is maximal, thus R/P_i is a field extension of $\mathbb{Z}/p\mathbb{Z}$ of degree $f_i = [R/P_i : \mathbb{Z}/p\mathbb{Z}]$. We have the formula

$$(1) \quad n = \sum_{i=1}^g e_i f_i.$$

If K/\mathbb{Q} is a Galois extension with group G , then $e_1 = e_2 = \cdots = e_g$, and thus

$$pR = (P_1 P_2 \cdots P_g)^e$$

where $e = e_1$. The integer e is the *ramification index of p in R* . If $e > 1$, then the rational prime $p \in \mathbb{Z}$ *ramifies* in R , and if $e = 1$ then p is *unramified* in R . If $e = [K : \mathbb{Q}]$, then p is *totally ramified* in R . If $p \nmid e$, then p is *tamely ramified* in R . Moreover, the degree $f_i = [R/P_i : \mathbb{Z}/p\mathbb{Z}]$ does not depend on i , that is, $f_1 = f_2 = f_3 = \cdots = f_g$, and so, with $f = f_1$, (1) can be written as

$$(2) \quad n = efg.$$

The *trace of K over \mathbb{Q}* is the map $\text{tr}_{L/K} : K \rightarrow \mathbb{Q}$ defined as $\text{tr}_{K/\mathbb{Q}}(x) = \sum_{g \in G} g(x)$, for $x \in K$. Let M be a free \mathbb{Z} -submodule of K of rank n which satisfies $\mathbb{Q}M = K$. Let $\{\alpha_i\}_{i=1}^n$ be a \mathbb{Z} -basis for M . The *discriminant of M over \mathbb{Z}* is the ideal of \mathbb{Z} defined as

$$(3) \quad \text{disc}(M/\mathbb{Z}) = \det(A)\mathbb{Z}$$

where A is the $n \times n$ matrix whose (i, j) th entry is $\text{tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j)$.

Suppose that N is a free \mathbb{Z} -submodule of K of rank n satisfying $\mathbb{Q}N = K$ and $N \subseteq M$. Let $\{\beta_i\}_{i=1}^n$ denote a \mathbb{Z} -basis for N . Then there exists an invertible matrix B so that

$$B \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix},$$

and one has the formula

$$(4) \quad \text{disc}(N/\mathbb{Z}) = \det(B)^2 \mathbb{Z} \cdot \text{disc}(M/\mathbb{Z})$$

with $\det(B)^2 \mathbb{Z}$ an ideal of \mathbb{Z} .

Formula (3) can be applied to the case $M = R$ to obtain the discriminant of R over \mathbb{Z} . The discriminant determines which primes in \mathbb{Z} are ramified.

Proposition 1.1. *The prime p in \mathbb{Z} ramifies in R if and only if p divides $\text{disc}(R/\mathbb{Z})$.*

Remark 1.2. By a result of H. Minkowski if $K \neq \mathbb{Q}$, then $\text{disc}(R/\mathbb{Z})$ is a non-zero proper ideal of \mathbb{Z} . Thus in any algebraic number field $K \neq \mathbb{Q}$ there is at least one prime that ramifies.

Now suppose K, L are Galois extensions of \mathbb{Q} with $\mathbb{Q} \subseteq K \subseteq L$. Let R be the ring of integers in K , and let S denote the ring of integers in L . Let p be a prime of \mathbb{Z} and suppose that Q is a prime ideal of R which lies above p . The ideal QS of S factors as

$$QS = P_1^{e_1} P_2^{e_2} \cdots P_g^{e_g},$$

where P_l is prime in S for $1 \leq l \leq g$. Let K_Q denote the completion of K at Q , with ring of integers R_Q , and for each l , let L_{P_l} denote the completion of L at P_l with ring of integers S_{P_l} . Let M be a free R_Q -submodule of L_{P_l} of rank n with basis $\{\alpha_i\}_{i=1}^n$, which satisfies $K_Q M = L_{P_l}$. Following (3), the discriminant $\text{disc}(M/R_Q)$ is defined as

$$(5) \quad \text{disc}(M/R_Q) = \det((\text{tr}_{L_{P_l}/K_Q}(\alpha_i \alpha_j)) R_Q),$$

where $\text{tr}_{L_{P_l}/K_Q} : L_{P_l} \rightarrow K_Q$ is the trace map of the Galois extension of local fields L_{P_l}/K_Q , that is, $\text{tr}_{L_{P_l}/K_Q}(x) = \sum_{g \in G_P} g(x)$, for $x \in L_{P_l}$, where

$$\text{Gal}(L_{P_l}/K_Q) = G_{P_l} = \{g \in \text{Gal}(L/K) \mid g(P_l) = P_l\}.$$

If $N \subseteq M$ is an inclusion of free R_Q -submodules of L_{P_l} with $K_Q N = K_Q M = L_{P_l}$, and B is the matrix which multiplies an R_Q -basis of M to give an R_Q -basis of N , then the analog of (4) is

$$(6) \quad \text{disc}(N/R_Q) = \det(B)^2 R_Q \cdot \text{disc}(M/R_Q)$$

Globally, S may not be a free R -module, though the localization S_{P_l} is a finitely generated torsion-free module over the PID R_Q . Thus S_{P_l} is a free R_Q -module and so $\text{disc}(S_{P_l}/R_Q)$ is defined by (3).

2. COMPUTING INTEGRAL BASES

In this section we apply the formulas of §1 to compute integral bases for the splitting fields of a collection of polynomials which we now define. Let $p \geq 3$ be prime, let $\zeta = \zeta_p$ denote a primitive p th root of unity. Let a, b satisfy the relations

$$(7) \quad a^p + b^p = 1 \text{ and } ab = 1.$$

Let x be an indeterminate and let

$$A = \begin{pmatrix} a & x & c & 0 & 0 & \cdots & 0 \\ 0 & a & x & c & 0 & \cdots & 0 \\ 0 & 0 & a & x & c & \cdots & 0 \\ \vdots & & & & & & \vdots \\ x & c & 0 & 0 & 0 & \cdots & a \end{pmatrix}$$

denote the $p \times p$ circulant matrix

$$\text{circ}(a, x, c, \underbrace{0, 0, \dots, 0}_{p-3}).$$

Then $\det(A)$ defines a polynomial in x :

$$(8) \quad f_p(x) = x^p + \sum_{i=1}^{(p-1)/2} (-1)^i \frac{p}{p-i} \binom{p-i}{i} x^{p-2i} + 1$$

which factors as

$$f_p(x) = \prod_{i=0}^{p-1} (x\zeta^i + a + b\zeta^{2i}).$$

We find specific values for a and b which satisfy the relations (7). Let $\eta = \frac{1 + i\sqrt{3}}{2}$ with conjugate $\bar{\eta} = \frac{1 - i\sqrt{3}}{2}$, and put $\theta = \eta^{1/p}$. Then $\theta^p + \bar{\theta}^p = \eta + \bar{\eta} = 1$ and $\theta\bar{\theta} = 1$, and so, with $a = \theta$, $b = \bar{\theta}$, $f_p(x)$ factors as

$$f_p(x) = \prod_{i=0}^{p-1} (x\zeta^i + \theta + \bar{\theta}\zeta^{2i}).$$

Thus the roots of $f_p(x)$ are

$$r_0 = -\theta - \bar{\theta}, \quad r_1 = -\theta\zeta^{-1} - \bar{\theta}\zeta, \quad r_2 = -\theta\zeta^{-2} - \bar{\theta}\zeta^2, \\ r_3 = -\theta\zeta^{-3} - \bar{\theta}\zeta^3, \dots, r_{p-1} = -\theta\zeta^{-(p-1)} - \bar{\theta}\zeta^{p-1}.$$

We consider the case $p = 3$ in (8).

The case $p = 3$. The polynomial in (8) is

$$f_3(x) = x^3 - 3x + 1,$$

which is irreducible over \mathbb{Q} . Moreover, the zeros of $f_3(x)$ are $r_0 = -\theta - \bar{\theta}$, $r_1 = -\theta\zeta^{-1} - \bar{\theta}\zeta$, and $r_2 = -\theta\zeta^{-2} - \bar{\theta}\zeta^2$, with $\theta = e^{\pi i/9}$. These roots are related by the equations

$$(9) \quad r_0^2 = r_1 + 2, \quad r_1^2 = r_2 + 2, \quad r_2^2 = r_0 + 2.$$

Thus the splitting field of $f_3(x)$ is $K = \mathbb{Q}(r_0)$. We have $[K : \mathbb{Q}] = 3$, so that $\text{Gal}(K/\mathbb{Q}) = C_3 = \langle g \rangle$ with $g(r_0) = r_1$, $g(r_1) = r_2$, and $g(r_2) = r_0$.

Proposition 2.1. *Let K be the splitting field of $f_3(x) = x^3 - 3x + 1$. Then $R = \mathbb{Z}[r_0]$, and thus, $\{1, r_0, r_0^2\}$ is an integral basis for K over \mathbb{Q} .*

Proof. Let $\mathbb{Z}[r_0]$ denote the free \mathbb{Z} -module on the basis $\{1, r_0, r_0^2\}$. Then formula (3) applies to give $\text{disc}(\mathbb{Z}[r_0]/\mathbb{Z}) = \det(M)\mathbb{Z}$, where M is the 3×3 matrix

$$M = \begin{pmatrix} \text{tr}(1) & \text{tr}(r_0) & \text{tr}(r_0^2) \\ \text{tr}(r_0) & \text{tr}(r_0^2) & \text{tr}(r_0^3) \\ \text{tr}(r_0^2) & \text{tr}(r_0^3) & \text{tr}(r_0^4) \end{pmatrix}$$

Now, in view of the relations in (9),

$$M = \begin{pmatrix} \text{tr}(1) & \text{tr}(r_0) & \text{tr}(r_1 + 2) \\ \text{tr}(r_0) & \text{tr}(r_1 + 2) & \text{tr}(3r_0 - 1) \\ \text{tr}(r_1 + 2) & \text{tr}(3r_0 - 1) & \text{tr}(r_2 + 4r_1 + 6) \end{pmatrix} = \begin{pmatrix} 3 & 0 & 6 \\ 0 & 6 & -3 \\ 6 & -3 & 18 \end{pmatrix},$$

and thus $\text{disc}(\mathbb{Z}[r_0]/\mathbb{Z}) = 81\mathbb{Z}$.

Since $\mathbb{Z}[r_0] \subseteq R$, $\text{disc}(R/\mathbb{Z})$ divides $\text{disc}(\mathbb{Z}[r_0]/\mathbb{Z})$, and so by Proposition 1.1 and Remark 1.2, 3 is the only prime which ramifies in R . By (2), $[K : \mathbb{Q}] = 3 = efg$, and so 3 is totally ramified in R . Thus $(3) = Q^3$ for some prime ideal of R .

Let R_Q be the completion of R at Q . By (6)

$$\text{disc}(\mathbb{Z}_{(3)}[r_0]/\mathbb{Z}_{(3)}) = [R_Q : \mathbb{Z}_{(3)}[r_0]]^2 \text{disc}(R_Q/\mathbb{Z}_{(3)}),$$

where $[R_Q : \mathbb{Z}_{(3)}[r_0]]$ is the module index of $\mathbb{Z}_{(3)}[r_0]$ in R_Q . Necessarily, $[R_Q : \mathbb{Z}_{(3)}[r_0]] = 3^a \mathbb{Z}_{(3)}$ for some $a \geq 0$. Since $\text{Gal}(K_Q/\mathbb{Q}_3) = \text{Gal}(K/\mathbb{Q}) = \langle g \rangle$,

$$\text{disc}(\mathbb{Z}_{(3)}[r_0]/\mathbb{Z}_{(3)}) = 81\mathbb{Z}_{(3)} = 3^4\mathbb{Z}_{(3)},$$

and so, $0 \leq a \leq 2$. If $a = 2$, then $\text{disc}(R_Q/\mathbb{Z}_{(3)}) = \mathbb{Z}_{(3)}$, which contradicts Remark 1.2.

Next, suppose that $a = 1$. Then $\text{disc}(R_Q/\mathbb{Z}_{(3)}) = 9\mathbb{Z}_{(3)}$. Let

$$R^D = \{x \in K \mid \text{tr}_{K/\mathbb{Q}}(xR) \subseteq \mathbb{Z}\}$$

denote the *dual module* of R , and let

$$\mathcal{D} = (R^D)^{-1} = \{x \in K \mid xR^D \subseteq \mathbb{Z}\}$$

denote the *different*, which is an integral ideal of R . By [1, Chapter I, §4, (4)] and [1, Chapter I, §4, Proposition 5(i)],

$$\text{disc}(R_Q/\mathbb{Z}_{(3)}) = N_{K_Q/\mathbb{Q}_3}(\mathcal{D}R_Q)$$

where $N_{K_Q/\mathbb{Q}_3}(z) = zg(z)g^2(z)$ is the norm map. Now,

$$9\mathbb{Z}_{(3)} = N_{K_Q/\mathbb{Q}_3}(\mathcal{D}R_Q),$$

and so, by [1, Chapter I, §5, Theorem 2], K/\mathbb{Q} is tamely ramified at 3, which contradicts K/\mathbb{Q} being totally ramified at 3.

Thus the only possibility is $a = 0$, and in this case, $\text{disc}(\mathbb{Z}_{(3)}[r_0]/\mathbb{Z}_{(3)}) = \text{disc}(R_Q/\mathbb{Z}_{(3)})$, and so $R_Q = \mathbb{Z}_{(3)}[r_0]$ by [1, Chapter I, §3, Corollary 1]. Therefore by [1, Chapter I, §3, Lemma 1], $R = \mathbb{Z}[r_0]$. \square

The case $p \geq 5$. For $p \geq 5$, the polynomial $f_p(x)$ is reducible. To see this observe that $p \geq 5$ implies $\eta^{p^2} = \eta$, and so, we may choose $\theta = \eta^p$. With this choice of θ , $r_0 = -\theta - \bar{\theta} = -1$. Dividing out this zero we obtain the polynomial

$$h_p(x) = \frac{f_p(x)}{x + 1},$$

which is irreducible over \mathbb{Q} by [2, Lemma 5]. The roots of $h_p(x)$ are $\{r_j\}_{j=1}^{p-1}$, and are related by the formula

$$r_j^2 = r_{p-2j} + 2,$$

where the subscript $p - 2j$ is taken to be the least positive residue modulo p . Thus, the splitting field of $h_p(x)$ is $\mathbb{Q}(r_1)$, with $[\mathbb{Q}(r_1) : \mathbb{Q}] = p - 1$.

It is known that the Galois group of $\mathbb{Q}(r_1)$ over \mathbb{Q} is C_{p-1} , cf. [2, Theorem A]. The map $g : \mathbb{Q}(r_1) \rightarrow \mathbb{Q}(r_1)$ defined by $r_j \mapsto r_{p-2j}$ is an automorphism of $\mathbb{Q}(r_1)$ which fixes \mathbb{Q} , and so, $g \in \text{Gal}(\mathbb{Q}(r_1)/\mathbb{Q})$. However, depending on the prime p , g may or may not generate $\text{Gal}(\mathbb{Q}(r_1)/\mathbb{Q})$.

We assume that the prime p is so that $\langle g \rangle = \text{Gal}(\mathbb{Q}(r_1)/\mathbb{Q})$. We write g as the permutation of the subscripts of the r_j (again taking these subscripts to be the least positive residue modulo p):

$$g = \begin{pmatrix} 1 & 2 & 3 & \cdots & p-2 & p-1 \\ p-2j & p-4j & p-6j & \dots & 4 & 2 \end{pmatrix}.$$

One has the sequence of fields $\mathbb{Q} \subseteq K \subseteq L$, with $K = \mathbb{Q}(r_1 + r_{p-1})$, and $L = \mathbb{Q}(r_1)$. Let S denote the ring of integers in L and let R denote ring of integers in K . Set $\zeta = \zeta_p$. Since

$$\begin{aligned} r_1 + r_{p-1} &= -\theta\zeta^{-1} - \bar{\theta}\zeta - \theta\zeta - \bar{\theta}\zeta^{-1} \\ &= -\theta(\zeta^{-1} + \zeta) - \bar{\theta}(\zeta + \zeta^{-1}) \\ &= -(\theta + \bar{\theta})(\zeta + \zeta^{-1}) \\ &= -(\zeta + \zeta^{-1}), \end{aligned}$$

$K = \mathbb{Q}(r_1 + r_{p-1}) = \mathbb{Q}(\zeta + \zeta^{-1})$, which is the maximal real subfield in the cyclotomic extension $\mathbb{Q}(\zeta)$. We have $[L : \mathbb{Q}] = p - 1$, $[L : K] = 2$, and $[K : \mathbb{Q}] = (p - 1)/2$. Moreover, $\text{Gal}(L/K) = \{1, d\}$ where

$$d = g^{(p-1)/2} = \begin{pmatrix} 1 & 2 & 3 & \cdots & p-2 & p-1 \\ p-1 & p-2 & p-3 & \cdots & 2 & 1 \end{pmatrix}.$$

For $z \in L$, define $\text{tr}_{L/K}(z) = z + d(z)$.

Proposition 2.2. *Assume that the prime p is so that $\langle g \rangle = \text{Gal}(\mathbb{Q}(r_1)/\mathbb{Q})$. Then $S = \mathbb{Z}[r_1]$, and thus, $\{1, r_1, r_1^2, \dots, r_1^{p-2}\}$ is an integral basis for L over \mathbb{Q} .*

Proof. We first show that $S = R[r_1]$, where $R[r_1]$ denotes the free R -module on the basis $\{1, r_1\}$. Let Q be any prime ideal of R , and let R_Q denote the completion of R at Q . For any R -module T , put $T_Q = R_Q \otimes_R T$. We show that

$$(10) \quad S_Q = R[r_1]_Q, \quad \text{for all } Q \text{ prime,}$$

for then

$$\bigcap_{Q \text{ prime}} S_Q = \bigcap_{Q \text{ prime}} R[r_1]_Q,$$

and so, $S = R[r_1]$, by [1, Chapter I, §3, Lemma 1].

Since $R[r_1]_Q \subseteq S_Q$, (10) holds if

$$(11) \quad \text{disc}(R[r_1]_Q/R_Q) = \text{disc}(S_Q/R_Q),$$

for all prime ideals Q in R . The discriminant in (11) is taken with respect to $\text{Gal}(L_P/K_Q)$, where P is a prime of S lying above Q . Now $\text{Gal}(L_P/K_Q)$ is either trivial, in which case (11) holds, or $\text{Gal}(L_P/K_Q) = \text{Gal}(L/K) = \{1, d\}$. We assume the latter case. Then $\text{disc}(R[r_1]_Q/R_Q) = \det(M)R_Q$, where M is the 2×2 matrix

$$\begin{aligned} \begin{pmatrix} \text{tr}_{L/K}(1) & \text{tr}_{L/K}(r_1) \\ \text{tr}_{L/K}(r_1) & \text{tr}_{L/K}(r_1^2) \end{pmatrix} &= \begin{pmatrix} 2 & r_1 + r_{p-1} \\ r_1 + r_{p-1} & r_{p-2} + r_2 + 4 \end{pmatrix} \\ &= \begin{pmatrix} 2 & -\zeta - \zeta^{-1} \\ -\zeta - \zeta^{-1} & -\zeta^{-2} - \zeta^2 + 4 \end{pmatrix}. \end{aligned}$$

Thus

$$(12) \quad \begin{aligned} \text{disc}(R[r_1]_Q/R_Q) &= (-3\zeta^2 - 3\zeta^{-2} + 6)R_Q \\ &= (3R_Q)((\zeta^2 + \zeta^{-2} - 2)R_Q), \end{aligned}$$

with $3R$ and $(\zeta^2 + \zeta^{-2} - 2)R$ relatively prime ideals of R .

If Q lies above 3, then $\text{disc}(R[r_1]_Q/R_Q) = 3R_Q$, and so, by (6)

$$3R_Q = [S_Q : R[r_1]_Q]^2 \text{disc}(S_Q/R_Q),$$

where $[S_Q : R[r_1]_Q]^2$ is the module index, an ideal of R_Q . Since 3 is unramified in R , $3R_Q = \text{disc}(S_Q/R_Q)$. Thus

$$\text{disc}(R[r_1]_Q/R_Q) = \text{disc}(S_Q/R_Q),$$

which yields

$$(13) \quad S_Q = R[r_1]_Q$$

for all Q lying above 3.

Since $(\zeta^2 + \zeta^{-2} - 2)R$ is a prime ideal of R , $\text{disc}(R[r_1]_Q/R_Q) = QR_Q$, with $Q = (\zeta^2 + \zeta^{-2} - 2)R$. Thus

$$QR_Q = [S_Q : R[r_1]_Q]^2 \text{disc}(S_Q/R_Q),$$

and so,

$$\text{disc}(R[r_1]_Q/R_Q) = \text{disc}(S_Q/R_Q),$$

hence

$$S_Q = R[r_1]_Q.$$

We conclude that for each prime ideal Q of R ,

$$\text{disc}(R[r_1]_Q/R_Q) = \text{disc}(S_Q/R_Q).$$

Thus, $R[r_1]_Q = S_Q$, which yields $S = R[r_1]$. Now since $R = \mathbb{Z}[\zeta + \zeta^{-1}] = \mathbb{Z}[r_1 + r_{p-1}]$, one has

$$S = R[r_1] = \mathbb{Z}[r_1 + r_{p-1}][r_1] = \mathbb{Z}[r_1].$$

□

REFERENCES

- [1] J. W. S. Cassels and A. Fröhlich (eds.), Algebraic Number Theory, Academic Press, London, 1967.
- [2] M. Filaseta, F. Luca, P. Stanica, and R. G. Underwood, Galois groups of polynomials arising from circulant matrices, *J. Num. Theory*, **128**, (2008), 59-70.
- [3] R. G. Underwood, An Introduction to Hopf Algebras, Springer, New York, to appear.

Received: February 6, 2008