RINGS OF INTEGERS WITHOUT A POWER BASIS

KEITH CONRAD

Let K be a number field, with degree n and ring of integers $\mathcal{O}_K$. If $\mathcal{O}_K = \mathbf{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$, then $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a $\mathbf{Z}$-basis of $\mathcal{O}_K$. We call such a basis a *power basis*.

When K is a quadratic field or a cyclotomic field, $\mathcal{O}_K$ admits a power basis, and the use of these two fields as examples in algebraic number theory can lead to the impression that rings of integers always have a power basis. This is false. While it is always true that

$$\mathcal{O}_K = \mathbf{Z}e_1 \oplus \cdots \oplus \mathbf{Z}e_n$$

for some $e_1, \ldots, e_n$, often we can not choose the e_i's to be powers of a single number. We will describe the first known cubic field K where $\mathcal{O}_K$ has no power basis, then describe an infinite set of Galois cubic fields whose ring of integers has no power basis, and then describe an infinite set of quadratic extensions of imaginary quadratic fields without a relative integral power basis.

1. Dedekind's cubic field

The following example is due to Dedekind. He showed how he found it in 1871 [1, pp. 1490–1492] (pp. 13-14 in the English translation). In later work, such as [2, pp. 30–36], it was introduced without explanation.

Theorem 1.1. *Let $K = \mathbf{Q}(\theta)$ where $\theta^3 - \theta^2 - 2\theta - 8 = 0$.*[1] *Then $\theta' := 4/\theta$ is in $\mathcal{O}_K$, $\mathcal{O}_K = \mathbf{Z} + \mathbf{Z}\theta + \mathbf{Z}\theta'$, and for all α in $\mathcal{O}_K - \mathbf{Z}$ we have $2 \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$, so $\mathcal{O}_K \neq \mathbf{Z}[\alpha]$.*

Proof. The field K is cubic since the polynomial is irreducible over $\mathbf{Q}$. By algebra,

$$\begin{aligned}\theta^3 - \theta^2 - 2\theta - 8 = 0 &\Longrightarrow \frac{8}{\theta^3} + \frac{2}{\theta^2} + \frac{1}{\theta} - 1 = 0 \\ &\Longrightarrow \left(\frac{4}{\theta}\right)^3 + \left(\frac{4}{\theta}\right)^2 + 2\frac{4}{\theta} - 8 = 0,\end{aligned}$$

so θ' is a root of $T^3 + T^2 + 2T - 8$ and thus $\theta' \in \mathcal{O}_K$. From the cubic relations of θ and θ' over $\mathbf{Q}$, we have $\theta' = 4/\theta = (\theta^2 - \theta)/2 - 1$ and $\theta = 4/\theta' = (\theta'^2 + \theta')/2 + 1$. Therefore

$$\theta^2 = 2 + \theta + 2\theta', \quad \theta'^2 = -2 + 2\theta - \theta', \tag{1.1}$$

so $\mathbf{Z} + \mathbf{Z}\theta + \mathbf{Z}\theta'$ is a subring of $\mathcal{O}_K$. Using (1.1) and the values $\mathrm{Tr}(\theta) = 1$ and $\mathrm{Tr}(\theta') = -1$, where $\mathrm{Tr} = \mathrm{Tr}_{K/\mathbf{Q}}$,

$$\mathrm{disc}(\mathbf{Z} + \mathbf{Z}\theta + \mathbf{Z}\theta') = \det\begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\theta) & \mathrm{Tr}(\theta') \\ \mathrm{Tr}(\theta) & \mathrm{Tr}(\theta^2) & \mathrm{Tr}(\theta\theta') \\ \mathrm{Tr}(\theta') & \mathrm{Tr}(\theta\theta') & \mathrm{Tr}(\theta'^2) \end{pmatrix} = \det\begin{pmatrix} 3 & 1 & -1 \\ 1 & 5 & 12 \\ -1 & 12 & -3 \end{pmatrix} = -503$$

which is a negative prime, and hence squarefree, so $\mathcal{O}_K = \mathbf{Z} + \mathbf{Z}\theta + \mathbf{Z}\theta'$.

---

[1] Some references define K using a root of $T^3 + T^2 - 2T + 8$, which is the minimal polynomial for $-\theta$. That mixture of positive and negative coefficients makes it harder to *remember* this polynomial, so don't use it. Dedekind didn't use it either.

For all α in $\mathcal{O}_K - \mathbf{Z}$, $K = \mathbf{Q}(\alpha)$, so $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$ is finite: when a finite free $\mathbf{Z}$-module contains another finite-free $\mathbf{Z}$-module of the same rank, the index $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$ is finite. To show this index is even, write $\alpha = a + b\theta + c\theta'$ for integers a, b, and c. Either b or c is not 0 (otherwise $\alpha \in \mathbf{Z}$). The index $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$ can be computed from the matrix A that expresses $1, \alpha, \alpha^2$ as $\mathbf{Z}$-linear combinations of $1, \theta, \theta'$:

$$\begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \end{pmatrix} = A \begin{pmatrix} 1 \\ \theta \\ \theta' \end{pmatrix} \Longrightarrow [\mathcal{O}_K : \mathbf{Z}[\alpha]] = |\det A|$$

by Theorem 5.19 in `https://kconrad.math.uconn.edu/blurbs/linmultialg/modulesoverPID.pdf`.

To compute $\det A$, we may assume $a = 0$ since $\mathbf{Z}[\alpha] = \mathbf{Z}[\alpha - a]$. Then

$$\begin{aligned} \alpha^2 &= (b\theta + c\theta')^2 \\ &= b^2\theta^2 + 2bc(\theta\theta') + c^2\theta'^2 \\ &= b^2(2 + \theta + 2\theta') + 8bc + c^2(-2 + 2\theta - \theta') \quad \text{by}(1.1) \\ &= (2b^2 + 8bc - 2c^2) + (b^2 + 2c^2)\theta + (2b^2 - c^2)\theta', \end{aligned}$$

so

$$\begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & b & c \\ 2b^2 + 8bc - 2c^2 & b^2 + 2c^2 & 2b^2 - c^2 \end{pmatrix} \begin{pmatrix} 1 \\ \theta \\ \theta' \end{pmatrix}$$

and the determinant of the matrix modulo 2 is $-bc^2 - cb^2 = -bc(c + b)$, which is even for all integers b and c. Thus $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$ is even for all α in $\mathcal{O}_K - \mathbf{Z}$. ☐

Corollary 1.2. *As α runs over $\mathcal{O}_K - \mathbf{Z}$, the gcd of the integers* $\operatorname{disc}(\mathbf{Z}[\alpha])$ *is* $4 \cdot 503$.

Proof. We have $\operatorname{disc}(\mathbf{Z}[\alpha]) = \operatorname{disc}(\mathcal{O}_K)[\mathcal{O}_K : \mathbf{Z}[\alpha]]^2 = -503[\mathcal{O}_K : \mathbf{Z}[\alpha]]^2$ and $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$ is even by Theorem 1.1, so $\operatorname{disc}(\mathbf{Z}[\alpha])$ is divisible by $4 \cdot 503$. The gcd of all $\operatorname{disc}(\mathbf{Z}[\alpha])$ is $4 \cdot 503$ since the discriminant is $-4 \cdot 503$ when $\alpha = \theta$:

$$\mathbf{Z}[\theta] = \mathbf{Z} + \mathbf{Z}\theta + \mathbf{Z}\theta^2 = \mathbf{Z} + \mathbf{Z}\theta + \mathbf{Z}2\theta'$$

since $\theta^2 = 2 + \theta + 2\theta'$, so $[\mathcal{O}_K : \mathbf{Z}[\theta]] = 2$ and thus $\operatorname{disc}(\mathbf{Z}[\theta]) = -503[\mathcal{O}_K : \mathbf{Z}[\theta]]^2 = -503 \cdot 4$. ☐

2. Many cubic Galois extensions without a power basis

We now describe infinitely many Galois cubic extensions of $\mathbf{Q}$ whose ring of integers has no power basis. The method is based on the following theorem about cubic fields.

Theorem 2.1. *In a cubic field F where the prime 2 splits completely, $\mathcal{O}_F \neq \mathbf{Z}[\alpha]$ for all $\alpha \in \mathcal{O}_F - \mathbf{Z}$.*

Proof. Suppose $\mathcal{O}_F = \mathbf{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_F - \mathbf{Z}$. Let $f(T)$ be the minimal polynomial of α over $\mathbf{Q}$, so $f(T)$ is an irreducible cubic in $\mathbf{Z}[T]$. Then

$$\mathcal{O}_F = \mathbf{Z}[\alpha] \cong \mathbf{Z}[T]/f(T).$$

Since we are assuming $\mathcal{O}_F = \mathbf{Z}[\alpha]$, the way each prime p decomposes in $\mathcal{O}_F$ matches the way $f(T) \bmod p$ decomposes. Therefore 2 splitting completely in F implies $f(T)$ splits completely in $(\mathbf{Z}/2\mathbf{Z})[T]$: $f(T) \bmod 2$ is a product of three distinct monic linear polynomials.

But $(\mathbf{Z}/2\mathbf{Z})[T]$ only has two such polynomials, T and $T+1$. We have a contradiction, so $\mathcal{O}_F \neq \mathbf{Z}[\alpha]$ for all $\alpha \in \mathcal{O}_F - \mathbf{Z}$. ☐

Now fix a prime $p \equiv 1 \bmod 3$. Since the group $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) \cong (\mathbf{Z}/p\mathbf{Z})^\times$ is cyclic, there is a *unique cubic subfield* F_p in $\mathbf{Q}(\zeta_p)$ and $\mathrm{Gal}(F_p/\mathbf{Q})$ is isomorphic to the quotient of $(\mathbf{Z}/p\mathbf{Z})^\times$ by its subgroup of cubes. A prime number that is unramified in an abelian Galois extension $F/\mathbf{Q}$ splits completely in F if and only if its Frobenius element in $\mathrm{Gal}(F/\mathbf{Q})$ is trivial, so 2 *splits completely in* F_p *if and only if* $2 \bmod p$ *is a cube.* (This reasoning about when 2 splits completely in F_p goes through for every unramified prime in F_p, which means all primes other than p, as p is the only prime ramifying in the larger field $\mathbf{Q}(\zeta_p)$.)

The primes p for which F_p fits the hypothesis of Theorem 2.1 are those $p \equiv 1 \bmod 3$ such that $2^{(p-1)/3} \equiv 1 \bmod p$. These are the primes that split completely in the splitting field of $T^3 - 2$ over $\mathbf{Q}$, and by the Chebotarev density theorem there are infinitely many such p and their density among all primes is 1/6. The first few such p are 31, 43, 109, and 127. For each of these p, Theorem 2.1 tells us the ring of integers of F_p does *not* have a power basis.

Remark 2.2. That the ring of integers of Dedekind's cubic field $\mathbf{Q}(\theta)$ from Theorem 1.1 lacks a power basis can be proved using Theorem 2.1: 2 splits completely in that field. However, showing 2 splits completely in $\mathbf{Q}(\theta)$ requires techniques other than those we used to show 2 splits completely in F_p when $p \equiv 1 \bmod 3$ and $2 \bmod p$ is a cube, since Dedekind's cubic field is not in a cyclotomic field (for example, $\mathbf{Q}(\theta)$ is not Galois over $\mathbf{Q}$).

For a cubic field F, it turns out that 2 splits completely in F *if and only if* $[\mathcal{O}_F : \mathbf{Z}[\alpha]]$ is even for all $\alpha \in \mathcal{O}_F - \mathbf{Z}$. Having that index always be even implies $\mathcal{O}_F \neq \mathbf{Z}[\alpha]$ for all $\alpha \in \mathcal{O}_K - \mathbf{Z}$ since the index can't be 1. In 1882, Kronecker [7, p. 119] said that back in 1858 he had found an example of a subfield K of $\mathbf{Q}(\zeta_{13})$ where $\mathcal{O}_K$ has no power basis over $\mathbf{Z}$. It is the quartic subfield K, and it turns out that $3 \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$ for all $\alpha \in \mathcal{O}_K$ such that $K = \mathbf{Q}(\alpha)$.

A generalization of a number field K satisfying $2 \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$ for all $\alpha \in \mathcal{O}_K$ such that $K = \mathbf{Q}(\alpha)$ is K satisfying $p \mid [\mathcal{O}_K : \mathbf{Z}[\alpha]]$ for some prime p and all $\alpha \in \mathcal{O}_K$ such that $K = \mathbf{Q}(\alpha)$. Call such p a *common index divisor* for K. The existence of such p is sufficient for $\mathcal{O}_K$ not to have a power basis.[2] Dedekind [2, Sect. 4] (and later Hensel [5, p. 138]) showed a prime p is a common index divisor for a number field K if and only if there is $d \geq 1$ such that the number of different prime ideal factors of $p\mathcal{O}_K$ with residue field degree d is greater than the number of monic irreducibles of degree d in $\mathbf{F}_p[T]$.[3] Using $d = 1$, p is a common index divisor for a number field K if $p < [K : \mathbf{Q}]$ since there are p monic irreducibles of degree 1 in $\mathbf{F}_p[T]$ while a prime splitting completely in K has $[K : \mathbf{Q}]$ prime ideal factors in $\mathcal{O}_K$. In particular, if K is a cubic field in which 2 splits completely, then $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$ is even for all $\alpha \in \mathcal{O}_K$ such that $K = \mathbf{Q}(\alpha)$. (A prime p that is a common index divisor for K must be less than $[K : \mathbf{Q}]$ by a theorem of von Zylinski [10].[4]) See [3] for a proof that there are infinitely many cubic fields without a power basis for which this even-index condition does *not* apply.

When $p \equiv 1 \bmod 3$, $\mathcal{O}_{F_p}$ may or may not have a power basis. The next theorem gives a $\mathbf{Z}$-basis for it in all cases.

---

[2] This criterion is not necessary: for $K = \mathbf{Q}(\sqrt[3]{175})$, $\mathcal{O}_K$ has no power basis but $[\mathcal{O}_K : \mathbf{Z}[\sqrt[3]{175}]] = 5$ and $[\mathcal{O}_K : \mathbf{Z}[\sqrt[3]{245}]] = 7$. This is explained in Example 4.15 in https://kconrad.math.uconn.edu/blurbs/gradnumthy/different.pdf.

[3] See Theorem 5.2 in https://kconrad.math.uconn.edu/blurbs/gradnumthy/dedekind-index-thm.pdf

[4] See Theorem 5.3 in https://kconrad.math.uconn.edu/blurbs/gradnumthy/dedekind-index-thm.pdf.

Theorem 2.3. *For each prime* $p \equiv 1 \bmod 3$*, let* $r \in (\mathbf{Z}/p\mathbf{Z})^\times$ *have order* 3*. Then* $\mathcal{O}_{F_p} = \mathbf{Z}\eta_0 + \mathbf{Z}\eta_1 + \mathbf{Z}\eta_2$*, where*

$$\eta_0 = \mathrm{Tr}_{\mathbf{Q}(\zeta_p)/F_p}(\zeta_p) = \sum_{t^{(p-1)/3} \equiv 1 \bmod p} \zeta_p^t, \quad \eta_1 = \sum_{t^{(p-1)/3} \equiv r \bmod p} \zeta_p^t, \quad \eta_2 = \sum_{t^{(p-1)/3} \equiv r^2 \bmod p} \zeta_p^t.$$

The numbers η_i are examples of (cyclotomic) periods [9, pp. 16–17].

Proof. For $c \in (\mathbf{Z}/p\mathbf{Z})^\times$, $c^{(p-1)/3}$ is a cube root of unity and therefore is in $\{1, r, r^2\}$. For suitable c each of the three values is achieved. Let $\sigma_c \in \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ send ζ_p to ζ_p^c. Then

$$\sigma_c(\eta_i) = \sigma_c\left(\sum_{t^{(p-1)/3} \equiv r^i \bmod p} \zeta_p^t\right) = \sum_{t^{(p-1)/3} \equiv r^i \bmod p} \zeta_p^{ct} = \sum_{t^{(p-1)/3} \equiv c^{(p-1)/3} r^i \bmod p} \zeta_p^t,$$

so σ_c permutes $\{\eta_0, \eta_1, \eta_2\}$ the same way multiplication by $c^{(p-1)/3}$ permutes $\{1, r, r^2\}$. Therefore η_0, η_1, and η_2 are $\mathbf{Q}$-conjugates, and since F_p is the unique cubic subfield of $\mathbf{Q}(\zeta_p)$ each of η_0, η_1, η_2 generates F_p as a field extension of $\mathbf{Q}$.

The standard basis of $\mathbf{Q}(\zeta_p)$ over $\mathbf{Q}$ is $\{1, \zeta_p, \ldots, \zeta_p^{p-2}\}$, and this is also a basis for $\mathbf{Z}[\zeta_p]$ over $\mathbf{Z}$. It is more convenient to multiply through by ζ_p and use instead $\mathcal{B} = \{\zeta_p, \zeta_p, \ldots, \zeta_p^{p-1}\}$ as a basis of $\mathbf{Q}(\zeta_p)$ over $\mathbf{Q}$ or $\mathbf{Z}[\zeta_p]$ over $\mathbf{Z}$, since this is a basis of Galois conjugates (a normal basis over $\mathbf{Q}$). For example, η_0, η_1, η_2 are sums of different numbers in $\mathcal{B}$, so η_0, η_1, and η_2 are linearly independent over $\mathbf{Q}$ and thus form a $\mathbf{Q}$-basis of F_p.

Each $x \in \mathcal{O}_{F_p}$ has the form $x = a_0\eta_0 + a_1\eta_1 + a_2\eta_2$ for $a_0, a_1, a_2 \in \mathbf{Q}$. On the left side, since x is an algebraic integer in $\mathbf{Q}(\zeta_p)$ it is a $\mathbf{Z}$-linear combination of the numbers in $\mathcal{B}$. Expanding the right side in terms of $\mathcal{B}$, the coefficients are a_0, a_1, and a_2, so comparing coefficients of the numbers in $\mathcal{B}$ on both sides shows a_0, a_1, and a_2 are all integers. $\square$

To measure how far $\mathbf{Z}[\eta_0]$ is from the full ring of integers $\mathcal{O}_{F_p}$ we'd like to compute the index $[\mathcal{O}_{F_p} : \mathbf{Z}[\eta_0]]$. This can be expressed in terms of discriminants: if $f(T) \in \mathbf{Z}[T]$ is the minimal polynomial of η_0 over $\mathbf{Q}$ then

$$\mathrm{disc}(f(T)) = [\mathcal{O}_{F_p} : \mathbf{Z}[\eta_0]]^2 \, \mathrm{disc}(\mathcal{O}_{F_p}). \tag{2.1}$$

What are these discriminants?

Theorem 2.4. *For* $p \equiv 1 \bmod 3$*,* $\mathrm{disc}(\mathcal{O}_{F_p}) = p^2$*.*

Proof. The discriminant of $\mathcal{O}_{F_p}$ is the 3×3 determinant

$$\begin{vmatrix} \mathrm{Tr}(\eta_0^2) & \mathrm{Tr}(\eta_0\eta_1) & \mathrm{Tr}(\eta_0\eta_2) \\ \mathrm{Tr}(\eta_1\eta_0) & \mathrm{Tr}(\eta_1^2) & \mathrm{Tr}(\eta_1\eta_2) \\ \mathrm{Tr}(\eta_2\eta_0) & \mathrm{Tr}(\eta_2\eta_1) & \mathrm{Tr}(\eta_2^2) \end{vmatrix},$$

where $\mathrm{Tr} = \mathrm{Tr}_{F_p/\mathbf{Q}}$. Since η_0, η_1, η_2 are $\mathbf{Q}$-conjugates, as are $\eta_0\eta_1, \eta_0\eta_2$, and $\eta_1\eta_2$, we have

$$\begin{aligned} \mathrm{disc}(\mathcal{O}_{F_p}) &= \begin{vmatrix} \mathrm{Tr}(\eta_0^2) & \mathrm{Tr}(\eta_0\eta_1) & \mathrm{Tr}(\eta_0\eta_1) \\ \mathrm{Tr}(\eta_0\eta_1) & \mathrm{Tr}(\eta_0^2) & \mathrm{Tr}(\eta_0\eta_1) \\ \mathrm{Tr}(\eta_0\eta_1) & \mathrm{Tr}(\eta_0\eta_1) & \mathrm{Tr}(\eta_0^2) \end{vmatrix} \\ &= a^3 - 3ab^2 + 2b^3, \qquad (2.2) \end{aligned}$$

where $a = \mathrm{Tr}(\eta_0^2)$ and $b = \mathrm{Tr}(\eta_0\eta_1)$.

The trace of η_0 is $\mathrm{Tr}(\eta_0) = \eta_0 + \eta_1 + \eta_2 = \sum_{(t,p)=1} \zeta_p^t = -1$. To compute $\mathrm{Tr}(\eta_0^2)$, we compute

$$\begin{aligned}
\eta_0^2 &= \sum_{a^{(p-1)/3}=1} \sum_{b^{(p-1)/3}=1} \zeta_p^{a+b} \\
&= \sum_{a^{(p-1)/3}=1} \sum_{b^{(p-1)/3}=1} \zeta_p^{a(1+b)} \\
&= \sum_{b^{(p-1)/3}=1} \sum_{a^{(p-1)/3}=1} \zeta_p^{a(1+b)} \\
&= \frac{p-1}{3} + \sum_{b^{(p-1)/3}=1, b\neq -1} \sigma_{1+b}(\eta_0) \\
&= \frac{p-1}{3} + c_0\eta_0 + c_1\eta_1 + c_2\eta_2, \qquad (2.3)
\end{aligned}$$

where

$$\begin{aligned}
c_0 &= |\{b \neq 0, -1 : b^{(p-1)/3} = 1, (1+b)^{(p-1)/3} = 1\}|, \\
c_1 &= |\{b \neq 0, -1 : b^{(p-1)/3} = 1, (1+b)^{(p-1)/3} = r\}|, \\
c_2 &= |\{b \neq 0, -1 : b^{(p-1)/3} = 1, (1+b)^{(p-1)/3} = r^2\}|.
\end{aligned}$$

(Recall r and r^2 are the elements of order 3 in $(\mathbf{Z}/p\mathbf{Z})^\times$.)

Taking the trace of both sides of (2.3) gives

$$\mathrm{Tr}(\eta_0^2) = (p-1) + (c_0 + c_1 + c_2)\,\mathrm{Tr}(\eta_0) = p - 1 - (c_0 + c_1 + c_2).$$

The sum of the c_i's is the number of solutions to $b^{(p-1)/3} = 1$ in $\mathbf{Z}/p\mathbf{Z}$ except for $b = -1$, so

$$\mathrm{Tr}(\eta_0^2) = p - 1 - \left(\frac{p-1}{3} - 1\right) = \frac{2}{3}(p-1) + 1. \qquad (2.4)$$

Writing

$$\begin{aligned}
\mathrm{Tr}(\eta_0^2) &= \eta_0^2 + \eta_1^2 + \eta_2^2 \\
&= (\eta_0 + \eta_1 + \eta_2)^2 - 2(\eta_0\eta_1 + \eta_1\eta_2 + \eta_0\eta_2) \\
&= (\mathrm{Tr}\,\eta_0)^2 - 2\,\mathrm{Tr}(\eta_0\eta_1) \\
&= 1 - 2\,\mathrm{Tr}(\eta_0\eta_1), \qquad (2.5)
\end{aligned}$$

we compare (2.4) and (2.5) to see that $\mathrm{Tr}(\eta_0\eta_1) = -(p-1)/3$.

Feeding the formulas for $\mathrm{Tr}(\eta_0^2)$ and $\mathrm{Tr}(\eta_0\eta_1)$ into the discriminant formula (2.2) gives

$$\mathrm{disc}(\mathcal{O}_{F_p}) = \left(\frac{2}{3}(p-1)+1\right)^3 - 3\left(\frac{2}{3}(p-1)+1\right)\left(\frac{p-1}{3}\right)^2 - 2\left(\frac{p-1}{3}\right)^3 = p^2. \qquad \square$$

Remark 2.5. The discriminant of F_p can be calculated using ramification rather than a basis: the extension $\mathbf{Q}(\zeta_p)/\mathbf{Q}$ is ramified only at p, so if K is an intermediate field then it is ramified only at p too. Since $\mathbf{Q}(\zeta_p)/\mathbf{Q}$ is totally ramified at p, K is totally ramified at p as well. If a number field is totally ramified at a prime p and has degree n not divisible by p then it can be shown that its discriminant is divisible by p^{n-1} but not p^n. Therefore if $[K : \mathbf{Q}] = d$, $\mathrm{disc}(K) = \pm p^{d-1}$. The sign of $\mathrm{disc}(K)$ is $(-1)^{r_2(K)}$ [9, Lemma 2.2], and when $p \equiv 1 \bmod 3$ the cubic field F_p has $r_2 = 0$ since a Galois cubic with a real embedding has $r_2 = 0$, so $\mathrm{disc}(F_p) = p^{3-1} = p^2$.

The first few primes $p \equiv 1 \bmod 3$ are

$$7,\ 13,\ 19,\ 31,\ 37,\ 43,\ 61,\ 67,\ 73,\ 79,\ 97.$$

For every prime $p \equiv 1 \bmod 3$ we can write $4p = A^2 + 27B^2$ and such an equation determines A and B up to sign [6, p. 119]. The table below gives the positive A and B for the above p.

p	7	13	19	31	37	43	61	67	73	79	97
(A,B)	(1,1)	(5,1)	(7,1)	(4,2)	(11,1)	(8,2)	(1,3)	(5,3)	(7,3)	(17,1)	(19,1)

Numerically, for each of the above p a calculation of $f(T)$ as $(T-\eta_0)(T-\eta_1)(T-\eta_2)$ shows the discriminant of $f(T)$ is $(pB)^2$. By (2.1) and Theorem 2.4, the formula $\operatorname{disc}(f(T)) = (pB)^2$ is equivalent to $[\mathcal{O}_{F_p} : \mathbf{Z}[\eta_0]] = |B|$, so by the above table $\mathbf{Z}[\eta_0]$ has index 2 in $\mathcal{O}_{F_p}$ when p is 31 and 43, the index is 3 when p is 61, 67, and 73, and the index is 1 (*i.e.*, $\mathcal{O}_{F_p} = \mathbf{Z}[\eta_0]$) for the other p in the table. For a more rigorous discussion of the formula $\operatorname{disc}(f(T)) = (pB)^2$, see [4]. Claude Quitte observed numerically for the above p an index formula using A: $[\mathcal{O}_{F_p} : \mathbf{Z}[\eta_0 - \eta_1]] = |A|$.

The formula $\operatorname{disc}(f(T)) = (pB)^2$ leads to a formula for $f(T)$. In terms of its roots η_i,

$$\begin{aligned} f(T) &= (T-\eta_0)(T-\eta_1)(T-\eta_2) \\ &= T^3 - (\eta_0+\eta_1+\eta_2)T^2 + (\eta_0\eta_1+\eta_0\eta_2+\eta_1\eta_2)T - \eta_0\eta_1\eta_2 \\ &= T^3 - \operatorname{Tr}(\eta_0)T^2 + \operatorname{Tr}(\eta_0\eta_1)T - \eta_0\eta_1\eta_2 \\ &= T^3 - (-1)T^2 - \frac{p-1}{3}T - \eta_0\eta_1\eta_2 \\ &= T^3 + T^2 - \frac{p-1}{3}T - \eta_0\eta_1\eta_2. \end{aligned}$$

We want to write the constant term of $f(T)$ in terms of p. The general formula

$$\operatorname{disc}\left(T^3 + T^2 + aT + b\right) = -4a^3 + a^2 + 18ab - 27b^2 - 4b$$

with $a = -(p-1)/3$ and $b = -\eta_0\eta_1\eta_2$ is

$$\begin{aligned} \frac{4}{27}p^3 - \frac{1}{3}p^2 + \left(\frac{2}{9} - 6b\right)p - 27b^2 + 2b - \frac{1}{27} &= \frac{p^2}{27}\left(4p - 9 - \frac{6(27b-1)}{p} - \frac{(27b-1)^2}{p^2}\right) \\ &= \frac{p^2}{27}\left(4p - \left(3 + \frac{27b-1}{p}\right)^2\right). \end{aligned}$$

Setting $4p = A^2 + 27B^2$, this discriminant is

$$\frac{p^2}{27}\left(A^2 + 27B^2 - \left(3 + \frac{27b-1}{p}\right)^2\right) = \frac{p^2}{27}\left(A^2 - \left(3 + \frac{27b-1}{p}\right)^2\right) + (pB)^2.$$

Therefore

$$\operatorname{disc}(f(T)) = (pB)^2 \Longleftrightarrow 3 + \frac{27b-1}{p} = \pm A.$$

Since $p \equiv 1 \bmod 3$ we have $3 + (27b-1)/p \equiv -1 \bmod 3$, so if we choose the sign on A to make $A \equiv 1 \bmod 3$ then $3 + (27b-1)/p = -A$. Rewrite this as $b = (1 - p(A+3))/27$, so the minimal polynomial of η_0 over $\mathbf{Q}$ is

$$f(T) = T^3 + T^2 - \frac{p-1}{3}T + \frac{1-p(A+3)}{27} \tag{2.6}$$

with $4p = A^2 + 27B^2$ and $A \equiv 1 \bmod 3$.

Example 2.6. The first $p \equiv 1 \bmod 3$ for which F_p fits the hypothesis of Theorem 2.1 (meaning 2 mod p is a cube) is $p = 31$, for which $4p = 124 = (4)^2 + 27(2)^2$. Therefore the cubic subfield of $\mathbf{Q}(\zeta_{31})$ is $\mathbf{Q}(\eta_0)$ where, by (2.6), η_0 has minimal polynomial

$$T^3 + T^2 - \frac{31-1}{3}T + \frac{1-31(4+3)}{27} = T^3 + T^2 - 10T - 8.$$

The field $\mathbf{Q}(\eta_0)$ is a cyclic cubic extension of $\mathbf{Q}$ in which 2 splits completely and its ring of integers has no power basis.

Example 2.7. The second p fitting the hypothesis of Theorem 2.1 is $p = 43$, for which $4p = 172 = (-8)^2 + 27(2)^2$ (we use -8 so that $A = -8 \equiv 1 \bmod 3$). Thus the cubic subfield of $\mathbf{Q}(\zeta_{43})$ is $\mathbf{Q}(\eta_0)$ where η_0 has minimal polynomial

$$T^3 + T^2 - \frac{43-1}{3}T + \frac{1-43(-8+3)}{27} = T^3 + T^2 - 14T + 8$$

and this cubic field has the properties indicated at the end of the previous example.

The minimal polynomial of $\eta_0 - \eta_1$ over $\mathbf{Q}$ is $(T - (\eta_0 - \eta_1))(T - (\eta_1 - \eta_2))(T - (\eta_2 - \eta_0))$. Expanding this out, we get

$$T^3 + (\eta_0\eta_1 + \eta_0\eta_2 + \eta_1\eta_2 - \eta_0^2 - \eta_1^2 - \eta_2^2)T + (\eta_0 - \eta_1)(\eta_1 - \eta_2)(\eta_2 - \eta_0). \tag{2.7}$$

The coefficient of T is $3\,\mathrm{Tr}(\eta_0\eta_1) - (\mathrm{Tr}\,\eta_0)^2 = -3(p-1)/3 - (-1)^2 = -p$ and the constant term is $\sqrt{\mathrm{disc}(f(T))} = \pm p|B|$. The sign of the constant term in (2.7) is sensitive to the choice of ζ_p and nontrivial cube root of unity $r \bmod p$ in the definition of the η_i, *e.g.*, changing r can change η_1 into η_2 but $\eta_0 - \eta_1$ and $\eta_0 - \eta_2$ are not $\mathbf{Q}$-conjugates. In fact $\eta_0 - \eta_2$ has minimal polynomial $T^3 - pT \mp p|B|$ with constant term of opposite sign to the minimal polynomial of $\eta_0 - \eta_1$. When the definition of the η_i uses $\zeta_p = e^{2\pi i/p}$ and r is the numerically least nontrivial cube root of unity mod p in $\{1, \ldots, p-1\}$ then for all $p < 100$ such that $p \equiv 1 \bmod 3$ the constant term of (2.7) turns out to be $p|B|$ except when $p = 61$.

The only $p < 500$ for which $p \equiv 1 \bmod 3$ and the class number of F_p is greater than 1 are 163, 277, 313, 349, and 397. For these p the class group of F_p is $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ except for $p = 313$, when it is $\mathbf{Z}/7\mathbf{Z}$.

3. Power bases in relative quadratic extensions

For number fields E and F where $F \subset E$, a power basis of $\mathcal{O}_E$ over $\mathcal{O}_F$ is called a relative integral power basis. If $\mathcal{O}_F$ is a PID, then $\mathcal{O}_E$ is a free $\mathcal{O}_F$-module, so $\mathcal{O}_E$ has an $\mathcal{O}_F$-basis, but there might not be a power basis over $\mathcal{O}_F$. We'll meet some examples of this when E/F is a quadratic extension, and necessarily $F \neq \mathbf{Q}$ since the ring of integers of a quadratic field is always of the form $\mathbf{Z}[w]$ for some w.

Here is a property of a quadratic extension E/F when $\mathcal{O}_E$ has a power basis over $\mathcal{O}_F$.

Theorem 3.1. *If $[E : F] = 2$ and $\mathcal{O}_E = \mathcal{O}_F[\alpha]$ for some α, then $\mathcal{O}_E/\mathcal{O}_F \cong \mathcal{O}_F$ as $\mathcal{O}_F$-modules.*

Proof. If $\mathcal{O}_E = \mathcal{O}_F + \mathcal{O}_F\alpha$ for some nonzero α in $\mathcal{O}_E$, then $\mathcal{O}_E = \mathcal{O}_F \oplus \mathcal{O}_F\alpha$, so $\mathcal{O}_E/\mathcal{O}_F \cong \mathcal{O}_F\alpha \cong \mathcal{O}_F$ as $\mathcal{O}_F$-modules. $\square$

Here are quadratic extensions of imaginary quadratic fields with no relative integral power basis. It is based on an answer to `https://math.stackexchange.com/questions/4620044`.

Example 3.2. Let d be an even squarefree integer and q be a prime not dividing d such that $q \equiv 1 \bmod 4$. Set $F = \mathbf{Q}(\sqrt{-q})$ and $E = F(\sqrt{d}) = \mathbf{Q}(\sqrt{-q}, \sqrt{d})$. It can be shown that $\mathcal{O}_E = \mathcal{O}_F \oplus \mathfrak{p}\sqrt{d}/2$ where $\mathfrak{p} = (2, 1+\sqrt{-q})$ is a nonprincipal ideal.[5] Then $\mathcal{O}_E/\mathcal{O}_F \cong \mathfrak{p}$ as $\mathcal{O}_F$-modules and $\mathfrak{p} \not\cong \mathcal{O}_F$ since an ideal in $\mathcal{O}_F$ that is isomorphic to $\mathcal{O}_F$ as an $\mathcal{O}_F$-module must be a principal ideal.[6] So $\mathcal{O}_E$ is not of the form $\mathcal{O}_F[\alpha]$ by Theorem 3.1.

In that example, $\mathcal{O}_F$ is not a PID (it has the nonprincipal ideal $\mathfrak{p}$). The next theorem shows that it was necessary for $\mathcal{O}_F$ not to be a PID.

Theorem 3.3. *If $[E:F] = 2$ and $\mathcal{O}_F$ is a* PID, *then $\mathcal{O}_E = \mathcal{O}_F[\alpha]$ for some α.*

Proof. Since $\mathcal{O}_F$ is a PID, $\mathcal{O}_E$ has an $\mathcal{O}_F$-basis $\{e_1, e_2\}$. In terms of this basis, we can write

$$1 = a_1e_1 + a_2e_2$$

for some a_1 and a_2 in $\mathcal{O}_F$. That equation implies a common factor of a_1 and a_2 in $\mathcal{O}_F$ is a unit in $\mathcal{O}_E$, and thus is a unit in $\mathcal{O}_F$, so a_1 and a_2 are relatively prime in $\mathcal{O}_F$. Since $\mathcal{O}_F$ is a PID,

$$a_1b_1 + a_2b_2 = 1$$

for some b_1 and b_2 in $\mathcal{O}_F$. Then

$$\begin{pmatrix} a_1 & a_2 \\ -b_2 & b_1 \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \end{pmatrix} = \begin{pmatrix} 1 \\ \alpha \end{pmatrix}$$

for some $\alpha \in \mathcal{O}_F$ and that 2×2 matrix has determinant 1, so 1 and α have the same $\mathcal{O}_F$-span as e_1 and e_2. Hence

$$\mathcal{O}_E = \mathcal{O}_F + \mathcal{O}_F\alpha = \mathcal{O}_F[\alpha]. \qquad \square$$

REFERENCES

[1] R. Dedekind, Göttingische gelehrte Anzeigen (1871), pp. 1481–1494. URL https://babel.hathitrust.org/cgi/pt?id=mdp.39015064404166&view=1up&seq=447.

[2] R. Dedekind, *Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Congruenzen*, Abhandlungen der Königlichen Gesellschaft der Wissenschaften in Göttingen **23** (1878), 3–38. URL https://eudml.org/doc/135827. English translation: https://arxiv.org/abs/2107.08905.

[3] D. S. Dummit and H. Kisilevsky, Indices in Cyclic Cubic Fields, pp. 29–42 of "Number Theory and Algebra" (H. Zassenhaus, ed.), Academic Press, New York, 1977.

[4] M-N. Gras, *Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de* **Q**, J. Reine Angew. Math. **277** (1975), 89–116. URL https://eudml.org/doc/151629.

[5] K. Hensel, *Arithmetische Untersuchungen über die gemeinsamen ausserwesentlichen Discriminantentheiler einer Gattung*, J. Reine Angew. Math. **113** (1894), 128–160. URL https://eudml.org/doc/148923.

[6] K. Ireland and M. Rosen, "A Classical Introduction to Modern Number Theory," 2nd ed., Springer-Verlag, New York, 1990.

[7] L. Kronecker, *Grundzüge einer arithmetischen Theorie der algebraischen Grössen*, J. Reine Angew. Mathematik **92** (1882), 1–122. URL https://eudml.org/doc/148487.

[8] P. Samuel, "Algebraic Number Theory," Houghton Mifflin, Boston, 1969.

[9] L. Washington, "An Introduction to Cyclotomic Fields," 2nd ed., Springer-Verlag, New York, 1997.

[10] E. von Zylinski, *Zur Theorie der ausserwesentlichen Diskiriminantenteiler algebraischer Körper*, Math. Ann. **73** (1913), 273–274. URL https://eudml.org/doc/158603.

---

[5] In the proof of Theorem 4.4 in https://kconrad.math.uconn.edu/blurbs/gradnumthy/notfree.pdf, see Step 2.

[6] See https://math.stackexchange.com/questions/423641.