RINGS OF INTEGERS WITHOUT A POWER BASIS

KEITH CONRAD

Let K be a number field, with degree n and ring of integers $\mathcal{O}_K$. When $\mathcal{O}_K = \mathbf{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$, the set $\{1, \alpha, \ldots, \alpha^{n-1}\}$ 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 should 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 algebraic integers $e_1, \ldots, e_n$, quite often we can not choose the e_i's to be powers of a single number.

The first example of a ring of integers lacking a power basis is due to Dedekind. It is the field $\mathbf{Q}(\theta)$ where θ is a root of $T^3 - T^2 - 2T - 8$. The ring of integers of $\mathbf{Q}(\theta)$ has $\mathbf{Z}$-basis $\{1, \theta, (\theta+\theta^2)/2\}$ but no power basis. We will return to this historically distinguished example later, but the main purpose of the discussion here is to give infinitely many examples of number fields whose ring of integers does not have a power basis. Our examples will be Galois cubic extensions of $\mathbf{Q}$.

Fix a prime $p \equiv 1 \bmod 3$. The field $\mathbf{Q}(\zeta_p)/\mathbf{Q}$ has cyclic Galois group $(\mathbf{Z}/p\mathbf{Z})^\times$, and in particular there is a unique cubic subfield F_p, so $F_p/\mathbf{Q}$ is Galois with degree 3. The Galois group $\mathrm{Gal}(F_p/\mathbf{Q})$ is the quotient of $(\mathbf{Z}/p\mathbf{Z})^\times$ by its subgroup of cubes. In particular, for any prime $q \neq p$, q splits completely in F_p if and only if its Frobenius in $\mathrm{Gal}(F_p/\mathbf{Q})$ is trivial, which is equivalent to q being a cube modulo p.

Theorem 1 (Hensel)**.** *If $p \equiv 1 \bmod 3$ and 2 is a cube in $\mathbf{Z}/p\mathbf{Z}$, then $\mathcal{O}_{F_p} \neq \mathbf{Z}[\alpha]$ for any $\alpha \in \mathcal{O}_{F_p}$.*

Proof. Suppose $\mathcal{O}_{F_p} = \mathbf{Z}[\alpha]$ for some α. Let α have minimal polynomial $f(T)$ over $\mathbf{Q}$, so f is an irreducibe cubic in $\mathbf{Z}[T]$. Then

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

Since 2 is a cube mod p, 2 splits completely in F_p, so f splits completely in $(\mathbf{Z}/2\mathbf{Z})[T]$. However, a cubic in $(\mathbf{Z}/2\mathbf{Z})[T]$ can't split completely: there are only two (monic) linear polynomials mod 2. $\square$

The set of primes that fit the hypotheses of Theorem 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 there is a positive proportion (precisely, 1/6) of such primes. The first few of them are 31, 43, 109, and 127. For each such p, Theorem 1 tells us the ring of integers of F_p does not have a power basis.

Hensel actually proved a result that is stronger than Theorem 1: for $p \equiv 1 \bmod 3$, 2 is a cube mod p if and only if the index $[\mathcal{O}_{F_p} : \mathbf{Z}[\alpha]]$ is even for all $\alpha \in \mathcal{O}_{F_p} - \mathbf{Z}$.

The proof that the integer ring of Dedekind's field $\mathbf{Q}(\theta)$ lacks a power basis operates on the same principle as Theorem 1: show 2 splits completely in the integers of $\mathbf{Q}(\theta)$, and that implies there is no power basis for the same reason as in Theorem 1. However, to show 2 splits completely in $\mathbf{Q}(\theta)$ requires different techniques than the ones we used in the fields F_p, since Dedekind's field does not lie in a cyclotomic field.

If K is a number field, a criterion for $\mathcal{O}_K$ not to have a power basis is that some prime number p divides every index $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$ for $\alpha \in \mathcal{O}_K$. When K is a cubic field, the only such prime p could be 2 (theorem of Engstrom), and this criterion applies (that is, $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$ is even for all $\alpha \in \mathcal{O}_K$) if and only if 2 splits completely in $\mathcal{O}_K$. See [1] for further details, including a proof that there are infinitely many cubic fields without a power basis for which this even-index criterion does not apply.

The integer ring of F_p (for $p \equiv 1 \bmod 3$) has some $\mathbf{Z}$-basis, which we now know need not be a power basis. What is a $\mathbf{Z}$-basis for this ring?

Theorem 2. *For $p \equiv 1 \bmod 3$ let*

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

Fixing an element $r \in (\mathbf{Z}/p\mathbf{Z})^\times$ with order 3, let

$$\eta_1 = \sum_{t^{(p-1)/3} \equiv r \bmod p} \zeta_p^t, \quad \eta_2 = \sum_{t^{(p-1)/3} \equiv r^2 \bmod p} \zeta_p^t.$$

Then $\mathcal{O}_{F_p} = \mathbf{Z}\eta_0 + \mathbf{Z}\eta_1 + \mathbf{Z}\eta_2$.

The numbers η_i are examples of (cyclotomic) periods [5, 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 $\mathbf{Q}(\zeta_p)$ any 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 $\{1, \zeta_p, \dots, \zeta_p^{p-2}\}$, 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 $\mathcal{B} = \{\zeta_p, \zeta_p, \dots, \zeta_p^{p-1}\}$ 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 $x \in \mathcal{O}_{F_p}$ can be written as $x = a_0\eta_0 + a_1\eta_1 + a_2\eta_2$ for rational a_0, a_1, and a_2. 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. □

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

$$\operatorname{disc}(f(T)) = [\mathcal{O}_{F_p} : \mathbf{Z}[\eta_0]]^2 \operatorname{disc}(\mathcal{O}_{F_p}). \tag{1}$$

What are these discriminants?

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

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

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

where $\operatorname{Tr} = \operatorname{Tr}_{F_p/\mathbf{Q}}$. 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

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

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

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

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

where

$$c_0 = \#\{b \neq 0, -1 : b^{(p-1)/3} = 1, (1+b)^{(p-1)/3} = 1\},$$

$$c_1 = \#\{b \neq 0, -1 : b^{(p-1)/3} = 1, (1+b)^{(p-1)/3} = r\},$$

$$c_2 = \#\{b \neq 0, -1 : b^{(p-1)/3} = 1, (1+b)^{(p-1)/3} = r^2\}.$$

(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 (3) gives

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

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

$$\operatorname{Tr}(\eta_0^2) = p - 1 - \left(\frac{p-1}{3} - 1\right) = \frac{2}{3}(p-1) + 1. \tag{4}$$

Writing

$$\begin{aligned}\operatorname{Tr}(\eta_0^2) &= \eta_0^2+\eta_1^2+\eta_2^2\\ &= (\eta_0+\eta_1+\eta_2)^2 - 2(\eta_0\eta_1+\eta_1\eta_2+\eta_0\eta_2)\\ &= (\operatorname{Tr}\eta_0)^2 - 2\operatorname{Tr}(\eta_0\eta_1)\\ &= 1-2\operatorname{Tr}(\eta_0\eta_1), \qquad (5)\end{aligned}$$

we compare (4) and (5) to see that $\operatorname{Tr}(\eta_0\eta_1) = -(p-1)/3$.

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

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

$\square$

Remark 4. 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 $[K:\mathbf{Q}] = d$, $\operatorname{disc}(K) = \pm p^{d-1}$. The sign of $\operatorname{disc}(K)$ is $(-1)^{r_2(K)}$ [5, 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 $\operatorname{disc}(F_p) = p^{3-1} = p^2$.

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 [3, 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 (1) and Theorem 3, 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.*, $\mathcal{O}_{F_p} = \mathbf{Z}[\eta_0]$) if and only if $4p-27$ is a perfect square. For a more rigorous discussion of the formula $\operatorname{disc}(f(T)) = (pB)^2$, see [2]. 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 $\operatorname{disc}(f(T)) = (pB)^2$ will lead 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

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

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

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

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

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

$$T^3 + (\eta_0\eta_1 + \eta_0\eta_2 + \eta_1\eta_2 - \eta_0^2 - \eta_1^2 - \eta_2^2)T + (\eta_0 - \eta_1)(\eta_1 - \eta_2)(\eta_2 - \eta_0). \tag{6}$$

The coefficient of T is $3\operatorname{Tr}(\eta_0\eta_1) - (\operatorname{Tr}\eta_0)^2 = -3(p-1)/3 - (-1)^2 = -p$ and the constant term is $\sqrt{\operatorname{disc}(f(T))} = \pm p|B|$. The sign of the constant term in (6) is sensitive to the choice of ζ_p and nontrivial cube root of unity r mod 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 (6) 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 $\mathbf{Z}/7\mathbf{Z}$.

References

[1] 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.

[2] M-N. Gras, Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de $\mathbf{Q}$, *J. Reine Angew. Math.* **277** (1975), 89–116.

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

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

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