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 $\{1, \alpha, \dots, \alpha^{n-1}\}$ 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 $e_1, \dots, e_n$, 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. □

The set of primes which 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 which 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, the ring of integers of F_p does not have a power basis.

Hensel actually proved a result which 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 $\alpha \in \mathcal{O}_{F_p}$.

The proof that the integer ring of Dedekind's field 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 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. *Let*

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

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

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

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 [4, pp. 16–17].

Proof. For $c \in (\mathbf{Z}/p\mathbf{Z})^\times$, let $\sigma_c \in \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ send ζ_p to ζ_p^c. It is left to the reader to check that η_0, η_1, η_2 are $\mathbf{Q}$-conjugates, so any of them generates $F_p/\mathbf{Q}$ as a field. (There is a unique cubic subfield of $\mathbf{Q}(\zeta_p)$.) Viewing them in $\mathbf{Q}(\zeta_p)$ shows they are linearly independent over $\mathbf{Q}$, so η_0, η_1, and η_2 form a $\mathbf{Q}$-basis of F_p.

Write $x \in \mathcal{O}_{F_p}$ in the form $x = a\eta_0 + b\eta_1 + c\eta_2$ with rational a, b, and c. Since x is an algebraic integer in $\mathbf{Q}(\zeta_p)$, whose integer ring is $\mathbf{Z}[\zeta_p]$, we can read off that a, b, and c are all integers. □

Theorem 3. *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

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

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

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

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

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 η_0^2 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

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

Writing

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

we compare (1) and (2) to see that $\operatorname{Tr}(\eta_0\eta_1)=-(p-1)/3$.

Feeding in the formulas for the trace of $\operatorname{Tr}(\eta_0^2)$ and $\operatorname{Tr}(\eta_0\eta_1)$ into the discriminant for $\mathcal{O}_{F_p}$ gives (after some careful algebra)

$$\operatorname{disc}(\mathcal{O}_{F_p})=p^2.$$

□

What is the minimal polynomial of η_0 over $\mathbf{Q}$? We give an informal discussion. From the formulas for $\operatorname{Tr}(\eta_0)$ and $\operatorname{Tr}(\eta_0\eta_1)$, η_0 has minimal polynomial

$$f(T)=T^3+T^2-\frac{p-1}{3}T-\eta_0\eta_1\eta_2$$

in $\mathbf{Q}[T]$ and

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

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

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

For each of these primes, using PARI it appears that $f(T)$ has discriminant $(pB)^2$, where $4p = A^2 + 27B^2$ (such an equation, valid for $p \equiv 1 \bmod 3$, determines A and B up to sign). For a more rigorous discussion of this discriminant formula, see [2]. If the formula $\operatorname{disc}(f) = (pB)^2$ is correct then $[\mathcal{O}_{F_p} : \mathbf{Z}[\eta_0]] = |B|$.

The general formula

$$\operatorname{disc}\left(T^3 + T^2 - \frac{p-1}{3}T + c\right) = \frac{4}{27}p^3 - \frac{1}{3}p^2 + \left(6c + \frac{2}{9}\right)p - 27c^2 + 2c - \frac{1}{27},$$

with $c = \eta_0\eta_1\eta_2$ and set equal to $(pB)^2$ leads, after some algebra, to

$$27\eta_0\eta_1\eta_2 = 1 - 3p \pm Ap.$$

Up to now A is only determined up to sign, so this formula can serve to fix a choice of sign, namely $27\eta_0\eta_1\eta_2 = 1 - 3p - Ap$ where $A \equiv 1 \bmod 3$. Then the minimal polynomial of η_0 over $\mathbf{Q}$ is

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

The first $p \equiv 1 \bmod 3$ for which $2 \bmod p$ is a cube and the class number of F_p is greater than 1 is $p = 277$: the cubic subfield of $\mathbf{Q}(\zeta_{277})$ is generated by a root of $T^3 + T^2 - 92T + 236$ and the class number of this cubic field is $h = 4$.

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 **Q**, *J. Reine Angew. Math.* **277** (1975), 89–116.

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

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