THE RING OF INTEGERS IN A RADICAL EXTENSION

KEITH CONRAD

1. Introduction

The integers of $\mathbf{Q}(\sqrt[n]{2})$ is $\mathbf{Z}[\sqrt[n]{2}]$ for $n = 2, 3$, 4, and 5. In fact this is true for $n \leq 1000$. Is $\mathbf{Z}[\sqrt[n]{2}]$ the ring of integers of $\mathbf{Q}(\sqrt[n]{2})$ for all $n \geq 2$? For comparison, the cyclotomic field $\mathbf{Q}(\zeta_n)$ has ring of integers $\mathbf{Z}[\zeta_n]$ for all n, so maybe this is something similar.

Let's broaden our scope. If $n \geq 2$ and $T^n - a$ is irreducible in $\mathbf{Z}[T]$, or equivalently $[\mathbf{Q}(\sqrt[n]{a}) : \mathbf{Q}] = n$, we seek necessary and sufficient conditions for the integers of $\mathbf{Q}(\sqrt[n]{a})$ to be $\mathbf{Z}[\sqrt[n]{a}]$. Some constraint is needed, since the integers of $\mathbf{Q}(\sqrt{5})$ are more than $\mathbf{Z}[\sqrt{5}]$, as $(1+\sqrt{5})/2$ is an algebraic integer. The conditions we find will turn out to have a connection to old work on Fermat's Last Theorem.

2. Reduction to prime-power n

Theorem 2.1. *For $n \geq 2$ and $T^n - a$ irreducible in $\mathbf{Z}[T]$, if $\mathbf{Z}[\sqrt[n]{a}]$ is the ring of integers of $\mathbf{Q}(\sqrt[n]{a})$ then a must be squarefree.*

Proof. We give a proof by example. If $\alpha = \sqrt[3]{p^2 q}$ for different primes p and q, then $(\alpha^2/p)^3 = pq^2$, so α^2/p is an algebraic integer not in $\mathbf{Z}[\alpha]$. Use this idea to find an algebraic integer in $\mathbf{Q}(\sqrt[n]{a})$ not in $\mathbf{Z}[\sqrt[n]{a}]$ if a is not squarefree. □

Since we are assuming $T^n - a$ is irreducible, a is not 1. If $a = -1$ then $T^n - a = T^n + 1$ is irreducible if and only if $n = 2^r$ is a power of 2, in which case $\sqrt[n]{-1} = \zeta_{2^{r+1}}$ and this generates the ring of integers of $\mathbf{Q}(\sqrt[n]{-1}) = \mathbf{Q}(\zeta_{2^{r+1}})$ since this is a cyclotomic field. So we assume from now on that a is squarefree and is not ± 1. Then a has a prime factor and $T^n - a$ is *automatically* irreducible in $\mathbf{Z}[T]$ for all n since it is Eisenstein at each prime factor of a. The next theorem reduces us to the case when n is a prime power.

Lemma 2.2. *Let $a \neq \pm 1$ be squarefree in $\mathbf{Z}$ and $T^n - a$ be irreducible over $\mathbf{Q}$. For each positive integer d dividing n, $T^d - a$ is irreducible over $\mathbf{Q}$. If $\mathbf{Q}(\sqrt[n]{a})$ has ring of integers $\mathbf{Z}[\sqrt[n]{a}]$, then $\mathbf{Q}(\sqrt[d]{a})$ has ring of integers $\mathbf{Z}[\sqrt[d]{a}]$*

Proof. Exercise. □

Theorem 2.3. *Let a be a squarefree integer other than ± 1. When $(m, n) = 1$, the following conditions are equivalent:*

(a) *The integers of $\mathbf{Q}(\sqrt[mn]{a})$ are $\mathbf{Z}[\sqrt[mn]{a}]$.*
(b) *The integers of $\mathbf{Q}(\sqrt[m]{a})$ and $\mathbf{Q}(\sqrt[n]{a})$ are $\mathbf{Z}[\sqrt[m]{a}]$ and $\mathbf{Z}[\sqrt[n]{a}]$.*

Proof. That (a) ⇒ (b) follows from Lemma 2.2. We will show (b) ⇒ (a) using properties of discriminants. It is obvious if m or n is 1, so we may assume $m > 1$ and $n > 1$.

The mth, nth, and mnth roots of a are, as abstract roots, only well-defined up to multiplication by roots of unity. The choice of root doesn't affect the number field up to isomorphism, but it's convenient to give the three roots the obvious multiplicative relation:

take $\sqrt[mn]{a}$ to be a fixed root of $T^{mn}-a$ and then define $\sqrt[m]{a} = \sqrt[mn]{a}^n$ and $\sqrt[n]{a} = \sqrt[mn]{a}^m$. If $a > 0$ we can use the positive real roots.

Let $K = \mathbf{Q}(\sqrt[m]{a})$ and $L = \mathbf{Q}(\sqrt[n]{a})$, so $[K : \mathbf{Q}] = m$ and $[L : \mathbf{Q}] = n$. Since $(m, n) = 1$, field theory implies $[KL : \mathbf{Q}] = mn$. Since $\sqrt[mn]{a}$ is an algebraic integer of degree mn inside of KL,[1] $KL = \mathbf{Q}(\sqrt[mn]{a})$ and $\mathbf{Z}[\sqrt[mn]{a}]$ has finite index in $\mathcal{O}_{KL}$. We will show the index is 1.

From the hypotheses $\mathcal{O}_K = \mathbf{Z}[\sqrt[m]{a}]$ and $\mathcal{O}_L = \mathbf{Z}[\sqrt[n]{a}]$,

$$\operatorname{disc}(K) = \operatorname{disc}(T^m - a) = \pm m^m a^{m-1} \quad \text{and} \quad \operatorname{disc}(L) = \operatorname{disc}(T^n - a) = \pm n^n a^{n-1}.$$

Let d be the greatest common divisor of these discriminants. Since $(m, n) = 1$, each prime factor of d is a factor of a. The ring $\mathcal{O}_K\mathcal{O}_L = \mathbf{Z}[\sqrt[m]{a}, \sqrt[n]{a}]$ lies in $\mathbf{Z}[\sqrt[mn]{a}]$. Then

$$\mathcal{O}_{KL} \subset \frac{1}{d}\mathcal{O}_K\mathcal{O}_L \subset \frac{1}{d}\mathbf{Z}[\sqrt[mn]{a}],$$

where the first containment is a general property of all pairs of number fields K and L. Thus $d\mathcal{O}_{KL} \subset \mathbf{Z}[\sqrt[mn]{a}]$. Therefore the quotient group $\mathcal{O}_{KL}/\mathbf{Z}[\sqrt[mn]{a}]$ is killed by d.

Since a is squarefree, for each prime p dividing a the polynomial $T^{mn} - a$ is Eisenstein at p, so $p \nmid [\mathcal{O}_K : \mathbf{Z}[\sqrt[mn]{a}]]$.[2] Therefore $[\mathcal{O}_K : \mathbf{Z}[\sqrt[mn]{a}]] = |\mathcal{O}_{KL}/\mathbf{Z}[\sqrt[mn]{a}]|$ is relatively prime to a, and thus also to d. A group that is killed by an integer relatively prime to its size is trivial (the order of each element of the group divides two relatively prime integers, so the order is 1), so $\mathcal{O}_{KL} = \mathbf{Z}[\sqrt[mn]{a}]$. □

Corollary 2.4. *Let a be a squarefree integer other than ± 1. For $n \geq 2$, if the ring of integers of $\mathbf{Q}(\sqrt[p^r]{a})$ is $\mathbf{Z}[\sqrt[p^r]{a}]$ for all $p^r \,||\, n$ then the ring of integers of $\mathbf{Q}(\sqrt[n]{a})$ is $\mathbf{Z}[\sqrt[n]{a}]$.*

Proof. Induct on the number of prime factors of n. The base case is a hypothesis and Theorem 2.3 provides the inductive step. □

We have reduced ourselves to figuring when $\mathbf{Q}(\sqrt[n]{a})$ has ring of integers $\mathbf{Z}[\sqrt[n]{a}]$ for squarefree $a \neq \pm 1$ and n a prime power.

3. Prime-power n

Let $n = p^r$ for prime p and $r \geq 1$. To study the integers of $\mathbf{Q}(\sqrt[n]{a})$ for squarefree $a \neq \pm 1$, we treat separately the cases that $p \mid a$ and $p \nmid a$. When $p \mid a$ we will have a definitive solution, while the case $p \nmid a$ will be solved only conditionally.

Theorem 3.1. *When a is squarefree other than ± 1 and p is a prime dividing a, the ring of integers of $\mathbf{Q}(\sqrt[p^r]{a})$ is $\mathbf{Z}[\sqrt[p^r]{a}]$ for all $r \geq 1$.*

Proof. Let $K = \mathbf{Q}(\sqrt[p^r]{a})$. The index $[\mathcal{O}_K : \mathbf{Z}[\sqrt[p^r]{a}]]$ divides $\operatorname{disc}(T^{p^r} - a) = \pm(p^r)^{p^r} a^{p^r - 1}$. Since $p \mid a$, the prime factors of $[\mathcal{O}_K : \mathbf{Z}[\sqrt[p^r]{a}]]$ all divide a.

For every prime q dividing a, $T^{p^r} - a$ is Eisenstein at q, so $q \nmid [\mathcal{O}_K : \mathbf{Z}[\sqrt[p^r]{a}]]$. Therefore $[\mathcal{O}_K : \mathbf{Z}[\sqrt[p^r]{a}]]$ has no prime factors, so it is 1. □

Theorem 3.2. *If a is squarefree other than ± 1 and p is a prime not dividing a such that*

$$a^{p-1} \not\equiv 1 \bmod p^2, \tag{3.1}$$

then the ring of integers of $\mathbf{Q}(\sqrt[p^r]{a})$ is $\mathbf{Z}[\sqrt[p^r]{a}]$ for all $r \geq 1$.

[1] Here we use our convention that $\sqrt[m]{a}$ and $\sqrt[n]{a}$ are powers of $\sqrt[mn]{a}$.

[2] For every root α of a polynomial that's Eisenstein at a prime p, the index $[\mathcal{O}_{\mathbf{Q}(\alpha)} : \mathbf{Z}[\alpha]]$ is not divisible by p.

Fermat's little theorem tells us $a^{p-1} \equiv 1 \bmod p$ for all prime p not dividing a. The noncongruence in (3.1) has modulus p^2 and may or may not hold, depending on p.

Proof. As in the previous proof, a prime factor of $[\mathcal{O}_K : \mathbf{Z}[\sqrt[p^r]{a}]]$ is p or is a factor of a, and no prime factor of a divides $[\mathcal{O}_K : \mathbf{Z}[\sqrt[p^r]{a}]]$ since $T^{p^r} - a$ is Eisenstein at every prime factor of a.

This time the prime p does not divide a, so we need a new argument to show p is not a factor of $[\mathcal{O}_K : \mathbf{Z}[\sqrt[p^r]{a}]]$, thus making the index 1. We can't use the polynomial $T^{p^r} - a$ directly, since it is not Eisenstein at p. But perhaps it has a translate $(T+c)^{p^r} - a$ that is Eisenstein at p. That would be good enough, since $\mathbf{Z}[\sqrt[p^r]{a}] = \mathbf{Z}[\sqrt[p^r]{a} - c]$. What c could be used?

In order for $(T+c)^{p^r} - a$ to be Eisenstein at p, there is no problem with the inner coefficients, which are all multiples of p. Is the constant term $c^{p^r} - a$ a multiple of p exactly once? This is equivalent to

$$c^{p^r} \equiv a \bmod p \qquad \text{and} \qquad c^{p^r} \not\equiv a \bmod p^2. \tag{3.2}$$

We will show the choice $c = a$ fits (3.2) when (3.1) holds. For all integers x, $x^p \equiv x \bmod p$, so by repeatedly taking the pth power we have $a^{p^r} \equiv a \bmod p$, which is the first condition in (3.2) with $c = a$. For all integers x and y,

$$x \equiv y \bmod p^j \Longrightarrow x^p \equiv y^p \bmod p^{j+1},$$

so starting from $a^p \equiv a \bmod p$ we get $a^{p^{r+1}} \equiv a^{p^r} \bmod p^{r+1}$ by raising to the pth power r times and increasing the modulus each time. Therefore $a^{p^r} \equiv a^p \bmod p^2$, so checking that $a^{p^r} \not\equiv a \bmod p^2$ is the same as checking $a^p \not\equiv a \bmod p^2$. This last noncongruence is equivalent to $a^{p-1} \not\equiv 1 \bmod p^2$ since $(p, a) = 1$, so (3.1) implies $(T+a)^{p^r} - a$ is Eisenstein at p. □

Remark 3.3. In the proof, we could have dropped the discussion of general c and focused on $c = a$ from the start for a shorter argument. The reason we did not do that is to show that if some choice of c works then the specific choice $c = a$ has to work.

Corollary 3.4. *When a is squarefree other than ± 1, the ring of integers of $\mathbf{Q}(\sqrt[n]{a})$ is $\mathbf{Z}[\sqrt[n]{a}]$ if every prime p factor of n that is not a factor of a satisfies (3.1).*

Proof. Combine Theorems 2.3, 3.1, and 3.2. □

Example 3.5. To show $\mathbf{Q}(\sqrt[n]{2})$ has ring of integers $\mathbf{Z}[\sqrt[n]{2}]$ for all $n \leq 1000$, it suffices to show for all odd primes $p \leq 1000$ that $2^{p-1} \not\equiv 1 \bmod p^2$. There are 168 primes below 1000 and it takes PARI almost no time to confirm the condition on those primes.

Example 3.6. Since $10^2 \equiv 1 \bmod 9$, Corollary 3.4 does not tell us $\mathbf{Z}[\sqrt[3]{10}]$ is the ring of integers of $\mathbf{Q}(\sqrt[3]{10})$, and in fact it isn't: $(1 + \sqrt[3]{10} + \sqrt[3]{100})/3$ is an algebraic integer, being a root of $T^3 - T^2 - 3T - 3$.

What happens if n has a prime factor p not dividing a for which (3.1) fails, meaning

$$a^{p-1} \equiv 1 \bmod p^2 \tag{3.3}$$

for a prime p dividing n that does not divide a?

4. A special congruence

The congruence (3.3) is famous in number theory because it appeared in the early 20th century in work on Fermat's last theorem. By the end of the 19th century, proving nonsolvability of $x^p + y^p = z^p$ in positive integers x, y, and z with an odd prime exponent p had fallen into two traditional cases: show no solutions where $p \nmid xyz$ (Case I) and show no solutions where $p \mid xyz$ (Case II). In 1909, Wieferich [9] showed that if Case I has a counterexample (making Fermat's last theorem false) for exponent p then $2^{p-1} \equiv 1 \bmod p^2$. He did not know a prime p fitting that congruence, but two were later found: 1093 and 3511. The first was found by Meissner [4] in 1913 and the second by Beeger [1] in 1922.[3] In 1910, Miramanoff [5] showed that if Case I has a counterexample for exponent p then $3^{p-1} \equiv 1 \bmod p^2$ too. The only known p satisfying Miramanoff's congruence are 11 and 1,006,003 (found by Kloss in 1965). Before Wiles proved Fermat's last theorem for all p, by an argument making no use of Case I vs. Case II and hardly using the Fermat equation directly at all, Case I was proved for p up to large bounds by checking numerically that no prime fits both Wieferich's congruence ((3.3) with $a = 2$) and Miramanoff's congruence ((3.3) with $a = 3$). In practice, Wieferich's congruence alone was sufficient except for the primes 1093 and 3511, since no other primes fitting Wieferich's congruence have been found.

Definition 4.1. For $a \in \mathbf{Z}$, a prime p is called a *Wieferich prime to base* a if (3.3) holds: $a^{p-1} \equiv 1 \bmod p^2$.

The known Wieferich primes for squarefree bases $a \leq 10$ are in Table 1. Searches have been made for $p < 1.25 \cdot 10^{15}$ when $a = 2$ [3] and for $p < 2^{32} \approx 10^{9.63}$ when $3 \leq a < 100$ [6].

a	Known Wieferich primes to base a
2	1093, 3511
3	11, 1006003
5	20771, 40487, 53471161, 1645333507
6	66161, 534851, 3152573
7	5, 491531
10	3, 487, 56598313

Table 1. Wieferich primes below 2^{32} for squarefree bases

Wieferich primes to a fixed base a are quite rare numerically, and for some a none are known: no Wieferich prime to base 47 or 50 has been found, for example. There is a simple probabilistic heuristic that supports the infrequent appearance of Wieferich primes to a fixed base, as follows. When $p \nmid a$, $a^{p-1} \equiv 1 \bmod p$, so $a^{p-1} \equiv 1 + pb \bmod p^2$, where $0 \leq b \leq p-1$. Having no compelling reason to believe otherwise, assume b takes each of the p values $0, 1, \ldots, p-1$ with equal probability. Since $b = 0$ corresponds to p being a Wieferich prime to base a, the "probability" some p not dividing a is a Wieferich prime to base a is $1/p$. Therefore the expected number of primes $p \leq x$ that are Wieferich primes to base a is found by adding up the "probabilities". This is $\sum_{p \leq x} 1/p$, which grows *very* slowly: it is asymptotic to $\log \log x$. Since $\log\log(2^{32}) \approx 3.1$, it is no surprise so few Wieferich primes for $p < 2^{32}$ are known to each particular base. (Strictly speaking, $\sum_{p \leq x} 1/p$ should not include the p dividing a, and removing these initial p makes $\sum_{p \nmid a, p \leq x} 1/p$ even smaller.)

[3] In 1950, Beeger [2] introduced the term "Carmichael number".

5. Resolution of the Wieferich case

Let's return to the problem of determining when, for squarefree $a \neq \pm 1$, $\mathbf{Z}[\sqrt[n]{a}]$ is the full ring of integers of $\mathbf{Q}(\sqrt[n]{a})$. Corollary 3.4 says this happens if no prime factor of n is a Wieferich prime to base a. What happens if n has a prime factor that is a Wieferich prime to base a?

By Lemma 2.2, we should first check the case when n itself is a Wieferich prime to base a, because if the ring of integers is not $\mathbf{Z}[\sqrt[n]{a}]$ in that case then it isn't when n is a multiple of such a prime. We obviously don't want to try this out numerically when $a = 2$, since the first such n is 1093. Instead of choosing a and looking for Wieferich primes to base a for examples, let's turn things around: pick a prime p and search for a such that p is a Wieferich prime to base a. There are always solutions a to (3.3), for instance every $a \equiv 1 \bmod p^2$. Table 2 lists squarefree Wieferich bases for small primes, and we can experiment with those.

p	Squarefree bases a with Wieferich prime p	As congruence mod p^2
2	5, 13, 17, 21, 29, 33, 37, 41, 53, 57, 61, 65	$a \equiv 1 \bmod 4$
3	10, 17, 19, 26, 35, 37, 46, 53, 55, 62, 71, 73	$a \equiv \pm 1 \bmod 9$
5	7, 26, 43, 51, 57, 74, 82, 93, 101, 107, 118	$a \equiv \pm 1, \pm 7 \bmod 25$
7	19, 30, 31, 67, 79, 97, 129, 146, 165, 166	$a \equiv \pm 1, \pm 18, \pm 19 \bmod 49$

Table 2. Bases a having small Wieferich primes p

For $p = 2$, you should know quite well that when $a \equiv 1 \bmod 4$ and a is not a perfect square, $\mathbf{Z}[\sqrt{a}]$ is not the full ring of integers of $\mathbf{Q}(\sqrt{a})$ thanks to $(1+\sqrt{a})/2$. The first entry for a in Table 2 when $p = 3$ is 10 and we saw $\mathbf{Z}[\sqrt[3]{10}]$ is not the ring of integers of $\mathbf{Q}(\sqrt[3]{10})$ in Example 3.6. Asking PARI for a $\mathbf{Z}$-basis of the integers of $\mathbf{Q}(\sqrt[p]{a})$ (use the command `nfbasis(x^p-a)`) for various a and p in Table 2 returns an answer of the form $\{1, \sqrt[p]{a}, \sqrt[p]{a}^2, \ldots, \sqrt[p]{a}^{p-2}, z\}$, where z is a linear combination of $\{\sqrt[p]{a}^i : 0 \leq i \leq p-1\}$ having coefficients that are rational with denominator p: a definite non-member of $\mathbf{Z}[\sqrt[p]{a}]$! Examining the expression for z in examples as p and a vary suggests the following candidate for an algebraic integer in $\mathbf{Q}(\sqrt[p]{a})$ that is not in $\mathbf{Z}[\sqrt[p]{a}]$:

$$\frac{1}{p}\sum_{k=0}^{p-1} a^{p-1-k}\sqrt[p]{a}^{k}. \tag{5.1}$$

(When $p = 2$, this is $\frac{a+\sqrt{a}}{2} = \frac{a-1}{2} + \frac{1+\sqrt{a}}{2}$.) In $\mathbf{F}_p[X, Y]$,

$$\sum_{k=0}^{p-1} X^{p-1-k}Y^k = \frac{X^p - Y^p}{X - Y} = (X - Y)^{p-1},$$

so (5.1) is an algebraic integer if and only if $(a - \sqrt[p]{a})^{p-1}/p$ is. We will work with this last expression.

Theorem 5.1. *If $a^{p-1} \equiv 1 \bmod p^2$ and $T^p - a$ is irreducible over $\mathbf{Q}$, then*

(*a*) *p is not totally ramified in $\mathbf{Q}(\sqrt[p]{a})$,*
(*b*) *the ratio $(\sqrt[p]{a} - a)^{p-1}/p$, which is not in $\mathbf{Z}[\sqrt[p]{a}]$, is an algebraic integer.*

Therefore the ring of integers of $\mathbf{Q}(\sqrt[p]{a})$ is not $\mathbf{Z}[\sqrt[p]{a}]$.

We do not assume a is squarefree, which is why we are explicit that $T^p - a$ is irreducible.

Proof. Set $K = \mathbf{Q}(\sqrt[p]{a})$ and $\alpha = \sqrt[p]{a} - a$, so $[K : \mathbf{Q}] = p$ and the minimal polynomial of α over $\mathbf{Q}$ is

$$(T + a)^p - a = T^p + p(\cdots) + a^p - a,$$

so $\mathrm{N}_{K/\mathbf{Q}}(\alpha) = \pm(a^p - a)$. Every prime $\mathfrak{p}$ that lies over p in $\mathcal{O}_K$ is a factor of (α): $\mathcal{O}_K/\mathfrak{p}$ is a field of characteristic p and the pth power map is one-to-one on such fields, so $\sqrt[p]{a}^{\,p} = a \equiv a^p \bmod \mathfrak{p} \Rightarrow \sqrt[p]{a} \equiv a \bmod \mathfrak{p}$. Thus $\mathfrak{p} \mid (\alpha)$.

(a) We will prove the contrapositive: if p is totally ramified in K and $(p, a) = 1$, then $a^{p-1} - 1$ is divisible by p just once. (Note that if $a^{p-1} \equiv 1 \bmod p^2$ then $(p, a) = 1$.)

Since $[K : \mathbf{Q}] = p$, having p be totally ramified means $(p) = \mathfrak{p}^p$. Let $\mathfrak{p}^r \,||\, (\alpha)$, so $r \geq 1$ since $\mathfrak{p} \mid (\alpha)$. Since $\mathfrak{p}$ is the only prime lying over p in $\mathcal{O}_K$ and $\mathrm{N}(\mathfrak{p}) = p$, from $\mathfrak{p}^r \,||\, (\alpha)$ we get $p^r \,||\, (a^p - a)$ in $\mathbf{Z}$. We want to show $r = 1$. Our argument is adapted from [8, p. 390].

In the expansion

$$\begin{aligned} 0 &= (\alpha + a)^p - a \\ &= \alpha^p + \sum_{i=1}^{p-1} \binom{p}{i} \alpha^i a^{p-i} + a^p - a, \end{aligned}$$

subtract $a^p - a$ from both sides:

$$\alpha^p + \sum_{i=1}^{p-1} \binom{p}{i} \alpha^i a^{p-i} = a - a^p. \tag{5.2}$$

We are going to look at the highest power of $\mathfrak{p}$ dividing both sides. Keep in mind the following: if $\mathfrak{p}^k \,||\, (x)$ and $\mathfrak{p}^{k+1} \mid (y)$, then $\mathfrak{p}^k \,||\, (x + y)$ provided $x + y \neq 0$. (Think about congruences modulo $\mathfrak{p}^k$ and $\mathfrak{p}^{k+1}$.)

On the right side of (5.2), $p^r \,||\, (a - a^p)$ in $\mathbf{Z}$, so $\mathfrak{p}^{rp} \,||\, (a - a^p)$ as ideals in $\mathcal{O}_K$. On the left side of (5.2), $\mathfrak{p}^{rp} \,||\, (\alpha^p)$. For $1 \leq i \leq p - 1$, $\binom{p}{i}$ is divisible by p exactly once. Since a is not divisible by p, $\binom{p}{i}\alpha^i a^{p-i}$ has highest $\mathfrak{p}$-power $\mathfrak{p}^{p+ir}$. So the $\mathfrak{p}$-power multiplicities of the terms on the left side of (5.2) are rp and $p + ir$ for $1 \leq i \leq p - 1$.

If $r \geq 2$, the *unique* minimum of the numbers $rp, p + r, p + 2r, \ldots, p + (p - 1)r$ is $p + r$ as long as $p \neq 2$. (The theorem can be checked directly when $p = 2$, so there's no harm in taking $p > 2$.) Therefore the highest $\mathfrak{p}$-power dividing the left side of (5.2) is $p + r$. Comparing this to the highest power of $\mathfrak{p}$ dividing the right side of (5.2), we get $p + r = pr$. But $p + r < pr$, so we have a contradiction. This forces $r = 1$, so $p \,||\, (a^p - a)$.

(b) We want to show $\alpha^{p-1}/p \in \mathcal{O}_K$. Since p is not totally ramified in K and $[K : \mathbf{Q}] = p$, each prime ideal factor of (p) has multiplicity at most $p - 1$. Every prime lying over p in $\mathcal{O}_K$ is a factor of (α), so $(\alpha)^{p-1}$ is divisible by (p) as ideals. Therefore $\alpha^{p-1}/p \in \mathcal{O}_K$. □

We now know that $\mathbf{Q}(\sqrt[n]{2})$ does not always have ring of integers $\mathbf{Z}[\sqrt[n]{2}]$ and the first counterexample is $n = 1093$.

Remark 5.2. If $(p, a) = 1$ then p is totally ramified in $\mathbf{Q}(\sqrt[p]{a})$ if and only if $a^{p-1} \not\equiv 1 \bmod p^2$. Theorem 5.1 implies the "only if" direction, while in the other direction p divides $a^p - a$ just once, so $(T + a)^p - a$ is Eisenstein at p and therefore p is totally ramified in $\mathbf{Q}(\sqrt[p]{a})$.

Here is the full description of when $\mathbf{Q}(\sqrt[n]{a})$ has integers $\mathbf{Z}[\sqrt[n]{a}]$ if $[\mathbf{Q}(\sqrt[n]{a}) : \mathbf{Q}] = n$.

Theorem 5.3. *If $a \neq \pm 1$, $n \geq 2$, and $T^n - a$ is irreducible in $\mathbf{Z}[T]$ then the integers of $\mathbf{Q}(\sqrt[n]{a})$ are $\mathbf{Z}[\sqrt[n]{a}]$ if and only if (i) a is squarefree and (ii) no prime factor of n is a Wieferich prime to base a.*

Proof. First suppose conditions (i) and (ii) are satisfied. Let p be a prime factor of n and p^r be the highest power of p dividing n. Then $\mathbf{Q}(\sqrt[p^r]{a})$ has integers $\mathbf{Z}[\sqrt[p^r]{a}]$ if $p \mid a$ by Theorem 3.1 and if $p \nmid a$ by Theorem 3.2. Since this holds for all prime factors of n, $\mathbf{Q}(\sqrt[n]{a})$ has integers $\mathbf{Z}[\sqrt[n]{a}]$ by Corollary 2.4.

Next we assume conditions (i) or (ii) fail.

- If a is not squarefree then the integers of $\mathbf{Q}(\sqrt[n]{a})$ are not $\mathbf{Z}[\sqrt[n]{a}]$ by Theorem 2.1.
- If a is squarefree and n has a prime factor p that is a Wieferich prime to base a, then Theorem 5.1 says the integers of $\mathbf{Q}(\sqrt[p]{a})$ are not $\mathbf{Z}[\sqrt[p]{a}]$, so Lemma 2.2 tells us that the integers of $\mathbf{Q}(\sqrt[n]{a})$ are not $\mathbf{Z}[\sqrt[n]{a}]$.

□

The results here give a setting other than Fermat's last theorem where solutions a to the congruence $a^{p-1} \equiv 1 \bmod p^2$ cause undesirable behavior. Another problem where solutions to $2^{p-1} \equiv 1 \bmod p^2$ lead to undesirable behavior is in the study of Fermat numbers $F_n = 2^{2^n} + 1$ and Mersenne numbers $M_n = 2^n - 1$. It is conjectured that every F_n and M_q for prime q is squarefree.[4] In [7] it is shown that if F_n or M_q is not squarefree, with a repeated prime factor p, then $2^{p-1} \equiv 1 \bmod p^2$, and moreover that 1093 and 3511 are not factors of an F_n or M_q.

References

[1] N. G. W. H. Beeger, "On a new case of the congruence $2^{p-1} \equiv 1 \pmod{p^2}$," *Messenger of Mathematics* **51** (1922), 149–150.

[2] N. G. W. H. Beeger, *On composite numbers n for which $a^{n-1} \equiv 1 \bmod n$ for every a prime to n*, Scripta Math. **16** (1950), 133–135. Online at https://books.google.com/books/about/Scripta_Mathematica.html?id=zeQSAAAAIAAJ.

[3] J. Knauer and J. Richstein, "The Continuing Search for Wieferich Primes," *Math. Comp.* **74** (2005), 1559–1563.

[4] W. Meissner, "Über die Teilbarkeit von $2^p - 2$ durch das Quadrat der Primzahl $p = 1093$," *Sitzungsber. Akad. D. Wiss. Berlin* (1913), 663–667.

[5] D. Miramanoff, "Sur le dernier théorème de Fermat," *C. Rendus hebdomadaires des séances de l'Academie des Sciences* **150** (1910), 193–206.

[6] P. Montgomery, "New Solutions of $a^{p-1} \equiv 1 \bmod p^2$," *Math. Comp.* **61** (1993), 361–363.

[7] L. J. Warren and H. G. Bray, "On the Squarefree-ness of Fermat and Mersenne Numbers," *Pacific J. Math.* **22** (1967), 563–564.

[8] J. Westlund, "On the Fundamental Number of the Algebraic Number-Field $k(\sqrt[p]{m})$," *Trans. Amer. Math. Soc.* **11** (1910), 388–392.

[9] A. Wieferich, "Zum letzten Fermatschen Theorem," *J. für die Riene und Angewandte Mathematik* **136** (1909), 293–302.

[4] Many M_n are not squarefree for composite n. For instance, $2^6 - 1 = 63$ is not squarefree, so $2^n - 1$ is not squarefree if $6 \mid n$ since $(2^6 - 1) \mid (2^n - 1)$.