On Power Bases in Number Fields

Yan Zhang
Prof. William Stein
Math 129

March 13th, 2005

Abstract

We survey the problem of existence and computation of power bases in number fields.

1 Preliminaries

A number field K has a *power basis* (or in some literature, a *power integral basis*) if its ring of integers is generated by a single element; i.e. $\mathbf{O}_k = \mathbf{Z}[\alpha]$. It is a long standing open problem in algebraic number theory to characterize all number fields with a power basis; and, if one exists, a list of potential generators. This in turn is a subproblem of characterizing all elements of a given index in a number field. Note that an algebraic integer has index 1 if and only if it is a generator for a power basis of O_K.

One problem with the unity of existing literature on this subject is many equivalent formulations of the problem (for one, the existence of a power basis is labelled *monogeneity*). This is the unfortunate (or fortunate?) result of the widespread interest of the topic.

2 Motivating Problems

It is a well-known result that at least one integral (not necessarily power) basis exists for a number field K. Suppose it has the form $\{1, w_2, \ldots, w_n\}$. The discriminant of the linear form $l(x) = x_2w_2 + x_3w_3 + \ldots + x_nw_n$ can be then expressed as $(I(x_2, \ldots, x_n))^2 Disc(K)$, where $Disc(K)$ is the field discriminant and I is called the *index form* corresponding to the given integral basis.

The problem of determining all elements of index i is equivalent to solving the *index form equation*

$$|I(x_2, \ldots, x_n)| = i. \tag{1}$$

So in particular, the existence of a power basis is equivalent to the existence of a solution to $|I(x_2, \ldots, x_n)| = 1$.

Let K be an algebraic number field, and N the norm function. The pair (α, N_0)[1], where $N_0 = \{0, 1, \ldots, |N(\alpha)| - 1\}$ is a *canonical number system (CNS)* in $\mathbf{O}_K$ for an algebraic integer α if each algebraic integer can be represented uniquely as

$$a_0 + a_1\alpha + \ldots + a_l\alpha^l, \tag{2}$$

[1]Note that the first decides the second, so an ordered pair is really not necessary. This, however, seems to be the convention.

$a_i \in N_0$.

The most important connection to our problem is in [20], where Kovács claims[2]:

Theorem 1. *In $\mathbf{O}_K$, where K is a number field of degree ≥ 3, there exists a CNS if and only if a power basis exists.*

There is already some possible problems here with two different sets of mathematical language. William Gilbert uses the same definition as above and calls a CNS a *radix representation* (see [14]), which has its own uses in fractal tilings and other computational topics.

Some further confusion arises with a more modern and general definition of a CNS, introduced by Attila Pethö: let $P \in Z[x]$ be monic, $N = |P(0)| > 1$. Then $(P, \mathbf{N})$, where $\mathbf{N} = \{0, 1, \ldots, N-1\}$, is called a canonical number system if every non-zero element of $\mathbf{Z}[x]/PZ[x]$ can be written uniquely as $a_0 + a_1 x + \ldots + a_l x^l$, where $a_i \in \mathbf{N}$ and a_l is nonzero. In this case, P is called a CNS polynomial, and it is possible that much of the work on CNS polynomials with this definition (usually done independently in the field of computer science) may be applicable to its special case in algebraic number theory. However, the two fields are not working in seclusion from each other. Akiyama et al. ([1]) gives a survey of the topic of canonical number systems with some reference to algebraic number fields.

The topic of power bases is widely-studied, with many deep and difficult aspects. We will try to give a survey of results and work through a couple of examples and theorems as length and difficulty permits.

3 Canonical Examples

The study of the existence of a power basis is trivialized if a power basis always exists. Indeed, one might be tempted to believe that any number field is monogenic after showing that $K = \mathbf{Q}(\sqrt{d})$ always has a power basis for d prime, as almost any algebraic number theory text will prove. In fact, there is a generalization for any quadratic extension:

Theorem 2. *For d squarefree and $K = \mathbf{Q}(\sqrt{d})$, a power basis always exists of the form $\mathbf{Z}[(1+\sqrt{d})/2]$ when $Disc(K) \equiv 1 \pmod 4$ and $\mathbf{Z}[\sqrt{d}]$ otherwise. In particular, the first case happens exactly when $d \equiv 1 \pmod 4$.*

Proof. The proof is similar to the prime case and does not offer real new insight. Many algebraic number theory texst such as [23] will do this in full. □

Of course, it is not true that a power basis always exists. A classical counterexample is Dedekind's example $\mathbf{Q}(a)$, where a has the minimal polynomial $x^3 + x^2 - 2x + 8$.

Proposition 1. *$\mathbf{Q}(a)$, $a^3 + a^2 - 2a + 8 = 0$, has no power basis.*

Proof. There are many ways of seeing this proof. They mostly all fall under the same category: suppose that there is a power basis $\mathbf{Z}[b]$. Then it has index 1 in O_K. Thus, the factoring of $2O_K$ corresponds to the factoring of b's minimal polynomial in $\mathbf{F}_2[x]$. But note that $2O_K$ splits completely as ideals $p_1 p_2 p_3$ (symbolic calculating software such as PARI or MAGMA does this easily). b has degree at most 3, so the factoring must correspond to 3 distinct linear factors in $\mathbf{F}_2[x]$. But there are only two irreducible linear polynomials in $\mathbf{F}_2[x]$, a contradiction. □

[2]The uses of the word "claims" in this paper does not suggest that the associated sources are dubious. Rather, due to availability and/or language difficulties, the author was only able to read abstracts or reviews of the associated papers, mostly through math.sci.net.

4 Biquadratic Fields

The existence of a power basis quickly gets difficult as the degree of the extension rises above 2. While a natural next step would be to look at cubic extensions, there is the clear possible benefit that we might be able to generalize quadratic extension results to biquadratic extensions.

Unfortunately, just because quadratic extensions always have a power basis, it is not necessarily the case for biquadratic extensions. We start with an example.

Proposition 2. *The ring of integers of* $\mathbf{Q}(\sqrt{x},\sqrt{y})$ *is not monogenic if* $x \equiv y \equiv 1 \pmod 3$.

Proof. For the first proof, we generalize and slightly improve on a sketched solution by J. Milne ([22]), who proves the special case for $(x,y) = (7,10)$:

First consider $a_1 = (1+\sqrt{x})(1+\sqrt{y})$, $a_2 = (1+\sqrt{x})(1-\sqrt{y})$, $a_3 = (1-\sqrt{x})(1+\sqrt{y})$, $a_4 = (1-\sqrt{x})(1-\sqrt{y})$. We know that the trace of $(a_i)^n$ is $a_1^n + a_2^n + a_3^n + a_4^n$. Note that

$$\begin{aligned} a_1^2 &\equiv (1+x+2\sqrt{x})(1+y+2\sqrt{y}) && (3)\\ &\equiv 4(1+\sqrt{x})(1+\sqrt{y}) && (4)\\ &\equiv (1+\sqrt{x})(1+\sqrt{y}) && (5)\\ &\equiv a_1 \pmod 3. && (6) \end{aligned}$$

This means that when taken $\pmod 3$:

$$\begin{aligned} Tr((a_i)^n) &\equiv a_1^n + a_2^n + a_3^n + a_4^n && (7)\\ &\equiv a_1 + a_2 + a_3 + a_4 && (8)\\ &\equiv 1 (mod 3) && (9) \end{aligned}$$

.

Sp $a_i^n/3$ is not an algebraic integer. If it were, then the minimal polynomial of a_i^n would have the second term, or trace, being a multiple of 3. Explicit computation gives that $a_i a_j$ for any $i \neq j$ is divisible by 3. A quick way to see this is to realize that the product either contains a term of the form $(1+\sqrt{x})(1-\sqrt{x})$ or $(1+\sqrt{y})(1-\sqrt{y})$.

Now suppose $O_K = \mathbf{Z}[a]$, a with minimal polynomial f. For $g(x) \in \mathbf{Z}[x]$, denote its image if $\mathbf{F}_3[x]$ as $\overline{g(x)}$.

It is an easy algebraic fact that $g(a)$ is divisible by 3 in $\mathbf{Z}[a]$ if and only if $\overline{f} | \overline{g}$ in $\mathbf{F}_3[x]$. Write $a_i = f_i(a)$ for all i, where $f_i \in \mathbf{Z}[x]$. Our results give $\overline{f} | \overline{f_i f_j}$ for $i \neq j$. But $\overline{f}$ does not divide $\overline{f_i}^n$ since no power of a_i is a multiple of 3, as we showed earlier in the proof. So for each i, we claim that $\overline{f}$ has an irreducible factor $\overline{g_i}$ that divides all other $\overline{f_j}$ but not $\overline{f_i}$.

So we know that $\overline{f}$ has at least 4 distinct factors, all irreducible, over $\mathbf{F}_3$. This is bad, since f has degree at most 4, so f must have degree 4. Therefore it splits into linear polynomials. But there are only 3 distinct linear polynomials $\pmod 4$, a contradiction.

□

The very elementary techniques in this proof hides the core of what is happening, as this alternative proof elucidates:

Proof. Assume there is a power basis $\mathbf{Z}[b]$. Then it has index 1 in O_K. Thus, the factoring of $3O_K$ corresponds to the factoring of b's minimal polynomial in $\mathbf{F}_3[x]$. But note that $3O_K$ splits as ideals $p_1 p_2 p_3 p_4$ (again, by PARI or MAGMA). b must factor as 4 distinct linear factors in $\mathbf{F}_3[x]$. But there are only 3 irreducible linear polynomials in $\mathbf{F}_3[x]$, a contradiction. □

Note the inherent similarity between the two proofs. Furthermore, we now see the nonmonogenity of this field in light of Dedekind's original example. We attempt to find a prime p which splits into many distinct ideals, which must correspond to distinct irreducible factors in $\mathbf{F}_p[x]$. As long as there are not enough irreducible polynomials, we can reach a contradiction.

An equivalent condition of the existence of a power basis in the most general form for biquadratic extensions was claimed by Gras ([15]):

Theorem 3. *Let $K = \mathbf{Q}(\sqrt{dm}, \sqrt{dn})$ be a biquadratic number field (where $d, m, n \in \mathbf{Z}$ are uniquely determined). Let δ be determined by $mn \equiv (-1)^{\delta} \pmod 4$. K is monogenic if and only if:*

1. $2^{\delta}m = 2^{\delta}n + 4(2^{-\delta}d)$.
2. $|(u^2 - v^2)^2(2^{\delta}m)(u^2 + v^2)^2(2^{\delta}n)| = 1$ *has solutions in* $\mathbf{Z}$.

While this is an exact characterization, it is not as exciting as we would hope for, considering that the problem reduces to finding the existence of solutions of a Diophantine equation. Still, it is an important development.

5 Cubic Extensions

The reformulation in the final theorem in the last section in terms of a diophantine equation is not unsurprising, recalling that an equivalent condition to the existence of a power basis is the existence of solutions of the index form equation for index equalling 1.

With this, we go back a step and look at cubic extensions. Gaál et al. wrote a paper on this ([8]), but they curiously left out the index equation. Here, attempting to make the theorems for the cubic and quartic (to come) cases parallel, we use a method that we will revisit later:

Theorem 4. *Let $K = \mathbf{Q}(\zeta)$ be a cubic number field with the minimal polynomial $f(t) = t^3 + a_1t^2 + a_2t + a_3$ satisfied by ζ. Let $\{1, w_2, w_3\}$, where $w_i = (1/d)\Sigma w_{ij}\zeta^{j-1}$, be an integral basis of K. Assume $\alpha = x_0w_2 + y_0w_3 = (1/d)(x\zeta + y\zeta^2)$. We have $I(\alpha) = m$ if and only if there is an integral solution to*

$$|x^3 - 2a_1x^2y + (a_1^2 + a_2)xy^2 - (a_1a_2 - a_3)y^3| = d^3m/|I(\zeta)| \tag{10}$$

Proof. Call the conjugates of ζ $\zeta_1, \ldots, \zeta_3$, and similarly for other variables. We start with $I(\alpha)/I(\zeta) = m/n$. Take $\alpha' = d\alpha = a + x\zeta + y\zeta^2$, we get exactly $I(\alpha')/I(\zeta) = d^3m/n$. The power of d is 3 since the index form is of order $\binom{3}{2}$.

We then have from above

$$\prod(\frac{(\alpha_i' - \alpha_j')}{(\zeta_i - \zeta_j)}) = d^3m/n, \tag{11}$$

where the product is over the ordered pairs $(1,2), (1,3), (2,3)$. For each one of these we may write

$$\begin{aligned} \frac{(\alpha_i' - \alpha_j')}{(\zeta_i - \zeta_j)} &= \frac{(x(\zeta_i - \zeta_j) + y(\zeta_i^2 - \zeta_j^2)}{(\zeta_i - \zeta_j)} &(12)\\ &= (x + y(\zeta_i + \zeta_j)). &(13)\end{aligned}$$

A product of these gives the equation above. This actually includes neat tricks, such as for the y^3 term we need

$$
\begin{aligned}
(\zeta_1+\zeta_2)(\zeta_2+\zeta_3)(\zeta_1+\zeta_3) &= (-a_1-\zeta_3)(-a_1-\zeta_2)(-a_1-\zeta_1) && (14)\\
&= f(-a_1) && (15)\\
&= (-a_1)^3+a_1(-a_1)^2+a_2(-a_1)+a_3 && (16)\\
&= -a_1a_2+a_3. && (17)
\end{aligned}
$$

But we digress. □

Note that in the trivial case when $I(\zeta)=1$, i.e. when we already have a power basis, Using $(x,y)=(d,0)$ solves the diophantine equation trivially.

Consider again the field generated by x^3+x^2-2x+8. It has an integral basis $\{1,\zeta,\zeta^2/2\}$, where ζ is a root. This shows that $I(\zeta)$ has index 2, so the equation we need to solve is

$$|x^3-2x^2y-xy^2+38y^3|=4. \tag{18}$$

Knowing that the Dedekind field is nonmonogenic, we know immediately that this equation should have no solutions[3].

Using the index form equation, [8] gives a feasible algorithm to compute all power integral bases in totally real and totally complex cubic number fields.

There are also some non-computational results. Dummit and Kisilevsky ([4]) claims that infinitely many cubic (in fact Galois) fields have power bases. Meanwhile, Gras ([16]) claims that infinitely many cubic fields do not. Furthermore, she asserts:

Theorem 5. *Let K be a cyclic extension of* $\mathbf{Q}$ *with conductor m. Then, K has a power basis if and only if K has a unit w such that*

1. $Tr(w+w^{-1})=-3$*; and*
2. $Tr((w^2-w^{-1})/m)=n^3$, $n\in\mathbf{Z}$.

In particular, Spearman and Williams ([29]) generates an entire family of cubic fields with minimal index 2 (so they cannot be monogenic).

6 Quartic Extensions, Revisited

In fact, there is an exact characterization of resolution of index form equations in the more general case of all quartic number fields (though not an immediate generalization of the results in the biquadratic section), found by Gaál et al. ([12]):

Theorem 6. *Let* $K=\mathbf{Q}(\zeta)$ *be a quartic number field with the minimal polynomial* $t^4+a_1t^3+a_2t^2+a_3t+a_4$ *satisfied by* ζ. *Let* $\{1,w_2,w_3,w_4\}$, *where* $w_i=(1/d)\Sigma w_{ij}\zeta^{j-1}$, *be an integral basis of K. Assume* $\alpha=x_0w_2+y_0w_3+z_0w_4=(1/d)(a+x\zeta+y\zeta^2+z\zeta^3)$. *We have* $I(\alpha)=m$ *if and only if there is an integral solution to*

$$u^3-a_2u^2v+(a_1a_3-4a_4)uv^2+(4a_2a_4-a_3^2-a_1^2a_4)v^3=\pm d^6m/I(\zeta) \tag{19}$$

[3]This suggests a perverse way to attack homogeneous Diophantine equations - by expressing them as index equations of non monogenic fields. While this idea is currently a mere jest, it might become reality with more theoretical and computational machinery.

such that (x,y,z) *above satisfies*

$$x^2 - xya_1 + y^2a_2 + xz(a_1^2 - 2a^2) + yz(a_3 - a_1a_2) + z^2(-a_1a_3 + a_2^2 + a_4) = u \quad (20)$$

$$y^2 - xz - a_1yz + z^2a_2 = v \quad (21)$$

where, for our purposes, we can just take the case $m = 1$.

Proof. We follow the proof given in the paper. In fact, this proof is the prototype of the proof of the cubic case we did previously, so they will look familiar. However, there are two extra equations here, making the problem a bit different.

Even so, this is not as difficult as it might sound - indeed, it is again an exercise in bookkeeping, as is the flavor of many of these theorems relating to the index form equations. However, using the auxiliary variables, this proof gives us a polynomial of degree 3 instead of 6, making this case much easier and much more interesting as a precedent computationally.

Call the conjugates of ζ $\zeta_1, \ldots, \zeta_4$, and similarly for other variables. We start with $I(\alpha)/I(\zeta) = m/n$. Take $\alpha' = d\alpha = a + x\zeta + y\zeta^2 + z\zeta^3$, we get exactly $I(\alpha')/I(\zeta) = d^6m/n$. The power of d is 6 since the index form is of order $\binom{4}{2}$, taken as

$$Disc(\alpha) = (I(\alpha))^2 Disc(K) \quad (22)$$

$$= \prod(\alpha_i - \alpha_j)^2, \quad (23)$$

taken over indices (i, j), $i < j$, between 1 and 4.

We then have from above

$$\Pi(\frac{(\alpha_i' - \alpha_j')(\alpha_k' - \alpha_l')}{(\zeta_i - \zeta_j)(\zeta_k - \zeta_l)}) = d^6m/n, \quad (24)$$

taken over $(i, j, k, l) = (1,2,3,4), (1,3,2,4), (1,4,2,3)$. Note these are just the permutations taken equivalent modulo cyclic rotation. Each of the 3 permutations accounts for two of the factors, of which we have 6 in total.

Now we see that

$$\frac{(\alpha_i' - \alpha_j')}{(\zeta_i - \zeta_j)} = \frac{(x(\zeta_i - \zeta_j) + y(\zeta_i^2 - \zeta_j^2) + z(\zeta_i^3 - \zeta_j^3))}{(\zeta_i - \zeta_j)} \quad (25)$$

$$= (x + y(\zeta_i + \zeta_j) + z(\zeta_i^2 + \zeta_i\zeta_j + \zeta_j)^2). \quad (26)$$

and by multiplying a pair of these, we see that each of the factors in our main equation can now be written as a linear polynomial $(u - (\zeta_i\zeta_j + \zeta_k\zeta_l)v)$. The coefficients are exactly u and v as stated in the theorem, and the product just becomes

$$(u - (\zeta_1\zeta_2 + \zeta_3\zeta_4)v)(u - (\zeta_1\zeta_3 + \zeta_2\zeta_4)v)(u - (\zeta_1\zeta_4 + \zeta_2\zeta_3)v) \quad (27)$$

Opening this up completes our proof.

□

The punchline of the paper is not this theorem, though it cleverly reduces the complicated 6-th degree index form equation to a cubic and two quadratics; rather, it gives an explicit algorithm that is too complicated to be included here, but has a running time dominated by finding a continued fraction

expression for algebraic integers. The result is good enough to find all "small"[4] cases. In fact, with a modified algorithm, the authors were able to find all, not just "small", solutions for totally complex quartic fields.

One might wonder if such an approach is the answer, and why we are bothering with any more cases if all we have to do is to explicitly compute the index form equations. The answer lies in what we are able to do with Thue equations.

A *Thue equation* is a homogeneous diophantine equation in two variables. Note that our cubic index form equation transforms naturally into a cubic Thue equation, and in our quartic case we get a cubic Thue equation in two auxiliary variables. As we go into higher degrees, the higher exponents and number of variables makes the problem much more difficult to work with. If not for the reduction we did, the quartic case itself would provide a sextic Thue equation, and a reasonable algorithm would probably not be in sight.

Gaál's 1996 survey ([13]) goes as far as to claim that success in computation for higher degrees" is only hopeful if the index form factorizes", which happens when our field has proper subfields besides **Q**. It is no surprise that a lot of new developments of higher-degree work on power bases revolves around fields with specific subfields.

7 Composite Fields

One case of interest that comes up as we move beyond degrees of 2 and 3 is the case of our field being the compositums of two or more fields. One might wonder if we get more information about this case alone, and if our results for bicyclic quartic fields are just natural consequences of some hidden structure of the existence of a power basis in the smaller contained fields.

Probably the first major theorem on composite fields was proven by Gaál in [7], where he proves that:

Theorem 7. *Let L be a number field of degree r, integral basis $\{l_1 = 1, l_2, \ldots, l_r\}$, with index form $I_L(x_2, \ldots, x_r)$. Similarly, let M be a number field of degree s, integral basis $\{m_1 = 1, m_2, \ldots, m_s\}$, with index form $I_M x_2, \ldots, x_s$. Assume that $(Disc(L), Disc(M)) = 1$. Let $K = LM$ be the composite of L and M. Suppose that*

$$\alpha = \sum_i \sum_j x_{ij} l_i m_j, \tag{28}$$

generates a power basis, where x_{ij} are integral. Then we must have

$$N_{M/Q}|(I_L(\sum_i x_{2i} m_i, \ldots, \sum_i x_{ri} m_i))| = 1; \tag{29}$$

$$N_{L/Q}|(I_M(\sum_i x_{i2} l_i, \ldots, \sum_i x_{is} l_i))| = 1. \tag{30}$$

$$\tag{31}$$

Later, Gaál et al. ([6]) give a condition that guarantees the nonexistence of a power basis of polynomial orders:

[4] By which the authors mean to bound $|x_0|$, $|y_0|$, and $|z_0|$ by 10^h for some h a priori. The authors uses the case $h = 10$. Furthermore, the authors also reference earlier papers in which they claim to have proven that it is "very unlikely" for index equations in quartic fields to have very large solutions and it can "take a considerable amount of time to prove" that there do not exist large solutions, even in very special cases, making this approach more reasonable.

Theorem 8. *Let f, g be distinct monic irreducible polynomials over $\mathbf{Q}$ of degrees m and n, respectively. Let a and b be roots of f and g respectively. Set $L = \mathbf{Q}(a)$ and $M = \mathbf{Q}(b)$ and assume that $K = LM$ has degree mn. If there exists a prime p such that both f and g have a linear factor appearing with multiplicity $(\mathrm{mod}\, p)$, then the index of any primitive element of $\mathbf{O}_{fg}$ is divisible by p, where $\mathbf{O}_{fg} = \mathbf{Z}[a,b]$.*

as a corollary, $\mathbf{O}_{fg}$ has no power bases. If this coincides with O_K, then we know O_K is not monogenic.

Similar results on composite fields interestingly makes it much easier to work with, say, certain sextic fields than quintic fields.

A good exhibition of both theoretical and computational results can be found in [10] by Gaál, where he attacks a nonic extension which is composed of two cubic extensions. This resulted in a pair of *relative Thue equations* (now Thue equations with coefficients in ring of integers of the base field, not necessarily $\mathbf{Z} \subset \mathbf{Q}$) which are cubic. The techniques involved seem generalizable. Relative Thue equations will come up again when we look at relative extensions.

8 Cyclotomic Fields and Equivalence of Generators

Theorem 9. *The cyclotomic field $\mathbf{Q}(\zeta_n)$ has ring of integers $\mathbf{Z}[\zeta_n]$.*

Proof. This is again a very instructional example, yet the proof is long. We provide a sketch of it:

First we prove it for primes. Then we show it for prime powers by first showing that $O_K, K = \mathbf{Q}(\zeta_{p^a})$ has a discriminant that is a power of p, and we may write any element in O_K as a sum of $z_j/p(1-\zeta_{p^a})^j$, where z_j^2 is divisible by the discriminant. This approach will show that

$$O_K = \mathbf{Z}[1-\zeta_{p^a}] = \mathbf{Z}[\zeta_{p^a}]. \tag{32}$$

Finally, we use the fact that

$$\mathbf{Z}[\zeta_{p^a}\zeta_{q^b}] = \mathbf{Z}[\zeta_{p^a}]\mathbf{Z}[\zeta_{q^b}] \tag{33}$$

for distinct primes p and q to get the result for a general n. Again, there is a proof in many algebraic number theoretical texts, such as Mollin([23]). □

In a very important paper to the field ([18]), György claims the absolute values of coefficients of a polynomial and its discriminant are bounded by certain computable functions (which he finds and refines in later papers), for polynomials equivalent up to **Z**-*equivalence*, which is the existence of a rational integer a such that $g(x) = f(x+a)$. The results have many corollaries, including showing that there are only finite algebraic integers with given norm and discriminant. The corollary that will be useful to us is that it can be shown that there are only finitely many possible power basis generators up to **Z**-equivalence, which in our language is having a equivalent to a' when

$$a = n + \rho(a'), \tag{34}$$

for $n \in \mathbf{Z}$, $\rho \in Gal(K/\mathbf{Q})$.

This shows another area to research on power bases, namely listing the possible power basis generators up to equivalence. One of the first notable papers is by Robertson ([26]), where it is shown that:

Theorem 10. *In $K = \mathbf{Q}(\zeta_{2^m})$, $O_K = \mathbf{Z}[\zeta_{2^m}] = \mathbf{Z}[\alpha]$ if and only if $\alpha = n \pm \zeta_{2^m}^i$, $n, i \in \mathbf{Z}$.*

For primes, A. Bremner ([3]) conjectured that for $p > 3$, the only non-equivalent generators of $\mathbf{Q}(\zeta_p)$ are ζ_p (from now on just ζ) and $\eta = \zeta + \zeta^2 + \ldots + \zeta^{(p-1)/2}$. He claims this is true for $p = 7$. T. Nagell ([25]) claims this for $p = 5$.

Robertson found a mechanism to check this conjecture to prove the conjecture for primes up through 23, except for the prime 17. He uses the key observation that

Proposition 3. *Let $\gamma = 1/(1+\zeta)$. Then γ is $\mathbf{Z}$-equivalent to η, and $\mathbf{Z}[\gamma] = \mathbf{Z}[\eta] = \mathbf{Z}[\zeta]$.*

Proof. First, consider the automorphism that sends ζ to its square. Then η is equivalent to

$$\zeta^2 + \zeta^4 + \ldots + \zeta^{p-1}, \tag{35}$$

adding 1 (which keeps $\mathbf{Z}$-equivalence) gives $1/(1+\zeta) = \gamma$.

$\mathbf{Z}[\gamma] \subset \mathbf{Z}[\zeta]$ since we can write γ as a polynomial in ζ. γ is a unit, since its reciprocal $(1+\zeta)$ is an algebraic integer. So its minimal polynomial has constant term with norm 1. Thus, we have

$$\begin{aligned} 1 + a_1\gamma + \ldots a_{p-1}\gamma^{p-1} &= 0 && (36)\\ (1+\zeta)(1 + a_1\gamma + \ldots a_{p-1}\gamma^{p-1}) &= 0 && (37)\\ 1 + \zeta + a_1 + a_2\gamma + \ldots + a_{p-1}\gamma^{p-2} &= 0 && (38)\\ \zeta &= p(\gamma), && (39) \end{aligned}$$

where p is a polynomial in γ with integral coefficients. □

With this approach, Robertson eventually arives at:

Theorem 11. *Let p be a regular prime, $q = (p-1)/2$, g a primitive root $\pmod p$. Consider*

$$\begin{pmatrix} 1-px_q & -px_{q-1} & -px_{q-2} & \ldots & -px_1 \\ x_1 & 1-px_q & -px_{q-1} & \ldots & -px_2 \\ x_2 & x_1 & 1-px_q & \ldots & -px_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_{q-1} & x_{q-2} & x_{q-3} & \ldots & 1-px_q \end{pmatrix}$$

Let S be the set of $(x_1,\ldots,x_q) \in (\mathbf{Z}/p\mathbf{Z})^q$ which gives this matrix a determinant of $1 \pmod{p^2}$ when $(x_1,\ldots,x_q)$ and all $(x_1(1-g^{3i})/(1-g^i), x_2(1-g^{5i})/(1-g^i), \ldots, x_{q-1}(1-g^{(p-2)i})/(1-g^i), x_q - s_i)$ (for $1 \le i \le q-1$) are used as the arguments, where $s_i \in \mathbf{Z}/p\mathbf{Z}$ satisfies

$$2^{p-1}(1-g^{pi}) \equiv (1+ps_i)(1-g^i)^p \pmod{p^2}. \tag{40}$$

If S has cardinality q then Bremner's conjecture is true for p.

Just in case, let us test this example on the case $p = 5$, which was the case Nagell worked on earlier.

Proof. Here we get the matrix

$$\begin{pmatrix} 1-5x_2 & -5x_1 \\ x_1 & 1-5x_2 \end{pmatrix}$$

The determinant is $(25x_2^2 - 10x_2 + 1 + 5x_1^2)$. We pick $g = 2$, skip the algebra that gets $s_1 = 4$, and we get the other determinant by using the ordered pair $(7x_1, x_2 - 4)$. Our two determinant conditions become:

$$25x_2^2 - 10x_2 + 1 + 5x_1^2 \equiv 1 \pmod{2)5} \quad (41)$$
$$25x_2^2 - 10x_2 + 441 - 5x_1^2 \equiv 1 \pmod{2)5}, \quad (42)$$

which easily transform into:

$$2x_2 - x_1^2 \equiv 0 \pmod{5} \quad (43)$$
$$2x_2 - 8 + x_1^2 \equiv 0 \pmod{5} \quad (44)$$

So we have exactly $q = 2$ solutions, $(2,2)$ and $(3,2)$. So indeed the conjecture is true for $p = 5$.

□

There is also work on the subfields of cyclotomic fields. Shah and Nakahara ([28]) explored subfields of $\mathbf{Q}(\zeta_m)$, with the results:

Theorem 12. *Let $K = \mathbf{Q}(\zeta_m)$. In the cases*

1. *$m = 2^n \geq 8$, L imaginary index 2 subfield of K distinct from $\mathbf{Q}(\zeta_{m/2})$; and*
2. *$m = 4p^n$, p an odd prime, L imaginary index 2 subfield of K distinct from $\mathbf{Q}(\zeta_{m/4})$,*

L has the ring of integers $\mathbf{Z}[\eta]$, $\eta = \zeta_m - \zeta_m^{-1}$. This value is called the Gauss period.

They also prove that if the 4 is replaced by 3, the second case in the theorem fails. Finally, they give a lemma

Lemma 1. *Let l be a prime number and $K/\mathbf{Q}$ Galois of degree $n = efg$ with ramification index e, relative degree f. If one of the following conditions is satisfied, then O_K has no power basis:*

1. *$el^f < n$;*
2. *$el^f \leq n + e - 1$ if $f \geq 2$.*

Proof. [5] Suppose $O_K = \mathbf{Z}[a]$. Now, if l factors in O_K as $\prod p_i^e$, we know that

$$a^{N_K(p_i)} \equiv a \pmod{p)_i} \quad (45)$$
$$a^{N_K(p_i)} \equiv a \pmod{\prod p_i^e} \quad (46)$$
$$(a^{N_K(p_i)} - a)^e \equiv 0 \pmod{l}, \quad (47)$$

where we get the second line through the Chinese Remainder Theorem.
Consider

$$b = (1/l)(a^{N_K(p_i)} - a)^e = (1/l)a^{el^f} + \ldots \pm (1/l)a^e. \quad (48)$$

This is in O_K.
If $el^f < n$, then it is not in $\mathbf{Z}[a]$ since we have represented b as a non-integral sum of powers of a lower than a^n.
Otherwise, suppose $f > 1$. If $(a,l) = 1$, $el^f \leq n + e - 1$, then we can divide by e powers of a to get

[5] The author would like to thank Anatoly Preygel for reading over this proof with him.

$$a^{-e}b = (1/l)a^{elf-e} + \ldots \pm (1/l), \tag{49}$$

which is again in O_K but not in $\mathbf{Z}[a]$ for the same reason. Finally, if $(a,l) \neq 1$, then without loss of generality $a = 0 \pmod{p}_i$. Since any integer c can be written as

$$c = c_0 + c_1 a + c_2 a + \ldots c_{n-1} a^{n-1}, \tag{50}$$

$c \equiv c_0 \pmod{p}_i$, meaning the residue field $O_K/(p_i)$ is just the elements $0, \ldots, l-1$, so $f = 1$ and we have a contradiction. □

This lemma leads us into the next section, where we also talk about the importance of the Galois group of the extension.

9 Examining the Galois Group

The case analysis which arose so far elude to the importance of the Galois group of the field. For example, we can classify the bicyclic quartic fields as fields with the Galois group $C_2 \times C_2$.

The previously quoted result that infinitely many cubic extensions have no power basis by Gras ([16]) considered their cyclic Galois groups. In [17] by the same author, it was claimed that:

Theorem 13. *Any cyclic extension $K/\mathbf{Q}$ of prime degree $l \geq 5$ is non-monogenic except for $\mathbf{Q}^+(\zeta_{2l+1})$, the maximal real subfield of the $(2l+1)$-th cyclotomic field, where $2l+1$ is prime.*

Motoda and Nakahara ([24]) continues the classical case of biquadratic fields (as in [15]) in extensions with 2-elementary abelian Galois groups (groups where every nonidentity element has order 2)for $[K : \mathbf{Q}] \geq 8$. Note that the biquadratic case in [15] accounts for $[K : \mathbf{Q}] = 4$, and the quadratic case takes care of $[K : \mathbf{Q}] = 2$, so their following result would almost make this branch complete:

Theorem 14. *If K has a 2-elementary abelian Galois group, then:*

1. *If $[K : \mathbf{Q}] \geq 16$, K is not monogenic;*
2. *If $[K : \mathbf{Q}] = 8$, $K = \mathbf{Q}(\sqrt{dm}, \sqrt{dn}, \sqrt{l})$, $mn \equiv 3, l \equiv 1, d \equiv 2 \pmod{4}, d > 0$, and dmnl is square-free, then K is monogenic if and only if $K = \mathbf{Q}(\sqrt{-1}, \sqrt{-2}, \sqrt{-3}) = \mathbf{Q}(\zeta_{24})$.*

Proof. We follow the proof for part (i) in [24]. The proof uses Lemma 1 from Shah ([28]), stated in the previous section.

First, note we can replace $\mathbf{Q}(a,b)$ with $\mathbf{Q}(a,ab)$. If we have two distinct a_i and a_j equivalent to 2 $\pmod 4$, we may multiply them to get $a'_j \equiv 0 \pmod 4$. We may pull out the square of their GCD and get an odd number, so it must be equal to either 1 or 3 $\pmod 4$. Now we only have up to one element which is 2 $\pmod 4$.

Of the remaining elements, if more than one is 3 $\pmod 4$, we may multiply them together to get an element which is 1 $\pmod 4$. Removing the square of the GCD (which must be 1 $\pmod 4$), we again get a number which is 1 $\pmod 4$. This means we may rewrite $K = \mathbf{Q}(\sqrt{a_1}, \ldots, \sqrt{a_n})$ so that only one a_i and a_j can be 2 or 3 $\pmod 4$, respectively[6].

The author claims[7] that as a result the ramification index e with respect to 2 is at most 4.

[6] We would like to thank professor William Stein for his help with this proof.

[7] We apologize for not understanding this step, and wish to make it clear to the reviewer of the paper that we are not pretending to. Our hypothesis is that we first show 2 can only ramify in $\mathbf{Q}(\sqrt{d})$ when $d \equiv 2$ or 3 $\pmod 4$, and ramification indices somehow multiply in the compositum of fields, and we can then deduce that 2 can be ramified with a contribution of up to 2 each from only two possible places, and get a maximum contribution of $2^{1+1} = 4$.

Suppose $r \geq 4$. Take $l = 2$. Then $f \leq 2$. Using $e \leq 4$. If $f = 1$ then

$$el^f \leq 8 < 16 \leq 2^r. \tag{51}$$

If $f = 2$ then

$$el^f \leq 16 \leq 2^r \leq 2^r + e - 1. \tag{52}$$

So the lemma shows that K is not monogenic.

This ends the proof for the first part, leaving the case of index 8 as the interesting one. The proof for the second part is very technical and involves much case analysis. The authors leave as an open problem if the monogenic fields for $[K : \mathbf{Q}] = 8$ coincide with $\mathbf{Q}(\zeta_{24})$ as well.

□

It is no wonder that looking at which Galois groups exhibit fields with power bases might give more insight, and some mathematicians are looking in this direction. For example, the proceedings of the West Coast Number Theory Conference ([21]) included questions on which field with Galois group $S_n, n \geq 5$ has a power basis. Kiran Kedlaya claimed to have exhibited examples for general S_n. Possible techniques used here include noting that

Proposition 4. *$x^n - x - 1$ has Galois group S_n for $n \geq 2$, with discriminant of absolute value $n^n + (-1)^n(n-1)^{n-1}$,*

and a squarefree discriminant yields a field with a power basis by adjoining a root of the corresponding polynomial.

In the same vein, a very recent calculation by Bilu, György, Gaál, and Kálmán ([2]) claims that the totally real sextic field with Galois group S_6, generated by

$$f(x) = x^6 - 5x^5 + 2x^4 + 18x^3 - 11x^2 - 19x + 1 \tag{53}$$

took 4.8 months of total CPU time to enumerate the power basis generators. The group noted that this combination took more time than all of the previous smaller degree fields combined. This just goes on to show this problem gets difficult very quickly.

10 Relative Extensions

We revisit the spirit of Dedekind's classic proof. Recall that the proof succeeded since 2 split completely in O_K. In this light, we have the result that:

Theorem 15. *Let L/K denote a Galois extension. Suppose that there is an unramified prime ideal $p \in O_L$ with norm $< [L : K]$, then we do not have $\alpha \in L$ such that*

$$O_L = O_K[\alpha]. \tag{54}$$

Proof. We follow the proof given in Fröhlich ([5])[8].

This proof relies on a technique by Euler:

[8]This approach was found through John Voight's online resource at http://math.berkeley.edu/ jvoight/expository/index.html. We would again like to thank Anatoly Preygel.

Lemma 2. *Suppose R is a Dedekind domain with K its field of fractions. Let $L = K(a)$, where a's minimal polynomial $g(x)$ lies in $R[x]$. Then*

$$Disc(R[a]) = N_{L/K}(g'(a))R = Disc(g)R. \tag{55}$$

Suppose the assertion holds. Since the norm is less than $[L : K]$, by the pidgeonhole principle we can find x and y such that

$$\begin{aligned} a^x &\equiv a^y \pmod{p} && (56)\\ x &\neq y. && (57) \end{aligned}$$

So $Disc(g)$ is $0 \pmod{p}$ by looking at it as the Vandermonde determinant - it must have two equal columns from what we have just gotten. By the lemma, $p' = p \cap O_K$ divides $Disc(R[a]) \cap O_K = Disc(O_K[a])$. Now we use the well-known fact that

Lemma 3. *Suppose all residue class fields of R are perfect, then p ramifies in L if and only if p divides $Disc(L/K)$.*

So p does not divide $Disc(L/K)$. But by looking at lattice indices we have

$$\begin{aligned} Disc(O_K[a]) &= Disc(O_L)[O_L : O_K[a]]^2 && (58)\\ &= Disc(L/K)[O_L : O_K[a]]^2. && (59) \end{aligned}$$

So in particular p divides $[O_L : O_K[a]]^2$, which is 1 by our assumption. So we have a contradiction. □

This leads us to look at another popular approach used in recent years for the power basis problem is to attack relative extensions L/K instead of just extensions over $\mathbf{Q}$. Here, as in the previous theorem, we are interested in a *relative power basis*, which exists when $O_L = O_K[\alpha]$ for $\alpha \in O_L$.

Both the theoretical and computational aspects of the problem run into two main obstacles. While an integral (not necessarily power integral) basis always existed for $\mathbf{Q}$, this is not necessarily true for relative extensions. Also, like in composite fields, attacking the index form equations naturally results in relative Thue equations which are a bit harder to handle. Naturally, Gaál has done some work here, such as in cubic relative extensions ([9]) and quartic relative extensions ([11]).

We end with an interesting theorem found in [19], due to Kawamoto, Suwa, and Inchimura:

Theorem 16. *Let p be a fixed prime, and K containing a fixed ζ_p. Set $\pi = \zeta_p - 1$. Let L/K be a cyclic extension of degree p. The following are equivalent:*

1. *L/K is unramified (that is, it is unramified at all finite prime divisors), and $O_L = O_K[\alpha]$ for $\alpha \in O_L$ such that $\alpha^\rho - \zeta_p\alpha \in O_K$ for some $\rho \in Gal(L/K)$.*
2. *$L = K(u^{1/p})$, u a unit such that $u \equiv v^p \pmod{\pi^p}$ for $v \in O_K$.*

The proof involves difficult algebra, and is a good indicator of the depth the maturing topic had acquired.

11 Further Thoughts and Conclusion

The difficulty of theoretical attacks on the problem, and accompanying computational attacks when a power basis exists, should be apparent from this survey. Different angles opened up different research, though some old problems still remain unsolved (for example, a complete algorithm for cubic and quartic extensions that are *mixed*, i.e. neither totally real nor totally complex).

In its basic form, the problem is still split between the computational and theoretic side; the former tries to improve known bounds and give explicit generators, the latter is non-constructive but gives more insight into the general structure. At present, the former seems to be more developed than the latter, as most of the work so far, primarily due to Gaál, et al., are algorithmic in nature.

In all, the field of finding the existence of power bases and solving index form equations retains fairly intensive study in the recent years.

There are also parallel developments of the theory under different names (such as canonical number systems) for which we did not do justice, mainly due to the existence of multiple definitions of budding concepts and language barriers between fields.

References

[1] Akiyama, Borbly, Brunotte, Pethö, and Thuswaldner, On a generalization of the radix representation - a survey. *High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams*, 1927, *Fields Institute Communications*, 41, American Mathematics Society, Providence, RI, 2004.

[2] Bilu, Gaál, György, Kálmán, Index form equations in sextic fields: a hard computation. *Acta Arithmetica* 115 (2004), no. 1, 85–96.

[3] Bremner, A., On power bases in cyclotomic number fields, *Journal of Number Theory*. 28 (1988), 288–298.

[4] Dummit and Kisilevsky, Indices in cyclic cubic fields. *Number theory and algebra*, pp. 29–42. Academic Press, New York, 1977.

[5] Frölich and Taylor, *Algebraic Number Theory*, Cambridge studies in advanced mathematics, vol. 27, Cambridge: Cambridge University Press, 1991.

[6] Gaál, Olajos, and Pohst, Michael Power integral bases in orders of composite fields. *Experimental Mathematics.* 11 (2002), no. 1, 87–90.

[7] Gaál, I., Power Integral Bases in Composits of Number Fields. *Canadian Mathematics Bulletin*. Vol. 41 (2), 1998, pp. 158-165.

[8] Gaál and Schulte, Computing all power integral bases of cubic number fields, *Mathematics of Computation*, 53 (1989), 689–696.

[9] Gaál, I., Power integral bases in cubic relative extensions. *Experimental Mathematics*. 10 (2001), no. 1, 133–139.

[10] Gaál, I., Solving index form equations in fields of degree 9 with cubic subfields. *Journal of Symbolic Computation*. 30 (2000), no. 2, 181–193.

[11] Gaál, I., Computing power integral bases in quartic relative extensions. *Journal of Number Theory* 85 (2000), no. 2, 201–219.

[12] Gaál, Peth, and Pohst, On the resolution of index form equations in quartic number fields, *J. Symbolic Computing* 16 (1993), no. 6, 563–584. MR1279534 (95f:11109)

[13] Gaál, Istvn, Computing power integral bases in algebraic number fields. *Number theory (Eger, 1996)*, 243–254, de Gruyter, Berlin, 1998.

[14] Gilbert, William J., Radix representations of quadratic fields. *Journal of Mathematical Analysis and Applications*. 83 (1981), no. 1, 264–274.

[15] Gras, Marie-Nicole, Tano, Franois Corps biquadratiques monognes. (French) [Monogenic biquadratic fields] *Manuscripta Math.* 86 (1995), no. 1, 63–79.

[16] Gras, Marie-Nicole, Sur les corps cubiques cycliques dont l'anneau des entiers est monogne. (French) *Annales Scientifiques de l'Universit de Besanon. Mathmatiques. 4e Srie* No. 6, 26 pp. (1973).

[17] Gras, Marie-Nicole, Non monognit de l'anneau des entiers des extensions cycliques de Q de degr premier $l \geq 5$. (French) [Nonmonogeneity of the ring of integers of cyclic extensions of Q of prime degree $l \geq 5$] *J. Number Theory* 23 (1986), no. 3, 347–353.

[18] Györy, Klmn Sur les gnrateurs des ordres monognes des corps de nombres algbriques. (French) [Generators of monogenic orders of algebraic number fields] *Seminar on number theory*, 1983–1984 (Talence, 1983/1984), Exp. No. 32, 12 pp., Univ. Bordeaux I, Talence, 1984.

[19] Ichimura, H., On power integral bases of unramified cyclic extensions of prime degree. *Journal of Algebra* 235 (2001), no. 1, 104–112.

[20] Kovács, B., Canonical number systems in algebraic number fields. *Acta Math. Acad. Sci. Hungar.* 37(1981), no. 4, 405-407.

[21] http://lsze.cosam.calpoly.edu/wcntc/2000.pdf

[22] Milne, J.S., Algebraic Number Theory, http://www.jmilne.org/math/CourseNotes/math676.html

[23] Mollin, Richard A. Algebraic number theory. *CRC Press Series on Discrete Mathematics and its Applications.* Chapman & Hall/CRC, Boca Raton, FL, 1999.

[24] Motoda, Y. and Nakahara, T., Power integral bases in algebraic number fields whose Galois groups are 2-elementary abelian. *Archiv der Mathematik* (Basel) 83 (2004), no. 4, 309–316.

[25] Nagell, T., Sur les discriminants des nombres algbriques. *Arkiv för Matematik* 7 1967 265–282 (1967).

[26] Robertson, L., Power bases for 2-power cyclotomic fields. *J. Number Theory*. 88 (2001), no. 1, 196–209.

[27] Robertson, L., Power bases for cyclotomic integer rings. *Journal of Number Theory*. 69 (1998), no. 1, 98–118.

[28] Shah and Nakahara, Monogenesis of the rings of integers in certain imaginary abelian fields. *Nagoya Mathematics Journal*. 168 (2002), 85–92.

[29] Spearman and Williams, Cubic fields with index 2. *Monatshefte fr Mathematik* 134 (2002), no. 4, 331–336.