Monogenic Fields and Power Bases

Michael Decker 12/07/07

1 Introduction

Let K be a number field of degree k and $\mathcal{O}_K$ its ring of integers. Then considering $\mathcal{O}_K$ as a $\mathbb{Z}$-module, the nicest possible case is that it has a basis of the form $\{1, \alpha, \alpha^2, \ldots, \alpha^{k-1}\}$ for some $\alpha \in \mathcal{O}_K$. If so, we call α a power generator and this basis a power basis and say that K is monogenic. The existence of a power generator is a handy thing indeed, simplifying arithmetic in $\mathcal{O}_K$. For instance, if K is monogenic, then the task of factoring $p\mathcal{O}_K$ into prime ideals over $\mathcal{O}_K$, a difficult task in general, reduces to factoring the minimal polynomial of α over $\mathbb{F}_p$, which is significantly easier.

Unfortunately, we cannot always find such an α. It is easy to see that all quadratic fields are monogenic, if $K = \mathbb{Q}(\sqrt{D})$ where D is square-free, then $\mathcal{O}_K = \mathbb{Z}[\alpha]$ where

$$\alpha = \begin{cases} \frac{1+\sqrt{D}}{2} & \text{if} \quad D \equiv 1 \mod 4 \\ \sqrt{D} & \text{if} \quad D \equiv 2, 3 \mod 4 \end{cases}$$

Even in the cubic case, however, things begin to get more complicated. While it is easy to construct examples of monogenic cubic extensions, Dedekind showed that if $K = \mathbb{Q}(a)$ where a is a root of $f(x) = x^3 + x^2 - 2x + 8$, then K cannot be monogenic since the ideal (2) splits into three distinct prime ideals in $\mathcal{O}_K$ while there are only two possible linear polynomials over $\mathbb{F}_2$. In fact there are an infinite number of cyclic cubic fields which have a power basis and also an infinite number which do not [2, 4] and similarly for quartic fields.

As the degree of the extension grows, we are forced to place restrictions on the type of field in consideration if we hope to obtain any results. The most commonly studied quartic extensions are the biquadratic ones, i.e. those of the form $\mathbb{Q}(\sqrt{dm}, \sqrt{dn})$. Marie-Nicole Gras and François Tanoé [5] showed that this field is monogenic if and only if the following two conditions are satisfied:

i) $2^\delta m = 2^\delta n + 4(2^{-\delta} d)$, where $\delta =, 0, 1$ is defined by $mn \equiv (-1)^\delta \mod 4$
ii) the equation $(u^2 - v^2)^2(2^\delta m) - (u^2 + v^2)^2(2^\delta n) = \pm 1$ has solutions in $\mathbb{Z}$.

This allowed them to manually check all fields where m, n, d are small and demonstrate that relatively few have power bases – 12% of those with discriminant under 4000.

This paucity of monogenic fields continues, at least in the known cases. The next common restriction to take is the assumption that K is either abelian or cyclic. Here again the main theorem is due to Gras [3], who proved that if n is relatively prime to 6, then there are only a finite number of monogenic abelian extensions of degree n. In particular, if n is prime, her result shows that $\mathcal{O}_K$ has a power basis only in the special case when $K = \mathbb{Q}(\zeta + \bar{\zeta})$ is the maximal real subfield of a cyclotomic field.

One general obstruction to monogenicity is the existence of an inessential discriminant divisor, i.e. a prime which divides the discriminant of every element of $\mathcal{O}_K$ but does not divide the discriminant of $\mathcal{O}_K$. Since

$$\mathrm{Disc}(\alpha) = \mathrm{Disc}(\mathbb{Z}[\alpha]) = \mathrm{Disc}(\mathcal{O}_K) \cdot [\mathcal{O}_K : \mathbb{Z}[\alpha]]$$

we see that if $\mathcal{O}_K = \mathbb{Z}[\alpha]$, then K cannot have any inessential discriminant divisors. The converse, however, is not true. Pleasants constructed an infinite family of fields of all orders $k \geq 3$ where $k+1$ is prime, which have no inessential discriminant divisors but yet are still non-monogenic [8].

Thus we see that the task of determining the monogenicity of a given field is quite difficult. Relatively little is known for extensions of degree larger than six. Such theorems as do exist are generally negative, that is they demonstrate that a certain family of fields cannot be monogenic, so we do not have a large store of monogenic fields of large degree or a way to prove that a given field has a power basis. The main result in this direction is by Kalman György [6]. Note that if α is a power generator, then so is $\alpha - n$ for any $n \in \mathbb{Z}$. Call two such elements $\mathbb{Z}$-equivalent or simply equivalent. Denote by $H(f)$ the maximum of the absolute values of the coefficients of f.

Theorem 1.1. *György (1976)*
If K is a number field of degree k and discriminant D_K, then for all $\alpha \in \mathcal{O}_K$ there exists $\alpha^* \in \mathcal{O}_K$ which is equivalent to α with minimal polynomial m_{α^*} satisfying

$$H(m_{\alpha^*}) < \exp\left[\left(5k^3\right)^{30k^3}\left(|D_K|^{3/2}(\log|D_K|)^k\right)^{3(k-1)(k-2)}\right]$$

The set of such polynomials is finite, so the number of elements in $\mathcal{O}_K$ which are roots of such polynomials must be finite. Thus in principal at least, we can test for monogenicity simply by checking whether each of element in a finite set is a power generator. In practice, however, this bound is already unusably huge for quadratic extensions and grows super exponentially. And though this bound has been considerably improved over the last thirty years, there is still no feasible version of it.

2 Bremner's Conjecture

While György's theorem is not practical as a monogenicity test, note the corollary that there can be, up to equivalence as above, only a finite number of power generators α for a given field K. Denote by $S(K)$ the set of equivalence classes of elements such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. The theorem gives us an upper bound for $|S(K)|$, but in practice the number is much smaller. In the quadratic case there are always two possibilities, so $|S(K)| = 2$, while in almost all cubic cases $|S(K)| \leq 12$, as opposed to György's bound which is several orders of magnitude larger than the size of universe in even these simple cases. We thus look for a better way to compute $S(K)$.

Of course if we could not in general even determine whether a field is monogenic, we have little hope of being able to find all possible power generators for all possible fields. Nagell spends an entire paper determining $S(K)$ set for a single quartic example [7]. One fact that makes this task slightly easier is that once we have found a single power generator, we can then use it in our search for others. Most algorithms then reduce to solving a system of Diophantine equations, as in the method discussed below.

One particularly nice case is the cyclotomic fields $K = \mathbb{Q}(\zeta)$ where ζ is a primitive p-th root of unity for some prime p. Then we always have that K is monogenic, in fact $\mathcal{O}_K = \mathbb{Z}[\zeta]$. Since there is more structure here than in the general case, we will now call two elements of $\mathcal{O}_K$ equivalent if they differ by integer translation, Galois conjugation, or multiplication by -1, i.e. $a \sim a^*$ if $a = n \pm \sigma(a^*)$ for some $n \in \mathbb{Z}$, $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Since this refines the previous definition of $\mathbb{Z}-$equivalence, György's result implies the

set of classes of equivalent power generators is finite. Bremner's conjecture [1] is that it consists of exactly two elements ζ and $\eta = 1 + \zeta^2 + \zeta^4 + \ldots + \zeta^{p-1} = 1/(1+\zeta)$.

Proposition 2.1. $\mathbb{Z}[\eta] = \mathbb{Z}[\zeta]$.

Proof. Since η is defined in terms of powers of ζ, we have trivially that $\mathbb{Z}[\eta] \subseteq \mathbb{Z}[\zeta]$. For the reverse inclusion, note that η is a unit with inverse $1+\zeta$, and hence the constant term of the minimal polynomial is ± 1. Switching signs if necessary, we can therefore find $a_i \in \mathbb{Z}$ such that $1 + a_1\eta + \ldots + a_{p-1}\eta^{p-1} = 0$. Multiplication by $1+\zeta$ yields $1 + \zeta = -(a_1 + a_2\eta + a_3\eta^2 + \ldots + a_{p-1}\eta^{p-2})$, and $\zeta \in ZZ[\eta]$. □

While η is equivalent to ζ for $k = 3$, it is clear that this will never happen for larger k. The initial cases $p = 3, 5, 7$, were known to Bremner and were the basis for his conjecture. Leanne Robertson proved the conjecture for the cases $p = 11, 13, 19, 23$ and gave a general criterion by which it could be checked for any regular prime [9]. The main idea of the paper is to reduce to two separate cases, when α lies on the unit circle and when it lies on the line Im $z = 1/2$ under the usual embedding of $\mathbb{Q}(\zeta) \hookrightarrow \mathbb{C}$. This follows from the following theorem.

Theorem 2.2. *Robertson 2.4*
If $\mathbb{Z}[\alpha] = \mathbb{Z}[\zeta]$ and α is not equivalent to ζ, then $\alpha + \overline{\alpha}$ is equal to an odd integer and so possibly by adding an integer to α, we may assume that Im $\alpha = 1/2$.

Proof. The main idea is to consider separately the cases when $\alpha + \overline{\alpha} \in \mathbb{Z}$ and $\alpha + \overline{\alpha} \notin \mathbb{Z}$. So suppose $\alpha + \overline{\alpha} = k \in \mathbb{Z}$. If k is even then

$$\frac{\alpha + \overline{\alpha}}{2} = \alpha - \frac{k}{2}$$

is an element of $\mathbb{Z}[\zeta]$. But this is impossible since α has norm $\pm p$ and so this element will have norm $\pm p/2^{p-1}$. Thus we must have that $\alpha + \overline{\alpha}$ is odd in this case. The second case is more complicated, but is based on the idea that if $\alpha + \overline{\alpha} \notin \mathbb{Z}$, then $\alpha + \overline{\alpha} \notin \mathbb{Q}$ and so there exists an element $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ which does not fix $\alpha + \overline{\alpha}$. Then we can show

$$\gamma = \frac{\alpha - \sigma(\alpha)}{\alpha - \overline{\alpha}} \notin \mathbb{R}$$

A couple of short lemmas show that this implies

$$\gamma = \frac{\zeta^b - \zeta^a}{\zeta^b - \zeta^{-b}}$$

for some $a, b \in \mathbb{Z}$ and from this that α is equivalent to ζ. □

If we write α with respect to the basis $\{1, \zeta, \ldots, \zeta^{p-1}\}$, we get p norm equations which must be simultaneously satisfied if α is to generate $\mathbb{Z}[\zeta]$. The previous theorem reduces the number of integer indeterminants defining α from p to $(p-1)/2$. Considering these equations led Robertson to the following sufficient criterion:

Theorem 2.3. *Robertson 3.1*
Let p be a regular prime, $q = (p-1)/2$, and g be a primitive root modulo p. Define $D(x_1, \ldots, x_q)$ to be the determinant of the matrix

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

Let Ψ be the set of elements $(x_1, \ldots, x_q) \in (\mathbb{Z}/p\mathbb{Z})^q$ which satisfy

$$D(x_1, \ldots, x_q) \equiv 1 \mod p^2,$$

and for $1 \leq i \leq q-1$

$$D\left(\frac{x_1(1-g^{3i})}{1-g^i}, \frac{x_2(1-g^{5i})}{1-g^i}, \ldots, \frac{x_{q-1}(1-g^{(p-2)i})}{1-g^i}, x_q - s_i\right) \equiv 1 \mod p^2$$

where $s_i \in \mathbb{Z}/p\mathbb{Z}$ is defined by $2^{p-1}(1-g^{pi}) \equiv (1+ps_i)(1-g^i)^p \mod p^2$. If Ψ has cardinality q then Bremner's conjecture is true for p.

This theorem gives us a feasible method to determine all power generators of a cyclotomic field by solving q polynomial equations in q unknowns over a finite field. Notice that since D is a polynomial in $x_1, \ldots, x_q$, and in each of the "twisted" forms we have just multiplied each term by a constant, so the monomials which appear are the same in all instances. We see that $D(x_1, \ldots, x_q) \equiv 1 \mod p$, for all $(x_1, \ldots, x_q)$ since the matrix is lower triangular $\mod p$ with 1's along the diagonal. Thus instead of checking whether $D(x_1, \ldots, x_q) \equiv 1 \mod p^2$, it suffices to check whether $(D(x_1, \ldots, x_q)-1)/p \equiv 0 \mod p$. Also note that if $(x_1, \ldots, x_q)$ is a solutions then $(x_1m^2, x_2m^4, \ldots, x_qm^{2q})$ is also a solution for any $m \in (\mathbb{Z}/p\mathbb{Z})^\times$. Since there are exactly $q = (p-1)/2$ squares in $(\mathbb{Z}/p\mathbb{Z})^\times$, this shows that q always divides the order of Ψ.

Example 2.4. $p = 7$

The matrix is then

$$\begin{bmatrix} 1-7x_3 & -7x_2 & -7x_1 \\ x_1 & 1-7x_3 & -7x_2 \\ x_2 & x_1 & 1-7x_3 \end{bmatrix}$$

and $D(x_1, x_2, x_3) \equiv 1 - 7(3x_3 - 3x_1x_2 + x_1^3) \mod 7^2$. This then reduces as above to $3x_3 - 3x_1x_2 + x_1^3 \equiv 0 \mod p$. Here $g = 3$ and $s_1 = 2, s_2 = 6$, so computing the two twisted forms, we get the following system of equations:

$$\begin{aligned} 3x_3 - 3x_1x_2 + x_1^3 &\equiv 0 \mod p \\ 3x_3 + 3 &\equiv 0 \mod p \\ x_3 - x_1x_2 - x1^3 + 1 &\equiv 0 \mod p \end{aligned}$$

The only simultaneous solutions in $(\mathbb{Z}/7\mathbb{Z})^3$ are $(2,2,6), (1,4,6)$ and $(4,1,6)$. Thus Ψ has cardinality 3 and so Bremner's conjecture is true for $p = 7$.

3 Computations

We now seek an efficient method to quickly generate these equations and then find all solutions. A link to SAGE code I wrote to do this task is given in the appendix. The main difficulty is computing the solution set to the polynomials. Brute force methods quickly become unusable as the number of equations to check grows like $q * p^q$ while the equations themselves are getting longer. One initial approach I made was to try to exploit the fact that the same monomials appear in all equations. Thus, ignoring any relations between the monomials, we can view the equations as elements in a $\mathbb{F}_p$ vector space whose basis is these monomials. We can then make the matrix of the system of equations and row reduce it, finding another system of equations with the same solution

set but where substantially fewer monomials have a non-zero coefficient. Of course since each equation will in general contain more monomials than unknowns, these matrices will be wider than they are tall, so there is some choice as to which columns we wish to row reduce along. Different choices may lead to systems of equations with quite different number of terms remaining. Experimentally, I found that I could eliminate roughly half the terms appearing in each equation in this manner. In this way I could compute up to the case $p = 13$ in a reasonable amount of time. Further progress however, appeared unlikely, as the running time was growing quickly. To push on, I learned that SAGE, via MAGMA, has a very fast Groebner basis algorithm. Using this, I was able to finish the $p = 17, 19$, and 23 cases. The running time for each was roughly 5 seconds, 5 minutes, and 9 hours respectively.

4 Conclusion

The results, as shown in the appendix, prove Bremner's conjecture in the cases $p = 3, 5, 7, 13, 19$, and 23 since in each of these Ψ has the desired size. When $p = 11$ or 17, however, we get more solutions than desired. Robertson's criterion is not a necessary one, though, as it may happen that more solutions occur modulo a prime than do in the integers. In her paper, Robertson was able to show via an auxiliary calculation that the conjecture is still true for $p = 11$ and stated but did not solve another, much more complicated, set of equations whose solution set would determine the $p = 17$ case. In fact, it appears that something strange is happening in the 17 case. The Groebner basis in this case has 13 elements, while in all other cases it has exactly q elements. Also the elements which appear are not nearly as nice. In the other cases, most of the elements look like $x_i + p(x_{q-1}, x_q)$, so we can solve for x_i immediately once we have determined the values x_{q-1} and x_q. This corresponds to the fact that solutions appear in nice families as noted previously. One other observation here is that if $p - 1$ is divisible by an odd number, then one of the terms $1 - g^{3i}, 1 - g^{5i}, \ldots 1 - g^{(q-2)i}$ appearing in the twists will be zero and so this particular twist will have substantially fewer terms than others. But when $p = 17$, we have that $p - 1 = 16$ has no odd factors, hence all of the equations are of full size.

Using the unspecialized Groebner basis algorithm can only take us so far, however. If $p = 23$ took nine hours, I doubt that $p = 29$ would halt in less than a week and that larger examples would be impossible. I believe that further progress could be made by exploiting some of the recurring structure which occurs in the equations and their solutions. One easy trick is that since we know solutions come in families as before, we can pick two elements $a, b \in \mathbb{Z}/p\mathbb{Z}$, one of which is a square and the other is not, and assume that the first entry is always equal to one of these numbers, effectively reducing the number of unknowns by one. Also, depending on how the Groebner basis algorithm is running, it may be advantageous to "pre-optimize" the equations via linear algebra as described above. Finally, since we know there is this nice structure to the solution sets, we may be able to recover it, or at least the number of solutions, which is all we truly care about, from the Groebner basis computed with respect to some other ordering than the lexicographical one, which would substantially increase the speed of the algorithm.

We would also like to consider whether this method, or a similar one, can be applied to prove Bremner's conjecture in other cases. Robertson generalized her criterion in [10] and [11] to deal with powers of 2 and prime powers generally. In the first case, she was able to prove the conjecture for all powers, thus giving us the first infinite family for which all power generators are known non-trivially. Rainière apparently has a preprint wherein he proves similar statement that all generators not equivalent to ζ can be on

the line Im $z = 1/2$ for any cyclotomic field, raising the possibility that we could find a criterion which applies in all cases.

Appendix

My SAGE code appears at https://sage.math.washington.edu:8101/home/pub/1635/. The matrixes, polynomials, and Groebner bases can all be computed quickly by simply entering the desired prime p and evaluating all fields. The results are listed below:

$\Psi_5 = \{(3,2),(2,2)\}$

$\Psi_7 = \{(2,2,6),(1,4,6),(4,1,6)\}$

$\Psi_{11} = \{(8,5,1,2,5),(10,3,9,6,5),(7,4,4,7,5),(2,1,5,8,5),(6,9,3,10,5),(2,7,6,1,9),$
$(8,2,10,3,9),(6,8,8,4,9),(7,6,7,5,9),(10,10,2,9,9)\}$

$\Psi_{13} = \{(12,9,3,4,1,6),(4,1,3,10,3,6),(3,3,10,12,4,6),(10,3,3,12,9,6),$
$(9,1,10,10,10,6),(1,9,10,4,12,6)\}$

$\Psi_{17} = \{(4,16,8,2,6,6,0,3),(13,16,9,2,11,6,0,3),(15,4,16,15,3,7,0,3),$
$(2,4,1,15,14,7,0,3),(8,13,13,15,5,10,0,3),(9,13,4,15,12,10,0,3),(16,1,2,2,7,11,0,3),$
$(1,1,15,2,10,11,0,3),(7,1,0,10,3,7,1,6),(12,13,0,7,7,11,2,6),(6,16,0,10,5,10,4,6),$
$(3,4,0,7,6,6,8,6),(14,4,0,7,11,6,9,6),(11,16,0,10,12,10,13,6),(5,13,0,7,10,11,15,6),$
$(10,1,0,10,14,7,16,6)\}$

$\Psi_{19} = \{(9,6,14,9,17,15,12,2,6),(6,9,14,6,16,15,8,3,6),(7,17,2,1,1,10,2,8,6),$
$(17,1,3,5,4,13,15,10,6),(11,16,2,7,11,10,14,12,6),(16,7,3,17,9,13,13,13,6),$
$(4,4,14,4,5,15,18,14,6),(5,11,3,16,6,13,10,15,6),(1,5,2,11,7,10,3,18,6)\}$

$\Psi_{23} = \{(5,7,8,13,19,17,10,19,19,5,12),(20,20,6,16,21,11,11,10,17,7,12),$
$(14,19,1,8,20,15,22,14,7,10,12),(19,10,4,4,7,10,21,15,11,11,12),$
$(10,5,18,1,10,7,15,11,22,14,12),(17,11,2,3,5,14,5,7,10,15,12),$
$(15,17,9,18,17,19,20,22,20,17,12),(11,21,16,2,22,22,19,21,14,19,12),$
$(7,22,3,12,15,20,7,20,5,20,12),(22,15,13,9,14,5,17,17,15,21,12),$
$(21,14,12,6,11,21,14,5,21,22,12)\}$

Bibliography

1. 1. A. Bremner, On power bases in cyclotomic number fields, *J. Number Theory* **28** (1988), 288-298.

2. 2. D. Dummit and H. Kisilevsky, Indices in cyclic cubic fields, *in* "Number Theory and Algebra" (H. Zassenhaus, Ed), pp. 29-42, Academic Press, New York, 1977.

3. 3. M.-N. Gras, Sur les corps cubique cycliques dont l'anneau des entiers est monogène, *Ann. Sci. Univ. Besançon* (3) Fasc. 6 (1973).

4. 4. M.-N. Gras, Non monogénéité de l'anneau des entiers des extensions cycliques de $\mathbf{Q}$ de degré premier $l \geq 5$, *J. Number Theory* **23** (1986), 347-353.

5. 5. M.-N. Gras and F. Tanoé, Corps biquadratiques mongènes, *Manuscripta Math.* **86** (1995), 63-79.

6. 6. K. György, Sur les polynômes à coefficients entiers et de discriminant donné, III, *Publ. Math. Debrecen* **23** (1976), 141-165.

7. 7. T. Nagell, Sur les discriminants des nombres algébriques, *Ark. Mat.* **7** (1967), 265-282.

8. 8. P.A.B. Pleasants, The number of generators of the integers of a number field, *Mathematika* **21** (1974), 160-167.

9. 9. L. Robertson, Power bases for cyclotomic integer rings, *J. Number Theory* **69** (1998), 98-118.

10. 10. L. Robertson, Power bases for 2-power cyclotomic fields, *J. Number Theory* **88** (200), 196-209.

11. 11. L. Robertson, Power integral bases in prime-power cyclotomic fields, *J. Number Theory* **120** (2006) 372-384.