International Journal of Modern Physics C (c) World Scientific Publishing Company

# Monogenic period equations are cyclotomic polynomials 

Jason A.C. Gallas<br>Instituto de Altos Estudos da Paraíba, Rua Silvino Lopes 419-2502, 58039-190 João Pessoa, Brazil,<br>Complexity Sciences Center, 9225 Collins Ave. 1208, Surfside FL 33154, USA, Max-Planck-Institut für Physik komplexer Systeme, 01187 Dresden, Germany jgallas@pks.mpg.de

Received 19 December 2019
Accepted 30 December 2019
https://doi.org/10.1142/S0129183120500588


#### Abstract

We study monogeneity in period equations, $\psi_{e}(x)$, the auxiliary equations introduced by Gauss to solve cyclotomic polynomials by radicals. All monogenic $\psi_{e}(x)$ of degrees $4 \leq e \leq 250$ are determined for extended intervals of primes $p=e f+1$, and found to coincide either with cyclotomic polynomials, or with simple de Moivre reduced forms of cyclotomic polynomials. The former case occurs for $p=e+1$, and the latter for $p=2 e+1$. For $e \geq 4$, we conjecture all monogenic period equations to be cyclotomic polynomials. Totally real period equations are of interest in applications of quadratic discrete-time dynamical systems.

Keywords: Quadratic dynamics; Monogenic equations; Cyclotomic period equations; Symbolic computation. PACS Nos.: 02.70.Wz, 02.10.De, 03.65.Fd


## 1. Introduction

A recent paper in this Journal has shown that, in the partition generating limit ${ }^{1}$, several orbital equations and clusters of orbital equations of the quadratic (logistic) map coincide with cyclotomic period equations ${ }^{2}$. Period equations were introduced in 1801 by Gauss as auxiliary equations to solve cyclotomic polynomials by radicals.

The purpose of this paper is to report a startling finding obtained by extensive empirical computations: we find monogenic period equations to be either cyclotomic polynomials, or simple de Moivre reduced forms of cyclotomic polynomials, thereby implying the existence of a hierarchical interdependence among fields and subfields of cyclotomic polynomials, or orbital equations. This fact is quite remarkable because, although cyclotomic polynomials are among the most extensively studied polynomials for nearly 220 years, it seems to have hitherto escaped attention that, in essence, Gauss auxiliary monogenic period equations are nothing else than just cyclotomic polynomials themselves.

## 2. Context and basic definitions

As shown by Dedekind ${ }^{3}$, it is always possible to fix a number field $K$ of finite degree $n$ over $\mathbb{Q}$ by selecting an algebraic integer $\alpha \in K$ such that $K=\mathbb{Q}(\alpha)$. In other words, a number field $K$ may be determined by selecting $\alpha$ as a root of a monic $n$-degree $\mathbb{Q}$-irreducible polynomial $f(x)$ and expressing it in terms of $n$ integers $\alpha_{1}, \alpha_{2}, \cdots, \alpha_{n}$, independent of each other, forming a basis for $\mathcal{O}_{K}$, the ring of integers in $K$. In this context, a key problem is to decide whether or not the ring $\mathcal{O}_{K}$ is monogenic, namely if there exists an element $\alpha \in K$ such that $\mathcal{O}_{K}$ is a polynomial ring $\mathbb{Z}[\alpha]$, i.e. if powers of the type $\left(1, \alpha, \cdots, \alpha^{n-1}\right)$ constitute a power integral basis 45617. Every algebraic number field has an integral basis, not necessarily a power integral basis.

In a monogenic field $K$, the field discriminant $\Delta$ coincides with the standard discriminant $D$ of the minimal polynomial of $\alpha$. For non-monogenic fields such identity does not hold. Generically, $D$ and $\Delta$ are interconnected by the harmless-looking relation $5|6| 7 \mid 8$

$$
\begin{equation*}
D=k^{2} \Delta \tag{1}
\end{equation*}
$$

for some $k \in \mathbb{Z}$, called index by Dedekind $\sqrt{3}$, and "ausserwesentlicher Theiler der Discriminante", inessential discriminant divisor, by Kronecker ${ }^{8}$. As pointed out by Vaughan 9 , "while $D$ can be found by straightforward (if tedious) computation, the value of $k$ is quite another story. According to Cohr 10 , page 77, for example, to determine $k$, one would have to test a finite number (which may be very large) of elements of $K$ to see if they are integral." An additional complication to obtain $k$ is the fact that the choice of $\alpha$ is not unique and, therefore, there are several distinct minimal polynomials from which to compute $D$. So, one may consider $k$ as a sort of "quality measure" for minimal polynomial representation and for monogeneity. As described in $\S 4$ of Dedekind's paper ${ }^{33}$, for quite some time he believed to be always possible to find a suitable $\alpha$ leading to a power basis. This, until he found what became a popular textbook example of a non-monogenic field generated by a root of $x^{3}-x^{2}-2 x-8=0$, for which $\Delta=-503, k^{2}=4$, and $D=-4 \cdot 503$.

The computation of the index $k$ and the verification whether or not a given number field has a power basis are two hard problems $\sqrt{415}$. A taste for the difficulties and the representative computation times involved in such tasks may be obtained from a paper by Bilu et al. 11. Efficient algorithms for determining generators of power integral bases involve solving Diophantine equations known as index form equations 5

The first general algorithm for determining all power integral bases in number fields was given in 1976 by Győry $\frac{12}{}$. Subsequently, efficient algorithms were elaborated to determine power integral bases for number fields of degree at most six and some special classes of higher degree number fields 41511 . Section 7.3 of the book by Evertse and Győry 5 discusses significant results by Gras on Abelian number fields of degree $n$, where $n$ is relatively prime to 6 . See also Ref. 13 . Finally, we mention a general and still largely open problem stated by Hasse: to give a characterization of monogenic number fields ${ }^{5|6| 7]}$. Hasse's problem has been considered, among others, by Nakahara and co-authors in several contexts during the last 50 years or so. See Refs. $1314|1516| 17$ and references therein. See also Evertse ${ }^{18}$.

This paper reports results of an extended investigation of the distribution of monogeneity in cyclotomic period equations $\psi_{e}(x)$, a wide class of functions underlying the solution of cyclotomic polynomials $19|20| 21$. We find that all monogenic period equations are either cyclotomic polynomials or simple reduced forms of cyclotomic polynomials. Here, monogenic period equations are obtained with the help of an expression for the field discriminant $\Delta_{e}$ of period equations ${ }^{2}$, Eq. (3) below. Since the polynomial discriminant $D$ may be easily computed, knowledge of $\Delta_{e}$ gives at once

$$
\begin{equation*}
k^{2}=D / \Delta_{e} \tag{2}
\end{equation*}
$$

which is a convenient tool to sort out all equations with index $k=1$. In what follows, we present results obtained for such monogenic period equations. Equations (2) and (3) grant access to families of equations of arbitrarily high degrees $e$, opening the possibility of studying monogeneity well beyond the aforementioned low-degree limits. Note that for high degrees the division in Eq. (2) involves exceedingly large integers.

## 3. Field discriminants of cyclotomic period equations

Let $g$ be a primitive root of a prime $p=e f+1$, and $r=\exp (2 \pi i / p)$. In the Disquisitiones Arithmeticæ, Gauss defined $e$ sums $\eta_{i}$ called "periods" $19|20| 21|2| 22$.

$$
\eta_{i}=\sum_{k=0}^{f-1} r^{g^{k e+i}}, \quad i=0,1, \cdots, e-1
$$

With them, he defined period equations $\psi_{e}(x)$, polynomials of degree $e$ whose roots are the periods $\eta_{i}$

$$
\psi_{e}(x)=\prod_{k=0}^{e-1}\left(x-\eta_{k}\right)=x^{e}+x^{e-1}+\alpha_{2} x^{e-2}+\cdots+\alpha_{e}, \quad \alpha_{\ell} \in \mathbb{Z}
$$

Period equations $\psi_{e}(x)$ constitute a wide class of equations for which the computation of the field discriminant $\Delta_{e}$ presents no difficulties, being given by $2^{2}$

$$
\Delta_{e}=\left\{\begin{align*}
-p^{e-1}, & \text { if }(e-1) \bmod 4=1 \quad \text { and } \quad f \bmod 2=1  \tag{3}\\
p^{e-1}, & \text { if otherwise }
\end{align*}\right.
$$

Together with Eq. (2), this discriminant provides a handy criterion to sort out $k^{2}=1$ monogenic equations through a simple division of two (possibly very large) integers.

## 4. Properties of monogenic period equations

Table 1 lists monogenic period equations as a function of $e$ for the first few equations of a much longer list, containing seven equations for every $e \leq 250$. The table also displays the signature of $\psi_{e}(x)$. The signature ${ }^{7}$ of a polynomial is the doublet $\left(n_{R}, n_{P}\right)$, sometimes written more economically as $n_{R}$, informing the number $n_{R}$ of real roots of $\psi_{e}(x)$, and the number $n_{P}$ of pairs of complex roots. Table 1illustrates regularities that are consistently observed for $e$ up to 250 .

Among the equations obtained for a given $e$ we find no more than two types of polynomials leading to $k=1$. They have either totally complex roots, $n_{R}=0$, or totally real, $n_{R}=e$. Polynomials with $n_{R}=0$ are highlighted differently, to reflect the sign of their discriminants.

For $e=2$, period equations are quadratic and, as known, are all monogenic ${ }^{4}$. For $e=3$, we determined the growth of the number of $k=1$ equations as a function of $e$, up to $e=9000$. Such growth obeys a power-law distribution, implying the existence of an infinite number of monogenic cubic equations.

For $e \geq 4$, we find no more than two monogenic equations for each value of $e$, as illustrated in Table 1. From the Table one recognizes a trend observed also for higher values of $e$ : the absence of monogenic equations for several values of $e$. For instance, for $e \leq 100$ we find no monogenic period equations for $e=7,13,17,19,24,25,27,31,32,34,37,38,43,45,47,49,55,57,59,61,62,64,67$, $71,73,76,77,79,80,84,85,87,91,92,93,94$, and 97 . Analogously, there are 62 cases of missing cyclotomic polynomials with degree $\leq 100$.

Period equations are not difficult to generate fast and explicitly up to very high degrees. As already mentioned, this means that Eqs. (2) and (3) open the possibility to investigate monogeneity systematically for an important family of equations well beyond the aforementioned low-degree limits.

## 5. Monogenic period equations are cyclotomic polynomials

Gauss showed how to decompose and to solve explicitly in terms of radicals cyclotomic polynomials $x^{p}-1=0$, for prime $p$. The procedure is described in $\S 343$ of his Disquisitiones Arithmeticæ $x^{19|20| 21 \mid 22}$. To this end, he introduced period equations as mere auxiliary equations.

Table 1. Monogenic period equations as a function of $e$ for primes $p=e f+1$ and signature $n_{R}$. Highlighted equations have signature $n_{R}=0$ and coincide with cyclotomic polynomials $\Phi_{p}(x)$. Non-highlighted equations and signature $n_{R}=e$ are reduced cyclotomic polynomials.

| $e$ | $p$ | $n_{R}$ | $D=\Delta_{e}$ | $\psi_{e}(x)$ |
| :---: | :---: | :---: | :---: | :---: |

This fact notwithstanding, by examining Table 1 we deduce that all monogenic period equations $\psi_{e}(x)$ are nothing else than cyclotomic polynomials $\Phi_{p}(x)$, interconnected either by $p=e+1$ or $p=2 e+1$. This latter interconnection may be identified as follows.

Consider, e.g., $e=5$ and $p=2 \cdot 5+1=11$, when the corresponding cyclotomic polynomial is

$$
\Phi_{11}(x)=\frac{x^{11}-1}{x-1}=x^{10}+x^{9}+\cdots+x^{2}+x+1
$$

By changing variables according to a standard de Moivre transformation 23

$$
\begin{equation*}
z=x+1 / x \tag{4}
\end{equation*}
$$

and replacing $z$ by $x$ in the equation so obtained, one finds

$$
\psi_{5}(x)=x^{5}+x^{4}-4 x^{3}-3 x^{2}+3 x+1
$$

This quintic, listed in Table 1, was solved explicitly by radicals in a Mémoire read in November 1770 by Vandermonde $24 \mid 25$.

Conversely, changing $x$ in $\psi_{5}(x)$ according to the dual transformation

$$
\begin{equation*}
x=z+1 / z \tag{5}
\end{equation*}
$$

(and replacing $z$ by $x$ ) one recovers the cyclotomic $\Phi_{11}(x)$. Thus, it is an easy matter to pass from one polynomial to the other one, showing that, essentially, monogenic period equations are cyclotomic polynomials. Here is another example.

In 1796, almost three decades after Vandermonde ${ }^{26}$, Gauss recorded in his mathematical diary $27 / 28 \mid 29$ that the regular 17-gon can be constructed by ruler and compass alone. In print, his construction appeared 19 only in 1801 . The solution amounts to reducing by two, four times in succession, the degree of the 17-gon cyclotomic polynomial, namely

$$
\Phi_{17}(x)=\frac{x^{17}-1}{x-1}=x^{16}+x^{15}+\cdots+x^{2}+x+1
$$

Applying de Moivre's transformation, Eq. (4), to $\Phi_{17}(x)$ one gets the first of such reductions, also present in Table 1

$$
\psi_{8}(x)=x^{8}+x^{7}-7 x^{6}-6 x^{5}+15 x^{4}+10 x^{3}-10 x^{2}-4 x+1
$$

Many additional examples are obtained in a similar way, by using the dual transformation, Eq. (5), to unfold $\psi_{e}(x)$ with signature $n_{R}=e$ for all equations listed in Table 1. thereby obtaining the associated cyclotomic $\Phi_{2 e+1}(x)$. The dual transformation worked also for all additional equations up to $e=250$ (not all in Table 1). For instance, $e=96$ is the largest value $\leq 100$ with two monogenic period equations. For signature $n_{R}=0$ and $f=1$ we find

$$
\psi_{96}(x)=x^{96}+x^{95}+x^{94}+x^{93}+x^{92}+\cdots+x^{4}+x^{3}+x^{2}+x+1
$$

while for $n_{R}=96$ and $f=2$ we find

$$
\begin{aligned}
\psi_{96}(x)= & x^{96}+x^{95}-95 x^{94}-94 x^{93}+4371 x^{92}+4278 x^{91}-129766 x^{90}+\cdots \\
& -18009460 x^{6}-2118760 x^{5}+230300 x^{4}+18424 x^{3}-1176 x^{2}-48 x+1
\end{aligned}
$$

Similar doublets occur for $e=6,18,30,36,78,96,138,156,198,210,228,270,306,330, \ldots$ There are 187 doublets for $e \leq 10^{4}, 1164$ for $e \leq 10^{5}, 7750$ for $e \leq 10^{6}$, etc.

## 6. Conclusions

The compelling computational evidence reported here leads us to conjecture that for $e \geq 4$ there are two classes of coincidences between monogenic period equations $\psi_{e}(x)$ and cyclotomic polynomials $\Phi_{p}(x)$ interconnected by $p=e f+1$ : The class of totally complex period equations, for which $p=e+1$, and the class of totally real period equations, for which $p=2 e+1$. For all other values of $f$ in these
classes, we only found non-monogenic period equations and no connections to cyclotomic polynomials. For $e=3$, as already mentioned, it is possible to find an apparently unbounded supply of monogenic period equations with $f>2$. Totally real period equations are of significant interest for applications in quadratic discrete-time dynamical systems in the partition generating limit $12|30| 31 \mid 32$.

## Acknowledgments

The author would like to thank Prof. K. Győry, Debrecen, and Prof. W. Narkiewicz, Wrocław, for their kind feedback and helpful suggestions. This work was supported by the Max-Planck Institute for the Physics of Complex Systems, Dresden, in the framework of the Advanced Study Group on Forecasting with Lyapunov vectors. The author was supported by CNPq, Brazil.

## References

1. M. Cencini, F. Cecconi, and A. Vulpiani, Chaos - From Simple Models to Complex Systems (World Scientific, Singapore, 2010).
2. J.A.C. Gallas, Field discriminants of cyclotomic period equations, Int. J. Mod. Phys. C 31, xxx-yyy (2020), in print. DOI: 10.1142/S0129183120500217
3. R. Dedekind, Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Congruenzen, Abh. König. Ges. der Wissensch. zu Göttingen 23, 1-37 (1878) = Werke, Band 1.
4. I. Gaál, Diophantine Equations and Power Integral Bases, Second Edition (Birkhäuser, Boston, 2019).
5. J.H. Evertse, and K. Győry, Discriminant Equations in Diophantine Number Theory (Cambridge University Press, Cambridge, 2017).
6. W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, (Springer, Berlin, 2004).
7. H. Hasse, Vorlesungen über Zahlentheorie (Springer, Berlin, 1964).
8. L. Kronecker, Über die Discriminante algebraischer Functionen einer Variabeln, J. reine angew. Math. 91, 301-334 (1881).
9. T.P. Vaughan, On computing the discriminant of an algebraic number field, Math. Comput. 45, 569-584 (1985).
10. H. Cohn, A Classical Invitation to Algebraic Numbers and Class Fields (Springer, New York, 1978).
11. Y. Bilu, I. Gaál, and K. Győry, Index form equations in sextic fields: a hard computation, Acta Arithm. 115, 85-96 (2004).
12. K. Győry, Sur les polynômes à coefficients entiers et de discriminant donné III, Publ. Math. Debrecen 23, 141-165 (1976).
13. A. Shahzad, T. Nakahara, and S.M. Husmine, Power integral bases for certain pure sextic fields, Int. J. Number Theory 10, 2257-2265 (2014).
14. A. Hameed and T. Nakahara, Integral bases and relative monogenity of pure octic fields, Bull. Math. Soc. Sci. Math Roumanie 58, 419-433 (2015).
15. N. Khan, S. Katayama, T. Nakahara, and T. Uehara, Monogenity of totally real algebraic extension fields over a cyclotomic field, J. Number Theory 158, 348-355 (2016).
16. N. Khan, T. Nakahara, and H. Sekiguchi, An ideal theoretic proof on monogenity of cyclic sextic fields of prime power conductor, J. Number Theory 198, 43-51 (2019).
17. M. Sultan and T. Nakahara, On certain octic biquadratic fields related to a problem of Hasse, Monatsh. Math. 176, 153-162 (2015).
18. J.H. Evertse, A survey on monogenic orders, available at http://pub.math.leidenuniv.nl/~evertsejh/11-monord-survey.pdf
19. C.F. Gauss, Disquisitiones Arithmeticae (Fleischer, Leipzig, 1801). English translation by Yale University Press and Springer, 1986.
20. P. Bachmann, Die Lehre von der Kreistheilung (Teubner, Leipzig, 1872).
21. C.G. Reuschle, Tafeln Complexer Primzahlen, Welche aus Wurzeln der Einheit Gebildet Sind, (Vogt, Berlin, 1875).
22. H. Rademacher, Lectures on Elementary Number Theory (Blaisdell, New York, 1964).
23. A. de Moivre, Miscellanea Analytica (Tonson and Watts, London, 1730).
24. A.T. Vandermonde, Mémoire sur la résolution des équations, Histoire de l'Académie Royale des Sciences, 365-416 (1771).
25. C. Itzigsohn, Abhandlungen aus der reinen Mathematik von N. Vandermonde (Springer, Berlin, 1888).
26. A. Loewy, Inwieweit kann Vandermonde als Vorgänger von Gauss bezüglich der algebraischen Auflösung der Kreisteilungsgleichungen $x^{n}=1$ angesehen werden? Jahresber. Deutschen Mathematiker Vereinigung 27, 189-195 (1918).
27. F. Klein, Gauss wissenschaftliches Tagebuch 1796-1814, Mit Anmerkungen, Math. Ann. 57, 1-34 (1903).
28. C.F. Gauss, Mathematisches Tagebuch, 1796-1814, Ostwalds Klassiker der Exakten Wissenschaften \#256, 5th Edition, K.R. Biermann, Editor (Harri Deutsch Verlag, Frankfurt, 2005).
29. G.W. Dunnington, Gauss, Titan of Science, (Mathematical Association of America, Washington DC, 2004).
30. J.A.C. Gallas, Lasers, stability, and numbers, Physica Scripta 94, 014003 (2019).
31. A. Endler and J.A.C. Gallas, Reductions and simplifications of orbital sums in a Hamiltonian repeller, Phys. Lett. A 352, 124-128 (2006).
32. A. Endler and J.A.C. Gallas, Conjugacy classes and chiral doublets in the Hénon Hamiltonian repeller, Phys. Lett. A 356, 1-7 (2006).
