CIRCULANTS (Extract)

Alun Wyn-jones

Last revised in December 2013.

Appendix A
Basic Cyclotomic Theory

This appendix assumes knowledge of basic field theory as in Birkoff and McLane's "Survey of Modern Algebra".

A.1 **Cyclotomic Extensions.** Cyclotomic theory studies integral domains which are extended by the addition of a root of unity. The archetypical example is the addition of an n^{th} root of unity to the rational integers.

To extend an integral domain R to include all n^{th} roots of unity is to construct another domain E which is to include R and in which $x^n - 1$ splits. That is, E is contructed so that $x^n - 1$ factorizes into a product of linear factors of the form $x - e$ with $e \in E$.

In this text, we always denote a primitive n^{th} root of unity with ζ_n or ζ if n is understood. A root of unity, ζ, is an n^{th} **primitive root** of unity if $\zeta^n = 1$ and $n > 0$ is least such. There are $\phi(n)$ primitive n^{th} roots of unity where ϕ is the Euler function. The set of all n^{th} roots of unity is a cyclic group under multiplication. Each primitive root is a generator of this group.

When R is extended to include ζ we write the extension as $R(\zeta)$ or R_ζ. R_ζ is called a **cyclotomic** extension of R. If R is a field, then so is R_ζ, and R_ζ is called a **cyclotomic field extension**. Please note that **the** n^{th} cyclotomic field means specifically $\mathbb{Q}(\zeta_n)$, and **the** n^{th} cyclotomic domain means specifically $\mathbb{Z}(\zeta_n)$.

The polynomial $x^n - 1$ always factorizes over any ring. For example,

$$x^{20} - 1 \;=\; (x-1)(x+1)(x^2+1)(x^4+x^3+x^2+x+1)(x^4-x^3+x^2-x+1)(x^8-x^6+x^4-x^2+1)$$

Over the integers, there is no further factorization possible: each of the given factors is irreducible over the rationals. Over other integral domains some, none, or all these factors might be reducible. For instance, when R is the Gaussian integers, $x^2 + 1$ will factorize, but no other.

A.2 **Cyclotomic Polynomials.** The factors appearing in the above reduction of $x^{20}-1$ are examples of **cyclotomic polynomials**. More generally, the n^{th} cyclotomic polynomial is defined to be that polynomial whose roots are exactly the primitive n^{th} roots of unity. In this text it is always denoted by the capital Greek letter phi:

$$\Phi_n(x) \;:=\; \prod\{x - \zeta \vdash \zeta^n = 1 \text{ and } \zeta^r \neq 1 \text{ for } r = 1, 2, \ldots, n-1\}$$

$\Phi_n(x)$ is irreducible over the rationals. Indeed, it is sometimes defined as the unique monic polynomial in $\mathbb{Z}[x]$ irreducible over the rationals which is zero at a complex primitive n^{th} root of unity, for instance at $\zeta_n = e^{2\pi\iota/n}$.

It can be shown that over $\mathbb{Q}$, $\Phi_n(x)$ is the highest degree irreducible monic polynomial dividing $x^n - 1$. In a fortuitous coincidence of notation, the degree of $\Phi_n(x)$ is $\phi(n) = |\mathbb{Z}_n^*|$.

A.3 **Other Examples of Cyclotomic Polynomials.** Let p and q be distinct primes.

(i) $\Phi_p(x) \;=\; x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1.$

(ii) Let $N = p^n$ with $n > 1$.

$$\Phi_N(x) \;=\; x^{N-N/p} \;+\; x^{N-2N/p} \;+\; \cdots \;+\; x^{2N/p} \;+\; x^{N/p} \;+\; 1 \;=\; \frac{x^N - 1}{x^{N/p} - 1}$$

(iii) $\Phi_{pq}(x) \;=\; \dfrac{x^{pq}-1}{(x^p-1)(x^q-1)}(x-1).$

(iv) (Palindromic) For all $n > 2$, $\quad \Phi_n(0) = 1,$ and $\; x^{\phi(n)}\, \Phi_n\left(x^{-1}\right) \;=\; \Phi_n(x).$

(v) $\Phi_{12}(x) = x^4 - x^2 + 1.$

(vi) $\Phi_{30}(x) = x^8 + x^7 - x^5 - x^4 - x^3 + x + 1.$

(vii) $\Phi_{75}(x) = x^{40} - x^{35} + x^{25} - x^{20} + x^{15} - x^5 + 1.$

(viii) $\Phi_{105}(x) = x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2x^{41} - x^{40} - x^{39}$
$+x^{36} + x^{35} + x^{34} + x^{33} + x^{32} + x^{31} - x^{28} - x^{26} - x^{24} - x^{22} - x^{20}$
$+x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} - x^9 - x^8 - 2x^7 - x^6 - x^5 + x^2 + x + 1.$

The last example shows that the non-zero coefficients of the cyclotomic polynomials are not necessarily ± 1. (The coefficients of x^{41} and x^7 in $\Phi_{105}(x)$ are both equal to -2.) Indeed, arbitrarily high coefficients are possible if N has enough prime factors.

A.4 **The Galois Group.** Let F be a field, and let $P(x)$ be an irreducible polynomial in $F[x]$ whose roots are primitive n^{th} roots of unity. Then $P \mid \Phi_n$. (If $F = \mathbb{Q}$, then $P = \Phi_n$.) Let ζ be one such root, $P(\zeta) = 0$. By definition, the Galois group of $F(\zeta)/F$, denoted by $\mathcal{G}\left(F(\zeta)/F\right)$, is that permutation group on the roots of P which can be extended to automorphisms of $F(\zeta)$.

The Galois groups of cyclotomic extensions are always abelian, and for the fields of interest here, namely, sub-domains of $\mathbb{C}$ and finite fields, they are always cyclic.

Let $G = \mathcal{G}\left(F(\zeta)/F\right)$, and let $\alpha \in G$. Then, $\alpha : \zeta \mapsto \zeta^j$ where ζ^j is another primitive n^{th} root of unity. But, ζ^j is a primitive n^{th} root of unity iff $j \in \mathbb{Z}_n^*$. Hence, $G \subset \{\zeta \mapsto \zeta^j \vdash j \in \mathbb{Z}_n^*\}$. In particular, $|G| \le \phi(n)$, and in fact, $|G| \,|\, \phi(n)$.

A.5 **Vector Space Basis.** Let F be a field which does not contain a primitive n^{th} root of unity. Then, F_ζ is an extension of dimension d where d is the degree of an irreducible polynomial dividing $\Phi_n(x)$. For the remainder of this section we shall suppose that $d = \phi(n)$, that is, we assume that $\Phi_n(x)$ is irreducible.

We can regard F_ζ as a vector space over F of dimension $f = \phi(n)$. For a basis, we can take the first f powers of ζ, $\mathcal{B} = \{1, \zeta, \zeta^2, \ldots, \zeta^{f-1}\}$. Let $\lambda_1(c) = \sum_i c_i \zeta^i$ be a linear combination of the n roots of unity. It is also a polynomial in ζ, and it can be reduced to a linear combination in $\mathcal{B}$ by reducing it as a polynomial modulo $\Phi_n(\zeta)$. This process in effect treats R_ζ as the quotient ring $R[x]/(\Phi_n(x))$.

In the special case of $F = \mathbb{Q}$, and $n = p$, prime, all but the highest power of ζ will be in the basis, and the formula for ζ^{p-1} is

$$\zeta^{p-1} = -1 - \zeta - \zeta^2 - \cdots - \zeta^{p-2}$$

A.6 **Cyclotomic Norm.**

The norm of an algebraic integer in an integral domain R plays a fundamental role in algebraic number theory in general and cyclotomic theory in particular. The norm of an algebraic integer z is the number of elements in the quotient ring $R/(z)$. Let Q be the field of quotients of R. It can be shown that the norm is always finite and is the least positive integer in the ideal generated by z, raised to the power of $\dim_Q Q(\zeta)$ divided by $\dim_Q Q(z)$. Arithmetically, this equals the product of z with all its algebraic conjugates all raised to a power $\dim_Q Q(\zeta)/\dim_Q Q(z)$. More simply, the norm is always given by

$$\mathcal{N}(z) = \prod_{\nu \in \mathcal{G}} \nu(z) \quad \text{where } \mathcal{G} \text{ is the Galois group of } Q(\zeta)/Q.$$

The function $\mathcal{N}$ is called the **cyclotomic norm**. The set $\nu(z)$ where $\nu \in \mathcal{G}$ are called the conjugates of z. Given an expression for z as polynomial in ζ, the conjugates can be obtained by substituting the various primitive roots of unity for ζ.

The norm is a multiplicative, non-zero function on R_ζ: $\mathcal{N}(z_1 z_2) = \mathcal{N}(z_1)\mathcal{N}(z_2)$ taking values in $\mathbb{N}$. It is invaluable for determining divisibility properties of cyclotomic integers.

The simplest example of a norm is the norm of an integer. Let $R = \mathbb{Z}(\zeta)$ where $\zeta = \zeta_{15}$, and let $n \in \mathbb{Z}$. We shall calculate $|R/(n)|$. As in §A.5 we take $\{1, \zeta, \zeta^2, \ldots, \zeta^7\}$ as a basis for $\mathbb{Q}(\zeta)$. Then, the

quotient ring $R/(n)$ is the set of all elements of the form $c_0 + c_1\zeta + c_2\zeta^2 + \cdots + c_7\zeta^7$ where each c_i is a residue modulo n. There are clearly n^8 such elements, so $\mathcal{N}(n) = n^8$. We get the same result using the product over the Galois group. There are $\phi(15)$ group elements, $\nu_h : \zeta \mapsto \zeta^h$ where $h \in \mathbb{Z}_{15}^*$. Therefore, $\mathcal{N}(n) = n\nu_2(n)\nu_4(n)\nu_7(n)\nu_8(n)\nu_{11}(n)\nu_{13}(n)\nu_{14}(n) = n^8$.

For a second example, let $\xi = 1+2\zeta^2 \in \mathbb{Z}(\zeta_{15})$. We substitute conjugates for ζ in ξ and multiply obtaining

$$\begin{aligned}
\mathcal{N}(\xi) &= (1+2\zeta^2)(1+2\zeta^4)(1+2\zeta^8)(1+2\zeta^{14})(1+2\zeta^{16})(1+2\zeta^{22})(1+2\zeta^{24})(1+2\zeta^{28}) \\
&= (1+2\zeta^2)(1+2\zeta^4)(1+2\zeta^{-7})(1+2\zeta^{-1})(1+2\zeta)(1+2\zeta^7)(1+2\zeta^{-6})(1+2\zeta^{-2}) \\
&= |1+2\zeta|^2 \cdot \left|1+2\zeta^2\right|^2 \cdot \left|1+2\zeta^4\right|^2 \cdot \left|1+2\zeta^7\right|^2 \\
&= 8.654181830\ldots \times 7.676522425\ldots \times 4.581886146\ldots \times 1.087409597\ldots \\
&= 331
\end{aligned}$$

We cheated at the end by using a computer to evaluate the absolute values. Our only excuse is that it would probably take another page of detailed calculations to derive the result in integer arithmetic.

As a final example, let $\xi = 1 + 2\zeta^5 \in \mathbb{Z}(\zeta_{15})$ then ξ is contained in the subdomain $\mathbb{Z}(\omega)$ where $\omega = \zeta^5 = \frac{1}{2}(-1+\sqrt{3}\iota)$. Hence, its norm can be calculated by taking a single product only and raising it to the power $\dim(\mathbb{Q}(\zeta)/\mathbb{Q}) \;/\; \dim(\mathbb{Q}(\omega)/\mathbb{Q}) = \phi(15)/\phi(3) = 4$.

$$\mathcal{N}(\xi) \;=\; (1+2\zeta^5)^4(1+2\zeta^{10})^4 \;=\; (1+2\omega)^4(1+2\omega^2)^4 \;=\; (5+2\omega+2\omega^2)^4 \;=\; 3^4$$

In general, the norm depends not only on the element but also on the domain and on the base ring. But, in here, the base ring is always the integers, and the domain is always cyclotomic, and so the norm depends only on the element and order of the cyclotomic domain. Hence, we can safely indicate which norm we mean by subscripting the norm symbol by the order of the cyclotomic domain. Thus, in the above example where $\xi = 1 + 2\zeta^5$, $\mathcal{N}_{15}(\xi) = 3^4$ as was shown, whereas $\mathcal{N}_3(\xi) = 3$.

A.7 **Integral Elements** The **integral elements** of a field over the rationals is the set of elements which are roots of a monic polynomial with integer coefficients. We have the following proposition for cyclotomic domains.

A.7.1 **Proposition**

(i) The set of integral elements of $\mathbb{Q}(\zeta_N)$ is $\mathbb{Z}(\zeta_N)$.

(ii) $\mathbb{Z}(\zeta_N) \cap \mathbb{Q} \;=\; \mathbb{Z}$. □ ([Lang1])

An integral domain, R, is said to be **integrally closed** if all its integral elements which are in its ring of quotients are actually in R.

It is known that all principal ideal domains are integrally closed.