Cyclotomic Polynomials and Division Rings

By

Kenneth Rogers*, Los Angeles

(Received August 18, 1964)

1. In [2] Witt gave a very short proof of *Wedderburn*'s Theorem that every finite division-ring is a field. The only "non-elementary" step was his proof that, for integers $q > 1$ and $n > 1$, the set of integers $\{(q^n - 1)/(q^d - 1) \mid d|n, d < n\}$ has a common divisor greater than $q - 1$. This was done by proving

$$\varphi_n(q) > q - 1 \tag{1}$$

for the same q and n as above, where $\varphi_n(x)$ denotes the n'th cyclotomic polynomial over the rationals. We propose to prove (1) without using the complex plane or the extension of ordinary absolute value up to the field of n'th roots of unity. By deriving the cyclotomic polynomials purely within the unique factorisation domain $Z[x]$, and by proving (1) by elementary number-theory, we make *Witt*'s proof more elementary. The method of treating $\varphi_n(x)$ may also have independent interest, especially as it avoids using Möbius' inversion formula or induction.

2. LEMMA 1. *In any unique factorisation domain,*

$$[a_1, a_2, \ldots, a_n] = \prod_{1 \leq i_1 < \ldots < i_k \leq n} (a_{i_1}, \ldots, a_{i_k})^{(-1)^{k+1}}$$

where $[a, b]$ *and* (a, b) *denote respectively the least common multiple and greatest common divisor of* a *and* b.

Proof. By the factorisation formulae for (a, b) and $[a, b]$, the Lemma asserts only that

$$c_1 \vee c_2 \vee \ldots \vee c_n = \sum_{1 \leq i_1 < \ldots < i_k \leq n} (-1)^{k+1} (c_{i_1} \wedge c_{i_2} \wedge \ldots c_{i_k}), \tag{2}$$

for all non-negative integers c_i, where $\vee$ and $\wedge$ denote respectively 'max' and 'min'. Since both sides of (2) are not changed in value by

* This research was supported by Contract NSF GP — 1925.

permutation of the c, we may assume that $c_1 \geq c_2 \geq \ldots \geq c_n$, and so the left side of (2) is c_1. Since c_1 occurs with the same coefficient on the right, it remains only to show that all other terms go out after using $c_{i_1} \wedge \ldots \wedge c_{i_k} = c_{i_k}$. The coefficient of c_{j+1} is then equal to n_j, the number of subsets of $\{1, 2, \ldots, j\}$ of even cardinal minus the number of odd cardinal. The contribution of those containing j is $-n_{j-1}$, while those not containing j contribute n_{j-1}. Hence $n_j = 0$ for $j \geq 1$.

LEMMA 2. $(x^a - 1, x^b - 1) = x^{(a,b)} - 1$.

Proof.
$$(x^a - 1, x^b - 1) = (x^a - 1, x^b - 1 - x^{b-a}(x^a - 1)) = (x^a - 1, x^{b-a} - 1),$$

where we assumed that $a \leq b$. Since this parallels the division process on the exponents, we terminate with $x^{(a,b)} - 1$. The proof can obviously be done by induction also.

The first Lemma is new to me, but it must be a known result in lattice theory. Lemma 2 is "well known". We shall use these to obtain the usual formulae relating $x^n - 1$ to the cyclotomic polynomials.

In the unique factorisation domain $Z[x]$, the polynomial $x^n - 1$ is squarefree, because it has no common factor with nx^{n-1}, its "derivative". We now show that $x^n - 1$ has a factor which does not divide $x^d - 1$ for any proper divisor d of n.

THEOREM. *The least common multiple of the set of all $x^d - 1$, where d goes over the proper divisors of n, is*

$$f_n(x) = \prod_{\substack{d/n \\ d \neq 1}} (x^{n/d} - 1)^{-\mu(d)}.$$

Since all the $x^d - 1$ divide $x^n - 1$, so does $f_n(x)$, and if we write

$$x^n - 1 = f_n(x) \cdot \varphi_n(x),$$

then $\varphi_n(x)$ is of degree $\varphi(n)$,

$$\varphi_n(x) = \prod_{d/n} (x^{n/d} - 1)^{\mu(d)}, \tag{3}$$

and

$$\varphi_n(x) \mid x^m - 1 \Longleftrightarrow n \mid m.$$

Proof. If $p_1, \ldots, p_s$ are the distinct primes dividing n, each of the $x^d - 1$ divides some of

$$x^{n/p_1} - 1, \ldots, x^{n/p_s} - 1,$$

and so the least common multiple of $\{x^d - 1 \mid d \mid n, d < n\}$ is just

$$f_n(x) = [x^{n/p_1} - 1, \ldots, x^{n/p_s} - 1].$$

Now apply Lemmas 1 and 2, noting that the empty set contributes a unit to the product and using the fact that $(n/p_{i_1}, \ldots, n/p_{i_k}) = n/p_{i_1} \ldots p_{i_k}$:

$$\begin{aligned} f_n(x) &= \prod_{1 \leq i_1 < \ldots < i_k \leq s} (x^{n/p_{i_1} \cdots p_{i_k}} - 1)^{(-1)^{k+1}} \\ &= \prod_{\substack{d \mid n \\ d \neq 1}} (x^{n/d} - 1)^{-\mu(d)}. \end{aligned}$$

Formula (3) for $(x^n - 1)/f_n(x)$ now follows. Lastly, since $f_n(x)$ is the least common multiple of the $x^d - 1$ for $d \mid n$, $d < n$, and since $x^n - 1$ is squarefree, we know that $\varphi_n(x) \nmid x^d - 1$ for these d. Hence

$$\begin{aligned} \varphi_n(x) \mid x^m - 1 &\Longrightarrow \varphi_n(x) \mid x^{(m,n)} - 1 \\ &\Longrightarrow (m, n) = n \\ &\Longrightarrow n \mid m. \end{aligned}$$

From (3), the degree of $\varphi_n(x)$ is

$$\begin{aligned} \sum_{d \mid n} n\, \mu(d)/d &= n \,.\, \varphi(n)/n \\ &= \varphi(n). \end{aligned}$$

3. We shall now prove (1) in the stronger form:

$$n > 1,\ q > 1 \Longrightarrow \varphi_n(q) \geq q + 1. \tag{4}$$

The general case is reduced to that where n is squarefree by the familiar rule:

$$\begin{aligned} p \mid n,\ p \text{ prime} \Longrightarrow \varphi_{np}(x) &= \prod_{d \mid n} (x^{np/d} - 1)^{\mu(d)} \\ &= \varphi_n(x^p). \end{aligned}$$

Repeated use of this shows that $\varphi_{p_1^{\nu_1} \ldots p_s^{\nu_s}}(x) = \varphi_{p_1 \ldots p_s}(x^{p_1^{\nu_1 - 1} \cdots p_s^{\nu_s - 1}})$, and hence when (4) is established for squarefree n, an even stronger result holds for general n. Now use (3) with $x = q$ and read modulo q^2:

$$\begin{aligned} \varphi_n(q) &\equiv (q - 1)^{\mu(n)} \,.\, \prod_{\substack{d \mid n \\ d < n}} (-1)^{\mu(d)} \bmod q^2 \\ &\equiv (1 - q)^{\mu(n)} \,.\, (-1)^{\sum_{d \mid n} \mu(d)} \bmod q^2 \\ &\equiv (1 - q)^{\mu(n)} \bmod q^2. \end{aligned}$$

Thus,

$$\varphi_n(q) \equiv \begin{cases} q^2 - q + 1 \bmod q^2 \text{ if } \mu(n) = 1, \\ \qquad q + 1 \bmod q^2 \text{ if } \mu(n) = -1. \end{cases}$$

Since $\varphi_n(x) \in Z[x]$, $\varphi_n(q)$ is an integer which by (3) is positive for $q > 1$. Inequality (4) now follows from the above remainders mod q^2.

4. Since one purpose of this work was to free *Witt*'s proof of its implied dependence on valuation theory, we ought to note that more group-theoretic proofs of *Wedderburn*'s Theorem have appeared recently, such as [1].

Although the development of $\varphi_n(x)$ given here is in some ways easier than the traditional one, the same cannot be said if one tries to prove that $\varphi_n(x)$ is irreducible in $Z[x]$. One works modulo an irreducible factor of $\varphi_n(x)$, which is the same as going to a field of roots of unity. At this point, staying in $Z[x]$ is unnatural.

References

1. *T. J. Kaczynski*, Another proof of Wedderburn's Theorem, American Mathematical Monthly, vol. **71**, No. 6 (1964), 652–653.

2. *E. Witt*, Über die Kommutativität endlicher Schiefkörper, Abh. Math. Sem. Hamburg, Bd. **8** (1931), 413.