SEVERAL PROOFS OF THE IRREDUCIBILITY OF THE CYCLOTOMIC POLYNOMIALS

STEVEN H. WEINTRAUB

ABSTRACT. We present a number of classical proofs of the irreducibility of the n-th cyclotomic polynomial $\Phi_n(x)$. For n prime we present proofs due to Gauss (1801), in both the original and a simplified form, Kronecker (1845), and Schönemann/Eisenstein (1846/1850), and for general n proofs due to Dedekind (1857), Landau (1929), and Schur (1929).

Let $\Phi_n(x)$ denote the n-th cyclotomic polynomial, defined by

$$\Phi_n(x) = \prod (x - \zeta)$$

where ζ ranges over the primitive n-th roots of unity. $\Phi_n(x)$ is also given inductively by

$$\Phi_n(x) = \frac{x^n - 1}{\prod \Phi_d(x)}$$

where d ranges over the proper divisors of n. In case $n = p$ is prime, $\Phi_p(x) = (x^p - 1)/(x - 1) = x^{p-1} + x^{p-2} + \cdots + x + 1$.

It is a basic result in number theory that $\Phi_n(x)$ is irreducible for every positive integer n. It is our objective here to present a number of classical proofs of this theorem (certainly not all of them).

The irreducibility of $\Phi_p(x)$ for p prime was first proved by Gauss [4, article 341], with a simpler proof being given by Kronecker [5] and even simpler and more general proofs being given by Schönemann [8] and Eisenstein [3]. We give these proofs here. (The last of these has become the standard proof.) Gauss's proof is rather complicated, so we also give a simpler proof along the same lines. The irreducibility of $\Phi_n(x)$ in general was first proved by Kronecker [6], with simpler proofs being given by Dedekind [2], Landau [7], and Schur [9]. We give the last three of these proofs here. (A variant of Dedekind's proof has become the standard proof.)

With the exception of Schur's proof, which uses some results about algebraic integers, these proofs all just use basic results about polynomials. We have organized this paper to collect background material about polynomials in a preliminary section, to have it available when we present the main results.

BACKGROUND MATERIAL

The first result we need about polynomials is Gauss's Lemma [4, article 42], which we state in the form in which we will use it.

Lemma. *Let $f(x)$ be a monic polynomial with integer coefficients, and suppose that $f(x) = g(x)h(x)$ where $g(x)$ and $h(x)$ are monic polynomials with rational coefficients. Then $g(x)$ and $h(x)$ have integer coefficients.*

2000 *Mathematics Subject Classification.* 12-03, Secondary 12E05, 01A55.
Key words and phrases. cyclotomic polynomial, irreducibility.

Proof. See [11, Corollary 4.1.6].

Now let $f(x)$ be an arbitrary monic polynomial, $f(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_0$. Let $f(x)$ have roots $r_1, \ldots, r_m$, so that $f(x) = (x-r_1)\cdots(x-r_m)$. Expanding this last expression we see that $f(x) = x^m + \sum_{i=1}^{m}(-1)^i s_i(r_1, \ldots, r_m)x^{m-i}$ where $s_i(r_1, \ldots, r_m)$ is the i-th *elementary symmetric polynomial* in the roots $r_1, \ldots, r_m$, i.e., the sum of product of these roots taken i at a time. Thus

$$\begin{aligned} s_1(r_1, \ldots, r_m) &= r_1 + \ldots + r_m, \\ s_2(r_1, \ldots, r_m) &= r_1 r_2 + \ldots + r_{m-1} r_m, \\ &\ldots \\ s_m(r_1, \ldots, r_m) &= r_1 \cdots r_m. \end{aligned}$$

Comparing these two expressions we see that, up to sign, the coefficients of $f(x)$ are the values of these polynomials; more precisely $a_{m-i} = (-1)^i s_i(r_1, \ldots, r_m)$.

In general a polynomial in m variables is *symmetric* if it is invariant under any permutation of the variables. The second result we need is the fundamental theorem on symmetric polynomials, which was already well-known in the eighteenth century and perhaps earlier.

Theorem. *Let $f(x)$ be a monic polynomial with integer (respectively, rational) coefficients. Let $g(x)$ be any symmetric polynomial in the roots of $f(x)$ with integer (respectively, rational) coefficients. Then $g(x)$ can be written as a polynomial in the elementary symmetric polynomials of the roots of $f(x)$, and hence as a polynomial in the coefficients of $f(x)$, with integer (respectively, rational) coefficients.*

Proof. See [11, Lemma 3.1.14 and Lemma 3.1.15].

THE RESULTS THEMSELVES

Theorem 1. *Let p be a prime. Then the cyclotomic polynomial $\Phi_p(x)$ is irreducible.*

Proof (Gauss). This is trivial for $p = 2$ so we suppose p is odd. We begin with some general considerations.

First, let $f(x)$ be an arbitrary monic polynomial with rational coefficients, with roots $r_1, \ldots, r_m$, so that $f(x) = (x-r_1)\cdots(x-r_m)$, and let $g(x)$ be the monic polynomial whose roots are the k-th powers of the roots of $f(x)$, for some positive integer k, so that $g(x) = (x - r_1^k)\cdots(x - r_m^k)$. Then the coefficients of $g(x)$ are symmetric polynomials in $\{r_1^k, \ldots, r_m^k\}$, and hence are symmetric polynomials in $\{r_1, \ldots, r_m\}$. Then by the fundamental theorem on symmetric polynomials they can be expressed as polynomials with rational coefficients in the coefficients of $f(x)$. Hence $g(x)$ has rational coefficients as well.

Second, let $\varphi(x_1, x_2, \ldots)$ be any polynomial with integer coefficients and let ζ be any primitive p-th root of unity. Substituting $x_i = \zeta^{k_i}$ for each i, we obtain a value for this polynomial that we may write as

$$\varphi(\zeta^{k_1}, \zeta^{k_2}, \ldots) = A_0 + A_1\zeta + \ldots + A_{p-1}\zeta^{p-1}$$

for some integers $A_0, \ldots, A_{p-1}$, and then for any t

$$\varphi(\zeta^{tk_1}, \zeta^{tk_2}, \ldots) = A_0 + A_1\zeta^t + \ldots + A_{p-1}\zeta^{(p-1)t}.$$

Then

$$\varphi(1, 1, \ldots) = \varphi(\zeta^{pk_1}, \zeta^{pk_2}, \ldots) = A_0 + A_1 + \ldots + A_{p-1}$$

and

$$\varphi(\zeta^{k_1},\zeta^{k_2},\ldots)+\varphi(\zeta^{2k_1},\zeta^{2k_2},\ldots)+\ldots+\varphi(\zeta^{pk_1},\zeta^{pk_2},\ldots)=pA_0,$$

and in particular this sum is divisible by p.

Now suppose that $\Phi_p(x)=f(x)g(x)$ for nonconstant monic polynomials $f(x)$ and $g(x)$, with $f(x)$ a polynomial of degree d. Then $f(x)$ and $g(x)$ each have integer coefficients. (This is Gauss's Lemma. Note that $\Phi_p(x)$ itself has integer coefficients.) Write $f(x)=x^d+a_{d-1}x^{d-1}+\ldots+a_1x+a_0$. Let Ω be the set of primitive p-th roots of unity. Let F be the set of roots of $f(x)$ and let G be the set of roots of $g(x)$. Then $F\cup G=\Omega$ and $F\cap G=\{\}$. Let F' be the set of reciprocals of the elements of F and let G' be the set of reciprocals of the elements of G. Then similarly $F'\cup G'=\Omega$ and $F'\cap G'=\{\}$. Let $f'(x)$ be the monic polynomial who roots are the elements of F'. Observe that $f'(x)=x^d+(a_1/a_0)x^{d-1}+\ldots+(a_{d-1}/a_0)x+(1/a_0)$. We have four cases:

Case 1: $F'=F$. Then $f'(x)=f(x)$. In this case the roots of $f(x)$ occur in conjugate pairs, so $f(x)$ is a product of $d/2$ factors each of the form $(x-\zeta)(x-\zeta^{-1})=x^2-(\zeta+\zeta^{-1})x+1$, and each of these factors is positive for every real number x. Let F_k be the set of k-th powers of the elements of F, and $f_k(x)$ the monic polynomial whose roots are the elements of F_k, for each $k=1,\ldots,p-1$. Then the same property holds for each $f_k(x)$. Let $q_k=f_k(1)$ for $k=1,\ldots,p-1$. Thus $q_1,\ldots,q_{p-1}$ are all positive rational numbers. But in fact each polynomial $f_k(x)$ has rational coefficients, by the first observation above, and hence integer coefficients (by Gauss's Lemma), so $q_1,\ldots,q_{p-1}$ are all positive integers.

If $\varphi(x_1,\ldots,x_d)=(1-x_1)\cdots(1-x_d)$, then $q_k=\varphi(\zeta_1^k,\ldots,\zeta_d^k)$, for $k=1,\ldots,p-1$, where $F=\{\zeta_1,\ldots,\zeta_d\}$, and $\varphi(\zeta_1^p,\ldots,\zeta_d^p)=\varphi(1,\ldots,1)=0$, so from the second observation above we see that $q_1+\ldots+q_{p-1}$ is divisible by p. But also $f_1(x)\cdots f_{p-1}(x)=\Phi_p(x)^d$, as every primitive p-th root of unity is a root of the left-hand side of multiplicity d. Hence, letting $x=1$, we obtain $q_1\cdots q_{p-1}=p^d$.

Since p is a prime and $d<p-1$, we must have g of the integers $q_1,\ldots,q_{p-1}$ equal to 1 for some $g>0$, and then the rest of them are powers of p. But then $q_1+\ldots+q_{p-1}\equiv g \pmod p$, and so this sum is certainly not divisible by p, a contradiction.

Case II: $F\neq F'$ but $T=F\cap F'\neq\{\}$. Let $t(x)$ be the monic polynomial whose roots are the elements of T. Then $t(x)$ is the greatest common divisor (gcd) of $f(x)$ and $f'(x)$. Then by the argument of Case I $t(x)$ cannot have all of its coefficients rational. But $f(x)$ and $f'(x)$ are polynomials with rational coefficients, and hence their gcd is a polynomial with rational coefficients, a contradiction.

Case III: $G\cap G'\neq\{\}$. Applying the arguments of cases I or II to $g(x)$ yields the same contradiction.

Case IV: $G=F'$ and $F=G'$. Then

$$\begin{aligned}\Phi_p(x)&=f(x)f'(x)\\&=(x^d+a_{d-1}x^{d-1}+\ldots+a_1x+a_0)(x^d+(a_1/a_0)x^{d-1}+\ldots+(a_{d-1}/a_0)x+(1/a_0)),\end{aligned}$$

and setting $x=1$ we obtain

$$a_0p=(1+a_{d-1}+\ldots+a_0)^2.$$

But (by Gauss's Lemma) $f'(x)$ has integer coefficients, so $a_0=\pm1$ and we obtain that $\pm p$ is a perfect square, a contradiction.

Proof (in the spirit of Gauss). We have the identity

$$\prod_{i=1}^{d}(x-r_i)=\sum_{i=0}^{d}(-1)^i s_i(r_1,\ldots,r_d)x^{d-i},$$

where the s_i are the elementary symmetric functions.

Let $\varphi(r_1,\dots,r_d) = \prod_{i=1}^{d}(1-r_i)$. Then we see that

$$\varphi(r_1,\dots,r_d) = \sum_{i=0}^{d}(-1)^i s_i(r_1,\dots,r_d).$$

The theorem is trivial for $p=2$ so we may suppose p is an odd prime.

Suppose that $\Phi_p(x)$ is not irreducible and let $f_1(x)$ be an irreducible factor of $\Phi_p(x)$ of degree d. Then $f_1(x) = (x-\zeta_1)\cdots(x-\zeta_d)$ for some set of primitive p-th roots of unity $\{\zeta_1,\dots,\zeta_d\}$. For $k=1,\dots,p-1$, let $f_k(x) = (x-\zeta_1^k)\cdots(x-\zeta_d^k)$. The coefficients of $f_k(x)$ are symmetric polynomials in $\{\zeta_1^k,\dots,\zeta_d^k\}$, hence symmetric polynomials in $\{\zeta_1,\dots,\zeta_d\}$, hence polynomials in the coefficients of $f_1(x)$, and so $f_k(x)$ has rational coefficients. Since each $f_k(x)$ divides $\Phi_p(x)$, by Gauss's Lemma in fact each $f_k(x)$ is a polynomial with integer coefficients.

(It is easy to see that each $f_k(x)$ is irreducible, that d must divide $p-1$, and that there are exactly $(p-1)/d$ distinct polynomials $f_k(x)$, but we do not need these facts.)

Since $f_k(x)$ has leading coefficient 1 and no real roots, $f_k(x) > 0$ for all real x. Also,

$$\Phi_p(x)^d = \prod_{k=1}^{p-1} f_k(x)$$

since every primitive p-th root of 1 is a root of the right-hand side of multiplicity d. Then

$$p^d = \Phi_p(1)^d = \prod_{k=1}^{p-1} f_k(1)$$

and $d < p-1$, so we must have $f_k(1) = 1$ for some $g > 0$ values of k, and $f_k(1)$ a power of p for the remaining values of k, and hence

$$\sum_{k=1}^{p-1} f_k(1) \equiv g \not\equiv 0 \pmod{p}.$$

But

$$\varphi(\zeta_1^k,\dots,\zeta_d^k) = f_k(1) \text{ for } k=1,\dots,p-1, \text{ and } \varphi(\zeta_1^p,\dots,\zeta_d^p) = \varphi(1,\dots,1) = 0.$$

Thus

$$\begin{aligned}\sum_{k=1}^{p-1} f_k(1) &= \sum_{k=1}^{p-1}\varphi(\zeta_1^k,\dots,\zeta_d^k)\\ &= \sum_{k=1}^{p}\varphi(\zeta_1^k,\dots,\zeta_d^k)\\ &= \sum_{k=1}^{p}\sum_{i=0}^{d}(-1)^i s_i(\zeta_1^k,\dots,\zeta_d^k)\\ &= \sum_{i=0}^{d}(-1)^i\sum_{k=1}^{p} s_i(\zeta_1^k,\dots,\zeta_d^k).\end{aligned}$$

But $s_i(r_1,\dots,r_d)$ is a sum of terms of the form $r_{j_1}\cdots r_{j_i}$, so each term in the inner sum above is a sum of terms

$$\sum_{k=1}^{p}\zeta_{j_1}^k\cdots\zeta_{j_i}^k = \sum_{k=1}^{p}(\zeta_{j_1}\cdots\zeta_{j_i})^k = 0 \text{ or } p$$

according as $\zeta_{j_1}\cdots\zeta_{j_i}$ is a primitive p-th root of unity or is equal to 1. Thus

$$\sum_{k=1}^{p-1} f_k(1) \equiv 0 \pmod{p},$$

a contradiction.

Proof (Kronecker). We first prove the following lemma: Let $f(x)$ be an arbitrary polynomial with integer coefficients. Let ζ be a primitive p-th root of 1. Then $f(\zeta)\cdots f(\zeta^{p-1})$ and $f(1)$ are both integers and

$$f(\zeta)\cdots f(\zeta^{p-1}) \equiv f(1)^{p-1} \pmod{p}.$$

To prove that the product $f(\zeta)\cdots f(\zeta^{p-1})$ is an integer, observe that it is a symmetric polynomial in $\{\zeta,\ldots,\zeta^{p-1}\}$ so, by the fundamental theorem of symmetric functions, is an integer polynomial in the coefficients of the polynomial having $\{\zeta,\ldots,\zeta^{p-1}\}$ as roots. But this polynomial is simply $\Phi_p(x) = x^{p-1}+\ldots+1$. To prove that the congruence holds, let $g(x) = f(x)\cdots f(x^{p-1}) = \sum_n A_n x^n$ and consider $\sum_{i=0}^{p-1} g(\zeta^i)$. The first expression for $g(x)$ gives the value $f(1)^{p-1}+(p-1)f(\zeta)\cdots f(\zeta^{p-1})$ for this sum while the second expression for $g(x)$ gives the value $\sum_n$ a multiple of ${}_pA_n p$. Thus $f(1)^{p-1}+(p-1)f(\zeta)\cdots f(\zeta^{p-1}) \equiv 0 \pmod{p}$ and the lemma immediately follows.

Now suppose $\Phi_p(x)$ is not irreducible and write $\Phi_p(x) = f(x)g(x)$, a product of non-constant polynomials. By Gauss's lemma, $f(x)$ and $g(x)$ both have integer coefficients. Then $p = \Phi_p(1) = f(1)g(1)$. One of these factors must be ±1, so suppose $f(1) = \pm1$. On the one hand, $f(\zeta^k) = 0$ for some k that is nonzero $\pmod{p}$ (as these are the roots of $\Phi_p(x)$), so $f(\zeta)\cdots f(\zeta^{p-1}) = 0$, but on the other hand $f(1)^{p-1} \equiv 1 \pmod{p}$, contradicting the above congruence.

Proof (Schönemann). We have the following irreducibility criterion: Let $f(x)$ be a polynomial of degree k with integer coefficients. Suppose that, for some prime p, and some integer a, $f(x) = (x-a)^k + pg(x)$ for some polynomial $g(x)$ with integer coefficients with $g(a)$ not divisible by p. (As we might phrase this nowadays, suppose that $f(x) \equiv (x-a)^k \pmod{p}$ and $f(a)$ is not divisible by p^2.) Then $f(x)$ is irreducible. Now, by the binomial theorem, $x^p - 1 \equiv (x-1)^p \pmod{p}$, so $\Phi_p(x) = \frac{x^p-1}{x-1} \equiv (x-1)^{p-1} \pmod{p}$, and also $\Phi_p(x) = x^{p-1}+\cdots+1$ so $\Phi_p(1) = p$, and hence $\Phi_p(x)$ satisfies the hypotheses of this criterion.

Proof (Eisenstein). We have the following irreducibility criterion: Let $f(x) = c_k x^k + \cdots + c_0$ be a polynomial with integer coefficients. Suppose that, for some prime p, c_k is not divisible by p, $c_{k-1},\ldots,c_0$ are divisible by p, and c_0 is not divisible by p^2. Then $f(x)$ is irreducible. Now $\Phi_p(x)$ is irreducible if and only if $\Phi_p(x+1)$ is irreducible. But, by the binomial theorem, $\Phi_p(x+1) = \frac{(x+1)^p-1}{x} = x^{p-1} + a_{p-2}x^{p-2} + \cdots + a_1 x + p$, with $a_{p-2},\ldots,a_1$ all divisible by p, which satisfies the hypotheses of this criterion.

Remark. Schönemann's irreducibility criterion and his proof of the irreducibility of $\Phi_p(x)$ are little remembered now, with Eisenstein's irreducibility criterion and his proof of the irreducibility of $\Phi_p(x)$ being very well known. But in fact these two are equivalent. A beautiful discussion of this point (both the mathematics and the history) has been given by Cox [1].

Theorem 2. *Let n be an arbitrary positive integer. Then the cyclotomic polynomial $\Phi_n(x)$ is irreducible.*

Proof (Dedekind). Let $f(x)$ be an irreducible factor of $\Phi_n(x)$. Since $f(x)$ divides the polynomial x^n-1, it follows from Gauss's Lemma that $f(x)$ has integral coefficients. Let ζ be an n-th root of 1 with $f(\zeta)=0$. It suffices to prove that if p is any prime not dividing n, then $f(\zeta^p)=0$ (as by repeated applications of this result, we obtain that $f(\zeta^j)=0$ for any j relatively prime to n).

Suppose this is not the case. Let $f(x)$ have roots $\zeta_1=\zeta,\ldots,\zeta_k$, so that $f(x)=(x-\zeta_1)\cdots(x-\zeta_k)=x^k-c_{k-1}x^{k-1}+\ldots\pm c_0$. Let $g(x)=(x-\zeta_1^p)\cdots(x-\zeta_k^p)=x^k-d_{k-1}x^{k-1}+\ldots\pm d_0$. Then $c_i=s_i(\zeta_1,\ldots,\zeta_k)$ and $d_i=s_i(\zeta_1^p,\ldots,\zeta_k^p)$ for each i, where s_i is the i-th elementary symmetric function. By the multinomial theorem, we have the polynomial identity $s_i(x_1^p,\ldots,x_k^p)\equiv s_i(x_1,\ldots,x_k)^p \pmod p$, i.e., $s_i(x_1^p,\ldots,x_k^p)-s_i(x_1,\ldots,x_k)^p=pt_i(x_1,\ldots,x_k)$ for some polynomial $t_i(x_1,\ldots,x_k)$ with integral coefficients. Thus, for each i, $d_i-c_i^p=s_i(\zeta_1^p,\ldots,\zeta_k^p)-s_i(\zeta_1,\ldots,\zeta_k)^p=pt_i(\zeta_1,\ldots,\zeta_k)$. But $t_i(x_1,\ldots,x_k)$ is a symmetric polynomial, so by the fundamental theorem on symmetric polynomials $t_i(\zeta_1,\ldots,\zeta_k)$ is a polynomial in $\{s_j(\zeta_1,\ldots,\zeta_k)=c_j\}$ with integer coefficients. Hence $d_i\equiv c_i^p\equiv c_i \pmod p$ for each i, where the last congruence is Fermat's Little Theorem, and so $g(x)$ is also a polynomial with integer coefficients and furthermore $g(x)\equiv f(x) \pmod p$.

The polynomial $g(x)$ is also irreducible (a fact which follows from the observation that $\zeta=(\zeta^p)^q$ where q is an integer with $pq\equiv 1 \pmod n$), and $g(x)\neq f(x)$. Hence $f(x)g(x)$ divides $m(x)=x^n-1$. Let $\overline{e}(x)$ denote the $(\mathrm{mod}\, p)$ reduction of the polynomial $e(x)$. Then $\overline{f}(x)\overline{g}(x)=\overline{f}(x)^2$ divides $\overline{m}(x)$, which is impossible as $\overline{m}(x)$ and its formal derivative $\overline{m}(x)'=nx^{n-1}$ are relatively prime.

Remark. This proof can be simplified to remove the argument about symmetric functions. It follows immediately from the multinomial theorem and Fermat's Little Theorem that for any polynomial $k(x)$ with integer coefficients, $k(x)^p\equiv k(x^p) \pmod p$ for any prime p. Let $f(x)$ be as above and let $g(x)$ be an irreducible polynomial having $g(\zeta^p)=0$. Clearly ζ is a root of the polynomial $g(x^p)$, so $f(x)$ divides $g(x^p)$. Reducing $(\mathrm{mod}\, p)$, $\overline{f}(x)$ divides $\overline{g}(x^p)=\overline{g}(x)^p$, so $\overline{f}(x)$ and $\overline{g}(x)$ have a common irreducible factor $\overline{h}(x)$. But then $\overline{h}(x)^2$ divides $\overline{m}(x)$, which is impossible as above. This simplification is already to be found in van der Waerden [10, article 53].

Proof (Landau). Let $f(x)$ be an irreducible polynomial with integer coefficients of degree d with $f(\zeta)=0$ for some n-th root of unity ζ. By the division algorithm, for any j there are unique polynomials $q_j(x)$ and $r_j(x)$ with $f(x^j)=f(x)q_j(x)+r_j(x)$ and $r_j(x)$ of degree less than d (perhaps $r_j(x)=0$). Since the value of $f(\zeta^j)$ only depends on $j \pmod n$, we have a finite set $\{r_0(x),\ldots,r_{n-1}(x)\}$ of polynomials such that, for any integer j, $f(\zeta^j)=r(\zeta)$ for $r(x)$ some polynomial in this set. Furthermore, if $s(x)$ is any polynomial of degree less than d with $f(\zeta^j)=s(\zeta)$, then we must have $s(x)=r(x)$ (as otherwise ζ would be a root of the nonzero polynomial $s(x)-r(x)$ of degree less than d, which is impossible).

In particular, for any prime p, $f(\zeta^p)=f(\zeta^p)-f(\zeta)^p=r(\zeta)$ for some such polynomial $r(x)$. But $f(x^p)\equiv f(x)^p \pmod p$, so $f(x^p)-f(x)^p=pg(x)$ for some polynomial $g(x)$. But, again by the division algorithm, there is a unique polynomial $h(x)$ of degree less than d with $h(\zeta)=g(\zeta)$. Thus $r(\zeta)=ph(\zeta)$ with $r(x)$ and $ph(x)$ both of degree less than d, so $r(x)=ph(x)$. In particular, all the coefficients of $r(x)$ are divisible by p. Now if A is the largest absolute value of the coefficients of all of the polynomials $\{r_j(x)\}$, we must have $f(\zeta^p)=r(\zeta)=0$ for $p>A$, and so $f(\zeta^m)=0$ for any integer m not divisible by any prime $p\leq A$.

Now let k be any integer relatively prime to n, and consider $m=k+n\prod q$, where q runs over all the primes $\leq A$ that do not divide k. Let p be any prime $\leq A$. If p divides k, then,

since k and n are relatively prime, p does not divide $n\prod q$ and hence does not divide m. If p does not divide k, then p divides $n\prod q$ and hence does not divide m. Thus we see that m is such an integer, and $m \equiv k \pmod{n}$, so $f(\zeta^k) = f(\zeta^m) = 0$. Thus $\Phi_n(x)$ has ζ^k as a root for every k relatively prime to n, and so $\Phi_n(x)$ is irreducible.

Remark. This proof, written in Landau's usual telegraphic style, takes 8 lines in the original.

Proof (Schur). Let $g(x) = x^n - 1$, and let Δ be the discriminant of $g(x)$, i.e., the product of the squares of the differences of the distinct roots. Then $\Delta = \pm n^n$, as we see from the following computation:

$$\begin{aligned}
\Delta &= \prod_{i<j} (\zeta^i - \zeta^j)^2 \\
&= \pm \prod_{i \neq j} (\zeta^i - \zeta^j) \\
&= \pm \prod_{i \neq j} \zeta^i (1 - \zeta^{j-i}) \\
&= \pm \prod_i \zeta^i \Big(\prod_{k \neq 0} (1 - \zeta^k) \Big) \\
&= \pm \prod_i \zeta^i (n) = \pm n^n.
\end{aligned}$$

In this computation, the equality $\prod_{k\neq 0}(1-\zeta^k) = n$ comes from the fact that the left-hand side is the value $h(1)$ for $h(x)$ the polynomial $h(x) = \prod_{k\neq 0}(x-\zeta^k) = (x^n-1)/(x-1) = x^{n-1} + \ldots + 1$.

Now suppose that $f(x)$ is a factor of $x^n - 1$. Let ζ be a root of $f(x)$ and let p be any prime not dividing n. We claim that ζ^p is also a root of $f(x)$. Suppose not. Then $f(x) = (x-\zeta_1)\cdots(x-\zeta_k)$ for some n-th roots of unity $\zeta_1 = \zeta, \zeta_2, \ldots, \zeta_k$, not including ζ^p. Thus $0 \neq f(\zeta^p)$ is a product of differences of n-th roots of unity, so is an algebraic integer dividing n^n. But $f(x^p) \equiv f(x)^p \pmod{p}$, so $f(\zeta^p) \equiv f(\zeta) = 0 \pmod{p}$, i.e., p divides $f(\zeta^p)$. But that implies p divides n^n, a contradiction. (A rational integer a divides a rational integer b as rational integers if and only if a divides b as algebraic integers.)

Remark. Schur observes that Landau's proof and his proof are both simplifications of proofs due to Mertens.

REFERENCES

[1] Cox, D. A. Why Eisenstein proved the Eisenstein criterion and why Schönemann discovered it first, Normat 57 (2009), 49-73, reprinted in Amer. Math. Monthly 118 (2011), 3-21.

[2] Dedekind, R. Beweis für die Irreduktibilität der Kreisteilungsgleichung, J. reine angew. Math. 54 (1857), 27-30.

[3] Eisenstein, F. G. M., Über die Irreductibilität und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt, J. reine angew. Math. 39 (1850), 160-179.

[4] C.-F. Gauss, *Disquisitiones Arithmeticae*, Leipzig 1801, available in German tranlation in *Untersuchungen über höhere Arithmetik* (trans. H. Maser), American Mathematical Society/Chelsea, Providence 2006.

[5] Kronecker, L., Beweis dass für jede Primzahl p die Gleichung $1 + x + \ldots + x^{p-1} = 0$ irreductibel ist, J. reine angew. Math. 29 (1845), 280.

[6] Kronecker, L. Mémoire sur les facteures irréductibles de l'expression $x^n - 1$, J. math. pures et appls. 19 (1854), 177-192.

[7] Landau, E. Über die Irreduzibilität der Kreisteilungsgleichung, Math. Zeit. 29 (1929), 462.

[8] Schönemann, T. Von denjenigen Moduln, welche Potenzen von Primzahlen sind, J. reine angew. Math. 32 (1846), 93-105.
[9] Schur, I. Zur Irreduzibilität der Kreisteilungsgleichung, Math. Zeit. 29 (1929), 463.
[10] van der Waerden, B. L. *Moderne Algebra*, Springer Verlag, Berlin 1931.
[11] Weintraub, S. H. *Galois Theory*, second edition, Springer Verlag, New York 2009.

DEPARTMENT OF MATHEMATICS, LEHIGH UNIVERSITY, BETHLEHEM, PA 18015-3174, USA
E-mail address: shw2@lehigh.edu