A PROOF OF THE IRREDUCIBILITY OF THE p-TH CYCLOTOMIC POLYNOMIAL, FOLLOWING GAUSS

STEVEN H. WEINTRAUB

ABSTRACT. We present a proof of the fact that for a prime p, the p-th cyclotomic polynomial $\Phi_p(x)$ is irreducible, that is a simplification of Gauss's proof.

It is well-known and very easy to prove that the p-th cyclotomic polynomial $\Phi_p(x)$ is irreducible for p prime by using Eisenstein's criterion. But this result is originally due to Gauss in the *Disquisitiones Arithmeticae* [1, article 341], by a rather complicated proof. We present a simplified version of Gauss's proof.

Theorem 1. *Let p be a prime. Then the p-th cyclotomic polynomial $\Phi_p(x) = x^{p-1} + x^{p-2} + \ldots + 1$ is irreducible.*

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

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

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 $\{\zeta_1,\ldots,\zeta_d\}$. For $k = 1,\ldots,p-1$, let $f_k(x) = (x-\zeta_1^k)\cdots(x-\zeta_d^k)$. The coefficients of $f_k(x)$ are symmetric polynomials in $\{\zeta_1^k,\ldots,\zeta_d^k\}$, hence symmetric polynomials in $\{\zeta_1,\ldots,\zeta_d\}$, 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,

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

2000 *Mathematics Subject Classification.* 12E05.
Key words and phrases. cyclotomic polynomial, irreducibility.

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

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

Thus

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

But $s_i(r_1, \ldots, r_d)$ 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.

References

[1] C.-F. Gauss, *Disquisitiones Arithmeticae*, Leipzig 1801, available in German translation in *Untersuchungen über höhere Arithmetik* (trans. H. Maser), American Mathematical Society/Chelsea, Providence 2006 and in English translation in *Disquisitiones Arithmeticae* (trans. A. Clarke), Yale University Press 1966 and Springer Verlag 1986.

Department of Mathematics, Lehigh University, Bethlehem, PA 18015-3174, USA
E-mail address: shw2@lehigh.edu