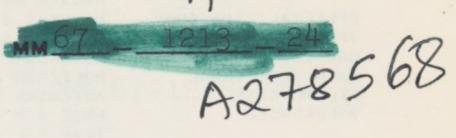
BELL TELEPHONE LABORATORIES

COVER SHEET FOR TECHNICAL MEMORANDUM A33945

TITLE- Irreducible Polynomials Over the Integers Which Factor mod p for

Every p

FILING SUBJECTS - Polynomials



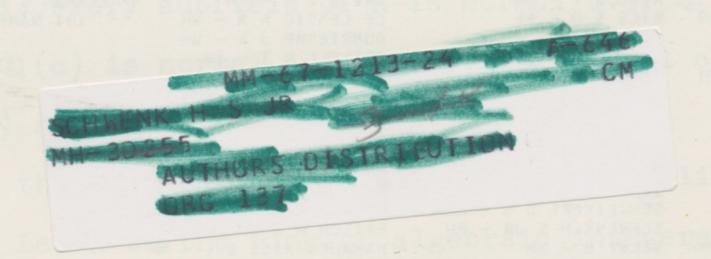
DATE- September 7, 1967

AUTHOR- L. J. Corwin Ext. MH 3422

ABSTRACT

It is proved that if f is an irreducible polynomial over the integers whose splitting field has a noncyclic Abelian Galois group, then f will be reducible mod p for every p. The cyclotomic polynomials $Q_8(x) = x^4 + 1$ and $Q_{15}(x) = \frac{(x^{15}-1)(x-1)}{(x^5-1)(x^3-1)}$ are examples of this.

3 pages of text 4 references



BELL TELEPHONE LABORATORIES

SUBJECT: Irreducible Polynomials Over the Integers DATE: September 7, 1967
Which Factor mod p for Every p Case 20878

MM 67-1213-24

MEMORANDUM FOR FILE

E. R. Berlekamp [1] has noted that $Q_{15}(x) = \frac{(x^{15}-1)(x-1)}{(x^3-1)(x^5-1)}$ factors mod p for every prime p, but is irreducible over the integers. A simpler example of this phenomenon is $Q_8(x) = x^4 + 1$. These examples represent special cases of a general theorem.

Theorem. Let F(x) be a monic polynomial with integer coefficients irreducible over the integers whose splitting field has a noncyclic Abelian Galois group. Then F(x) is reducible mod p for every prime p.

<u>Proof.</u> Suppose F has degree n. Denote the rationals by Q and the integers by Z; let K be the splitting field for P(x), and let α be any root of F(x) = 0. Then:

- 1) By the Fundamental Theorem of Galois Theory ([4], pp. 156, 160), every subfield of K is normal over Q. In particular, Q(α) is normal and hence contains all conjugates of α . Thus F(x) splits over Q(α), and so K = Q(α). (Here is where we use the fact that the Galois group is Abelian.)
- 2) Let A be the ring of algebraic integers in K. The ring A/pA is not ordinarily a field (since pA is usually not a maximal ideal of A). However, pA is contained in a maximal ideal

- P of A. By [2], Prop. 14 (p. 11), A/P is a normal extension of \mathbb{Z}/p , and there is a natural map of the Galois group G of K (over Q) onto the Galois group H of A/P over \mathbb{Z}/p .
- 3) Considered as a polynomial mod p, F(x) splits in A/P. For if $F(x) = (x-\alpha_1) \dots (x-\alpha_n)$ in K, the α 's are algebraic integers and hence in A. Let $\bar{\alpha}_1, \dots, \bar{\alpha}_n$ be their images in A/P. Then $F(x) = (x-\bar{\alpha}_1) \dots (x-\bar{\alpha}_n)$ in A/P.
- 4) The Galois group H is cyclic, since the fields are finite. (See [4], p. 117.) Since G is not cyclic, by hypothesis, G is not isomorphic to H. Thus, by 2), H has smaller order than G. (In fact, the order of H divides the order of G.)
- 5) By 1), K is of degree n over \mathbb{Q} (since \mathbb{Q} (α) clearly is). By the Fundamental Theorem of Galois Theory, G is of order n. Hence H is of order < n, and so A/P is of degree m < n over \mathbb{Z}/p . Let $\bar{\alpha}$ be any root of F(x) = 0 in A/P. Then $1, \bar{\alpha}, \ldots, \bar{\alpha}^m$ are linearly dependent, and so $\bar{\alpha}$ satisfies an equation of degree $\leq m$. Thus F(x) is not the minimal polynomial for $\bar{\alpha}$, and so F(x) is reducible mod p. This proves the theorem.
- 6) Actually slightly more can be proved. Let the irreducible polynomial for α have degree d, and let ℓ be the field $(\mathbb{Z}/p)(\bar{\alpha})$; then $[\ell\colon\mathbb{Z}/p]=d$. Then A/P is an extension field of ℓ ; since $[A/p\colon\ell][\ell\colon\mathbb{Z}/p]=[A/P\colon\mathbb{Z}/p]=m|n$, d divides n. Therefore the degree of the minimal polynomial for $\bar{\alpha}$ divides the degree of F. In other words, the degrees of the factors of F mod p divide n.

The theorem, unfortunately, looks more general than it is. A famous result of Kummer says that all Abelian extensions of the rationals are subfields of cyclotomic fields. Hence the roots of the polynomial F(x) must be a linear combination of roots of unity.

In general, the Galois group of the cyclotomic field with the n^{th} roots of unity is isomorphic to the multiplicative group of the integers mod n relatively prime to n. (See [4], p. 162.) This group is cyclic only if n is 1,2,4, a power of an odd prime, or twice a power of an odd prime. (See [3], p. 55, Theorem 4.11, for a proof.) Thus the two examples given at the beginning of this note are two of the simplest. Another easy one is $Q_{16}(x) = x^8 + 1$.

MH-1213-LJC-ek

L. J. CORWIN

Att. References

REFERENCES

- 1. Berlekamp, E. R., "The Factorization of the 15th Cyclotomic Polynomial", BTL Technical Memorandum MM 67-1213-13.
- 2. Lang, S., "Algebraic Numbers", Addison-Wesley, Reading, Massachusetts, 1956.
- 3. Leveque, W., "Topics in Number Theory", Vol. I, Addison-Wesley, Reading, Massachusetts, 1956.
- 4. Van der Waerden, B. L., "Modern Algebra", 2nd Ed., New York, Frederick Ungar, 1948.