MATH. SCAND. 3 (1955), 124–126

ON A THEOREM OF STICKELBERGER

KÅRE DALEN

1. This paper contains a wholly algebraic proof of a theorem of Stickelberger which is a little more general than that given by Carlitz [1]. The notations are as in [2, p. 263] which also contains a proof of the general Hensel lemma. This lemma is fundamental in the following discussion.

2. Let Ω be a perfect field with respect to the valuation w. The elements a with $w(a) \geqq 0$ constitute an integral domain I, and the elements b with $w(b) > 0$ constitute a prime ideal $\mathfrak{P}$ of I. Then $P = I/\mathfrak{P}$ is a field. We suppose P to be isomorphic with either the Galois field $GF(p^n)$ or the field of real numbers. The field P then admits only algebraic extensions which are normal and cyclic, and we have the theorem:

If $f(x)$ and $g(x)$ are irreducible polynomials in $P[x]$ and the degree of $f(x)$ is a divisor of the degree of $g(x)$, then the extension $P(\vartheta)$ defined by $g(x)$ contains all the roots of $f(x)$.

3. We shall now study a special extension of Ω. This extension is performed by adjoining the roots of a polynomial

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$$

in $I[x]$ with discriminant $D \not\equiv 0 \ (\mathfrak{P})$. Let the factorization of $f(x)$ in the field $P[x]$ mentioned in section 2 be

$$f(x) = f_1(x) f_2(x) \ldots f_s(x)$$

where the degree of $f_i(x)$ is r_i. By the Hensel lemma we obtain:

The factorization of $f(x)$ in $\Omega[x]$ is of the same type, that is, the degrees of the irreducible factors of $f(x)$ in $\Omega[x]$ are $r_1, r_2, \ldots, r_s$.

Now, let

$$r(x) = x^m + b_1 x^{m-1} + \ldots + b_m$$

be an irreducible polynomial in $P[x]$ of degree l.c.m. of the r_i. Clearly $r(x)$, being an element of $\Omega[x]$, is irreducible in $\Omega[x]$. We shall show that $r(x)$ is a resolvent of $f(x)$. By adjoining a root ϑ of $r(x)$ to Ω we

Received January 5, 1955.

obtain $\Omega_1 = \Omega(\vartheta)$, which is perfect with respect to the uniquely determined continuation w_1 of w. The valuation w_1 defines an I_1, $\mathfrak{P}_1$ and $P_1 = I_1/\mathfrak{P}_1$. Evidently $w_1(\vartheta) \geqq 0$ and thus $r(x)$, as a polynomial of $P[x]$, has a root in P_1. By section 2 we then obtain that all the roots of $f(x) \in P[x]$ are in P_1. From the Hensel lemma it follows that $f(x)$ factorizes with linear factors in $\Omega_1[x]$. Thus we have

THEOREM 1. *Let*

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$$

be a polynomial of $I[x]$ *with discriminant* $D \not\equiv 0$ $(\mathfrak{P})$ *and* $r_1, r_2, \ldots, r_s$ *the degrees of the irreducible factors of* $f(x)$ *in* $P[x]$. *The Galois group* G *of* $f(x)$ *is then generated by*

$$\delta\colon\ (1, 2, \ldots)(\ldots)\ldots(\ldots)$$

where the lengths of the cycles are $r_1, r_2, \ldots, r_s$.

4. We shall now discuss the Stickelberger theorem. Let

$$H = \prod_{i>j} (\alpha_i - \alpha_j)$$

where the α_i are the different roots of the polynomial $f(x)$ in a suitable Ω_1. Clearly $H \in \Omega$ if and only if the number

$$(r_1 - 1) + (r_2 - 1) + \ldots + (r_s - 1) = n - s$$

of inversions of δ is even. Since $H^2 = D$ we obtain

THEOREM 2. *Let*

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$$

be a polynomial of $I[x]$ *with discriminant* $D \not\equiv 0$ $(\mathfrak{P})$, *and let* s *be the number of irreducible factors of* $f(x)$ *in* $P[x]$. *Then we have*

$$(D/\Omega) = (-1)^{n-s},$$

where $(D/\Omega) = +1$ *or* -1 *according to whether* $x^2 - D$ *is reducible or not in* $\Omega[x]$.

5. Special cases. Let Ω be the perfect p-adic field. P is then a $GF(p)$ and we obtain theorems A and B of Carlitz [1]. Let Ω be the field of formal power series with real coefficients. P is then the field of real numbers. Since $(D/\Omega) = 1$ is equivalent to $D > 0$, we obtain the following corollary.

Corollary. *Let $f(x)$ be a polynomial of degree n with real coefficients, discriminant $D \neq 0$ and k real roots. Then*

$$(-1)^{\frac{1}{2}(n-k)} D > 0 .$$

We may also let Ω be the perfect $\mathfrak{p}$-adic field of an algebraic number field K and obtain similar theorems.

REFERENCES

1. L. Carlitz, *A theorem of Stickelberger*, Math. Scand. 1 (1953), 82–84.
2. B. L. van der Waerden, *Moderne Algebra* I, Dritte Auflage, Berlin·Göttingen·Heidelberg, 1950.

BRYN, OSLO, NORWAY