MATH. SCAND. 1 (1953)

A THEOREM OF STICKELBERGER

L. CARLITZ

1. In a recent paper [3] Professor Skolem proved the following

THEOREM A. *Let D denote the discriminant of*

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

where the a_r are rational integers. Let p be an odd prime, $p \nmid D$, and let

$$f(x) \equiv f_1(x) \ldots f_s(x) \pmod{p} ,$$

where the $f_j(x)$ are irreducible (mod p). *Then the Legendre symbol*

$$\left(\frac{D}{p}\right) = (-1)^{n-s} . \tag{1.1}$$

This theorem is contained in a theorem of Stickelberger [4], *namely if k is an algebraic field of degree n over the rationals and of discriminant D, and if $(p) = \mathfrak{p}_1 \ldots \mathfrak{p}_s$ is the factorization of p into distinct prime ideals then* (1.1) *holds*. For other proofs of Theorem A, see [1], [2], [5]. As for the prime 2 we have the following supplementary

THEOREM B. *In the notation of Theorem A with $p = 2$, we have*

$$\left(\frac{D}{2}\right) = (-1)^{n-s} . \tag{1.2}$$

Here $(D/2)$ denotes the Kronecker symbol, that is

$$(D/2) = +1 \text{ for } D \equiv 1 \pmod 8,\ (D/2) = -1 \text{ for } D \equiv 5 \pmod 8 .$$

We remark that any odd D is necessarily $\equiv 1 \pmod 4$. Theorem B is also contained in a result of Stickelberger's, but the proof is rather complicated. In this note we shall sketch a simple proof of Theorem B.

2. If $g(x)$ is a polynomial with rational integral coefficients then it is familiar that

$$g^p(x) - g(x^p) = ph(x) , \tag{2.1}$$

Received March 14, 1953

where $h(x)$ also has integral coefficients; p is a prime. Now let α be an integral algebraic number of k and put

$$\gamma_r = g(\alpha^{p^r}),\ \eta_r = h(\alpha^{p^r}) \quad (r = 0, 1, 2)\,. \tag{2.2}$$

Thus (2.1) implies in particular

$$\gamma_0^p - \gamma_1 = p\eta_0,\ \gamma_1^p - \gamma_2 = p\eta_1\,. \tag{2.3}$$

Assume (p) a prime ideal of k. We shall require the

LEMMA. *γ_2 is congruent to a rational number* (mod p^2) *if and only if* $\gamma_2 \equiv \gamma_1 \pmod{p^2}$.

PROOF. Let $\gamma_2 \equiv \gamma_1 \pmod{p^2}$. Then in particular by the second of (2.3), $\gamma_2^p \equiv \gamma_2 \pmod p$ and since (p) is prime it follows that $\gamma_2 \equiv a \pmod p$, where a is rational. It also follows that $\gamma_0 \equiv \gamma_1 \equiv a \pmod p$. Hence $\gamma_0^p \equiv \gamma_1^p \pmod{p^2}$ and (2.2) implies $p\eta_0 \equiv p\eta_1 \pmod{p^2}$ so that $\eta_0 \equiv \eta_1 \pmod p$. But by the second of (2.2) we have $\eta_1 \equiv \eta_0^p \pmod p$. Consequently $\eta_0 \equiv \eta_1 \equiv b \pmod p$ where b is rational. Again $\gamma_1^p \equiv a^p \pmod{p^2}$ so that the second of (2.3) yields $\gamma_2 \equiv a^p - bp \pmod{p^2}$.

Conversely let $\gamma_2 \equiv c \pmod{p^2}$. It then follows from the second of (2.3) that $\gamma_1^p \equiv c + p\eta_1 \pmod{p^2}$, so that $\gamma_1 \equiv c \pmod p$, $\gamma_1^p \equiv c^p \pmod{p^2}$, and therefore $\eta_1 \equiv b \pmod p$, where b is rational. Also $\gamma_0 \equiv c \pmod p$. Since as before $\eta_1 \equiv \eta_0^p \pmod p$, we get $\eta_0 \equiv b \pmod p$. Hence (2.3) implies $\gamma_1 - \gamma_2 = (\gamma_0^p - \gamma_1^p) - p(\eta_0 - \eta_1) \equiv 0 \pmod{p^2}$. This completes the proof of the Lemma.

3. We now prove Theorem B in the case $s = 1$, that is $f(x)$ irreducible (mod 2). Let $\alpha_1, \ldots, \alpha_n$ denote the roots of $f(x)$ and put

$$\delta_r = \prod_{0 \le i < j \le n-1} (\alpha_i^{2^r} - \alpha_j^{2^r}),\ D_r = \delta_r^2 \quad (r = 0, 1, 2)\,. \tag{3.1}$$

It follows at once that

$$D_0 \equiv D_1 \equiv D_2 \pmod 8\,. \tag{3.2}$$

Now if $\alpha = \alpha_0$ is any fixed root of $f(x)$ then we may put

$$\alpha_j \equiv \alpha^{2^j} \pmod 2\,,$$

which implies

$$\alpha_j^{2^r} \equiv \alpha^{2^{r+j}} \pmod{2^{r+1}}\,. \tag{3.3}$$

If we write

$$\gamma_r = \prod_{0 \le i < j \le n-1} (\alpha^{2^{r+i}} - \alpha^{2^{r+j}}) \quad (r = 0, 1, 2)\,,$$

it is clear from (3.1) and (3.3) that

$$\delta_r \equiv \gamma_r \pmod{2^{r+1}}\,. \tag{3.4}$$

Now we have also from (3.1)

$$\gamma_2 \equiv (-1)^{n-1}\gamma_1 \pmod 4 . \tag{3.5}$$

Hence by the above lemma γ_2 is congruent to a rational number (mod 4) if and only if n is odd. On the other hand by (3.2) and (3.4)

$$D \equiv D_2 \equiv \gamma_2{}^2 \pmod 8 ,$$

so that $D \equiv 1 \pmod 8$ if and only if $\gamma_2{}^2 \equiv 1 \pmod 8$. Since $\gamma_2 \equiv 1+2\beta$, $\gamma_2{}^2 = 1+4\beta(\beta+1) \equiv 1 \pmod 8$ if and only if $\beta \equiv 0$ or $1 \pmod 2$ so that $\gamma_2 \equiv 1$ or $3 \pmod 4$. Hence $D \equiv 1 \pmod 8$ if and only if n is odd. This completes the proof of Theorem B in the case $s = 1$.

4. It is now easy to complete the proof of the theorem. For by a familiar theorem

$$D = d_1 \ldots d_s m^2 ,$$

where d_i is the discriminant of $f_i(x)$ and m is an integer, which is necessarily odd. Consequently

$$D \equiv d_1 \ldots d_s \pmod 8 ,$$

so that

$$\left(\frac{D}{2}\right) = \left(\frac{d_1}{2}\right) \cdots \left(\frac{d_s}{2}\right) = (-1)^{n-s} ,$$

which proves (1.2) .

REFERENCES

1. K. Hensel, *Über die zu einem algebraischen Körper gehörigen Invarianten*, J. reine angew. Math. 129 (1905), 68–85.
2. A. E. Pellet, *Sur la décomposition d'une fonction entière en facteurs irréducibles suivant un module premier p*, C. R. Acad. Sci. Paris 86 (1878), 1071–1072.
3. Th. Skolem, *On a certain connection between the discriminant of a polynomial and the number of its irreducible factors mod p*, Norsk Mat. Tidsskr. 34 (1952), 81–85.
4. L. Stickelberger, *Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper*, Verhandlungen des ersten internationalen Mathematiker-Kongresses in Zürich 1897, Leipzig, 1898, 182–193.
5. G. Voronoï, *Sur une propriété du discriminant des fonctions entières*, Verhandlungen des dritten internationalen Mathematiker-Kongresses in Heidelberg 1904, Leipzig, 1905, 186–189.

DUKE UNIVERSITY, DURHAM, N. C., U.S.A.