ON A THEOREM OF HIGHER RECIPROCITY*

BY ALBERT WHITEMAN†

1. *Introduction*. Let $\mathfrak{D}$ denote the totality of polynomials in an indeterminate x, with coefficients in a fixed Galois field $GF(p^\pi)$ of order p^π. Let P be a primary irreducible polynomial in $\mathfrak{D}$; then, if A is any polynomial in $\mathfrak{D}$ not divisible by P, we define $\{A|P\}$ as that element in $GF(p^\pi)$ for which

$$\left\{\frac{A}{P}\right\} \equiv A^{(p^{\pi\nu}-1)/(p^\pi-1)} \pmod{P},$$

where ν is the degree of P.

We have then the following theorem of reciprocity due to H. Kuhne‡ and rediscovered by Schmidt§ and Carlitz.‖

If P and Q are primary irreducible polynomials in $\mathfrak{D}$ of degree ν and ρ respectively, then

$$\left\{\frac{P}{Q}\right\} = (-1)^{\rho\nu}\left\{\frac{Q}{P}\right\}.$$

If $M=P_1^{a_1}\cdots P_k^{a_k}$ and $(A, M)=1$ we use the definition,

$$\left\{\frac{A}{M}\right\} = \left\{\frac{A}{P_1}\right\}^{a_1}\cdots\left\{\frac{A}{P_k}\right\}^{a_k}.$$

The purpose of this note is to give a simple new proof of the following theorem:

---

* Presented to the Society, February 20, 1937.

† Harrison Scholar in Mathematics, University of Pennsylvania.

‡ H. Kuhne, *Eine Wechselbeziehung zwischen Funktionen mehrerer Unbestimmter die zu Reziprozitätsgesetzen führt*, Journal für die reine und angewandte Mathematik, vol. 124 (1901–02), pp. 121–133.

§ F. K. Schmidt, *Zur Zahlentheorie in Körpern von der Charakteristik p*, Sitzungsberichte der Physikalish-medizinischen Societät zu Erlangen, vol. 58–59 (1928), pp. 159–172.

‖ L. Carlitz, *The arithmetic of polynomials in a Galois field*, American Journal of Mathematics, vol. 54 (1932), pp. 39–50.

If M and N are primary relatively prime polynomials in $\mathfrak{D}$ of degree m and n respectively, then

$$\left\{\frac{M}{N}\right\} = (-1)^{mn}\left\{\frac{N}{M}\right\}.$$

This generalized form of Kuhne's theorem is, of course, not new. The novelty of our method consists in proving the case M, N directly (rather than P, Q) by making use of the generalized analog of Gauss's lemma* proved in §2.

2. *Generalization of the Analog of Gauss's Lemma.* We shall employ the following notation. If

$$F = a_0x^\nu + a_1x^{\nu-1} + \cdots + a_\nu, \qquad a_0 \neq 0,$$

is a polynomial in $\mathfrak{D}$, then

$$\operatorname{sgn} F = a_0, \qquad \deg F = \nu;$$

for sgn $F=1$, F is said to be *primary*. Let $\mathcal{R}(A/B)$ denote the remainder in the division of A by B. Then the generalization in question is furnished by the following lemma.

LEMMA. *Let A and M be in $\mathfrak{D}$, M primary and relatively prime to A; then*

$$\left\{\frac{A}{M}\right\} = \prod_{\deg H<m} \operatorname{sgn} \mathcal{R}\left(\frac{HA}{M}\right),$$

the product extending over all primary H of degree less than the degree of M.

We shall now give a proof of this lemma along lines suggested by Schering's† proof in the numerical case.

3. *Proof of the Lemma.* Following Dedekind,‡ we define $\phi(M)$ to be the number of polynomials in a reduced residue system, mod M; the number of primary polynomials prime to M

---

* L. Carlitz, loc. cit., p. 46.

† E. Schering, *Zur Theorie der quadratischen Reste*, Acta Mathematica, vol. 1 (1882), pp. 153–170; see also P. Bachmann, *Die Elemente der Zahlentheorie*, 1892, pp. 144–148.

‡ R. Dedekind, *Abriss einer Theorie der höheren Congruenzen in Bezug auf einer reellen Primzahl-Modulus*, Journal für die reine und angewandte Mathematik, vol. 54 (1857), pp. 1–26.

and of degree less than m is then evidently $\phi(M)/(p^\pi-1)$. Hence, just as in the numerical case, it is very easy to show that the number of primary polynomials H of degree less than m such that $(H, M)=D$ is $\phi(M/D)/(p^\pi-1)$.

Put $H=H_1D$, $M=M_1D$. Then the congruence

$$HA \equiv H' \operatorname{sgn} \mathcal{R}\left(\frac{HA}{M}\right) \pmod{M}, \quad \deg H' < m, \quad \operatorname{sgn} H' = 1,$$

becomes

$$H_1A \equiv H_1' \operatorname{sgn} \mathcal{R}\left(\frac{HA}{M}\right) \pmod{M_1}. \tag{1}$$

Evidently the polynomials H_1 are the polynomials H_1' in some order. Therefore, if we multiply all congruences of the type (1) together and divide each member of the resulting congruence by the product of the H_1 (which is prime to M_1), we have

$$A^{\phi(M_1)/(p^\pi-1)} \equiv \prod_{(H,M)=D} \operatorname{sgn} \mathcal{R}\left(\frac{HA}{M}\right) \pmod{M_1}. \tag{2}$$

For $M_1=P$, a primary irreducible polynomial of degree ν, the last congruence becomes

$$A^{(p^{\pi\nu}-1)/(p^\pi-1)} \equiv \left\{\frac{A}{P}\right\} \pmod{P}. \tag{3}$$

Writing this congruence in the form

$$A^{(p^{\pi\nu}-1)/(p^\pi-1)} = \left\{\frac{A}{P}\right\} + FP,$$

and raising both members to the $p^{\pi(k-1)\nu}$th power, we can readily show that

$$A^{p^{\pi(k-1)\nu}(p^{\pi\nu}-1)/(p^\pi-1)} = \left\{\frac{A}{P}\right\} + F'P^{p^{\pi(k-1)\nu}}.$$

But it is well known that

$$\phi(P^k) = p^{\pi(k-1)\nu}(p^{\pi\nu} - 1).$$

Hence

$$A^{\phi(P^k)/(p^\pi-1)} \equiv \left\{\frac{A}{P}\right\} \pmod{P^k}. \tag{4}$$

Finally, for $M_1=P_1^{b_1}\cdots P_k^{b_k}$, $0\leqq b_i\leqq a_i$, $k>1$, deg $P_i=\nu_i$, we have

$$\frac{\phi(M_1)}{p^\pi-1}=\frac{1}{p^\pi-1}\prod_{i=1}^{k}p^{(b_i-1)\pi\nu_i}(p^{\pi\nu_i}-1).$$

Hence, since

$$A^{p^{\pi\nu_i}}\equiv 1 \pmod{P_i},$$

it follows that

$$A^{\phi(M_1)/(p^\pi-1)}\equiv 1 \pmod{M_1}, \tag{5}$$

where, as already stated, M_1 is the product of at least two distinct irreducible polynomials.

Combining the results of (2), $\cdots$, (5) we now see that

$$\prod_{(H,M)=D}\operatorname{sgn}\mathcal{R}\left(\frac{HA}{M}\right) \tag{6}$$

has the value 1 unless $M_1=M/D$ is irreducible or the power of an irreducible polynomial. On the other hand, for $M_1=P_i^b$ $(b=1,\cdots,a_i)$, (6) has the value $\{A\,|\,P_i\}$. Consequently

$$\begin{aligned}\prod_{D\mid M}\prod_{(H,M)=D}\operatorname{sgn}\mathcal{R}\left(\frac{HA}{M}\right)&=\prod_{\deg H<m}\operatorname{sgn}\mathcal{R}\left(\frac{HA}{M}\right)\\&=\left\{\frac{A}{P_1}\right\}^{a_1}\cdots\left\{\frac{A}{P_k}\right\}^{a_k},\end{aligned}$$

from which the Lemma follows at once.

4. *Proof of the Theorem.* Let A, N denote primary polynomials of degrees a, n respectively; let $(A,N)=1$, $a\geqq n$. Consider the congruence

$$A\equiv\mathcal{R}(A/N) \pmod{N},\quad \deg\mathcal{R}(A/N)<n.$$

Evidently there exists a primary H(say H_0) of degree $a-n$ such that

$$A=\mathcal{R}(A/N)+H_0N.$$

But this equation may be written in the form

$$(7) \qquad H_0 N \equiv -\mathcal{R}(A/N) \pmod{A}.$$

Let E be any polynomial (not necessarily primary) of degree less than $a-n$. Then we may write

$$(8) \qquad (H_0 + E)N \equiv EN - \mathcal{R}(A/N) \pmod{A},$$

where

$$(9) \qquad \begin{gathered} 0 < \deg(EN - \mathcal{R}(A/N)) < a, \\ \operatorname{sgn}\,(EN - \mathcal{R}(A/N)) = \operatorname{sgn}\, EN = \operatorname{sgn}\, E. \end{gathered}$$

Furthermore, we have the obvious identity

$$(10) \qquad \prod_{\deg H = a-n} HN = H_0 N \prod_{\deg E < a-n} (H_0 + E)N, \qquad E \neq 0.$$

Therefore, by equations (7), $\cdots$, (10),

$$(11) \qquad \begin{aligned} &\prod_{\deg H = a-n} \operatorname{sgn} \mathcal{R}\left(\frac{HN}{A}\right) \\ &= \operatorname{sgn} \mathcal{R}\left(\frac{H_0 N}{A}\right) \prod_{\deg E < a-n} \operatorname{sgn} \mathcal{R}\left(\frac{(H_0 + E)N}{A}\right) \\ &= -\operatorname{sgn} \mathcal{R}\left(\frac{A}{N}\right) \prod_{\deg E < a-n} \operatorname{sgn} E. \end{aligned}$$

Now, by the generalization of Wilson's theorem for a Galois field,

$$\prod_b b = -1, \qquad b \text{ in } GF(p^\pi),$$

from which it follows at once that

$$\prod_{\deg E < a-n} \operatorname{sgn} E = (-1)^{a-n}.$$

Hence (11) becomes

$$(12) \qquad \prod_{\deg H = a-n} \operatorname{sgn} \mathcal{R}\left(\frac{HN}{A}\right) = (-1)^{a-n+1} \operatorname{sgn} \mathcal{R}\left(\frac{A}{N}\right).$$

Since

$$\mathcal{R}\left(\frac{HN}{A}\right) = -\mathcal{R}\left(\frac{A}{HN}\right), \deg HN = \deg A,$$

(12) may also be written in the form

$$(13)\qquad \prod_{\deg H=a-n} \operatorname{sgn} \mathcal{R}\left(\frac{A}{HN}\right) = (-1)^{a-n} \operatorname{sgn} \mathcal{R}\left(\frac{A}{N}\right).$$

Let us now assume, as we may without any loss of generality, that $m \geqq n$. In (12) replace A by KM, where K is any primary polynomial of degree $k (k < n)$. Then we have

$$\prod_{\deg H=k+m-n} \operatorname{sgn} \mathcal{R}\left(\frac{HN}{KM}\right) = (-1)^{k+m-n+1} \operatorname{sgn} \mathcal{R}\left(\frac{KM}{N}\right).$$

Now let K run through all the $p^{\pi k}$ primary polynomials of degree k; we get

$$(14)\qquad \prod_{\substack{\deg H=k+m-n \\ \deg K=k}} \operatorname{sgn} \mathcal{R}\left(\frac{HN}{KM}\right) = (-1)^{k+m-n+1} \prod_{\deg K=k} \operatorname{sgn} \mathcal{R}\left(\frac{KM}{N}\right).$$

In a similar manner we may obtain from (13),

$$(15)\qquad \prod_{\substack{\deg H=k+m-n \\ \deg K=k}} \operatorname{sgn} \mathcal{R}\left(\frac{HN}{KM}\right) = (-1)^{k} \prod_{\deg H=k+m-n} \operatorname{sgn} \mathcal{R}\left(\frac{HN}{M}\right).$$

Comparing (14) and (15), we obtain

$$\prod_{\deg K=k} \operatorname{sgn} \mathcal{R}\left(\frac{KM}{N}\right) = (-1)^{m+n-1} \prod_{\deg H=k+m-n} \operatorname{sgn} \mathcal{R}\left(\frac{HN}{M}\right).$$

Therefore

$$\prod_{\deg K<n} \operatorname{sgn} \mathcal{R}\left(\frac{KM}{N}\right) = (-1)^{mn+n^2-n} \prod_{m-n \leqq \deg H < m} \operatorname{sgn} \mathcal{R}\left(\frac{HN}{M}\right).$$

When we note that

$$\prod_{\deg H<m-n} \operatorname{sgn} \mathcal{R}\left(\frac{HN}{M}\right) = 1,$$

the theorem follows at once.

UNIVERSITY OF PENNSYLVANIA