THE SCHUR DERIVATIVE OF A POLYNOMIAL

by L. CARLITZ

(Received 31st January, 1953)

1. *Introduction.* For a given sequence $\{a_m\}$ and $p \neq 0$, Schur (2) defined

$$a'_m = \Delta a_m = (a_{m+1} - a_m)/p^{m+1},$$
$$a_m^{(r)} = \Delta^r a_m = \Delta\,(a_m^{(r-1)}), \quad a_m^{(0)} = m. \qquad (1.1)$$

In particular if p is a prime, a an integer and $a_m = a^{p^m}$, then by Fermat's theorem

$$a'_m = (a^{p^{m+1}} - a^{p^m})/p^{m+1}$$

is integral. Schur proved that if $p \nmid a$, then all the derivatives

$$\Delta^2 a^{p^m}, \quad \Delta^3 a^{p^m}, \quad \ldots, \quad \Delta^{p-1} a^{p^m}$$

are integral. Zorn (3) using p-adic methods proved Schur's results and also found the residue of $X_m \pmod{p^m}$, where $X_m = (x^{p^m} - 1)/p^{m+1}$ and $x \equiv 1 \pmod p$. The writer (1) proved Zorn's congruences by elementary methods as well as certain additional results of a similar sort.

In the present note we consider polynomials

$$f(x) = f(x_1, \ldots, x_k) \qquad (1{\cdot}2)$$

in an arbitrary number of indeterminates; the coefficients of $f(x)$ are rational integers, or, a little more generally, rational numbers that are integral $(\text{mod } p)$, where p is a fixed prime. Let F denote the set of polynomials (1.2). Then as is familiar

$$f^p(x) = f(x^p) + pg(x), \qquad (1.3)$$

where $g(x) \in F$. It follows from (1.3) that

$$f^{p^{m+1}}(x) = f^{p^m}(x^p) + p^{m+1} f'_m(x), \qquad (1.4)$$

where $f'_m(x) \in F$. In analogy with (1.1) we define

$$\Delta f^{p^m}(x) = f'_m(x) = (f^{p^{m+1}}(x) - f^{p^m}(x^p))/p^{m+1}. \qquad (1.5)$$

Higher derivatives are defined by means of

$$\Delta^{r+1} f^{p^m}(x) = f_m^{(r+1)}(x) = (f_{m+1}^{(r)}(x) f^{p^{m+1}}(x) - f_m^{(r)}(x) f^{p^{m+r}}(x^p))/p^{m+1}, \qquad (1.6)$$

for $r \geqslant 1$. If $f(x) = a$, then it is easily verified that $\Delta^r f^{p^m}(x)$ reduces to $a^{p^{m+1}} + \ldots + p^{m+r-1}$ times the r-th Schur derivative as defined by (1.1).

With these definitions we show that $\Delta^r f^{p^m}(x)$ has integral coefficients $(\text{mod } p)$ for $1 \leqslant r \leqslant p-1$; if $g(x)$ in (1.3) is divisible by p then $\Delta^r f^{p^m}(x) \in F$ for all $r \geqslant 1$, $m \geqslant 0$. More precisely we have the congruence

$$\Delta^r f^{p^m}(x) \equiv \frac{1}{r!} (f'_m)^r f^{p^m(e_r - r)}(x^p) \frac{\prod_{i=1}^{r} (p^i - 1)}{(p-1)^r} \pmod{p^m} \qquad (1.7)$$

valid for $1 \leqslant r \leqslant p$, where e_r is defined in (3.1); if $r < p-1$, (1.7) holds $(\text{mod } p^{m+r})$.

Finally we consider a generalization of (1.5) and (1.6) valid for any commutative ring that contains the rational integers. The results stated above carry over with very slight change.

Remark. One might think it natural to define $\Delta^r f^{p^m}(x)$ by means of

$$\Delta^{r+1} f^{p^m}(x) = (f_{m+1}^{(r)}(x) - f_m^{(r)}(x^p))/p^{m+1}\,; \qquad (1.8)$$

however, (1.8) does not lead to a generalization of Schur's results.

2. *Some Lemmas.* We shall require the following lemmas.

LEMMA 1.

$$\prod_{s=0}^{r-1} (x - p^s) = \sum_{s=0}^{r} (-1)^s \begin{bmatrix} r \\ s \end{bmatrix} p^{\frac{1}{2}s(s-1)} x^{r-s}, \qquad (2.1)$$

where

$$\begin{bmatrix} r \\ s \end{bmatrix} = \frac{(p^r-1)\dots(p^{r-s+1}-1)}{(p-1)\dots(p^s-1)} = \begin{bmatrix} r \\ r-s \end{bmatrix}, \quad \begin{bmatrix} r \\ 0 \end{bmatrix} = 1.$$

This is well known.

LEMMA 2. *In the notation of* (1.5) *and* (1.6), *we have*

$$p^{rm+\frac{1}{2}r(r+1)} f_m^{(r)}(x) = \sum_{s=0}^{r} (-1)^{r-s} \begin{bmatrix} r \\ s \end{bmatrix} p^{\frac{1}{2}(r-s)(r-s-1)} f_{m+1} \dots f_{m+s} \bar{f}_{m+s} \dots \bar{f}_{m+r-1}, \qquad (2.2)$$

where

$$f_m = f^{p^m}(x), \quad \bar{f}_m = f^{p^m}(x^p). \qquad (2.3)$$

Lemma 2 is easily proved by induction making use of familiar properties of $\begin{bmatrix} r \\ s \end{bmatrix}$.

The following lemma is a slight extension of Lemma 2 of (1).

LEMMA 3. *Put*

$$W_{r,i} = \frac{1}{i!} \sum_{s=0}^{r} (-1)^s \begin{bmatrix} r \\ s \end{bmatrix} g_i(p^{r-s}) p^{\frac{1}{2}s(s-1)},$$

where $g_i(u)$ is a polynomial of degree i with integral coefficients. Then

$$W_{r,i} = \left\{ \begin{array}{ll} 0 & (i<r) \\ \dfrac{a_0}{i!} \displaystyle\prod_{s=0}^{r-1} (p^r - p^s) & (i=r) \\ \dfrac{1}{i!} p^{\frac{1}{2}r(r-1)} U_{r,i} & (i>r) \end{array} \right\}, \qquad (2.4)$$

where a_0 is the highest coefficient of $g_i(u)$, and $U_{r,i}$ is integral.

3. *Formulas for $\Delta^r f^{p^m}(x)$.* Using the abbreviated notation (2.3), we rewrite (1.4) as

$$f_{m+1} = \bar{f}_m + p^{m+1} f'_m.$$

If we put

$$e_s = (p^s - 1)/(p-1) \qquad (3.1)$$

it is seen that

$$\begin{aligned} f_{m+1} \dots f_{m+s} \bar{f}_{m+s} \dots \bar{f}_{m+r-1} &= (\bar{f}_m + p^{m+1} f'_m)^{e_s} (\bar{f}_m)^{p^s e_{r-s}} \\ &= \sum_{i=0}^{e_s} \binom{e_s}{i} p^{i(m+1)} (f'_m)^i (f_m)^{e_r - i}, \end{aligned}$$

since $e_s + p^s e_{r-s} = e_r$. Thus substituting in the right member of (2.2), we obtain

$$\left. \begin{aligned} & p^{rm+\frac{1}{2}r(r+1)} f_m^{(r)}(x) \\ &= \sum_{s=0}^{r} (-1)^{r-s} \begin{bmatrix} r \\ s \end{bmatrix} p^{\frac{1}{2}(r-s)(r-s-1)} \sum_{i=0}^{e_s} \binom{e_s}{i} p^{i(m+1)} (f'_m)^i (\bar{f}_m)^{e_r - i} \\ &= \sum_{i=0}^{e_r} p^{i(m+1)} (f'_m)^i (\bar{f}_m)^{e_r - i} \sum_{s=0}^{r} (-1)^{r-s} \begin{bmatrix} r \\ s \end{bmatrix} \binom{e_s}{i} p^{\frac{1}{2}(r-s)(r-s-1)} \\ &= \sum_{s=0}^{e_r} p^{i(m+1)} (f'_m)^i (\bar{f}_m)^{e_r - i} \sum_{s=0}^{r} (-1)^s \begin{bmatrix} r \\ s \end{bmatrix} \binom{e_{r-s}}{i} p^{\frac{1}{2}s(s-1)} \end{aligned} \right\}, \qquad (3.2)$$

https://doi.org/10.1017/S204061850003567X Published online by Cambridge University Press

where, for $e_s < i$, $\binom{e_s}{i}$ is taken to be zero. We now apply Lemma 3 to the inner sum, and (3.2) becomes

$$\Delta^r f^{p^m}(x) = \frac{1}{r!}(f'_m)^r (\bar{f}_m)^{e_r - r} \frac{\prod_{i=1}^{r}(p^i - 1)}{(p-1)^r} + \sum_{i=r+1}^{e_r} \frac{1}{i!} p^{(m+1)(i-r)} (f'_m)^i (f_m)^{e_r - i} U_{r,i}. \qquad (3.3)$$

We can generalize (3.3) in the following way. For arbitrary $h \geqslant 1$, consider $\Delta^r f^{hp^m}(x)$. Clearly Lemma 2 gives

$$p^{rm + \frac{1}{2}r(r+1)} \Delta^r f^{hp^m}(x) = \sum_{s=0}^{r} (-1)^{r-s} \begin{bmatrix} r \\ s \end{bmatrix} p^{\frac{1}{2}(r-s)(r-s-1)} f^h_{m+1} \cdots f^h_{m+s} \bar{f}^h_{m+s} \cdots \bar{f}^h_{m+r-1}.$$

Since

$$f^h_{m+1} \cdots f^h_{m+s} \bar{f}^h_{m+s} \cdots \bar{f}^h_{m+r-1} = (\bar{f}_m + p^{m+1} \bar{f}'_m)^{he_s} (f_m)^{hp^s e_{r-s}}$$
$$= \sum_{s=0}^{he_s} \binom{he_s}{i} p^{i(m+1)} (f'_m)^i (\bar{f}_m)^{he_r - i},$$

a little manipulation leads to

$$\Delta^r f^{hp^m}(x) = \frac{1}{r!} h^r (f'_m)^r (\bar{f}_m)^{he_r - r} \frac{\prod_{i=1}^{r}(p^i - 1)}{(p-1)^r} + \sum_{i=r+1}^{he_r} \frac{1}{i!} p^{(m+1)(i-r)} (f'_m)^i (\bar{f}_m)^{he_r - i} U_{r,i,h}, \qquad (3.4)$$

where $U_{r,i,h}$ is integral $(\bmod\ p)$. For $h = 1$, (3.4) reduces to (3.3); for $h = p-1$, (3.4) becomes

$$\Delta^r f^{(p-1)p^m}(x) = \frac{1}{r!}(f'_m)^r (\bar{f}_m)^{p^r - 1 - r} \prod_{i=1}^{r}(p^i - 1) + \sum_{i=r+1}^{p^r - 1} \frac{1}{i!} p^{(m+1)(i-r)} (f'_m)^i (\bar{f}_m)^{p^r - 1 - i} V_{r,i}, \qquad (3.5)$$

where $V_{r,i} = U_{r,i,p-1}$ is integral $(\bmod\ p)$.

It is perhaps worth noting that for $f(x) = a$, (3.4) yields

$$\Delta^r a^{hp^m} = \frac{1}{r!} h^r (a'_m)^r a^{p^m(he_r - r)} \frac{\prod_{i=1}^{r}(p^i - 1)}{(p-1)^r} + \sum_{i=r+1}^{he_r} \frac{1}{i!} p^{(m+1)(i-r)} (a'_m)^i a^{p^m(he_r - i)} U_{r,i,h},$$

in agreement with (2.11) of (**1**).

4. *The main result.* Using (3.4) we can determine when $\Delta^r f^{hp^m}(x) \in F$, that is when $\Delta^r f^{hp^m}(x)$ has integral coefficients $(\bmod\ p)$. It is only necessary to examine $p^{(m+1)(i-r)}/i!$. As in [1, § 3] we suppose $i > r$, $r \leqslant p$. Then $p^{i-r}/i!$ is integral $(\bmod\ p)$; moreover, $p^{i-r}/i!$ is divisible by p unless (i) $i = p$, $r = p-1$, or (ii) $i = p+1$, $r = p$. An immediate consequence is

THEOREM 1. *Let* $h \geqslant 1$. *Then* $\Delta^r f^{hp^m}(x)$ *has integral coefficients* $(\bmod\ p)$ *for* $1 \leqslant r \leqslant p-1$.

In the next place since $p^i/i!$ is always integral $(\bmod\ p)$, and since $f^p(x) \equiv f(x^p) \pmod{p^2}$ implies

$$f^{p^{m+1}}(x) \equiv f^{p^m}(x) \pmod{p^{m+1}}$$

(that is, $f'_m \equiv 0 \pmod{p}$), we have also

THEOREM 2. *Let* $h \geqslant 1$. *If* $f^p(x) \equiv f(x^p) \pmod{p^2}$ *then* $\Delta^r f^{hp^m}(x) \in F$ *for all* $r \geqslant 1$, $m \geqslant 0$.

We may also state the following more precise

THEOREM 3. *Let* $h \geqslant 1$, $1 \leqslant r \leqslant p$. *Then*

$$\Delta^r f^{hp^m}(x) \equiv \frac{1}{r!} h^r (f'_m)^r (\bar{f}_m)^{he_r - r} \frac{\prod_{i=1}^{r} (p^i - 1)}{(p-1)^r} \pmod{p^m}. \qquad (4.1)$$

If $r < p-1$, *the congruence* (4.1) *holds* (mod p^{m+1}).

For $h=1$, (4.1) reduces to (1.7). The special case

$$\Delta^r f^{(p-1)p^m}(x) \equiv \frac{1}{r!} (f'_m)^r (\bar{f}_m)^{p^r - 1 - r} \prod_{i=1}^{r} (p^i - 1) \pmod{p^m}$$

may also be mentioned.

A word may be added about the additional hypothesis $f^p(x) \equiv f(x^p) \pmod{p^2}$. In general this will, of course, not be satisfied. It is not difficult to show that $f'_0 \equiv 0 \pmod p$ if and only if

$$f(x) \equiv a x_1^{c_1} \dots x_k^{c_k}, \quad a^p \equiv a \pmod{p^2}.$$

5. *A generalization.* The notation (2.3) suggests a possible generalization of the results of §§ 3, 4. Let now Ω denote a commutative ring which contains the integers; in particular then we can define congruences (mod p^m) in Ω. Let a, b denote numbers of Ω such that $a^p \equiv b \pmod p$, which implies

$$a^{p^{m+1}} \equiv b^{p^m} \pmod{p^{m+1}} \quad (m = 0, 1, 2, \dots). \qquad (5.1)$$

We rewrite (5.1) in the form

$$a^{p^{m+1}} = b^{p^m} + p^{m+1} a'_m, \qquad (5.2)$$

and define

$$\Delta a^{p^m} = a'_m = (a^{p^{m+1}} - b^{p^m})/p^{m+1}. \qquad (5.3)$$

Higher derivatives are defined recursively by means of

$$\Delta^{r+1} a^{p^m} = a_m^{(r+1)} = (a_{m+1}^{(r)} a_{m+1} - a_m^{(r)} b_{m+r})/p^{m+1}, \qquad (5.4)$$

where we put $a_m = a^{p^m}$. (For $a=b$, $\Delta^r a^{p^m}$ reduces to $a_{m+1} \dots a_{m+r-1}$ times the r-th Schur derivative (1.1). It is now not difficult to verify that the results of § 3 can be carried over to the general case. In particular (3.3) becomes

$$\Delta^r a^{p^m} = \frac{1}{r!} (a'_m)^r b_m^{e_r - r} \frac{\prod_{i=1}^{r} (p^i - 1)}{(p-1)^r} + \sum_{i=r+1}^{e_r} \frac{1}{i!} p^{(m+1)(i-r)} (a'_m)^i b_m^{e_r - i} U_{r,i}, \qquad (5.5)$$

where e_r has the same meaning as in (3.1) and $U_{r,i} \in \Omega$. Since (5.1) implies

$$a^{hp^{m+1}} \equiv b^{hp^m} \pmod{p^{m+1}}$$

it follows that (3.4) can also be generalized. We have indeed

$$\Delta^r a^{hp^m} = \frac{1}{r!} h^r (a'_m)^r b_m^{he_r - r} \frac{\prod_{i=1}^{r} (p^i - 1)}{(p-1)^r} + \sum_{i=r+1}^{he_r} \frac{1}{i!} p^{(m+1)(i-r)} (a'_m)^i b_m^{he_r - i} U_{r,i,h} \qquad (5.6)$$

valid for $h \geqslant 1$.

https://doi.org/10.1017/S204061850003567X Published online by Cambridge University Press

Finally, using (5.6), we obtain immediate generalizations of the theorems of § 4. We may state

THEOREM 4. *Let* $h \geqslant 1$. *Then* $\Delta^r a^{hp^m} \in \Omega$ *for* $1 \leqslant r \leqslant p-1$.

THEOREM 5. *Let* $h \geqslant 1$. *If* $a_0' \equiv 0 \pmod p$ *then* $\Delta^r a^{hp^m} \in \Omega$ *for all* $r \geqslant 1$, $m \geqslant 0$.

THEOREM 6. *Let* $h \geqslant 1$, $1 \leqslant r \leqslant p$; *then*

$$\Delta^r a^{hp^m} \equiv \frac{1}{r!} h^r (a_m')^r b_m^{he_r - r} \frac{\prod_{i=1}^{r} (p^i - 1)}{(p-1)^r} \pmod{p^m}. \qquad (5.7)$$

If $r < p-1$, *then congruence* (5.7) *holds* $\pmod{p^{m+1}}$.

6. *An application.* As an instance of the generalization, let Ω be the ring of Gaussian integers $a+bi$ and let the prime $p \equiv 3 \pmod 4$. If $\alpha = a+bi \in \Omega$ we put $\bar{\alpha} \doteq a - bi$, so that we have the familiar congruence

$$\alpha^p \equiv \bar{\alpha} \pmod p. \qquad (6.1)$$

In view of (6.1), it is evident that (5.3) and (5.4) become

$$\begin{aligned} \Delta \alpha^{p^m} &= \alpha_m' = (\alpha^{p^{m+1}} - \bar{\alpha}^{p^m})/p^{m+1}, \\ \Delta^{r+1} \alpha^{p^m} &= \alpha_m^{(r+1)} = (\alpha_{m+1}^{(r)} \alpha^{p^{m+1}} - \alpha_m^{(r)} \alpha^{p^{m+r}})/p^{m+1}. \end{aligned} \qquad (6.2)$$

Then Theorems 4 and 5 apply without change, while Theorem 6 yields the congruence

$$\Delta^r \alpha^{hp^m} \equiv \frac{1}{r!} h^r (\alpha_m')^r (\bar{\alpha})^{p^m(he_r - r)} \frac{\prod_{i=1}^{r} (p^i - 1)}{(p-1)^r} \pmod{p^m} \qquad (6.3)$$

for $h \geqslant 1$, $1 \leqslant r \leqslant p$; if $r < p-1$, (5.7) holds $\pmod{p^{m+1}}$.

It is clear how (6.2) and (6.3) can be stated for any quadratic field and how other applications of the same kind can be constructed. We remark that the generalization of the Schur derivative for algebraic numbers in [1, § 4] is of a somewhat different nature from the above.

Finally one can also consider polynomials with coefficients in the Gaussian ring. The starting point is now (compare (1.3))

$$f^p(x) = \bar{f}(x^p) + pg(x),$$

where $\bar{f}(x)$ is obtained by replacing each coefficient of $f(x)$ by its conjugate. It is clear how to modify the definitions (1.5), (1.6). The final results are exactly like those of § 4.

REFERENCES

(1) L. Carlitz., "Some theorems on the Schur derivative," *Pacific Journal of Mathematics*, vol. 3 (1953), pp. 321–332.

(2) I. Schur, "Ein Beitrag zur elementaren Zahlentheorie," *Sitzungaberichte der Preussischen Akademie der Wissenschaften* (1933), pp. 145–151.

(3) M. Zorn, "p-adic analysis and elementary number theory," *Annals of Mathematics* (2) vol. 38 (1937), pp. 451–464.

DUKE UNIVERSITY
DURHAM
NORTH CAROLINA

https://doi.org/10.1017/S204061850003567X Published online by Cambridge University Press