Conspectus materiae tomi XXXVI, fasciculi 4

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange	Address of the Aditorial Board and of the exchange	Die Adresse der Schriftleitung und des Austausches	Адрес редакции и книгообмена

ACTA ARITHMETICA
ul. Śniadeckich 8, 00-950 Warszawa

Les auteurs sont priés d'envoyer leurs manuscrits en deux exemplaires
The authors are requested to submit papers in two copies
Die Autoren sind gebeten um Zusendung von 2 Exemplaren jeder Arbeit
Рукописи статей редакция просит предлагать в двух экземплярах

PRINTED IN POLAND

ISBN 83-01-01331-1 ISSN 0065-1036

WROCŁAWSKA DRUKARNIA NAUKOWA

ACTA ARITHMETICA
XXXVI (1980)

On systems of three quadratic forms

by

SUSAN E. SCHUUR (East Lansing, Mich.)

1. Introduction. In this paper we correct the proof of the following theorem of Birch and Lewis [1]:

THEOREM. *If f_1, f_2, f_3 are quadratic forms in at least* 13 *variables over a* p*-adic field k, where the residue class field k^* has odd characteristic and contains at least* 49 *elements, then f_1, f_2, f_3 have a common non-trivial zero in k.*

The mistake, the omission of several cases, was found in the process of extending the theorem to fields k with smaller residue class field [4]; in fact, the correction and the theorem hold for fields whose residue class field k^* has odd cardinality q greater than or equal to 11.

We refer the reader to the original paper [1] for all notation and for the numbering of the lemmas.

2. The corrections.

LEMMA 16. *If V^* contains a line defined over k^* then V^* has a non-singular point.*

Revised proof. The hypothesis implies that the dimension of the largest linear space contained in V^*, defined over k^*, is at least 1; i.e., $\sigma \geqslant 2$. A suitable nonsingular transformation makes this the space $x_{\sigma+1} = \ldots = x_q = 0$, so that

$$f_i^* = x_1 L_{i1} + \ldots + x_\sigma L_{i\sigma} + g_i \quad (i = 1, 2, 3),$$

where the L's are linear forms and the g's are quadratic forms in $x_{\sigma+1}, \ldots, x_q$.

Suppose the result is not true: suppose that all the points of V^* are singular. In particular $\boldsymbol{e}_1 = (1, 0, 0, \ldots)$ is a singular point of V^*, so there exist $a_1, a_2, a_3 \in k^*$, not all zero, such that

$$a_1 L_{11} + a_2 L_{21} + a_3 L_{31} = 0.$$

If also $a_1 L_{1j} + a_2 L_{2j} + a_3 L_{3j} = 0$ for $j = 2, \ldots, \sigma$ then the proof given in [1] yields the desired contradiction. Otherwise $a_1 L_{1j} + a_2 L_{2j} + a_3 L_{3j} \neq 0$ for some j, say $j = 2$. In this event the set f_1^*, f_2^*, f_3^* is equivalent to the

set $f_1^*, f_2^*, f_3^{*\prime}$, where $f_3^{*\prime} = a_1 f_1^* + a_2 f_2^* + a_3 f_3^* = x_2 L'_{32} + \ldots + x_\sigma L'_{3\sigma} + g'_3$, and $L'_{32} \not\equiv 0$. Following a change of variable we can suppose that $L'_{32} = x_{\sigma+1}$.

Now, e_2 is also a singular point of V^*, so there exist b_1, b_2, b_3, not all zero, such that

$$b_1 L_{12} + b_2 L_{22} + b_3 x_{\sigma+1} = 0.$$

Here b_1 and b_2 cannot both be zero; say $b_2 \neq 0$. Replacing f_2^* by $f_2^{*\prime} = b_1 f_1^* + b_2 f_2^* + b_3 f_3^{*\prime} = x_1 L'_{21} + x_3 L'_{23} + \ldots + x_\sigma L'_{2\sigma} + g'_2$, we obtain a system $f_1^*, f_2^{*\prime}, f_3^{*\prime}$, equivalent to $f_1^*, f_2^*, f_3^{*\prime}$, in which $f_2^{*\prime}$ is free of x_2. Following changes of variable, we have the two cases

(a) $L'_{32} = x_{\sigma+1}, L'_{21} = x_{\sigma+2}$; (b) $L'_{32} = x_{\sigma+1}, L'_{21} = \gamma x_{\sigma+1}$.

(a) In this case

$$\begin{aligned} f_1^* &= x_1 L + x_2 M + Q_1, \\ f_2^* &= x_1 x_{\sigma+2} + Q_2, \\ f_3^* &= x_2 x_{\sigma+1} + Q_3, \end{aligned}$$

where to simplify the notation we have dropped the primes and put

$$L_{11} = L, \quad L_{12} = M, \quad \text{and} \quad x_3 L_{i3} + \ldots + x_\sigma L_{i\sigma} + g_i = Q_i, \quad i = 1, 2, 3.$$

Note that, by replacing x_1 and x_2 by appropriate linear forms $x_1 + ax_3 + bx_4 + \ldots$ and $x_2 + cx_3 + dx_4 + \ldots$, respectively, and then by subtracting appropriate multiples of the resulting f_2^* and f_3^* from f_1^*, we can ensure that L, M, Q_1, Q_2 and Q_3 are free of x_1 and x_2, that L and Q_2 are free of $x_{\sigma+1}$ and that M and Q are free of $x_{\sigma+1}$.

Recall that $\sigma \geqslant 2$, so that, by Lemma 12, $\varrho(f_3^*) \geqslant 5$ and $\varrho(Q_3) \geqslant 3$. Hence if $M \not\equiv 0$, there is a nonsingular zero $\boldsymbol{a} = (a_3, \ldots, a_\sigma, a_{\sigma+2}, \ldots, a_\varrho)$ of Q_3 such that $a_{\sigma+2} M(\boldsymbol{a}) \neq 0$ (by Lemma 5). Taking $a_{\sigma+1} = 0$, $a_\sigma = -Q_2(\boldsymbol{a})/a_{\sigma+2}$, and $a_2 = \big(-a_1 L(\boldsymbol{a}) - Q_1(\boldsymbol{a})\big)/M(\boldsymbol{a})$, we get a nonsingular solution of our system.

A similar argument works if $M \equiv 0$ but $L \not\equiv 0$. If $L \equiv M \equiv 0$ let $\boldsymbol{a} = (a_3, \ldots, a_\varrho)$ be a nonsingular zero of Q_1 such that $a_{\sigma+1} a_{\sigma+2} \neq 0$, take $a_1 = -Q_2(\boldsymbol{a})/a_{\sigma+2}$ and $a_2 = -Q_3(\boldsymbol{a})/a_{\sigma+1}$. The point so obtained is a nonsingular point of V^*.

(b) We have

$$\begin{aligned} f_1^* &= x_1 L + x_2 M + Q_1, \\ f_2^* &= \gamma x_1 x_{\sigma+1} + Q_2, \\ f_3^* &= x_2 x_{\sigma+1} + Q_3. \end{aligned}$$

Suppose first that $\gamma = 0$. Then $L \not\equiv 0$, or else the order of the system would be less than ϱ. Hence we can find a non-singular zero $\boldsymbol{a}$ of Q_2 such that $a_{\sigma+1} L(\boldsymbol{a}) \neq 0$. Taking $a_2 = -Q_3(\boldsymbol{a})/a_{\sigma+1}$, $a_1 = \big(-a_2 M(\boldsymbol{a}) - Q_1(\boldsymbol{a})\big)/L(\boldsymbol{a})$ we get a nonsingular point of V^*.

From now on we may suppose $\gamma \neq 0$; dividing $f_2^* = 0$ by γ, we may suppose $\gamma = 1$. Replacing x_1 by $x_1 + ax_3 + bx_4 + \ldots$ and x_2 by $x_2 + cx_3 + dx_4 + \ldots$, and subtracting multiples of f_2^*, f_3^* from f_1^*, we get an equivalent system in which L, M, Q_2, Q_3 are all free of $x_{\sigma+1}$.

If $L \equiv M \equiv 0$ one obtains a nonsingular solution almost exactly as in the last part of case (a); so we assume henceforth that L, M are not both identically zero, say (without loss of generality) $L \not\equiv 0$. Suppose we take $x_{\sigma+1} \neq 0$, $x_1 = -Q_2/x_{\sigma+1}$, $x_2 = -Q_3/x_{\sigma+1}$. Then, substituting into the equation $f_1^* = 0$, we get

$$-LQ_2/x_{\sigma+1} - MQ_3/x_{\sigma+1} + Q_1 = 0$$

so that we need to solve the cubic equation

$$C = LQ_2 + MQ_3 - x_{\sigma+1} Q_1 = 0$$

with $x_{\sigma+1} \neq 0$. Since, as is easily checked,

$$\begin{vmatrix} \partial f_1^*/\partial x_1 & \partial f_1^*/\partial x_2 & \partial f_1^*/\partial x_j \\ \partial f_2^*/\partial x_1 & \partial f_2^*/\partial x_2 & \partial f_2^*/\partial x_j \\ \partial f_3^*/\partial x_1 & \partial f_3^*/\partial x_2 & \partial f_3^*/\partial x_j \end{vmatrix} = -x_{\sigma+1} \partial C/\partial x_j, \quad j = 3, \ldots, \varrho,$$

a nonsingular solution of $C = 0$ with $x_{\sigma+1} \neq 0$ will yield a nonsingular point of V^*.

Now, C contains at least 4 variables, or else the order of f_1^*, f_2^*, f_3^* would be less than 7, contrary to Lemma 12. Hence C has a nontrivial zero in k^*, and so by Theorem 2 of [3] it has a nonsingular zero with $x_{\sigma+1} \neq 0$, unless $x_{\sigma+1} | C$. But if $x_{\sigma+1} | C$, then $x_{\sigma+1} | (LQ_2 + MQ_3)$, and since $LQ_2 + MQ_3$ is free of the variable $x_{\sigma+1}$, we have

$$LQ_2 + MQ_3 \equiv 0.$$

Hence $L | MQ_3$, and since Q_3 does not factor over k^*, $L | M$. Say $M = \alpha L$. Then we have

$$L(Q_2 + \alpha Q_3) \equiv 0$$

so

$$Q_2 + \alpha Q_3 \equiv 0,$$

but then $f_2^* + \alpha f_3^* = x_{\sigma+1}(x_1 + \alpha x_2)$, contradicting the Corollary to Lemma 12. It follows that the required nonsingular solution exists, and the proof is complete.

LEMMA 17. *If V^* contains a planar conic defined over k^*, then V^* has a nonsingular point.*

Revised proof. We assume that V^* has only singular points and obtain a contradiction. By the preceding lemma, we can suppose that V^* does not contain a line. After a change of variable we can assume that

$x_2^2 = x_1x_3$ is the equation of the conic contained in V^*; then each of the forms $f_i^*(x_1, x_2, x_3, 0, \ldots, 0)$ is proportional to $x_2^2 - x_1x_3$. Hence we can make a change of basis of Λ^* so that

$$\begin{aligned} f_1^* &= x_2^2 - x_1x_3 + x_1L_1 + x_2L_2 + x_3L_3 + g_1, \\ f_2^* &= x_1M_1 + x_2M_2 + x_3M_3 + g_2, \\ f_3^* &= x_1N_1 + x_2N_2 + x_3N_3 + g_3, \end{aligned}$$

where the L's, M's and N's are linear forms and the g's are quadratic forms in $x_4, \ldots, x_q$. As a further simplification, if we replace x_1 by $x_1 + L_3$, x_3 by $x_3 + L_1$, and x_2 by $x_2 - \frac{1}{2}L_2$, we can assume that the L's are identically zero.

For all s, t in k^*, $(s^2, st, t^2, 0, \ldots, 0)$ is a point of V^*, which must be singular. In particular, $\boldsymbol{e}_1$ is a point of this form, so the Jacobian $J(\boldsymbol{e}_1)$ has rank < 3. It follows that there exist μ, ν in k^* such that $\mu M_1 + \nu N_1 = 0$; again changing our basis for Λ^*, we may suppose that N_1 is identically zero. A similar argument using the point $\boldsymbol{e}_3$ shows that one of M_3, N_3 can be assumed to be identically zero, though we are no longer free to specify which one.

We now divide the proof into cases, according to the dimension of the linear space $\langle N_2, N_3\rangle$ generated by N_2 and N_3.

(a) $\dim\langle N_2, N_3\rangle = 0$. This is the case considered in [1]. One obtains the desired contradiction provided $q \geqslant 11$.

(b) $\dim\langle N_2, N_3\rangle = 2$. We can assume without loss of generality that $N_2 = x_4$, $N_3 = x_5$, so that $f_3^* = x_2x_4 + x_3x_5 + g_3$ and $M_3 \equiv 0$. Since $(s^2, st, t^2, 0, \ldots, 0)$ is a singular point of V^* for all s, t, every 3×3 minor of the Jacobian $J(s^2, st, t^2, 0, \ldots, 0)$ has determinant 0. Considering the minors formed from columns 2, 4 and j, $j \geqslant 6$, we have $-2s^2t^2(s^2\,\partial M_1/\partial x_j + st\,\partial M_2/\partial x_j) = 0$ for all $s, t \in k^*$ and all $j \geqslant 6$. Hence

$$s\,\partial M_1/\partial x_j + t\,\partial M_2/\partial x_j = 0 \qquad (j \geqslant 6)$$

for all $s, t \neq 0$. But then by Lemma 4

$$\partial M_1/\partial x_j = \partial M_2/\partial x_j = 0,$$

for $j \geqslant 6$. Further, taking the determinant of the minor formed from columns 2, 4 and 5, we obtain

$$2s^2t^2[t^2\,\partial M_2/\partial x_4 + st(\partial M_1/\partial x_4 - \partial M_2/\partial x_5) - s^2\,\partial M_1/\partial x_5] = 0$$

for all $s, t \in k^*$, whence

$$\partial M_2/\partial x_4 = 0, \qquad \partial M_1/\partial x_5 = 0, \qquad \partial M_1/\partial x_4 = \partial M_2/\partial x_5$$

since $q \geqslant 5$. It follows that

$$M_1 = ax_4, \qquad M_2 = ax_5.$$

If $a = 0$ then we have $M_1 \equiv M_2 \equiv M_3 \equiv 0$, and we are back in case (a). Thus we may suppose $a \neq 0$, and we may divide f_2^* by a. Then we have

$$\begin{aligned} f_1^* &= x_2^2 - x_1x_3 + g_1, \\ f_2^* &= x_1x_4 + x_2x_5 + g_2, \\ f_3^* &= x_2x_4 + x_3x_5 + g_3. \end{aligned}$$

If we write $g_2 = x_5S + h$, where h is a form in $x_4, x_6, x_7, \ldots, x_q$, then $h \not\equiv 0$; for if $h \equiv 0$, then $f_2^* = x_1x_4 + x_5(x_2 + S)$, contrary to the corollary to Lemma 12. Hence for $q \geqslant 5$ there exist points not on $x_4h = 0$. Now take $a_5 = 0$; choose $a_4, a_6, \ldots, a_q$ such that $a_4h \neq 0$; and take $a_2 = -g_3/a_4$, $a_1 = -g_2/a_4 = -h/a_4$, and $a_3 = (a_2^2 + g_1)/a_1 = -a_4(a_2^2 + g_1)/h$. The result is a nonsingular point of V^*.

(c) $\dim\langle N_2, N_3\rangle = 1$. In this case we can assume, after a change of variable, that

$$N_2 = cx_4, \qquad N_3 = dx_4,$$

where at least one of c, d is not zero. We still have rank $J(s^2, st, t^2, 0, \ldots, 0) < 3$, whence

$$\begin{aligned} st^2[s^3c\,\partial M_1/\partial x_j + s^2t(c\,\partial M_2/\partial x_j + d\,\partial M_1/\partial x_j) + \\ + st^2(c\,\partial M_3/\partial x_j + d\,\partial M_2/\partial x_j) + t^3d\,\partial M_3/\partial x_j] = 0 \end{aligned}$$

for all $s, t \in k^*$ and all $j > 4$. (This is the determinant of columns 2, 4 and j of $J(s^2, st, t^2, 0, \ldots, 0)$.) Hence

$$c\,\partial M_1/\partial x_j = c\,\partial M_2/\partial x_j + d\,\partial M_1/\partial x_j = c\,\partial M_3/\partial x_j + d\,\partial M_2/\partial x_j = d\,\partial M_3/\partial x_j = 0 \qquad (j > 4).$$

It follows that $M_1 = ax_4$, $M_2 = bx_4$, $M_3 = ux_4$, and we can assume that at least one of a, b, u is not zero or else we would be back in case (a). We have

$$\begin{aligned} f_1^* &= x_2^2 - x_1x_3 + g_1, \\ f_2^* &= ax_1x_4 + bx_2x_4 + ux_3x_4 + g_2, \\ f_3^* &= cx_2x_4 + dx_3x_4 + g_3. \end{aligned}$$

In studying this system it is convenient to consider separately the two (inequivalent) cases $d = 0$ and $d \neq 0$; however, as the arguments are quite similar, we shall give the proof only for the case $d = 0$.

If $d = 0$, then $c \neq 0$, and we can divide f_3^* by c to make the coefficient of x_2x_4 equal to 1. Subtracting a multiple of f_3^* from f_2^*, we can make b equal to 0. Finally, we can assume $a \neq 0$ (and thus $a = 1$) because x_1 and x_3 can be permuted without changing the shape of f_1^*, f_2^*, f_3^*. Hence we have $f_2^* = x_1x_4 + ux_3x_4 + g_2$ and $f_3^* = x_2x_4 + g_3$.

Now take $x_4 \neq 0$, $x_2 = -g_3/x_4$ and $x_1 = -ux_3 - g_2/x_4$. Substituting in the equation $f_1^* = 0$, we find that we need to solve

$$G = ux_4^2x_3^2 + (x_4g_2)x_3 + g_1x_4^2 + g_3^2 = 0$$

nonsingularly with $x_4 \neq 0$. This equation, considered as a quadratic in x_3, has discriminant

$$\Delta = x_4^2\left(g_2^2 - 4u(g_1x_4^2 + g_3^2)\right).$$

Suppose there exist $a_4, \ldots, a_q$ such that $a_4 \neq 0$ and $\Delta(a_4, \ldots, a_q)$ is a nonzero square. Then $G = 0$ is solvable with $x_4 \neq 0$; and furthermore $\partial G(\boldsymbol{a})/\partial x_3 = 2ua_4^2a_3 + a_4g_2 = \pm\sqrt{\Delta}$, so the solution is nonsingular. Hence we may suppose $\Delta(\boldsymbol{a})$ is zero or a nonsquare whenever $a_4 \neq 0$. Thus for each choice of $a_6, \ldots, a_q \in k^*$, the equation

$$\eta\,\Delta(1, x_5, a_6, \ldots, a_q) = y^2$$

(where η is a nonsquare of k^*) has at least $4 + 2(q-4) = 2q-4$ solutions (x_5, y) in k^*. It follows (see Hasse [2], and the proof of Theorem 2 of [3]) that either

$$|2q - 4 + 1 - q| \leqslant 2\sqrt{q}$$

or

$$\Delta = \eta R^2,$$

R a quadratic form. The inequality cannot hold for $q \geqslant 11$. Hence

$$\Delta = x_4^2\left(g_2^2 - 4u(g_1x_4^2 + g_3^2)\right) = \eta R^2,$$

so there is a quadratic form Q such that

$$g_2^2 - 4u(g_1x_4^2 + g_3^2) = \eta Q^2,$$

or

$$g_2^2 - \eta Q^2 = 4u(g_1x_4^2 + g_3^2).$$

Now if we write $g_2 = x_4L_2 + Q_2$, $g_3 = x_4L_3 + Q_3$, $Q = x_4L' + Q'$, where the L's are linear forms in $x_4, \ldots, x_q$ and the Q's are quadratic forms in $x_5, \ldots, x_q$, and if we set $x_4 = 0$ in the last equation, we still have an identity:

$$Q_2^2 - \eta Q'^2 = 4uQ_3^2.$$

We show that this identity cannot hold by considering what happens to it over the extension field $k^*(\eta^{1/2})$. Recall that $f_3^* = x_4(x_2 + L_3) + Q_3$, so that $\varrho(Q_3) \geqslant 2$ and Q_3 is irreducible over k^*. If $\varrho(Q_3) \geqslant 3$, then Q_3 is irreducible over $k^*(\eta^{1/2})$ as well, while $Q_2^2 - \eta Q'^2$ factors into two quadratic factors,

$$Q_2^2 - \eta Q'^2 = (Q_2 - \eta^{1/2}Q')(Q_2 + \eta^{1/2}Q');$$

so Q_3 divides one of these factors, say

$$Q_2 - \eta^{1/2}Q' = \gamma Q_3, \qquad \gamma \in k^*(\eta^{1/2}).$$

Write $\gamma = \gamma_1 + \eta^{1/2}\gamma_2$. Then

$$(\gamma_1Q_3 - Q_2) + \eta^{1/2}(\gamma_2Q_3 + Q') = 0.$$

But $\gamma_1Q_3 - Q_2$ and $\gamma_2Q_3 + Q'$ have coefficients in k^*, so this implies

$$\gamma_1Q_3 = Q_2 \quad \text{and} \quad \gamma_2Q_3 = -Q'.$$

The first of these two equations is enough to yield a contradiction. We have

$$\begin{aligned}\gamma_1f_3^* - f_2^* &= \gamma_1x_4(x_2 + L_3) + \gamma_1Q_3 - (x_1x_4 + ux_3x_4 + x_4L_2 + Q_2)\\ &= x_4(\gamma_1x_2 + \gamma_1L_3 - x_1 - ux_3 - L_2),\end{aligned}$$

which is impossible by the Corollary to Lemma 12.

There remains the possibility that $\varrho(Q_3) = 2$. In that case, since Q_3 is irreducible over k^*, we must have

$$Q_3 = L^2 - \eta M^2,$$

where L and M are nonproportional linear forms. Then, over $k^*(\eta^{1/2})$, we have

$$(Q_2 - \eta^{1/2}Q')(Q_2 + \eta^{1/2}Q') = 4u(L - \eta^{1/2}M)^2(L + \eta^{1/2}M)^2.$$

Suppose $(L - \eta^{1/2}M) \mid (Q_2 - \eta^{1/2}Q')$. (Essentially the same argument works if $(L - \eta^{1/2}M) \mid (Q_2 + \eta^{1/2}Q')$.) If also $(L + \eta^{1/2}M) \mid (Q_2 - \eta^{1/2}Q')$, then $Q_3 \mid (Q_2 - \eta^{1/2}Q')$, and we get the contradiction as above. Hence we may suppose

$$Q_2 - \eta^{1/2}Q' = \gamma(L - \eta^{1/2}M)^2 = (\gamma_1 + \eta^{1/2}\gamma_2)(L - \eta^{1/2}M)^2.$$

Upon simplifying this equation, we obtain

$$(Q_2 - \gamma_1L^2 + 2\eta\gamma_2LM - \eta\gamma_1M^2) + \eta^{1/2}(-Q' - \gamma_2L^2 + 2\gamma_1LM - \eta\gamma_2M^2) = 0.$$

It follows, in particular, that

$$Q_2 = \gamma_1L^2 - 2\eta\gamma_2LM + \eta\gamma_1M^2,$$

whence

$$\gamma_1f_3^* - f_2^* = x_4(\gamma_1x_2 + \gamma_1L_3 - x_1 - ux_3 - L_2) + M(-2\eta\gamma_1M + 2\eta\gamma_2L),$$

an impossibility (by the Corollary to Lemma 12).

This completes the proof.

3. Remarks. As noted in the Introduction, the rest of Birch and Lewis's proof can also be extended to $q \geqslant 11$ (although we only had $q \geqslant 17$ in [4]). One has to consider many cases, and in some places the computations are quite lengthy, but the arguments are similar to those used here. We also showed in [4] that a system of three quadratic forms in at least 31 variables has a nontrivial zero in k for $q \geqslant 3$.

References

[1] B. J. Birch and D. J. Lewis, *Systems of three quadratic forms*, Acta Arith. 10 (1965), pp. 423–442.

[2] H. Hasse, *Vorlesungen über Zahlentheorie*, Berlin 1950.

[3] D. J. Lewis and S. E. Schuur, *Varieties of small degree over finite fields*, J. Reine Angew. Math. 262/263 (1973), pp. 293–306.

[4] S. E. Schuur, *Systems of quadratic forms over local fields*, Dissertation, University of Michigan, Ann Arbor 1969.

DEPARTMENT OF MATHEMATICS
MICHIGAN STATE UNIVERSITY

Received on 6. 4. 1977
and in revised form on 2. 1. 1978 (933)

ACTA ARITHMETICA
XXXVI (1980)

Equivalence classes of sets of functions over a finite field

by

GARY L. MULLEN (Sharon, Penn.)

1. Introduction. In [3] and [6] S. Cavior and the author studied properties of left equivalence of functions over a finite field. In [4] S. Cavior extended the notion of left equivalence to sets of functions. In the present paper we study a further generalization of left equivalence of functions over a finite field.

In Section 2 we develop a notion of left equivalence which generalizes all of the forms of left equivalence studied in [3], [4], and [6]. In particular, we consider left equivalence of sets of functions over a finite field relative to arbitrary groups of permutations. Moreover, we show that many of the results in this general setting can be reduced to the single function case, which was studied in detail in [6].

Let $K = \mathrm{GF}(q)$ denote the finite field of order q and K^r $(r \geqslant 1)$ the product of r copies of K. Let $K[x_1, \ldots, x_r] = K[\bar{x}]$ represent the ring of polynomials in r indeterminates over K. By the Lagrange Interpolation Formula ([5], p. 55), each function from K^r into K can be expressed uniquely as a polynomial of degree $< q$. The group of all permutations of K will be represented by Φ so that Φ is isomorphic to S_q. That Ω is an arbitrary subgroup of Φ will be denoted by $\Omega < \Phi$ and $|\Omega|$ will denote the order of Ω.

2. General theory. If $k \geqslant 1$ is a positive integer the k-tuple of functions $(f_1, \ldots, f_k)$ will be denoted by (f_i) so that there are a total of q^{kq^r} distinct k-tuples of functions each containing k functions.

DEFINITION 2.1. Let $\Omega_1, \ldots, \Omega_k < \Phi$. Then (f_i) is *left equivalent* to (g_i) relative to $\Omega_1, \ldots, \Omega_k$ if there exist $\varphi_i \in \Omega_i$ such that $\varphi_i f_i = g_i$ for $i = 1, \ldots, k$.

This is clearly an equivalence relation which, if $k = 1$, reduces to that of the author in [6]. If $k = 1$ and $\Omega_1 = \Phi$, we obtain the left equivalence considered by Cavior in [3]. If $k \geqslant 1$ and $\Omega_i = \Phi$ for $i = 1, \ldots, k$, then Definition 2.1 reduces to that of Cavior in [4].

As an illustration, consider the case where $K = \mathrm{GF}(5)$, $r = 1$, and $k = 2$. Suppose that in cyclic notation $\varphi_1 = (01)$ and $\varphi_2 = (234)$. For