BULL. AUSTRAL. MATH. SOC.
VOL. 20 (1979), 321-344.

20N05

Stein quasigroups II: algebraic aspects

M.J. Pelling and D.G. Rogers

This paper furthers the foundation of the theory of quasigroups obeying the law $x(xy) = yx$ by studying their algebraic properties. Much information is obtained by analysing the cycle decomposition of left translations regarded as permutations, and other results are obtained by representation in terms of abelian groups with an operation.

1. Definitions and elementary properties

Our paper [5] considered quasigroups obeying the law $x(xy) = yx$, also known as Stein quasigroups or systems, from a combinatorial viewpoint: in this sequel we explore their algebraic properties. The main achievement is perhaps the analysis, in Section 3, of medial Stein systems - that is those obeying the medial law $(xy)(zt) = (xz)(yt)$. This section also contains results on canonical forms for abelian groups with an automorphism which are of interest in their own right.

Elementary consequences of the defining law are idempotence, $xx = x$, and anticommutativity, $xy = yx \Rightarrow x = y$, and while the associative law can not hold universally except in the trivial system of order 1 (since an idempotent group is trivial) we do have the special case $x(yx) = (xy)x$. The cartesian product of Stein systems is also a Stein system. Less trivial is the following theorem.

THEOREM 1. *If S is a finite Stein system with a proper subsystem T then $|S| \geq 3|T| + 1$.*

Received 21 February 1978.

Proof. Let $a \in S\backslash T$. Since T is a subsystem, for any $x \in T$ there exists $b_x \in S\backslash T$, $b_x \neq a$, such that $b_x x = a$, and then $c_x \in S\backslash T$, $c_x \neq a, b_x$, such that $xb_x = b_x a = c_x$.

Let $y \in T$, $y \neq x$. Then $b_x x = b_y y$ implies $b_x \neq b_y$, and hence $c_x \neq c_y$. Further, if $b_x = c_y$ then

$$(c_y y)b_x = (c_y y)c_y = c_y(yc_y) = c_y(y(yb_y)) = c_y(b_y y)$$
$$= c_y a = b_x(b_x x) = xb_x \Rightarrow c_y y = x \Rightarrow c_y \in T$$

which is a contradiction.

So for any choice of $x, y \in T$, $b_x \neq c_y$, and it follows that the set T , $\{b_x \mid x \in T\}$, $\{c_x \mid x \in T\}$, $\{a\}$ are all disjoint; so $|S| \geq 3|T| + 1$. //

COROLLARY. *There are no Stein systems of orders* 2 *and* 3 . *For in the theorem, if* $|S| > 1$ *one may always take* $|T| = 1$ *and deduce* $|S| \geq 4$.

Cases when equality holds in the theorem are discussed in [5]. Note also that any Stein system S such that $|S| < 13$ must be *minimal*; that is there are no non-trivial proper subsystems.

The notions of homomorphism, endomorphism, isomorphism, automorphism of Stein systems are defined in the usual way. Thus we have the following definition and theorem, whose proof, being elementary, is omitted.

DEFINITION. If S and K are Stein systems then a *homomorphism* f of S to K is a map $f : S \to K$ such that $f(xy) = f(x)f(y)$ for all x, y in S .

THEOREM 2. *If* $f : S \to K$ *is a homomorphism of Stein systems and* B *is any subsystem of* K *then* $f^{-1}(B)$ *is a (possibly empty) subsystem of* S . *In particular if* $a \in f(S)$ *then* $f^{-1}(\{a\})$ *is a non-empty subsystem of* S .

Any homomorphism f *of* S *defines an equivalence relation* R *on* S *by* $xRy \iff f(x) = f(y)$, *with the property that* xRy & $uRv \Rightarrow (xu)R(yv)$. *Conversely given an equivalence relation* R *with this property then if*

https://doi.org/10.1017/S0004972700011059 Published online by Cambridge University Press

$[x]$ denotes the equivalence class of $x \in S$, the set of equivalence classes becomes a Stein system, denoted S/R, on defining $[x][y] = [xy]$, and the map $x \to [x]$ is a homomorphism of S onto S/R. Further if $f : S \to K$ is an onto homomorphism with associated equivalence relation R then $K \simeq S/R$ and the map $[x] \to f(x)$ is an isomorphism.

EXAMPLE. Let Z_4 be the cyclic group of order 4 and let $S = Z_4 \oplus Z_4$ with quasigroup multiplication defined by $\overline{x} = (x_1, x_2)$, $\overline{y} = (y_1, y_2)$, $\overline{x}.\overline{y} = T^2\overline{x} + T\overline{y}$ where $T\overline{x} = (x_2, x_1 - x_2)$. Then S is a Stein system of order 16 ($S \simeq J(16)$ in the notation of Section 3) and $\overline{x} \to 2\overline{x}$ defines a homomorphism f of S onto a subsystem K ($\simeq J(4)$) of order 4. As a runs through the elements of K, $f^{-1}(\{a\})$ runs through four disjoint subsystems of S all isomorphic to K. Thus the equivalence classes composing S/R are actually subsystems of S, as is the case generally.

An important technique in the study of finite Stein systems is the analysis of the cycle decomposition of a left translation $x \to ax$ regarded as a permutation P_a of $S\backslash\{a\}$, where a is a given element of the system S. The notation $P_a = [m_1] + [m_2] + \ldots + [m_k]$ will mean that P_a has a decomposition into cycles of lengths $m_1, m_2, \ldots, m_k$. For example the system $J(16)$ above has $P_a = [3] + [6] + [6]$ for any a, while its subsystem $J(4)$ has $P_a = [3]$ for all a. The cycle decomposition can be different for different a (see, for example, Section 6), and a system for which P_a is a single cycle for at least one a will be called *cyclic*.

2. The analysis of cycles in P_a

THEOREM 3. *Let S be a finite Stein system, $|S| > 1$. Then*

(i) for any $a \in S$ the length of a cycle in P_a is at least 3,

(ii) if $(x_0 x_1 \ldots x_{k-1})$ is a cycle in P_a of length k, the

https://doi.org/10.1017/S0004972700011059 Published online by Cambridge University Press

$ax_i = x_{i+1}$, $x_i a = x_{i+2}$, $x_i x_{i+2} = x_{i+1}$,

$x_i x_{i+1} = x_{i+2} x_i$, *suffices being reduced modulo* k ,

(iii) if P_a *has a cycle* C *of length* k *where* $k = 3$ *or* $k = 4$, *then* $C \cup \{a\}$ *is a subsystem of* S *of order* $k + 1$.

Proof. Given $a \in S$ suppose $b \neq a$. Then $P_a(b) = ab$, $P_a^2(b) = a(ab) = ba$, and by introductory remarks in Section 1, b, ab, ba are all distinct. This proves *(i)*.

For *(ii)*, by definition of P_a , $ax_i = x_{i+1}$ so

$$x_i a = a(ax_i) = ax_{i+1} = x_{i+2} .$$

Also

$$x_i x_{i+2} = x_i(x_i a) = ax_i = x_{i+1} ,$$

and

$$x_i x_{i+1} = x_i(x_i x_{i+2}) = x_{i+2} x_i .$$

For *(iii)*, suppose first P_a has a 3-cycle $C = (x_0 x_1 x_2)$. Then, by *(ii)*,

$$x_i a = x_{i+2} = x_{i+1} x_{i+3} = x_{i+1} x_i = x_i(x_i x_{i+1}) \Rightarrow x_i x_{i+1} = a .$$

Using *(ii)*, it follows that $C \cup \{a\}$ is closed under the quasigroup operation, and so constitutes a subsystem of order 4 .

If P_a has a 4-cycle $C = (x_0 x_1 x_2 x_3)$, then

$$x_i x_{i+1} = x_{i+2} x_i = x_{i-2} x_i = x_{i-1} = x_{i+3}$$

and

$$x_i a = x_{i+2} = x_{i-1} x_i = x_{i+3} x_i = x_i(x_i x_{i+3}) ,$$

so that $x_i x_{i+3} = a$. Thus again $C \cup \{a\}$ is closed under the quasigroup operation, and forms a subsystem of order 5 . //

The method of proof also shows that there do exist unique (up to

https://doi.org/10.1017/S0004972700011059 Published online by Cambridge University Press

isomorphism) systems of orders 4 and 5 which in conformity with Section 3 we denote $J(4)$, $J(5)$ respectively. These systems are cyclic, minimal, medial, and have sharply 2-transitive automorphism groups - see Sections 3 and 5.

A P_a cycle C is said to be *self-reciprocating* (relative to a) if x, y exist in C with $xy = a$. The following theorem describes the basic properties of self-reciprocating cycles.

THEOREM 4. *In a finite Stein system S suppose P_a has a self-reciprocating cycle $C = (x_0 x_1 \ldots x_{m-1})$ of length m. Then*

(i) if m is odd, $m = 3$, and the only cyclic system of even order is $J(4)$;

(ii) if $m = 2k$ is even and $x_0 x_i = a$ then, if i is even k is odd, $i = k + 1$ and $x_j x_{j+k+1} = a$, $x_{j+k+1} x_j = x_{j+2}$ for all even j;

(iii) if $m = 2k$ and $x_0 x_i = a$ with i odd, the relations $x_j x_{j+i} = a$, $x_{j+1} x_j = x_{j+2}$ hold for j even, and the relations $x_j x_{j+2-i} = a$, $x_{j+2-i} x_j = x_{j+2}$ hold for j odd.

Proof. With no assumptions about the parities of m and i, if $x_0 x_i = a$ then $x_i x_0 = x_0(x_0 x_i) = x_0 a = x_2$, $x_i x_2 = x_i(x_i x_0) = x_0 x_i = a$. Repeating this argument starting from $x_i x_2 = a$ it follows $x_2 x_{i+2} = a$, and so iterating,

(1) $$x_{2t} x_{i+2t} = a, \quad x_{i+2t} x_{2+2t} = a \quad \text{for all } t.$$

If m is odd then $2t$ runs through all residues (mod m), so in particular

$$x_i x_{2i} = a = x_i x_2 \Rightarrow x_{2i} = x_2 \Rightarrow 2i \equiv 2 \pmod{m} \Rightarrow i = 1.$$

But then $x_0 x_1 = a$, $x_0 a = x_2$, $x_0 x_2 = x_1$, which means that P_{x_0} has a 3-cycle $(x_1 a x_2)$ so that, by Theorem 3 *(iii)*, $\{a, x_0, x_1, x_2\}$

https://doi.org/10.1017/S0004972700011059 Published online by Cambridge University Press

constitutes a $J(4)$ subsystem and $m = 3$.

If $m = 2k$ and i are even then taking $2t = i$ in (1), $x_i x_{2i} = a$ whence $2i \equiv 2 \pmod{2k}$ so that $i = 1$ or $i = k + 1$. But, as before, $i = 1$ leads to $m = 3$, which is impossible, and so $i = k + 1$. Part *(ii)* now follows on putting $2t = j$ in (1) and noting that

$$x_{j+k+1}x_j = x_j(x_j x_{j+k+1}) = x_j a = x_{j+2} .$$

Part *(iii)* follows similarly from (1). //

COROLLARY. *If* $m = 2k > 4$ *then* $i \neq 1, 3, 2k-1$. *In particular a self-reciprocating cycle of length* 6 *is impossible.*

Proof. If $i = 1$ then $x_0 x_1 = a$ leads, as above, to $\{a, x_0, x_1, x_2\} = J(4)$, contradicting $m > 4$. If $i = 3$ then $x_0 x_3 = a$, $x_1 x_0 = a$ by part *(iii)*, so that

$$x_1 x_0 = x_0(x_0 x_1) = a = x_0 x_3 \Rightarrow x_0 x_1 = x_3 .$$

But then P_{x_0} has a 4-cycle $(x_1 x_3 a x_2)$, whence $\{a, x_0, x_1, x_2, x_3\} = J(5)$, contradicting $m > 4$.

If $i = 2k - 1$ then, by part *(iii)* with $j = 2$, $x_1 x_2 = x_4$. But by Theorem 3 *(ii)*, $x_1 x_2 = x_3 x_1 = x_4 = x_3 x_5 \Rightarrow x_1 = x_5$, again contradicting $m > 4$.

If $C = (x_0 x_1 x_2 x_3 x_4 x_5)$ were self-reciprocating of length 6 and $x_0 x_i = a$ then by the preceding, i is not odd whence, by part *(ii)*, $i = k + 1 = 4$. Taking $j = 0$ in part *(ii)*, $x_4 x_0 = x_2 = x_4 x_6 = x_5$, a contradiction since $x_2 \neq x_5$. So C can not exist. //

If S were a system of order 9 then, since S must be minimal, P_a can have no cycles of length less than or equal to 4 and thus comprises a single cycle of length 8 , which must of course be self-reciprocating. Part *(iii)* of the preceding theorem and corollary are then applicable to deduce that if $(x_0 x_1 \ldots x_7)$ is the cycle then $x_j x_{j+5} = a$, $x_j x_{j+3} = x_{j+5}$ for all j , and with this information it is easy to

https://doi.org/10.1017/S0004972700011059 Published online by Cambridge University Press

complete in a unique and consistent way the multiplication table for S. This unique system of order 9, denoted $J(9)$, is cyclic, minimal, medial, and has a sharply 2-transitive automorphism group - see also Sections 3 and 5.

It may also be conjectured that in general if C is a self-reciprocating cycle in P_a of length 8 then $C \cup \{a\}$ forms a $J(9)$ subsystem though we have not been able to prove this. It is true if one assumes the system is left-distributive.

In the case where $xy = a$ with x, y in different cycles of P_a the following theorem may be proved by similar methods - we omit the details of the proof.

THEOREM 5. *Let* P_a *have disjoint cycles* $(x_0x_1 \ldots x_{m-1})$ *and* $(y_0y_1 \ldots y_{m'-1})$ *of lengths* m, m' *respectively, and suppose* $x_0y_0 = a$. *Then*

(i) if m, m' *are both even,* $m = m'$ *and* $x_{2i}y_{2i} = y_{2i}x_{2i+2} = a$, $y_{2i}x_{2i} = x_{2i+2}$, $x_{2i+2}y_{2i} = y_{2i+2}$ *for all* i,

(ii) if m, m' *are both odd,* $m = m'$ *and* $x_iy_i = y_ix_{i+2} = a$, $y_ix_i = x_{i+2}$, $x_{i+2}y_i = y_{i+2}$ *for all* i,

(iii) if m *is odd and* m' *is even,* $m' = 2m$ *and* $x_{2i}y_{2i} = y_{2i}x_{2i+2} = a$, $y_{2i}x_{2i} = x_{2i+2}$, $x_{2i+2}y_{2i} = y_{2i+2}$ *for all* i.

The preceding theorems can now be used to prove the non-existence of Stein systems of certain orders.

THEOREM 6. *There are no Stein systems of orders* 6, 7, 8, 10, 12, 14.

Proof. Orders 6, 7, 8, 10 are ruled out because P_a could have no cycles of length less than or equal to 4 and thus would consist of a single self-reciprocating cycle of length 5, 6, 7, 9 respectively. Such cycles can not exist by Theorem 4 and corollary.

https://doi.org/10.1017/S0004972700011059 Published online by Cambridge University Press

If S were of order 12 then S would be minimal so again P_a has no cycles of length less than or equal to 4. Thus $P_a = [11]$ or $P_a = [5] + [6]$ which are ruled out by Theorems 4 *(i)* and 5 *(iii)*.

If S were of order 14 then P_a can not have a cycle of length 4 since $14 < 3.5 + 1$ but conceivably cycles of length 3 could occur. The possibilities $P_a = [13]$, $[5] + [8]$, $[6] + [7]$, $[3] + [3] + [7]$ are ruled out by Theorems 4 *(i)* and 5 *(iii)* which leaves $[3] + [10]$ and $[3] + [5] + [5]$. It follows that each element of S would be contained in exactly one $J(4)$ subsystem: these subsystems would therefore be disjoint which is impossible since 4 does not divide 14. //

As regards other systems of low order it is easy to show that the cycle decomposition for a system of order 11 must be $[10]$ or $[5] + [5]$. Both are possible and by tedious construction of the multiplication tables one can show that there are precisely two systems of order 11, denoted $J(11, 7)$, $J(11, 3)$ respectively. These are medial and minimal with sharply 2-transitive automorphism groups (see Sections 3 and 5).

It seems unlikely that a system of order 15 exists - if it does P_a must have cycle decomposition $[14]$ or $[7] + [7]$ or $[3] + [3] + [8]$ and the last case can not occur for every a. It also seems unlikely that a system of order 18 exists. For further information about the spectrum see reference [5].

3. Medial Stein systems

In this section we consider Stein systems obeying the medial law ML : $(xy)(zt) = (xz)(yt)$. It is known [6] that for quasigroups the modular law ML' : $x(yz) = z(yx)$ implies ML, and in the case of Stein systems the converse is true: for given x, y, z we have $x = yx_1$, $z = yz_1$ for some x_1, z_1, and

$$x(yz) = (yx_1)(y(yz_1)) = (yx_1)(z_1y) = (yz_1)(x_1y) = z(y(yx_1)) = z(yx) .$$

Also, if a quasigroup is idempotent and obeys ML' then it is a Stein system since $x(xy) = y(xx) = yx$. Any quasigroup which is medial and

https://doi.org/10.1017/S0004972700011059 Published online by Cambridge University Press

idempotent is left and right distributive [6], and although the converse is not true in general, we do not know any Stein system which is left distributive but fails to be medial. However, by a result of Fischer [1] a left distributive minimal finite Stein system would be medial.

By Murdoch's result [3] on medial quasigroups with an idempotent Stein systems which are medial can be characterised in terms of abelian groups.

THEOREM 7. *Let S be a medial Stein system and $a \in S$ and let $T = T_a$ be the left translation by a, $Tx = ax$. Then there is a binary operation $+ = +_a$ on S which converts S into an abelian group $S(a)$ in which a is the group zero and T an automorphism of $S(a)$ satisfying*

$$T^2 + T = 1 , \tag{2}$$

and such that the quasigroup multiplication on S is given by $xy = T^2x + Ty$. Conversely this equation defines a medial Stein system, given any abelian group and automorphism satisfying (2). The groups $S(a)$ with automorphism T_a are all operator isomorphic for different choices of a.

Proof. Since S is left distributive, $T(xy) = (Tx)(Ty)$, and since S is a quasigroup, T has an inverse T^{-1}. Define $+$ on $S \times S$ by $x + y = (T^{-2}x)(T^{-1}y)$. Then

$$x + y = (T^{-2}x)(a(T^{-2}y)) = (T^{-2}y)(a(T^{-2}x)) = y + x$$

by ML', so that $+$ is commutative. Also

$$x + (y+z) = (T^{-2}x).T^{-1}((T^{-2}y)(T^{-1}z)) = (T^{-2}x).((T^{-3}y)(T^{-2}z))$$
$$= (T^{-2}z)((T^{-3}y)(T^{-2}x)) = z + (y+x) = (x+y) + z$$

using ML' and commutativity of $+$, so that $+$ is associative.

Since $x + a = a + x = (T^{-2}a)(T^{-1}x) = a(T^{-1}x) = x$ and since the equation $x + y = a \iff (T^{-2}x)(T^{-1}y) = a \iff (T^{-1}x)y = a$ always has a solution for y given x, it follows that under $+$, S is an abelian group $S(a)$ with zero a. Obviously $xy = T^2x + Ty$ and the law $x(xy) = yx$ requires $T^2 + T = 1$.

https://doi.org/10.1017/S0004972700011059 Published online by Cambridge University Press

If $b \neq a$, define $f : S(a) \to S(b)$ by $f(x) = x +_a b$, so that $T_a f T_a^{-1} x = x +_a T_a b$. Then

$$T_b x = bx = T_a^2 b +_a T_a x = T_a x -_a T_a b +_a b = f T_a f^{-1} x ,$$

so that $T_b = f T_a f^{-1}$ and

$$f(x) +_b f(y) = T_b^{-2} f(x) . T_b^{-1} f(y) = f T_a^{-2} x . f T_a^{-1} y = T_a^2 f T_a^{-2} x +_a T_a f T_a^{-1} y$$

$$= x +_a T_a^2 b + y +_a T_a b = x +_a y +_a b = f(x +_a y) .$$

Thus f is an operator isomorphism of $(S(a), T_a)$ and $(S(b), T_b)$. //

In the preceding proof f is an automorphism of S and in fact it is easy to determine $\mathrm{aut}(S)$ in terms of $S(a)$ and T_a. If $g \in \mathrm{aut}(S)$ then $g(x) = h(x) + b$ for some b where h is an automorphism of S leaving a invariant. Then

$$h(xy) = h(x)h(y) \Rightarrow h(T^2 x + Ty) = T^2 h(x) + Th(y) .$$

Putting $x = a$, $h(Ty) = Th(y)$ so that h, T commute, whence $h(x+y) = h(x) + h(y)$ for all $x, y \in S$. Hence $\mathrm{aut}(S)$ is the set of maps $g(x) = h(x) +_a b$ where h is an automorphism of $S(a)$ commuting with T_a. The left translations of S are the maps $x \to T_a x +_a b$ and the group translations $x \to x +_a b$ form a transitive normal subgroup of $\mathrm{aut}(S)$.

If K is a subsystem of S and $a \in K$, then $K(a)$ is a T_a-invariant subgroup of $S(a)$, and conversely. Any other subsystem can be obtained by translating in $S(a)$ a subsystem containing a. Also, as S is medial, one may form [6] the cosets xK, $x \in S$, and the quotient system S/K with multiplication $(xK)(yK) = (xy)K$. In terms of $S(a)$ the coset xK is the group coset $T_a^2 x + K(a)$ and

$$(xK)(yK) = T_a^2(xy) + K(a) = T_a^4 x + T_a^3 y + K(a) = T_a^2(xK) + T_a(yK) .$$

It follows that S/K may be identified with the quotient group $S(a)/K(a)$

https://doi.org/10.1017/S0004972700011059 Published online by Cambridge University Press

and its induced automorphism $T_K(x+K(a)) = T_a x + K(a)$ where in S/K, $\xi\eta = T_K^2\xi + T_K\eta$. In the sense of Section 1 the map $x \to xK$ defines a homomorphism of S onto S/K.

The preceding analysis is valid for all medial Stein systems; we now proceed to a detailed analysis of finitely generated systems.

LEMMA 1. *S is finitely generated as a quasigroup if and only if $S(a)$ is finitely generated as a group.*

Proof. Let $a, x_1, \ldots, x_k$ generate S as a quasigroup. Then $S(a)$ is generated by $x_1, \ldots, x_k, T_a x_1, \ldots, T_a x_k$ since the subgroup generated by these elements is T_a-closed and contains $a, x_1, \ldots, x_k$.

Conversely if $S(a)$ is generated by $y_1, \ldots, y_k$ then, since $x + y = \left(T_a^{-2}x\right)\left(T_a^{-1}y\right)$, any sum $n_1y_1 + \ldots + n_ky_k$ can be obtained from $a, y_1, \ldots, y_k$ by repeated quasigroup multiplication and left division by $a \left(\equiv T_a^{-1}\right)$ so that $a, y_1, \ldots, y_k$ generate S as a quasigroup.

The proof shows that if s, t are the smallest possible numbers of generators for S, $S(a)$ respectively, then $s \leq t+1$ and $t \leq 2s-2$. It is easy to construct examples which show that neither of these inequalities can be sharpened.

DEFINITIONS. (i) If p is a prime we say S is a p-system if $S(a)$ is a p-group and S is torsion-free if $S(a)$ is torsion-free.

(ii) If $p \equiv 1, 4 \pmod 5$ then $J(p^s, \lambda)$ will denote the p-system S given by $S(a) = Z_{p^s}$, $T_a x = \lambda x$ where $\lambda^2 + \lambda - 1 \equiv 0 \pmod{p^s}$ (there are two distinct possible values of λ for given p and s). $J(5)$ will denote the 5-system given by Z_5, $Tx = 2x$.

(iii) If $p \equiv 2, 3 \pmod 5$ or $p = 5$ then $J(p^{2s})$ will denote the p-system given by $S(a) = Z_{p^s} \oplus Z_{p^s}$, $T_a(x, y) = (y, x-y)$.

(iv) The torsion-free system given by $S(a) = Z \oplus Z$,

https://doi.org/10.1017/S0004972700011059 Published online by Cambridge University Press

$T_a(x, y) = (y, x-y)$ will be denoted by J .

THEOREM 8. *Let S be a finite medial Stein system. Then*

(i) $S \simeq \prod_p S_p$ *is isomorphic to a cartesian product of p-systems for various p ,*

(ii) if $p \equiv 1, 4 \pmod 5$ *then* $S_p \simeq \prod_i J\left(p^{s_i}, \lambda_i\right)$, *a cartesian product of various factors* $J\left(p^s, \lambda\right)$,

(iii) if $p \equiv 2, 3 \pmod 5$ *then* $S_p \simeq \prod_i J\left(p^{2s_i}\right)$, *a cartesian product of various factors* $J\left(p^{2s}\right)$.

In all cases the number and types of each factor are uniquely determined.

Proof. Part *(i)* follows directly from $S(a)$ being the direct sum of its Sylow p-subgroups, each of which must be T_a-invariant for the automorphism T_a . Each S_p is unique up to isomorphism by the uniqueness of $\left(S(a), T_a\right)$ up to operator isomorphism.

The proofs of parts *(ii)* and *(iii)* depend on finding canonical forms, in various cases, for a finite abelian p-group with an automorphism.

LEMMA 2. *Let U be a linear transformation of a finite dimensional vector space $V = V(F)$ over a field F such that its minimal polynomial $m(\lambda) = m_1(\lambda)m_2(\lambda) \ldots m_k(\lambda)$ factors into distinct irreducibles $m_i(\lambda)$ over F . Then if X is a U-invariant subspace of V there is a U-invariant subspace Y such that $V = X \oplus Y$.*

The proof is a simple exercise in linear algebra and is omitted.

LEMMA 3. *Let A be a finite abelian p-group and T an automorphism of A satisfying $f(T) = 0$ where f is a monic polynomial of degree n over Z which is irreducible* mod p . *Then A is a direct sum of summands of the form $[z] \oplus [Tz] \oplus \ldots \oplus \left[T^{n-1}z\right]$ where $z \in A$ is different for different summands and each $\left[T^j z\right] \simeq Z_{p^t}$ for some $t = t(z)$*

https://doi.org/10.1017/S0004972700011059 Published online by Cambridge University Press

depending on z *but not on* j .

Proof. Let s be the least integer such that $p^s A = 0$. Then $p^{s-1}A$ is a vector space V^1 over GF(p) and T acts on V^1 as a linear transformation with minimal polynomial $f(\lambda) \pmod p$. By the Jordan Canonical Form, V^1 is a direct sum of T-invariant subspaces $\left[y_i, Ty_i, \ldots, T^{n-1}y_i\right]$, $1 \le i \le i_1$. Let $y_i = p^{s-1}z_i^1$; then the $T^j z_i^1$, $0 \le j < n$, $1 \le i \le i_1$, are linearly independent $\pmod{p^s}$. For

$$\sum a_{ij}T^j z_i^1 = 0 \Rightarrow \sum a_{ij}T^j p^{s-1}z_i^1 = 0 \Rightarrow a_{ij} \equiv 0 \pmod p \Rightarrow a_{ij} = pb_{ij}$$

$$\Rightarrow \sum b_{ij}T^j p^{s-1}z_i^1 = 0 \Rightarrow b_{ij} \equiv 0 \pmod p \Rightarrow \ldots \Rightarrow a_{ij} \equiv 0 \pmod{p^s} .$$

Thus A has a subgroup $A_1 = \bigoplus_{i,j} \left[T^j z_i^1\right]$ where each $\left[T^j z_i^1\right] \simeq Z_{p^s}$.

Now let $V^2 = p^{s-2}\{x \mid x \in A \text{ and } p^{s-1}x = 0\}$, which is also a vector space over GF(p) and $V^1 \subseteq V^2$. V^1 and V^2 are T-invariant, so by Lemma 2, $V^2 = V^1 \oplus V_2$ for a T-invariant subspace V_2 . As before V_2 is a direct sum of T-invariant subspaces $\left[w_i, Tw_i, \ldots, T^{n-1}w_i\right]$, $1 \le i \le i_2$ (or is empty), and putting $w_i = p^{s-2}z_i^2$ where $p^{s-1}z_i^2 = 0$, we obtain a subgroup $A_2 = \bigoplus_{i,j} \left[T^j z_i^2\right]$ where each $\left[T^j z_i\right] \simeq Z_{p^{s-1}}$. Also, as is easily verified, $A_1 + A_2 = A_1 \oplus A_2$.

Continuing thus, $V^3 = p^{s-3}\{x \mid x \in A \text{ and } p^{s-2}x = 0\} = V^2 \oplus V_3$ and so on, we eventually express $A = A_1 \oplus A_2 \oplus \ldots \oplus A_s$ in the form required by the lemma.

COROLLARY. *If* A *is a finite abelian* p*-group,* $p^s A = 0$, *and* T *an automorphism of* A *with* $f(T) = 0$ *where* $f(\lambda) \equiv \prod_k f_k(\lambda) \pmod{p^s}$ *and the* f_k *are monic of degree* n_k *and distinct* $\pmod p$ *and irreducible*

https://doi.org/10.1017/S0004972700011059 Published online by Cambridge University Press

(mod p), *then* A *is a direct sum of summands of the form* $[z] \oplus [Tz] \oplus \ldots \oplus [T^{n_k-1}z]$ *where* $f_k(T)z = 0$ *and* $[T^j z] \simeq Z_{p^t}$ *for* $t = t(z)$. *The number and types of each summand are uniquely determined.*

For we may write $A = \bigoplus_k A^{(k)}$ where $A^{(k)} = \{x \mid f_k(T)x = 0\}$ and apply the lemma to each $A^{(k)}$ separately. The uniqueness follows by the uniqueness of the $A^{(k)}$ and the uniqueness of the canonical form for finite abelian groups (without automorphism).

Finally parts *(ii)* and *(iii)* of the theorem follow directly from Lemma 3 and its corollary applied to the case $T^2 + T - 1 = 0$, on noting that $\lambda^2 + \lambda - 1$ factors $(\lambda-\lambda_1)(\lambda-\lambda_2)$ $(\lambda_1 \neq \lambda_2)$ in Z_{p^s} for $p \equiv 1, 4$ (mod 5) and is irreducible in Z_{p^s} for $p \equiv 2, 3$ (mod 5). //

The case $p = 5$ is anomalous since $\lambda^2 + \lambda - 1 \equiv (\lambda-2)^2$ (mod 5) and is irreducible (mod 5^s) for $s > 1$. For an example of a 5-system not of the kinds appearing in Theorem 8 *(ii)* and *(iii)* consider $Z_{25} \oplus Z_5 \equiv [e_1] \oplus [e_2]$ with T defined by

$$T((5l+m)e_1 + ne_2) = (10l+2m-5n)e_1 + (2n+m)e_2 .$$

Then $T^2 + T - 1 = 0$, so this is a 5-system, which we denote P. We have developed a method for determining all 5-systems of a given order, but as it is complicated and does not yield the isomorphism classes explicitly we omit the details. The isomorphism classes for orders 5^s, $1 \leq s \leq 4$, are as follows:

Order	Associated group	Systems
5	Z_5	$J(5)$
25	$Z_5 \oplus Z_5$	$J(5) \times J(5)$, $J(25)$
125	$Z_5 \oplus Z_5 \oplus Z_5$	$J(5) \times J(5) \times J(5)$, $J(5) \times J(25)$
	$Z_{25} \oplus Z_5$	P
625	$Z_5 \oplus Z_5 \oplus Z_5 \oplus Z_5$	$J(5) \times J(5) \times J(5) \times J(5)$, $J(5) \times J(5) \times J(25)$
		$J(25) \times J(25)$
	$Z_{25} \oplus Z_5 \oplus Z_5$	$J(5) \times P$
	$Z_{25} \oplus Z_{25}$	$J(625)$

THEOREM 9. *Let S be an infinite finitely generated medial Stein system. Then $S \simeq H \times K$ where H is torsion-free and K is finite. Further $H \simeq \prod_{i=1}^{h} J_i$ where each J_i is a copy of J. The integer h is uniquely determined and K is unique up to isomorphism.*

Proof. (i) Assume first that if S is torsion-free; then $S \simeq \prod_{i=1}^{h} J_i$ for some h and copies J_i of H. Given any S and $a \in A$, let $K(a)$ be the torsion subgroup of $S(a)$, which will be T_a-invariant and so defines a finite subsystem K of S. $S(a)/K(a)$, which is the group associated with the quotient system S/K, is torsion-free; so by hypothesis $S(a)/K(a) \simeq \bigoplus_{i=1}^{h} (Z \oplus Z)_i$, where each summand $(Z \oplus Z)_i$ is invariant under the induced automorphism T_K, and T_K acts in it by $T_K(x, y) = (y, x-y)$.

By the canonical form theorem for finitely generated abelian groups it follows that we may write $S(a) = \bigoplus_{i=1}^{h} (Z \oplus Z)_i \oplus K(a)$, where if $(Z \oplus Z)_i = [e_{2i}] \oplus [e_{2i+1}]$, then $T_a e_{2i} = e_{2i+1} + y_{2i}$, $T_a e_{2i+1} = e_{2i} - e_{2i+1} + y_{2i+1}$ for some $y_{2i}, y_{2i+1} \in K(a)$, and also $Ty_{2i} + y_{2i} + y_{2i+1} = 0$, since $T_a^2 + T_a = 1$.

https://doi.org/10.1017/S0004972700011059 Published online by Cambridge University Press

Put $e'_{2i} = e_{2i}$, $e'_{2i+1} = e_{2i+1} + y_{2i}$ - then $T_a e'_{2i} = e'_{2i+1}$, $T_a e'_{2i+1} = e'_{2i} - e'_{2i+1}$, so that we may now write $S(a) = \bigoplus_{i=1}^{h} (Z \oplus Z)_i \oplus K(a)$ where each summand is T_a-invariant and in each $(Z \oplus Z)_i$, T_a acts by $T_a(x, y) = (y, x-y)$. From this the required representation $S \simeq H \times K$ follows.

Conversely given such a representation and any $a \in S$, then $K \simeq K(a)$ (*qua* quasigroup), so (by Theorem 7) K is unique up to isomorphism. Also $2h$ = rank $S(a)/K(a)$ (*qua* group), so h is uniquely determined.

(ii) Now suppose that S is torsion free so, $S(a) \simeq Z^k$ for some k, and $T = T_a : Z^k \to Z^k$ is a linear transformation satisfying $f(T) = T^2 + T - 1 = 0$. From the linear algebra theory for Z^k (see [4, Sections 15, 16]), we obtain a canonical form for T ; the matrix of T with respect to some basis of Z^k consists of $k/2$ diagonal blocks, each a copy of the companion matrix C_f of f, and zeros elsewhere. This completes the proof of Theorem 9. //

4. Extended medial systems

The class of finite medial Stein systems is not large and the spectrum consists of all integers whose square free part does not contain any prime $p \equiv 2, 3 \pmod 5$. A closely related but much larger class is that of *extended medial* (EM) systems, defined as Stein systems with the property that any 2-element generated subsystem is medial. Stein systems constructed by the method of block designs (see [5], Theorem 1) with medial block systems are EM-systems, and since there are medial systems of orders 4, 5, 11, it follows by ([5], Theorems 6 and 7) that EM-systems exist for all orders greater than or equal to 1198 , a figure which can probably be improved. All EM-systems satisfy the restricted modular law: $x(y(xy)) = (xy)(yx)$ - in fact we do not know of any Stein system in which the restricted modular law fails, although we have not proved its universal validity.

A Stein system which satisfies either of the laws $x(yx) = y$,

https://doi.org/10.1017/S0004972700011059 Published online by Cambridge University Press

$(yx)x = xy$ satisfies the other and is an EM-system in which every 2-element generated subsystem is isomorphic to $J(4)$; these subsystems form a block design (see Stein [7]). If a Stein system obeys the law $(xy)z = (zy)x$, then $(xy)y = yx$, so also $x(yx) = (xy)x = y$ holds. Then $(xy)(yt) = \big((yt)y\big)x = tx = t\big(y(xy)\big)$, so that putting $xy = z$ we see the modular law ML holds and the system is medial. It is easy now to verify that the law $(xy)z = (zy)x$ characterises the medial 2-systems S for which $2S(a) = 0$; hence if S is finite then S is isomorphic to a cartesian product of copies of $J(4)$.

Finite EM-systems have the interesting property that one can always deduce information about subsystems from a knowledge of the cycle decomposition of a left translation T_a regarded as a permutation of the system. For if T_a has an n-cycle $Y = (yy' \ldots)$ then

$$T_a^n y = y = F_{n-1} - F_n T_a y \quad (n \text{ even})$$
$$= F_n T_a y - F_{n-1} \quad (n \text{ odd})$$

(working in the associated group of the medial subsystem generated by a and y) where F_n is the nth Fibonacci number. This gives a relation of the form $my + m' T_a y = 0$ from which the possible types of subsystem $[a, y]$ can be determined.

For example if T_a has a 10-cycle,then

$$T_a^{10} y = y = 34y - 55T_a y \Rightarrow 55T_a y = 33y .$$

Since, in $[a, y]$, $T_a^{-1} = T_a + 1$, $33T_a y = 22y$, and so $(2.55-3.33)T_a y = 11T_a y = 0 \Rightarrow 11y = 0$. The group of $[a, y]$ is generated by y and $T_a y$, so is of order 11 or 121 according as $T_a y$ is linearly dependent on y or not. It follows that $[a, y] \simeq J(11, 7)$ or $J(11, 7) \times J(11, 3)$, since the system $J(11, 3)$ does not have any 10-cycles.

Similarly one can show that if T_a has an 8-cycle then $[a, y] \simeq J(9)$ or $J(9) \times J(5)$. As special cases of the general theory we can obtain again $[a, y] \simeq J(4)$ for a 3-cycle and $[a, y] \simeq J(5)$ for a

https://doi.org/10.1017/S0004972700011059 Published online by Cambridge University Press

4-cycle.

5. Further Constructions with abelian groups

THEOREM 10. *Let* $(S, *)$ *be any quasigroup of order* n *possessing a transitive abelian group* A *of* n *automorphisms. Then it is possible to define an addition* $+$ *on* S *so that* $(S, +) \simeq A$ *and* $x*y = x + U(y-x)$ *where* $U : S \to S$ *is a permutation of* S *such that* $U - 1$ *is also a permutation. The converse is true.*

Proof. Select any element of S as 0 and define $+$ by $x + y = f(x)$ where $f \in A$ is such that $f(0) = y$. Clearly $x + 0 = 0 + x = x$ and if $g(0) = x$ then

$$y + x = g(y) = gf(0) = fg(0) = f(x) = x + y .$$

Also if $h(0) = z$ then

$$(x+y) + z = h(x+y) = hfg(0) = gfh(0) = (z+y) + x = x + (y+z)$$

by commutativity of $+$. Finally $x + f(0) = 0$ if $f \in A$ is such that $f(x) = 0$ so that additive inverses exist and $(S, +)$ is an abelian group.

The group A is the set of translations $x \to x + a$. Define $U : S \to S$ by $Ux = 0*x$ so that $0*(y-x) = U(y-x)$ and $x*y = x + U(y-x)$ on translating by x. The equation $x*y = x + U(y-x) = z$ has a unique solution for any one of x, y, z given the other two just when U and $U - 1$ are permutations of S. The converse of the theorem can be verified directly from this equation. //

COROLLARY. S *constructed as above is a Stein system if and only if* U *has the property that* $U^2x = U(-x) + x$ *for all* $x \in S$.

Medial Stein systems are included in this construction (take $U = T$ in Section 3) but also some non-medial systems. For example if R is a right-distributive near ring with unit containing an element c such that $c^2 + c - 1 = 0$, $-c = c(-1)$, and $cc^{-1} = c^{-1}c = 1$ for some inverse c^{-1}, then defining $x*y = x + c(y-x)$ turns R into a Stein system which in general will not be medial if R is not a ring.

We have no general decomposition theorems for Stein systems constructed in this way, but in all known examples the restricted modular

law does hold. One may verify directly that if $U(-x) = -Ux$, $U(2x) = 2Ux$, $x \in S$, then the restricted modular law holds.

If stronger properties of $\mathrm{aut}(S)$ are assumed then more can be proved.

THEOREM 11 (see Stein [7]). *Suppose* $(S, *)$ *is a finite quasigroup with a sharply 2-transitive group of automorphisms. Then* S *can have the structure of a right-distributive near field imposed on it in such a way that* $x*y = x + c(y-x)$ *for some fixed* $c \neq 0, 1$ *in* S . *The converse is true.*

Proof. By the fundamental characterisation theorem on near fields (see, for example, [2], p. 382) S can certainly be presented as a near field so that the given group of automorphisms appears as the group of linear substitutions $x \to a + xb$, $b \neq 0$. Let $0*1 = c$. Then since $x \to a + x(b-a)$ is an automorphism when $a \neq b$ and maps $0 \to a$, $1 \to b$, it follows $a*b = a + c(b-a)$. Also if $0*0 = d$ then the same automorphism shows that $a*a = a + d(b-a)$ - but since this can not depend on b , $d = 0$, and $a*a = a = a + c(a-a)$. Obviously one does not get a quasigroup if $c = 0$ or $c = 1$.

For the converse note that

$$x + c(y-x) = z \iff c(y-x) = (z-x) \iff (c-1)(y-x) = (z-y) ,$$

so that provided $c \neq 0, 1$ one can always solve $x*y = z$ for any one of x, y, z, given the other two. //

COROLLARY. S *constructed as above is a Stein system if and only if* $c^2 + c - 1 = 0$.

We now proceed to construct a class of Stein systems on the basis of the preceding theorem and corollary. Any finite near field, excluding seven exceptional cases, can be constructed as follows (see, for example, [2], p. 390).

Let $q = p^h$ be a power of a prime p and let v be an integer all of whose prime factors divide $q - 1$, where also $v \not\equiv 0 \pmod 4$ if $q \equiv 3 \pmod 4$. Then with $hv = r$ a near field K of p^r elements can be defined thus:

N1. the elements of K are the elements of the Galois field

https://doi.org/10.1017/S0004972700011059 Published online by Cambridge University Press

$GF(p^r)$;

N2. addition in K is the same as addition in $GF(p^r)$;

N3. the product $w \circ u$ in K is defined in terms of the product $x.y$ in $GF(p^r)$ in the following way: let z be a fixed primitive root of $GF(p^r)$; then if $u = z^{kv+j}$, an integer i is uniquely determined (mod v) by $q^i \equiv 1 + j(q-1) \pmod{v(q-1)}$ and the product $w \circ u$ is given by $w \circ u = u.w^{q^i}$;

N4. the centre of K is $GF(q)$.

THEOREM 12. *The finite near fields K of the type described by* N1-N4 *and which contain an element c such that $c \circ c + c - 1 = 0$ and $c \circ c = c.c$ are precisely the following:*

(i) those with $p \equiv 0, 1, 4 \pmod 5$;

(ii) those with $p \equiv 2, 3 \pmod 5$ *and* $2|h$;

(iii) those with $p \equiv 2, 3 \pmod 5$ *and* $p \equiv 1 \pmod 4$ *and* $2 \nmid h$, $2|v$.

Proof. Cases *(i)* and *(ii)* are immediate since then c exists in the centre of K . Suppose then that $p \equiv 2, 3 \pmod 5$ and $2 \nmid h$. If c exists then $c \equiv GF(p^2)$, so $2|r$ and $2|v$, which excludes $p = 2$, since then $2 \nmid (q-1)$.

If z is the primitive root of $GF(p^r)$ defining K , suppose $c = z^{kv+j}$ and $c \circ c = c.c$. Then $q^i \equiv 1 + j(q-1) \pmod{v(q-1)}$ and

$$2|i \ (\text{since } c^{p^i} = c^{p^2} = c \text{ in } GF(p^r)) \iff 2|j \iff c^{\frac{1}{2}(p^r-1)} = 1$$

in $GF(p^r)$. Conversely if this last equation holds then $c \circ c = c.c$.

If c is a root of $x^2 + x - 1$ in $GF(p^2)$ then the other root is c^p , so that $c^{p+1} = -1$ and

https://doi.org/10.1017/S0004972700011059 Published online by Cambridge University Press

$$c^{\frac{1}{2}(p^r-1)} = c^{\frac{1}{2}(p^2-1)(1+p^2+\ldots+p^{r-2})} = (-1)^{\frac{1}{2}(p-1)(1+p^2+\ldots+p^{r-2})} = +1$$

if and only if $p \equiv 1 \pmod 4$ or $4 \mid r$. But if $4 \mid r$ then $4 \mid v$, and $q = p^h \not\equiv 3 \pmod 4 \Rightarrow p \equiv 1 \pmod 4$. So in all cases $p \equiv 1 \pmod 4$, which completes the proof. //

COROLLARY. *If p is a prime such that $p \equiv 2, 3 \pmod 5$ and $p \equiv 1 \pmod 4$ there exists a minimal Stein system of order p^2 which is neither medial nor left-distributive. The system has a sharply 2-transitive automorphism group. This follows on taking $h = 1$, $v = r = 2$ in the theorem - the smallest systems of this kind have orders $13^2 = 169$ and $17^2 = 289$.*

6. A system with trivial automorphism group

In contrast to the systems of the preceding section we conclude the paper by constructing a Stein system of order 21 which admits only the identity automorphism. As a set S is defined as $J(4) \times J(5) \cup \{e\}$ where e is an adjoined element and the multiplication is defined as follows.

(i) If $a \neq c$, $b \neq d$, then $(a, b).(c, d) = (ac, bd)$ where ac is multiplied in $J(4)$ and bd in $J(5)$.

(ii) Suppose $J(4) = \{a_1, a_2, a_3, a_4\}$, $J(5) = \{b_1, b_2, b_3, b_4, b_5\}$. Let $\{a_i\} \times J(5)$ be made into a copy C_i of $J(5)$ by imposing any suitable multiplication and similarly let $J(4) \times \{b_j\} \cup \{e\}$ be made into a copy R_j of $J(5)$.

Then $(a_i, b).(a_i, b') = (a_i, bb')$ where bb' is multiplied in C_i

(iii)

$$(a, b_j).(a', b_j) = (aa', b_j) \text{ if } aa' \text{ multiplied in } R_j \text{ is not } e,$$
$$= e \text{ if } aa' = e \text{ in } R_j.$$

(iv) $(a, b_j)e = (ae, b_j)$ and $e(a, b_j) = (ea, b_j)$ where ae, ea are multiplied in R_j.

https://doi.org/10.1017/S0004972700011059 Published online by Cambridge University Press

It is straightforward to check that S is a Stein system and that the cycle decompositions are $P_x = [4] + [4] + [12]$, $x \neq e$, and $P_e = [4] + [4] + [4] + [4] + [4]$. S is 2-generated by any pair of elements (a, b), (c, d) with $a \neq c$, $b \neq d$, and its subsystems are precisely the C_i and R_j , all of order 5 . S is not left-distributive or medial and is not an EM-system; however the restricted modular law does hold. We shall show that the multiplications in R_j and C_i can be chosen in such a way that if f is any automorphism of S then $f = 1_S$.

First, f must leave e invariant and map subsystems to subsystems, so will be of the form $g_1 \times g_2$ restricted to $J(4) \times J(5)$. The column subsystems $C_i = \{a_i\} \times J(5)$, $1 \leq i \leq 4$, are permuted amongst themselves by g_1 and the rows $J(4) \times \{b_j\}$, $1 \leq j \leq 5$, are permuted by g_2 , inducing a permutation of the row subsystems R_j , which may also be called g_2 without confusion. In virtue of (i), g_1 must be an automorphism of $J(4)$, and since $\mathrm{aut}(J(4))$ is the alternating group on 4 symbols, g_1 is an even permutation.

Let the Stein system of order 5 be represented as Z_5 with multiplication $x.y = 4x + 2y$ and define the multiplications on the subsystems R_j by mapping them onto Z_5 as follows: for $1 \leq j \leq 4$ map $(a_i, b_j) \to i$ and $e \to 0$, while for $j = 5$ map $(a_1, b_5) \to 1$, $(a_2, b_5) \to 2$, $(a_3, b_5) \to 4$, $(a_4, b_5) \to 3$, $e \to 0$.

Since g_2 must map some R_j to $R_{j'}$ with $1 \leq j, j' \leq 4$, g_1 must induce, via the representations of R_j and $R_{j'}$ as Z_5, an automorphism of Z_5 of the form $0 \to 0$, $i \to k$, where $g_1(a_i) = a_k$. But g_1 is an even permutation, and if not the identity, this automorphism can only be given by $x' = 4x$; that is $(14)(23)$.

However if g_2 maps R_5 to R_5 then g_1 via the representation of R_5 as Z_5 would induce an automorphism $(13)(24)$ of Z_5 , while if g_2

https://doi.org/10.1017/S0004972700011059 Published online by Cambridge University Press

maps R_5 to R_j, $j < 5$, then g_1 via the representations of R_5 and R_j as Z_5 would induce an automorphism (1423). This is contradictory, since neither (13)(24) or (1423) are in fact automorphisms of Z_5. From this it follows g_1 is the identity on $J(4)$ and also, by a similar argument, that g_2 maps R_5 to R_5.

Suppose without loss of generality that $J(5) = \{b_1, b_2, b_3, b_4, b_5\}$ is identifiable with Z_5 by the map $b_i \to i$, in which case, in virtue of (i) and $g_2(b_5) = b_5$, g_2 is an automorphism of $J(5)$ which induces one of the following automorphisms of Z_5: (1), (1243), (1342), (14)(23). Now define the multiplication on C_1 by mapping it onto Z_5 by $(a_1, b_1) \to 1$, $(a_1, b_2) \to 4$, $(a_1, b_3) \to 3$, $(a_1, b_4) \to 2$, $(a_1, b_5) \to 0$. Then g_1 maps C_1 to C_1 and g_2 induces an automorphism of C_1 by $(a_1, b_j) \to (a_1, g_2(b_j))$, which in turn, via the representation of C_1 as Z_5 and the known possibilities for g_2, induces an automorphism (1), (1423), (1324), (12)(34) of Z_5. But of these only (1) is in fact an automorphism, so that g_2 can only be the identity.

Hence $f = 1_S$ as required. //

References

[1] Bernd Fischer, "Distributive Quasigruppen endlicher Ordnung", *Math. Z.* 83 (1964), 267-303.

[2] Marshall Hall, Jr., *The theory of groups* (Macmillan, New York, 1959).

[3] D.C. Murdoch, "Structure of abelian quasi-groups", *Trans. Amer. Math. Soc.* 49 (1941), 392-409.

[4] Morris Newman, *Integral matrices* (Pure and Applied Mathematics, 45. Academic Press, New York and London, 1972).

[5] M.J. Pelling and D.G. Rogers, "Stein quasigroups I: Combinatorial aspects", *Bull. Austral. Math. Soc.* 18 (1978), 221-236.

[6] Sherman K. Stein, "On the foundations of quasigroups", *Trans. Amer. Math. Soc.* 85 (1957), 228-256.

[7] Sherman K. Stein, "Homogeneous quasigroups", *Pacific J. Math.* 14 (1964), 1091-1102.

Balliol College,
Oxford,
England;

68 Liverpool Road,
Watford,
Hertfordshire,
England.