1. Introduction. Generalizations of the Jordan-Hölder and Krull-Schmidt theorems to an abstract algebra can be obtained as lattice-theoretic results provided we assume that the algebra contains a one-element subalgebra and that all its congruence relations are permutable (see [3, Chapter VI]). Thurston [5] has given an example of a quasigroup with a pair of nonpermutable congruence relations and his method can be used to construct a similar example for loops. Birkhoff [3] has given sufficient conditions for all the congruence relations on a loop to be permutable. We shall weaken these conditions by showing that all the congruence relations on a loop with the weak inverse property are permutable. We shall further show that it is not possible to give necessary conditions for the permutability of a given congruence relation on a loop in terms of the image system alone; in fact we shall prove that any loop image $M$ is a homomorphic image of at least one loop $F$ such that the corresponding congruence relation permutes with all the congruence relations on $F$.

2. Quasinormal congruence relations. Sufficient conditions for permutability.

**Lemma A.** If $\theta$ and $\phi$ are congruence relations on a loop $G$, then a necessary and sufficient condition that $\theta$ and $\phi$ be permutable is that, for all $x \in G$, $C[C'(x)]$ be the congruence class containing $x$ for some congruence relation on $G$ where $C(x)$ is the $\theta$-class and $C'(x)$ is the $\phi$-class containing $x$.

**Proof.** Suppose $\theta$ and $\phi$ are permutable and let $y \in C[C'(x)]$ so that $y \theta b \phi x$ for some $b \in G$. Then, for some $b \in G$, $y \phi b \phi x$ and so $y \in C'[C(x)]$. Thus $C[C'(x)] \subset C'[C(x)]$. Similarly, $C[C(x)] \subset C[C'(x)]$ showing equality. Now $x \in C[C'(y)]$ and so $C[C'(x)] \subset C[C'[C'(y)]] = C[C'[C[C'(y)]]) \subset C[C[C'(x)]]) = C[C'(x)]$. Hence the sets $C[C'(x)]$ are equivalence classes. They are congruence classes since

---

Presented to the Society, September 3, 1954 under the title *Quasinormal kernels of loops*; received by the editors March 15, 1955 and, in revised form, August 20, 1955.

1 Parts of this paper are contained in the author's doctoral thesis at the University of Wisconsin written under the direction of R. H. Bruck.

583
Conversely, let the sets \( C[C'(x)] \), \( x \in G \) be congruence classes. Then, if \( \gamma \theta \alpha \phi x \), we have \( y \in C[C'(x)] \) and so \( C[C'(y)] = C[C'(x)] \). Then, clearly, \( x \theta \beta \phi y \) for some \( b \in G \). Similarly, \( x \theta \beta \phi y \) implies \( \gamma \theta \alpha \phi x \), showing that \( \theta \) and \( \phi \) are permutable.

If \( G \) is a loop and \( a \) and \( x \) are in \( G \) define the mapping \( a \mapsto \alpha \rho (x) \) of \( G \) upon \( G \) by \( \alpha \rho (x) = ax \). Similarly, \( a \lambda (x) = xa \). Now suppose that \( \theta \) is a congruence relation on \( G \) and \( K \) is the \( \theta \)-class containing 1 (or kernel of \( \theta \)). We shall say that \( \theta \) is quasinormal if \( C(x) = x \Delta (K) \) for all \( x \in G \) where \( C(x) \) is the \( \theta \)-class containing \( x \) and \( \Delta (K) \) is the semigroup generated by all \( \rho (k) \), \( \lambda (k) \) where \( k \in K \). If \( y \in C(x) \), we shall write \( y = x V(k_1, k_2, \ldots, k_n) = x V(k_1) \) where \( V(k_1, k_2, \ldots, k_n) = \pi (k_1) \pi (k_2) \cdots \pi (k_n) \), in which each \( \pi \) is either \( \rho \) or \( \lambda \).

**Theorem 1.** If \( \theta \) is quasinormal and \( \phi \) is any congruence relation on a loop \( G \), then \( \theta \) and \( \phi \) are permutable.

**Proof.** Let \( C(x) \) be a \( \theta \)-class and \( K \) the kernel of \( \theta \). Consider \( y \in C(x) \Delta (K) \). Let \( y = w V(k_i) \) where \( C(w) = C(x) \). Then \( C(x) V(k_i) \subseteq C(x) V[C(k_i)] = C(w) V[C(k_i)] \subseteq C(w V(k_i)] = C(y) \). Hence \( C(x) V(k_i) \Delta (K) = C(x) \Delta (K) \subseteq C(y) \Delta (K) \). Therefore \( x \in C(y) \Delta (K) \) and so, by the above argument, \( C(y) \Delta (K) \subseteq C(x) \Delta (K) \), showing equality and proving that the sets \( C(x) \Delta (K) \) are equivalence classes. Clearly \( C(a) \Delta (K) \cdot C(b) \Delta (K) \subseteq C(ab) \Delta (K) \) and, by Lemma A, \( \theta \) and \( \phi \) are permutable.

If \( G \) is a loop, let \( \Delta (G) \) be the semigroup generated by all \( \rho (x) \), \( \lambda (x) \) where \( x \in G \). We shall say that \( G \) possesses the weak inverse property if, for all \( a \), \( x \), and \( y \) in \( G \) such that \( ax = ya \), there exists at least one transformation \( \sigma \) in \( \Delta (G) \) such that \( a \sigma = 1 \) and either \( (ax) \sigma = x \) or \( (ya) \sigma = y \).

**Theorem 2.** If a loop \( G \) possesses the weak inverse property, then all the congruence relations on \( G \) are quasinormal (and hence permutable).

**Proof.** Let \( a \equiv b(\theta) \) in \( G \). Solve \( ax = ya = b \) for \( x \) and \( y \) in \( G \). Then either \( x = b \sigma \sigma \) or \( y = b \sigma \sigma \) for some \( \sigma \) in \( \Delta (G) \) such that \( a \sigma = 1 \). Since \( a \sigma = b \sigma \sigma = 1(\theta) \), \( b \in C(a) \) implies that either \( b = \alpha \rho (k) \) or \( b = a \lambda (k) \) for some \( k \) in the \( \theta \)-kernel. Thus \( \theta \) is quasinormal.

The following are examples of loops with the weak inverse property:

(i) a loop \( G \) with the property that for all \( a \), \( x \), and \( y \) in \( G \) such

---

2 The referee weakened the original form of this definition and the author wishes to express his thanks.
that \(ax = ya\), either \(a(ax) = x\) or \((ya)a^* = y\) where \(a\) and \(a^*\) are uniquely defined by \(aa = 1\) and \(aa^* = 1\). We note that \(a = a^*\) for all \(a\) in \(G\) (set \(x = a^*, y = a\)). This class of loops includes those which possess the left (or right) inverse property (see Brück [4]). If \(G\) possesses the (two-sided) inverse property then it is easy to show that every homomorphic image of \(G\) is a loop.

(ii) loops with the special property of Artzy [1].

3. Impossibility of necessary conditions for permutability in terms of the image. The work of Bates and Kiokemeister [2] shows that necessary and sufficient conditions for a groupoid \(M\) to be the homomorphic image of a loop are that (i) \(M\) contains an element \(1\) such that \(1 \cdot a = a \cdot 1 = a\) for all \(a \in M\), and (ii) if \(a\) and \(b\) are in \(M\) then there is at least one \(x\) and at least one \(y\) in \(M\) such that \(ax = b\) and \(ya = b\). We shall call such a groupoid a loop image.

If \(M\) is a loop image, \(a\) and \(z\) are in \(M\), \(z \neq 1\), and \(za = a\) \((az = a)\) then \(z\) will be called a local left (right) identity for \(a\). As an example of a loop image with local identities we could take the set of all non-negative rational integers under the operation \(a \circ b = |a - b|\).

**Lemma B.** Let \(\theta\) be a congruence relation on a loop \(G\) and let \(M\) be the associated loop image. A necessary and sufficient condition that \(M\) contain no elements with local left identities is that the \(\theta\)-classes shall be given by \(C(x) = Kx\) where \(K\) is the \(\theta\)-kernel.

**Proof.** Suppose \(M\) has no elements with local left identities. If \(a \equiv b(\theta)\), solve \(xa = b\) for \(x \in G\). Then \(C(x)C(a) \subseteq C(a)\). Hence \(C(x) = K\) so \(x \in K\). Clearly \(Ka \subseteq C(a)\) and so \(Ka = C(a)\).

Conversely, if \(C(x) = Kx\), all \(x \in G\), let \(y\) be such that \(Ky \cdot Kx \subseteq Kx\). Thus \(yx \in Kx\) so that \(Ky = K\) (since \(K\) is a subloop of \(G\)) and \(M\) has no elements with local left identities.

A similar result holds if \(M\) has no elements with local right identities, giving \(\theta\)-classes of the form \(xK\).

It may be remarked that Lemma B together with Theorem 1 provide a solution of Problem 32 proposed by Birkhoff [3].

That we cannot give necessary conditions for permutability in terms of the image system follows from

**Theorem 3.** Let \(M\) be a loop image. Then there exists a loop \(F\) homomorphic to \(M\) such that the corresponding congruence relation is quasi-normal (and hence permutable with all the congruence relations on \(F\)).

**Proof.** We shall show in an appendix how to construct a loop image \(H\) possessing a homomorphism \(\alpha\) upon \(M\) and having the following properties:
(I) If \( ab = b \) for \( a \) and \( b \) in \( H \), then \( a = 1 \).

(II) If \( a\alpha = b\alpha \) for \( a \) and \( b \) in \( H \), then there is an element \( c \) in \( H \) such that \( c\alpha = 1 \) and \( c\alpha = b \).

Let \( W = \{ w \in H \mid w\alpha = 1 \} \). Then certainly \( w\alpha = b \) for \( w \in W \), \( a \) and \( b \) in \( H \) if and only if \( a\alpha = b\alpha \) and so the coset containing \( a \) has the form \( Wa \).

Now let \( F \) be a loop possessing a homomorphism \( \beta \) upon \( H \). In view of property (I) and Lemma B, we know that the cosets of \( \beta \) are of the form \( Lx \) where \( L \) is the kernel of \( \beta \) and \( x \in F \). Let \( K \) be the kernel of the homomorphism \( \beta\alpha \) of \( F \) upon \( M \). We note that \( L \subseteq K \).

Suppose \( x\beta\alpha = y\beta\alpha \) for some \( x \) and \( y \) in \( F \). Then \( x\beta = w(y\beta) \) for some \( w \in W \subseteq H \). But \( w = k\beta \) for some \( k \in F \) and \( w\alpha = k\beta\alpha = 1 \) so \( k \in K \).

Then \( x\beta = (ky)\beta \) and so \( x = p(ky) \) for some \( p \in L \). Conversely, if \( x = p(ky) \) for \( x \) and \( y \) in \( F \), \( p \in L \), and \( k \in K \), then \( x\beta\alpha = (p\beta\alpha)(k\beta\alpha) \cdot y\beta\alpha = y\beta\alpha \) and so the cosets of \( \beta\alpha \) are of the form \( L \cdot Kx \). Furthermore,

\[
L \cdot Kx \subseteq (L(K \cdot x))(L \cdot Kx) \subseteq L(K \cdot Kx) \subseteq L(L \cdot Kx) = L \cdot Kx.
\]

Since \( LK = K \) we see that the cosets of \( \beta\alpha \) have the form \( K \cdot Kx \) and so the corresponding congruence relation is quasinormal, and hence permutable with all the congruence relations on \( F \).

**Remarks on Theorem 3.** The result is trivial if \( M \) is a loop or even if \( M \) has no elements with local left identities for then \( Kx = K \cdot Kx \) for all \( x \). If \( M \) contains elements with local left identities then \( Kx \) is property contained in \( K \cdot Kx \) for some \( x \). In particular, if \( M \) contains elements with local left identities but has no elements with local right identities then \( xK = K \cdot Kx \) for all \( x \) but \( xK \) contains \( Kx \) properly for at least one \( x \). A construction similar to the one given in the appendix would produce an \( H \) containing no elements with local right identities so that the cosets of \( \beta\alpha \) would have the form \( K \cdot Kx = Kx \cdot K \). If \( M \) contains an element with both a local left and a local right identity, then it is possible to construct a loop \( G \), having \( M \) as a homomorphic image, such that the corresponding congruence relation is not quasinormal.

**Appendix.** We shall use a construction similar to that devised by Bates and Kiokemeister [2] to obtain the loop image \( H \) required in the proof of Theorem 3.

Let \( J(i, 0) \) be a halfgroupoid possessing a homomorphism \( \alpha(i, 0) \) upon \( M \) and having the following properties:

(I') There is an element \( 1 \in J(i, 0) \) such that if \( a \in J(i, 0) \) and \( 1 \cdot a \in J(i, 0) \), then \( 1 \cdot a = a \) and if \( a \cdot 1 \in J(i, 0) \), then \( a \cdot 1 = a \).

(II') If \( a \) and \( b \) are in \( J(i, 0) \), and if \( ab = b \), then \( a = 1 \).
(III') If \( a \) and \( b \) are in \( J(i, 0) \), if both \( a \) and \( b \) are products in \( J(i, 0) \), and if \( a\alpha(i, 0) = b\alpha(i, 0) \), then there exist elements \( c \) and \( d \) in \( J(i, 0) \) such that \( ca(i, 0) = da(i, 0) = 1 \) and \( ca = b, \ db = a \).

Let \( J(i, 1) \) be an extension of \( J(i, 0) \) such that

(i) If \( a \in J(i, 0) \) but \( 1 \cdot a \notin J(i, 0) \), then \( 1 \cdot a = a \) in \( J(i, 1) \) and if \( a \cdot 1 \notin J(i, 0) \), then \( a \cdot 1 = a \) in \( J(i, 1) \).

(ii) If \( a \) and \( b \) are in \( J(i, 0) \) but \( ab \) is not in \( J(i, 0) \), then \( ab = c \) in \( J(i, 1) \) where \( c \in J(i, 1) - J(i, 0) \). It is understood that the elements \( c \) are distinct for different ordered pairs \( a, b \) and that \( J(i, 1) - J(i, 0) \) consists of exactly these elements \( c \).

We extend \( \alpha(i, 0) \) to a homomorphism \( \alpha(i, 1) \) of \( J(i, 1) \) upon \( M \) as follows:

1. If \( a \in J(i, 0) \), then \( \alpha a(i, 1) = \alpha a(i, 0) \).
2. If \( c \in J(i, 1) - J(i, 0) \) then there exists one and only one ordered pair \( a, b \) of elements of \( J(i, 0) \) such that \( c = ab \) in \( J(i, 1) \). Then define \( \alpha a(i, 1) = \alpha a(i, 0) \cdot \alpha b(i, 0) \).

Now let \( J(i, 2) \) be an extension of \( J(i, 1) \) such that

(i) If \( a \in J(i, 1) \) but \( 1 \cdot a \notin J(i, 1) \), then \( 1 \cdot a = a \) in \( J(i, 2) \) and if \( a \cdot 1 \notin J(i, 1) \), then \( a \cdot 1 = a \) in \( J(i, 2) \).

(ii) For each ordered pair \( a, b \) in \( J(i, 1) \) where \( a \neq b \) and \( a \neq 1 \), let \( J(i, 2) - J(i, 1) \) contain an element \( c \) such that \( ac = b \).

Again, the elements \( c \) adjoined in (ii) are distinct and are precisely the elements in \( J(i, 2) - J(i, 1) \).

Extend \( \alpha(i, 1) \) to a homomorphism \( \alpha(i, 2) \) of \( J(i, 2) \) upon \( M \) as follows:

1. If \( a \in J(i, 1) \), define \( \alpha a(i, 2) = \alpha a(i, 1) \).
2. If \( c \in J(i, 2) - J(i, 1) \) then \( ac = b \) where \( a \) and \( b \) are in \( J(i, 1) \). Define \( \alpha a(i, 2) = x \) where \( x \) is any element of \( M \) such that \( \alpha a(i, 1) \cdot x = \beta a(i, 1) \).

Next, let \( J(i+1, 0) \) be an extension of \( J(i, 2) \) such that

(i) If \( a \in J(i, 2) \) but \( 1 \cdot a \notin J(i, 2) \) then \( 1 \cdot a = a \) in \( J(i+1, 0) \) and if \( a \cdot 1 \notin J(i, 2) \), then \( a \cdot 1 = a \) in \( J(i+1, 0) \).

(ii) For each ordered pair \( a, b \) in \( J(i, 2) \) where \( a \neq b \) and \( a \neq 1 \), let \( J(i+1, 0) - J(i, 2) \) contain an element \( c \) such that \( ca = b \).

As before, the elements adjoined in (ii) are precisely the elements in \( J(i+1, 0) - J(i, 2) \) and they are all distinct.

Now we extend \( \alpha(i, 2) \) to a homomorphism \( \alpha(i+1, 0) \) of \( J(i+1, 0) \) upon \( M \) as follows:

1. If \( a \in J(i, 2) \), define \( \alpha a(i+1, 0) = \alpha a(i, 2) \).
2. If \( c \in J(i+1, 0) - J(i, 2) \), then \( ac = b \) where \( a \) and \( b \) are in \( J(i, 2) \). If \( \alpha a(i, 2) = \beta a(i, 2) \), define \( \alpha a(i+1, 0) = 1 \). In all other cases, define \( \alpha a(i+1, 0) = y \) where \( y \) is any element of \( M \) such that \( y \cdot a a(i, 2) = \beta a(i, 2) \).
We see that $J(i+1, 0)$ has properties (I'), (II'), (III') listed for $J(i, 0)$.

We may now define a countable sequence of halfgroupoids $J(0, 0)$, $J(1, 0)$, \ldots, as follows:

1. $J(0, 0)$ has the same elements as $M$ with no products defined. $J(0, 0)$ has properties (I'), (II'), (III') trivially.

2. $J(i+1, 0)$ is an extension of $J(i, 0)$ obtained in the manner described above.

If $\alpha(0, 0)$ is the identity mapping on $M$ then $H = \bigcup_{i=0}^{\infty} J(i, 0)$ is the required loop image and $\alpha = \bigcup_{i=0}^{\infty} \alpha(i, 0)$ is the required homomorphism of $H$ upon $M$.

References


Montana State University