Normal and characteristic structure in quasigroups and loops

Tim Hardcastle

Submitted for the degree of Doctor of Philosophy at the University of Leicester

September 2003

ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106-1346

Abstract

In this thesis I shall be exploring the normal and characteristic structure of quasigroups and loops. In recent years there has been a revival of interest in the theory of loops and in particular in the relationship between the properties of a loop and the properties of its multiplication group; and several powerful new theorems have emerged which allow the structural properties of a loop to be related to its multiplication group. I shall combine these ideas with tools developed at the beginning of loop theory to produce some interesting new theorems, principally relating the order of a finite multiplication group to the structure of its loop.

Acknowledgements

I should like first of all to thank my supervisor, Professor Rick Thomas, for his advice and encouragement throughout the writing of this thesis.

Gratitude is also due to Professor Markku Niemenmaa for keeping both of us informed as to what was known and what remained to be discovered in loop theory.

I am extremely grateful to the Engineering and Physical Sciences Research Council (EPSRC) for funding this research.

Contents

1 Introduction

1.1 Quasigroups and loops

Intuitively, a loop is a weakened form of a group. It has an identity, and a strong form of cancellation (for now, it's enough to say that for a finite loop, the multiplication table is a latin square — each element of the loop appears exactly once in each row and column). This is not equivalent to the existence of an inverse for each element, so this is a weakening of the group laws. Finally, associativity is just dropped, and in general loop theory no weaker law replaces it.

A quasigroup is a loop without an identity (or alternatively a loop is a quasigroup with an identity). Quasigroups are harder to work with than loops: as we shall see, an identity brings a whole lot of other structure with it.

It is the non-associativity which makes working with loops challenging. It also restricts the use for loops. The reason why group theory has been so successful is the fact that functions under composition are associative. There is simply not such a great demand for non-associative binary algebras, even if they do have identities and cancellation. Nonetheless, there are interesting applications for loops, principally in incidence geometry. I shall not discuss the geometric applications of loop theory in this thesis.

I was first drawn to loops and loop-like objects more or less recreationally.

I was interested in finding algebraic structures more primitive than groups which nonetheless had the group property of a one-to-one relation between congruences on the algebra and normal subalgebras (Loops are by no means the most primitive structure of this kind. For example, consider an algebra with left cancellation as for loops, and with a right pseudoidentity — an element e such that $(x.e).(y.e) = (x.y).e$.)

Many concepts in group theory do *not* translate well into loop theory. For example, without associativity it is hard to define the order of an element: again, without associativity and inverses, how are we to define conjugation? Lagrange's theorem fails, Sylow's theorem becomes meaningless, the idea of a p-subgroup needs serious revision. It is no longer true that a characteristic subalgebra must be normal ...

What remains is largely the theory associated with normal subgroups. For example, Lagrange's theorem does hold for normal subloops; the Jordan-Hölder theorem applies to loops; the concepts of solvability and nilpotence may be carried over to loops, as may the idea of the centre.

One important concept in loop theory is the idea of the multiplication group of a loop (for group theorists, the multiplication group of a group is its holomorph). In group theory, the relationship between the structure of the group and the structure of its holomorph is downright trivial: they will belong to the same algebraic varieties.

Another topic which is more interesting in loop theory than in group theory is the idea of isotopy. Isotopy is an equivalence relation on loops which is broader than isomorphy: as two isotopic *groups* must be isomorphic, isotopy plays no part in group theory.

1.2 Universal algebra

It is expected that the reader will be familiar with group theory: any group theory referred to in this thesis will be found in any reasonably detailed textbook on group theory such as Marshall Hall's *The Theory of Groups.* [17]. A little universal algebra will also be required, such as may be found in Cohn [9].

The idea of universal algebra is this: when, in the first year of our undergraduate studies, we are presented with some kind of algebra (groups, rings, lattices, semigroups) we are invariably told something along the lines of "A group" — (ring, lattice, whatever) — "is a set together with some operations (on the elements of the set) and obeying the following axioms". Universal algebra asks the sensible question: what can we say about such systems in the abstract — without knowing what the operations are, what the axioms are, or how big the set of elements is?

Hence universal algebra may be regarded as the natural generalisation of algebra. I shall sketch out the most important definitions I shall be using, and the most important theorem.

Definition 1.1 *The* **type** *of an algebra is the bag of arities of its operations. For example, the type of a group is to have one operation of arity 2 (multiplication), one operation of arity 1 (taking inverses) and one operation of arity 0 — otherwise called a constant operation — namely the identity.*

I should now define what is meant by a **law**. It is perhaps easier to give an example. Given the operations $*, ^{-1}, 1_G$, we may say exactly what is meant by a group by giving the following laws

- $1_G * x \approx x$
- $x * 1_G \approx x$
- $x * x^{-1} \approx 1_G$
- $x^{-1} * x \approx 1_G$
- $(x * y) * z \approx x * (y * z)$

where the $\approx$ symbol is to be read "this equation holds for *all* choices, from the elements of the algebra under question, of values for the variables".

Now this is a little different from the usual abstract definition of a group. Why so? The reason is that we want to present the variety of groups in terms of laws: claims that a certain equation holds in the algebra for all choices of the variables. The usual axiom $\exists\, 1_G \in G s.t. 1_G * x = x = x * 1_G$ is not in this form. We deal with the existence of the identity elelment by making the identity element part of the type, saying that 1_G is a constant operation of the algebra. In the same way, instead of having an axiom claiming that inverses exist — which would not be a law — we introduce an inverse operation into the type and have a law *telling us how this operation behaves.*

Some more examples: if we add to the laws for groups already listed the law $x * y \approx y * x$ then we are describing commutative groups. If instead we add the law $x^n = 1_G$ we are defining the nth Burnside variety. Semigroups have only one operation of arity 2 and the single law $x * (y * z) \approx (x * y) * z$. If we wish to describe rings (with unit) in this format we note that rings have two operations of arity 2 (multiplication and addition), one of arity 1 (sending an element to its additive inverse) and two constant operations, 0_R and 1_R. It is then fairly easy to write down the ring laws, except that within this format of specifying algebras by laws, it is impossible to claim that $0_R \neq 1_R$. Hence in universal algebra we have to put up with considering the trivial unring as a ring.

I might at this point give a formal definition of what is meant by "homomorphism", "subalgebra" and "direct product" in the context of universal algebra. However, it is sufficient in fact to say that the definitions are the same (only generalised) as they are for your own pet favourite algebra.

DEFINITION 1.2 *The class of all algebras (which must of course all be of the same type) obeying a given set of laws (suitable for that type) is called a* **variety***.*

Now it is easy to check that the homomorphic image of any algebra belonging to a given variety, or the subalgebra of any algebra belonging to a given variety, or the direct product of any set of algebras belonging to a given variety, must also belong to that variety. More surprisingly, the converse is true. I shall first need some definitions to formalise the statement of the theorem.

DEFINITION 1.3 *For any class C of algebras let* $\mathbf{H}C$ *be the class of all homomorphic images of algebras in* S, *let* $\mathbf{S}C$ *be the class of all algebras isomorphic to subalgebras of algebras in* C, *and let* $\mathbf{P}C$ *be the class of all algebras isomorphic to direct products of algebras in* C

The following theorem was proved by Birkhoff [4], and is known as the **HSP** theorem.

THEOREM 1.4 *A class C of algebras is a variety if and only if C is closed under* $\mathbf{H}$, $\mathbf{S}$ *and* $\mathbf{P}$. □

It is interesting to note that saying C is closed under $\mathbf{H}$, $\mathbf{S}$ and $\mathbf{P}$ is just equivalent to the claim that $C = \mathbf{HSP}C$

This is practically everything the reader needs to know about universal algebra in order to follow the reasoning in this thesis. Other results will be mentioned when needed. I might add that I sometimes, where there is no danger of confusion, I shall be very casual in my treatment of varieties. For example, I shall discuss conditions for a loop to “be a group”. Now strictly a loop can't be a group, because they're algebras of a different type. What I shall mean is that the multiplication table of the loop is such that it could also be the multiplication table of a group; in the same way, I may discuss conditions for a set with a single binary operation to “be a loop”: similar remarks apply.

1.3 Overview of the thesis

Section 1 is the present introduction. In Section 2 I define the variety of quasigroups and review some simple results concerning them. I shall introduce the multiplication group of a loop, and I shall also introduce the useful combinatorial ideas of projection and core, and discuss characteristic subquasigroups of quasigroups. In Section 3 I define the variety of loops, and give some of the best-known and most useful results. I review the theorem of Niemenmaa and Kepka which characterises those groups which may be multiplication groups of loops. I discuss characteristic subloops of loops, especially with reference to the concepts of projection and core introduced earlier, and show how this discussion relates to the ideas of solvability and nilpotence in loops and groups. I give a brief overview of the idea of loop isotopy.

In Section 4 I shall show how the concepts of projection and core, combined with the results of Niemenmaa, Kepka and Vesanen can be used to relate the structure of loops to their multiplication groups.

In Section 5 I discuss Bruck's generalisation of solvability in loops and groups, and give my own version of generalised solvability in groups, loops and rings using considerations from universal algebra. I show how an alternative route leads to the same generalisation, demonstrating that anything that behaves sufficiently like a (generalised) commutator subloop actually is one.

In Section 6 I show how the idea of nilpotence may be generalised, first for groups and loops and then for any variety. I conclude with some very general results on concepts analogous to nilpotence in the case of loops and similarly attractive varieties.

2 Quasigroups

This section introduces some definitions and well-known results concerning quasigroups.

DEFINITION 2.1 *A* **quasigroup** *is a quadruple* $(Q, . \;, \backslash\backslash, /\!/)$ *consisting of a set* Q *and three binary operations: multiplication, left division and right division, defined* $Q \times Q \to Q$ *such that*

- $x\backslash\backslash(x.y) \approx y$
- $x.(x\backslash\backslash y) \approx y$
- $(x.y)/\!/y \approx x$
- $(x/\!/y).y \approx x$

This is not the only definition of a quasigroup: there is another, which is not equivalent, but contains a slightly wider class of algebraic objects. However, it has the advantage that quasigroups as so defined are a variety, and so with this definition in place we may assert that direct products, subalgebras and homomorphic images of quasigroups are quasigroups. For other definitions this last assertion may be false. I shall call the variety of quasigroups $\mathcal{Q}$.

We may write the multiplication operation using juxtaposition only: that is, writing xy for $x.y$. However, as the multiplication operation is not guaranteed to be associative some bracketing would usually be necessary. For convenience, though, we shall adopt the convention that juxtaposition takes precedence over actually writing the operation, so that, for example we may write $a.bc$ for $a.(b.c)$ and $ab.cd$ for $(a.b).(c.d)$. Similarly, multiplication written by juxtaposition will take precedence over left or right division, so we may write, for example, $a\backslash\backslash bc$ for $a\backslash\backslash(b.c)$.

THEOREM 2.2 *The functions λ_q, ρ_q defined (for any $q \in Q$) from Q to Q by $\lambda_q x = qx$ and $\rho_q x = xq$ are bijections $L \leftrightarrow L$.*

PROOF: We shall give the proof only for λ_q, since the proofs are symmetric.

Let $\lambda_q x = \lambda_q y$. Then $qx = qy$, so $q\backslash\backslash qx = q\backslash\backslash qy$, so $x = y$ by quasigrouphood. So λ_q is one-to-one. Furthermore, for any $z \in L$ we have $\lambda_q(q\backslash\backslash z) = q.(q\backslash\backslash z) = z$. So λ_q is onto. □

DEFINITION 2.3 *Let Q be a quasigroup. Then the* **multiplication group** *of Q — denoted by $\mathcal{M}(Q)$ — is defined by $\mathcal{M}(Q) = \langle\lambda_Q, \rho_Q\rangle$, where by the natural abuse of notation $\lambda_Q = \{\lambda_q : q \in Q\}$ and similarly for ρ_Q.*

Clearly $\mathcal{M}(Q)$ is a subgroup of the symmetric group on the elements of Q.

DEFINITION 2.4 *A quasigroup Q is said to be* **commutative** *if and only if $xy \approx yx$*

DEFINITION 2.5 *A quasigroup Q is said to be* **Abelian** *if and only if $wx.yz \approx wy.xz$*

Definition 2.6 *A quasigroup Q is said to be* **associative** *if and only if* $x.yz \approx xy.z$

Clearly these definitions all give rise to subvarieties of quasigroups. Note that in quasigroup theory, "Abelian" doesn't mean the same thing as "commutative", nor does either one imply the other. The following well-known result shows why there is no discussion of associative quasigroups.

Theorem 2.7 *Let Q be an associative quasigroup. Then Q is a group.*

Proof: Note first of all that if Q is associative, then $yz \approx yz \Rightarrow (x(x\backslash\backslash y))z \approx yz \Rightarrow x((x\backslash\backslash y)z) \approx yz \Rightarrow (x\backslash\backslash y)z \approx x\backslash\backslash(yz)$. Then if we choose any $p, q \in Q$ we have $(p\backslash\backslash p)q = p\backslash\backslash(pq) = q$. Hence $p\backslash\backslash p$ is a left identity for the quasigroup. Similarly $p/\!/p$ is a right identity of the quasigroup. Hence $(p\backslash\backslash p) = (p\backslash\backslash p)(p/\!/p) = (p/\!/p)$, so $p\backslash\backslash p$ is a left and right identity, which I shall call 1_Q.

Then we know by theorem 2.2 that for each $x \in Q$ there is a unique element — call it x^{-L} such that $x^{-L}x = 1_Q$. Similarly there is a right inverse x^{-R}. Now using associativity, we have $x^{-L} = x^{-L}1_Q = x^{-L}(xx^{-R}) = (x^{-L}x)x^{-R} = x^{-R}$.

So we have an identity, inverses, and associativity as required. □

The following theorem will prove very useful:

THEOREM 2.8 *If Qisaquasigroup, then$\mathcal{M}(Q)$ is an Abelian group if and only if Q is an Abelian group.*

PROOF: For trivially if Q is an Abelian group then $Q \cong \mathcal{M}(Q)$. Conversely, let $\mathcal{M}(Q)$ be Abelian. Then for any x, y, z we have $x.yz = \lambda_x \rho_z y = \rho_z \lambda_x y = xy.z$, so Q is associative and hence a group. As Q is associative we have $\lambda_x \lambda_y = \lambda_{xy}$ for any x, y. So for any z we have have $xy.z = \lambda_{xy} z = \lambda_x \lambda_y z = \lambda_y \lambda_x z = \lambda_{yx} z = yx.z$. So cancelling on the right by z, we have $xy = yx$. So Q is a commutative group. □

DEFINITION 2.9 *A subquasigroup of a quasigroup Q is (as one would expect) a non-empty subset H of the elements of Q which is closed under the operations $., \backslash\backslash, //$ of the quasigroup, together with the restrictions of these operations to H.*

DEFINITION 2.10 *Let Q be a quasigroup. An equivalence relation $\sim$ having equivalence classes $[x] = \{q \in Q : x \sim q\}$ is said to be a* **congruence** *on Q if and only if for all $x, y \in Q$ we have*

$$[x].[y] = [x.y]$$

$$[x]\backslash\backslash[y] = [x\backslash\backslash y]$$

$$[x]//[y] = [x//y]$$

where by the usual abuse of notation we define $[x].[y] = \{pq : p \in [x], q \in [y]\}$ and similarly for $[x]\backslash\backslash[y]$ and $[x]//[y]$.

THEOREM 2.11 *Let Q be a quasigroup. Then for every homomorphism ϕ from Q to ϕQ the relation on Q given by $x \sim y \Leftrightarrow \phi x = \phi y$ is a congruence on Q; conversely, if R is a congruence on Q, then the function mapping q to $[q]_R$ is a homomorphism (with the natural operation on the congruence classes).* □

DEFINITION 2.12 *A quasigroup is said to be* **simple** *if and only if no congruences can be defined on its elements other than the trivial congruence (which relates each element of Q only to itself) and the complete congruence (which relates every element of Q to every other element of Q).*

The following theorem is very useful, so much so that I shall give it a name.

THEOREM 2.13 (THE COSET THEOREM) *Let Q be a quasigroup and let $\sim$ be an equivalence relation on Q. Then $\sim$ is a congruence if and only if $\mu[x] = [\mu x]$ for all $\mu \in \mathcal{M}(Q), x \in Q$.*

PROOF: Let $\sim$ be such an equivalence relation. Then we wish to prove that $[x][y] = [xy]$. (We should also prove that $[x]\backslash\backslash[y] = [x\backslash\backslash y]$ and $[x]/\!/[y] = [x/\!/y]$, but as the proofs are similar we shall omit them).

So for any $x, y \in Q$, choose any $x' \in [x]$ and any $y' \in [y]$. Now by hypothesis $\mu[x] = [\mu x]$ for any $\mu \in \mathcal{M}(Q)$, so this holds in particular for λ_x. Hence as y and y' lie in the same class, so do $\lambda_x y$ and $\lambda_x y'$ — that is, xy and

xy'. By similar reasoning we may esablish that xy' and $x'y'$ lie in the same class, and hence that xy and $x'y'$ lie in the same class — that is, $x'y' \in [xy]$; and so, since x' and y' are arbitrary members of $[x]$ and $[y]$, we may conclude that $[x][y] \subseteq [xy]$.

To see that $[x][y] \supseteq [xy]$, consider that $[x][y] \supseteq x[y] = \lambda_x[y] = [\lambda_x y]$ by hypothesis. But $[\lambda_x y] = [xy]$. Hence $[x][y] = [xy]$ as required.

Conversely, suppose that $\sim$ is a congruence. Then on the one hand, as $x \in [x]$, we have $x[y] \subseteq [x][y] = [xy]$. On the other hand, let $z \in [xy]$. Then $z = x(x\backslash\backslash z)$. So as $[z] = [xy]$ we have $[x(x\backslash\backslash z)] = [xy]$ so $[x][x\backslash\backslash z] = [x][y]$. Now as $Q/\sim$ is a quasigroup, $[x\backslash\backslash z] = [y]$. Hence $x\backslash\backslash z \in [y]$. So as $z = x(x\backslash\backslash z)$, we have $z \in x[y]$. Hence $x[y] = [xy]$. Similar reasoning shows that $[y]x = [yx]$.

Hence $\lambda_x[y] = [\lambda_x y]$ and $\rho_x[y] = [\rho_x y]$, and as $\mathcal{M}(Q) = \langle \lambda_Q, \rho_Q \rangle$, we deduce inductively that $\mu[y] = [\mu y]$ for all $\mu \in \mathcal{M}(Q)$. □

Another way of stating the result is to say that an equivalence relation is a congruence if and only if the elements of $\mathcal{M}(Q)$ permute the equivalence classes.

In the above theorem we deduced that for any congruence we have $x[y] = [xy] = [x]y$. It is then clear that just one given congruence class of any congruence serves to define the whole congruence, since the other congruence classes will all be cosets of the one given.

The following well-known result is also immediate from the Coset Theorem.

THEOREM 2.14 *Let Q be a finite quasigroup and $\sim$ any congruence on Q. Then the number and order of the congruence classes divide the order of Q.* □

DEFINITION 2.15 *A subquasigroup K of a quasigroup Q is said to be* **normal** *— in which case we write $K \trianglelefteq Q$ — if and only if K is a congruence class of some congruence on Q.*

Note that it is certainly not true in quasigroup theory — as it *is* in group theory — that every subquasigroup of a finite quasigroup Q must have order dividing the order of Q. Indeed, it has been proved that for any natural number n and any natural number k such that $k \leq n/2$ we may produce a quasigroup with order n having a subquasigroup of order k — so Lagrange's theorem fails as badly for quasigroups as it possibly can. However, by the definition above and by Theorem 2.14, it trivially holds for normal quasigroups.

DEFINITION 2.16 *The action of a permutation group on its set is said to be* **primitive** *if and only if there is no partition of its set (other than the trivial and complete partitions) such that every member of the group permutes the classes of the partition.*

Hence we have the following theorem. Of course, it follows directly from the Coset Theorem.

THEOREM 2.17 *Let Q be a quasigroup. Then Q is simple if and only if the action of $\mathcal{M}(Q)$ on Q is primitive.* □

2.1 Introducing the projection and core

The ideas of projection and core were introduced (not under those names, which are mine) by Albert [1] and Bruck [6] respectively, in the study of loops. As they may be introduced more generally in the context of quasigroups, I shall do so.

THEOREM 2.18 *Let $N \trianglelefteq \mathcal{M}(Q)$. Then the relation $\sim_N$ given by*

$$x \sim_N y \Leftrightarrow Nx = Ny$$

is a congruence on Q.

PROOF: Clearly $\sim_N$ is an equivalence relation. If $Nx = Ny$ then $y \in Nx$. Hence $[x] = Nx$. Now as N is normal in $\mathcal{M}(Q)$, we have

$$\lambda_x[y] = \lambda_x Ny = N\lambda_x y = N(xy) = [xy] = [\lambda_x y],$$

and similarly $\rho_x[y] = [\rho_x y]$. As $\mathcal{M}(Q) = \langle \lambda_Q, \rho_Q \rangle$, we have $\mu[y] = [\mu y]$ for all $\mu \in \mathcal{M}(Q)$ by induction. So the relation is a congruence by the Coset Theorem. □

DEFINITION 2.19 *The congruence* $\sim_N$ *will be called the* **projection** *of* N *onto* Q.

So we can get from normal subgroups of $\mathcal{M}(Q)$ to congruences on Q. Now let's try going the other way.

DEFINITION 2.20 *Let* Q *be a quasigroup and let* $\sim$ *be a congruence on* Q. *Then the* **core** *of* $\sim$ *in* $\mathcal{M}(Q)$ *— denoted* $\mathrm{cor}_{\mathcal{M}(Q)}(\sim)$ *— is defined by letting* $\mathrm{cor}_{\mathcal{M}(Q)}(\sim) = \{\mu \in \mathcal{M}(Q) : \mu[x] = [x] \ \forall x \in Q\}$.

Where there is no possible ambiguity (and there hardly ever is), I shall write $\mathrm{cor}(\sim)$ for $\mathrm{cor}_{\mathcal{M}(Q)}(\sim)$.

THEOREM 2.21 *For any quasigroup* Q *and any congruence* $\sim$ *on* Q *we have* $\mathrm{cor}(\sim) \trianglelefteq \mathcal{M}(Q)$.

PROOF: Choose any $\zeta \in \mathrm{cor}(\sim)$ and any $\mu \in \mathcal{M}(L)$. By the Coset Theorem we have $\mu^{-1}\zeta\mu[x] = \mu^{-1}\zeta[\mu x] = \mu^{-1}[\mu x]$ (by choice of ζ) $= [\mu^{-1}\mu x] = [x]$. Hence $\mu^{-1}\zeta\mu[x] \in \mathrm{cor}(\sim)$ as required. □

THEOREM 2.22 *For any quasigroup* Q *and any congruence* $\sim$ *on* Q *we have* $(\mathrm{cor}(\sim))x = [x]$.

PROOF: As $\mathrm{cor}(\sim)$ fixes every congruence class, and $x \in [x]$, we must have $(\mathrm{cor}(\sim))x \subseteq [x]$. On the other hand, if $y \sim z$ then $\lambda_y\lambda_z^{-1} \in \mathrm{cor}(\sim)$ and

so for any z we have $\lambda_{[z]}\lambda_z^{-1} \subseteq \operatorname{cor}(\sim)$. Now $\lambda_{[z]}\lambda_z^{-1}x = [z].(z\backslash\backslash x)$. Using the identities discovered in theorem 2.13, we have $[z].(z\backslash\backslash x) = z.[z\backslash\backslash x] = z.(z\backslash\backslash [x]) = [x]$. Hence we have $[x] \subseteq (\operatorname{cor}(\sim))x$ giving equality as required.
□

COROLLARY 2.23 $\sim$ *is trivial if and only if* $\operatorname{cor}(\sim)$ *is trivial.*

PROOF: On the one hand if $\sim$ is trivial then $\operatorname{cor}(\sim)$ must fix every member of Q and so contains only the identity. On the other hand, if $\operatorname{cor}(\sim)$ is trivial then by the result above we must have $[x] = \iota_{\mathcal{M}(Q)}x = \{x\}$ as required. □

Define the set

$$\operatorname{fix}(x) = \{\mu \in \mathcal{M}(Q) : \mu x = x\}.$$

Trivially this is a subgroup for any choice of x in Q, and it partitions the elements of $\mathcal{M}(Q)$ into cosets according to their action on x.

THEOREM 2.24 *Let* $N \trianglelefteq \mathcal{M}(Q)$ *and let* $x \in Q$. *Then* $\sim_N$ *is the complete congruence if and only if* $N\operatorname{fix}(x) = \mathcal{M}(Q)$.

PROOF: On the one hand if $N\operatorname{fix}(x) = \mathcal{M}(Q)$ then we have

$$[x] = Nx = N\operatorname{fix}(x)x = \mathcal{M}(Q)x = Q.$$

On the other hand, if $\sim_N$ is the complete congruence then $Nx = Q$, so as the cosets of $\operatorname{fix}(x)$ partition the elements of $\mathcal{M}(Q)$ according to their action on x we have at least one element of N in each coset of $\text{fix}(x)$. Hence $N\text{fix}(x) = \mathcal{M}(Q)$ as required. □

From the preceding results, we obtain the following:

THEOREM 2.25 *For any choice of $x \in Q$, Q is simple if and only if the following condition holds*

$$\{\iota_{\mathcal{M}(Q)}\} < N \trianglelefteq \mathcal{M}(Q) \Rightarrow N\text{fix}(x) = \mathcal{M}(Q)$$

□

THEOREM 2.26 *Let $N \trianglelefteq \mathcal{M}(Q)$. Then $N \subseteq \text{cor}(\sim_N)$.*

PROOF: Choose any $\nu \in N$ and any congruence class $[x]$. Then

$$\nu[x] = \nu N x = N x = [x].$$

□

COROLLARY 2.27 $\text{cor}(\sim) = \bigcup\{N \trianglelefteq \mathcal{M}(Q) : \ \sim_N \ \subseteq \ \sim \ \}$. □

THEOREM 2.28 $\mathcal{M}(Q)/\text{cor}(\sim) \cong \mathcal{M}(Q/\sim)$.

PROOF: For let $\Theta : \mathcal{M}(Q) \to \mathcal{M}(Q/\sim)$ be defined by $\Theta\lambda_x = \lambda_{[x]}$ and by $\Theta\rho_x = \rho_{[x]}$. As $\mathcal{M}(Q) = \langle \lambda_Q, \rho_Q \rangle$ and $\mathcal{M}(Q/\sim)$ is generated by elements of the form $\lambda_{[x]}$ and $\rho_{[x]}$ this does indeed give a mapping $\mathcal{M}(Q) \to \mathcal{M}(Q/\sim)$, though on the face of it, this mapping need not be well-defined. However, as by Theorem 2.13 we have

$$x[y] = [xy] = [x][y]$$

and similarly

$$[y]x = [yx] = [y][x],$$

we have $\lambda_{[x]}[y] = \lambda_x[y]$ and similarly $\rho_{[x]}[y] = \rho_x[y]$. Then by trivial induction Θ is well-defined and a homomorphism, and obviously is onto $\mathcal{M}(Q/\sim)$. Clearly it has kernel

$$\{\mu \in \mathcal{M}(Q) : \mu[x] = [x]\ \forall x \in Q\} = \mathrm{cor}(\sim)$$

as required. □

We may mention one interesting corollary here, which we shall apply a great deal in the loop case. Recall that $\mathcal{M}(Q)$ is an Abelian group if and only if Q is an Abelian group. Hence we have the following.

COROLLARY 2.29 *For any quasigroup Q and congruence $\sim$ it follows immediately that $\mathcal{M}(Q/\sim)$ is Abelian if and only if $\mathcal{M}(Q)'$ — the derived subgroup of $\mathcal{M}(Q)$ — is contained in* $\mathrm{cor}(\sim)$. *Hence $\sim_{\mathcal{M}(Q)'}$ is the unique smallest congruence on Q such that the quotient quasigroup is an Abelian group.* □

2.2 Automorphisms and characteristic congruences

In this subsection I shall introduce the idea of a "characteristic congruence", which appears to be my own, although the idea is straightforward enough. This subject will be tackled extensively in the final section of this thesis

DEFINITION 2.30 *Let Q be a quasigroup. The set of* **automorphisms** *of Q — written* $\mathrm{Aut}(Q)$ *— is the set of all bijections α on X such that, for all $x, y \in Q$ we have $\alpha(x.y) = \alpha x.\alpha y$.*

It is trivial to show that $\mathrm{Aut}(Q)$ with composition of functions is a group.

DEFINITION 2.31 *Let Q be a quasigroup. Then a congruence $\sim$ on Q is said to be* **characteristic** *if and only if $\alpha[x] = [\alpha x]$ for all $\alpha \in \mathrm{Aut}(Q)$ and $x \in Q$.*

Now if we choose any automorphism $\alpha \in \mathrm{Aut}(Q)$ this induces an automorphism $\overline{\alpha} \in \mathrm{Aut}(\mathcal{M}(Q))$ given by letting $\overline{\alpha}\lambda_x = \lambda_{\alpha x}$ and $\overline{\alpha}\rho_x = \rho_{\alpha x}$. Indeed, the mapping $\alpha \mapsto \overline{\alpha}$ is an embedding of $\mathrm{Aut}(Q)$ in $\mathrm{Aut}(\mathcal{M}(Q))$.

THEOREM 2.32 *Let N be characteristic in $\mathcal{M}(Q)$. Then $\sim_N$ is a characteristic congruence of Q.*

PROOF: Let α be any member of $\mathrm{Aut}(Q)$. Then there is an induced automorphism $\overline{\alpha} \in \mathrm{Aut}(\mathcal{M}(Q))$ defined by $\overline{\alpha}\lambda_x = \lambda_{\alpha x}$ and $\overline{\alpha}\rho_x = \rho_{\alpha x}$. It is trivial to check that this is indeed a well-defined automorphism. Then for any $x, y \in Q$ we have

$$\alpha(\lambda_y x) = \alpha(yx) = \alpha y.\alpha x = \lambda_{\alpha y}\alpha x = (\overline{\alpha}(\lambda_y))\alpha x$$

Similarly $\alpha(\rho_y x) = (\overline{\alpha}(\rho_y))\alpha x$. Hence by induction we have $\alpha\mu y = (\overline{\alpha}(\mu))\alpha y$ for all $\mu \in \mathcal{M}(Q)$. Hence $\alpha N x = (\overline{\alpha}(N))\alpha x$ and as (by hypothesis) N is characteristic we have $\overline{\alpha}(N) = N$. Hence $\alpha N x = N\alpha x$ as required. □

3 Loops

3.1 Loop varieties

DEFINITION 3.1 *A loop is a quintuple* $(L, ., \backslash\!\backslash, /\!/, 1_L)$ *such that the reduct* $(L, ., \backslash\!\backslash, /\!/)$ *is a quasigroup and such that*

- $1_L x \approx x$
- $x 1_L \approx x$

I shall call the variety of loops $\mathcal{L}$. Various subvarieties of the variety of loops have come under investigation for one reason or another. The following varieties, for example, arise naturally from the geometric applications of loop theory. For a wider survey, see [8].

DEFINITION 3.2 *A loop L is said to be* **right Bol** *if and only if* $(xy.z)y \approx x(yz.y)$

DEFINITION 3.3 *A loop L is said to be* **Moufang** *if and only if it obeys the law*

$$(x.zx)y \approx x(z.xy)$$

This definition is taken from [26]. Additional laws were once specified, but they were proved by Bruck and others to follow from the law given.

A loop will be said to be associative, commutative, or Abelian just if it obeys, respectively, the associative, commutative and Abelian laws for quasigroups. By our theorem for quasigroups, an associative loop is a group. We also have the following well-known result:

THEOREM 3.4 *L is an Abelian loop if and only if L is a commutative group.*

PROOF: If we have the Abelian law $wx.yz \approx wy.xz$ then we also have the law $w1_L.yz \approx wy.1_Lz$, i.e. $w.yz \approx wy.z$ — the associative law. So L is a group. Similarly, $wx.yz \approx wy.xz \Rightarrow 1_Lx.y1_L \approx 1_Ly.x1_L$, i.e. $xy \approx yx$ — the commutative law.

On the other hand, if a group is commutative then we certainly have $wx.yz \approx wy.xz$, since $xy \approx yx$. □

One obvious corollary is that the classes of Abelian groups and commutative groups are identical, in line with usual group-theoretic useage.

3.2 Normal subloops

You will recall that a normal subquasigroup of a quasigroup is defined as a subquasigroup which is a congruence class of some congruence on the quasigroup. A **normal subloop** of a loop may be defined the same way. If K is a normal subloop of L I shall write $K \trianglelefteq L$, and if K is a proper normal subloop of L I shall write $K \triangleleft L$.

Now on the one hand, for every congruence R we have

$$[1_L]_R[1_L]_R = [1_L1_L]_R = [1_L]_R,$$

so for every congruence $[1_L]_R$ is a normal subloop of L. On the other hand, some congruence class $[x]_R$ of L is a subloop of L if and only if $[x]_R[x]_R = [x]_R$. But the only idempotent element of $L/\sim$ is the identity of $L/\sim$, which obviously is $[1_L]_R$.

Hence:

THEOREM 3.5 *There is a bijective mapping between congruences on L and normal subloops of L given by mapping a congruence R to the class* $[1_L]_R$. □

From our discussion of quasigroups it is evident that the cosets of $[1_L]_R$ are precisely the equivalence classes of R. In short, we have demonstrated that the correspondence theorem for groups works just as well for loops, and so we may regard $[1_L]_R$ as being the **kernel** of the natural homomorphism from L to L/R, in precisely the group-theoretic sense.

Now we know in general that $x[y] = [xy]$ for congruences on quasigroups. So for a normal subloop K of L we must have $xK.yK = xy.K$ for all $x, y \in L$. Indeed, this would do as an alternative definition of "normal subloop", since the converse is also true: if for some $K \subseteq L$ we have $xK.yK = xy.K$ for all $x, y \in L$, then $K \trianglelefteq L$.

From this identity we may also deduce the two useful identities $xK = Kx$ and $xy.K = x.yK$ for any normal subloop K and any $x, y \in L$

For loops, then, as for groups, instead of writing $L/\sim$ we shall write L/K, where K is the normal subloop $[1_L]_\sim$. The following holds in loops just as in groups:

THEOREM 3.6 *Let $H \leq L$ and let $J, K \trianglelefteq L$. Then*

- $J \cap K \trianglelefteq L$
- $JK \trianglelefteq L$
- $H \cap J \trianglelefteq H$
- $HK = KH \leq L$

□

Furthermore, the three isomorphism theorems may be stated just the same for loops as for groups.

DEFINITION 3.7 *If H is a subloop of a loop L, then we may define $\underline{H}$ to be the largest normal subloop of L contained in H, and also we may define $\overline{H}$ to be the smallest normal subloop of L containing H.*

As in group theory, these are indeed well-defined for any $H \leq L$.

We may define normal subloops another way, as was first pointed out by Bruck.

DEFINITION 3.8 *If L is a loop, we may define a subgroup $\mathcal{I}(L)$ of $\mathcal{M}(L)$ by*

$$\mathcal{I}(L) = \mathrm{fix}(1_L) = \{\gamma \in \mathcal{M}(L) : \gamma 1_L = 1_L\},$$

which we shall call the **inner mapping group** *of the loop.*

Bruck offers us an alternative definition (see [6]): $\mathcal{I}(L)$ is that subgroup of $\mathcal{M}(L)$ generated by all elements of the form $\rho_{xy}^{-1}\rho_y\rho_x$ and $\rho_{xy}^{-1}\lambda_x\rho_y$. This definition is easier to work with for some purposes.

Now λ_L and ρ_L are both transversals to $\mathcal{I}(L)$ in $\mathcal{M}(L)$. This is trivial to prove just by considering that the cosets of $\mathcal{I}(L)$ must partition the elements of $\mathcal{M}(L)$ according to their action on 1_L.

It then follows from this and the Coset Theorem that a subloop of L is normal if and only if it is fixed by every element of $\mathcal{I}(L)$. For a group G the mappings $\mathcal{I}(G)$ are just the inner automorphisms of the group: this fits nicely with our ideas about groups.

Another definition of normal subloop was given by Albert [1]. Reviewing our results on projection and core in quasigroups, we might say that a subloop K is normal if and only if there is some $N \trianglelefteq \mathcal{M}(L)$ such that $N1_L = K$. In his classic paper, Albert urges this definition as "much more natural" than the others which had been put forward. One wonders what these definitions were, and what on earth Albert would consider unnatural and factitious.

In the second part of this paper [2], he gives the first proof that the refinement and Jordan-Hölder theorems work exactly the same for loops as they do for groups. Nowadays this would be proved from a more abstract universal-algebraic point of view.

DEFINITION 3.9 *A* **composition series** *for a loop is a series*

$$L = K_0 \rhd K_1 \rhd \ldots \rhd K_n = 1_L$$

such that for all $i < n$, K_{i+1} is maximal normal in K_i (that is, is not contained in any larger proper normal subloop of K_i).

DEFINITION 3.10 *The* **factor loops** *of a loop are the loops K_i/K_{i+1} for each $0 \leq i < n$, where the series $K_0 \ldots K_n$ are defined as above.*

Obviously we need to prove that these factor loops are well-defined, and that is exactly what the Jordan-Hölder theorem tells us.

THEOREM 3.11 (THE JORDAN-HÖLDER THEOREM) *If a loop has two composition series*

$$L = J_0 \rhd J_1 \rhd \ldots \rhd J_m = 1_L$$

and

$$L = K_0 \rhd K_1 \rhd \ldots \rhd K_n = 1_L$$

then $n = m$, and the factor loops from each series can be put into isomorphic pairs. □

Obviously, any loop with the descending chain condition on its lattice of subloops must *have* a composition series. I shall make use of the Jordan-Hölder theorem later, when I generalise Fitting's theorem.

The main structure theorems missing from loop theory when compared to group theory are the idea of the order of an element, Lagrange's theorem, Sylow's theorem, the idea of two subgroups being conjugate, the concept of an inner automorphism, and so forth. What we get to keep are largely the theorems about normal subgroups, which as can be seen from the discussion above, carry over very nicely from groups.

Usually when we think about a projection from a normal subgroup N of $\mathcal{M}(L)$ into L we shall only care about the coset $N1_L$. Similarly in loops we may talk about $\text{cor}(K)$ rather than $\text{cor}(\sim)$, where $K = [1_L]_\sim$.

3.3 Niemenmaa and Kepka

In this subsection I shall review an important result of Niemenmaa and Kepka [24] which characterises multiplication groups of loops.

Recall that the inner mapping group of a loop L is defined by

$$\mathcal{I}(L) = \text{fix}(1_L) = \{\gamma \in \mathcal{M}(L) : \gamma 1_L = 1_L\},$$

and that λ_L and ρ_L are both transversals to $\mathcal{I}(L)$ in $\mathcal{M}(L)$.

We can say something quite definite about $\mathcal{I}(L)$. First we need a little basic group theory.

Let G be any group and let $H \leq G$. We define $\underline{H}$ to be the largest subgroup of H which is normal in G. This is usually called the core of H in G, but as I am already using the word "core" extensively, I shall just refer to $\underline{H}$.

LEMMA 3.12 *Let G be any group, and let H be any subgroup of G. Let $K = \{h \in H : \forall g \in G \; g^{-1}hg \in H\}$. Then $K = \underline{H}$*

PROOF: Clearly $\underline{H} \subseteq K$, as $\underline{H} \trianglelefteq G$. So it remains only to prove that K is a normal subgroup, and the result follows.

Of course, $1_G \in K$. Now choose any $x, y \in K$. Then choose any $g \in G$. By hypothesis, $g^{-1}xg = h_1 \in H$ and $g^{-1}y^{-1}g = h_2 \in H$. So $g^{-1}xy^{-1}g = g^{-1}xgg^{-1}y^{-1}g = h_1h_2$, which is in H as H is a subgroup. Hence $K \leq G$, and clearly K is normal in G. Hence $K \subseteq \underline{H}$ so $K = \underline{H}$ as required. □

Then we obtain the following result.

LEMMA 3.13 *Let L be a loop. Then $\underline{\mathcal{I}(L)}$ is trivial.*

PROOF: Choose any $\phi \in \mathcal{I}(L)$ other than the identity. Then there exists $p \in L$ such that $\phi(p) = q$ with $p \neq q$. Now consider the element $\lambda_p^{-1}\phi\lambda_p \in \mathcal{M}(L)$. Then

$$\lambda_p^{-1}\phi\lambda_p(1_L) = \lambda_p^{-1}\phi(p.1_L) = \lambda_p^{-1}\phi(p) = \lambda_p^{-1}(q).$$

We know that $\lambda_p^{-1}(p) = 1_L$ and by hypothesis $p \neq q$. So $\lambda_p^{-1}(q) \neq 1_L$, so $\lambda_p^{-1}\phi\lambda_p(1_L) \neq 1_L$, so $\lambda_p^{-1}\phi\lambda_p$ is not in $\mathcal{I}(L)$ so ϕ is not in $\underline{\mathcal{I}(L)}$. □

Now this is as much as to say that $\mathcal{I}(L)$ contains no non-trivial normal subgroups of $\mathcal{M}(L)$.

LEMMA 3.14 *Let L be a loop. Then $[\lambda_L, \rho_L] \subseteq \mathcal{I}(L)$.*

PROOF: For choose any $\lambda_p \in \lambda_L$ and any $\rho_q \in \rho_L$. Then

$$\lambda_p^{-1}\rho_q^{-1}\lambda_p\rho_q(1_L) = (p\backslash\!\backslash((p.(1_L.q))/\!\!/q) = p\backslash\!\backslash((p.q))/\!\!/q) = p\backslash\!\backslash p = 1_L$$

as required. □

THEOREM 3.15 *So, from the two previous lemmas, we obtain the following: if G is (isomorphic to) a multiplication group of a loop, then it necessarily contains a subgroup H containing no non-trivial normal subgroup of G and having transversals A and B such that $[A, B] \subseteq H$ and $\langle A, B\rangle = G$.*

We shall now prove that these are in fact sufficient conditions for G to be (isomorphic to) the multiplication group of a loop. We require a few preliminary results. Recall that where H is a subloop of a loop L I am using $\underline{H}$ to denote the largest normal subloop of L contained in H.

LEMMA 3.16 *Let G be any group, and let H be any subgroup of G. Suppose A and B are transversals to H in G such that $[A, B] \subseteq H$ (in which case we* *say that A and B are H-connected) and suppose that the $\underline{H}$ is trivial. Then the representative of H in A (i.e. $a \in A$ such that $aH = H$) must be the identity, and similarly with the representative of H in B.*

As the proofs are symmetric I shall give the proof for A only.

Let $aH = H$ (so $\{a\} = A \cap H$) and choose any $g \in G$. As B is a transversal to H in G we may write $g = bh$ for some $b \in B$ and $h \in H$. Now as A and B are H-connected, $a^{-1}b^{-1}ab \in H$; so as $a \in H$, we have $aa^{-1}b^{-1}ab \in H$, so $b^{-1}a^{-1}b \in H$, so $h^{-1}b^{-1}a^{-1}bh \in H$.

This shows that $g^{-1}a^{-1}g \in H$, for any $g \in G$. So by Lemma 3.12, a^{-1} is in the $\underline{H}$, which by hypothesis is trivial. So $a^{-1} = 1_G$ and so $a = 1_G$ as required.

DEFINITION 3.17 *A* **stable (left) transversal** *to H in G is a transversal T such that Tg is also a transversal for any $g \in G$.*

LEMMA 3.18 *Let A and B be H-connected transversals to H in G. Then they are stable.*

I shall prove this only for A, as the proofs are symmetric. For choose any $x \in G$. We require that Ax is a transversal: that is, for any $g \in G$ there exist unique $a \in A$ and $k \in H$ such that $axk = g$. First we shall prove existence. Note that we may write $x = bh$ for some $b \in B$, $h \in H$. Having chosen such b, h , we may then pick, for our given g, some $a \in A$ and some

$h' \in H$ such that $g = bah'$. Hence $g = axx^{-1}a^{-1}bah' = axh^{-1}b^{-1}a^{-1}bah'$. So let $k = h^{-1}b^{-1}a^{-1}bah'$. Then as A and B are H-connected, $b^{-1}a^{-1}ba \in H$ and so $h^{-1}ba^{-1}bah' \in H$. So $g = axk$ with $k \in H$ as required.

Secondly, we must prove uniqueness. Suppose there exists $g \in G$ such that $g = a_1xh_1 = a_2xh_2$ with $a_1, a_2 \in A$ and $h_1, h_2 \in H$. Then

$$a_1xh_1 = a_2xh_2$$

$$\Rightarrow a_1xh_1H = a_2xh_2H$$

$$\Rightarrow a_1xH = a_2xH$$

$$\Rightarrow (a_1x)^{-1}a_2x \in H.$$

As before, we shall write $x = bh$: hence $(a_1bh)^{-1}a_2bh \in H$ so $h^{-1}b^{-1}a_1^{-1}a_2bh \in H$ and so $b^{-1}a_1^{-1}a_2b \in H$. Furthermore, as A and B are H-connected, we have $a_1^{-1}b^{-1}a_1b \in H$ and $b^{-1}a_2^{-1}ba_2 \in H$.

So multiplying these together, since H is a subgroup, we get

$$(a_1^{-1}b^{-1}a_1b)(b^{-1}a_1^{-1}a_2b)(b^{-1}a_2^{-1}ba_2) \in H$$

i.e. (by cancelling) $a_1^{-1}a_2 \in H$. So $a_1H = a_2H$ so as $a_1, a_2 \in A$, and A is a transversal, we must have $a_1 = a_2$. But then we have $g = a_1xh_1 = a_1xh_2$ and so $h_1 = h_2$ as required.

THEOREM 3.19 *Let G contain a subgroup H such that $\underline{H}$ is trivial and having H-connected transversals A and B such that $\langle A, B\rangle = G$. Then G is the multiplication group of a loop.*

PROOF: First of all, since A is a transversal to H in G, we may define a function f from $G \to A$ defined by letting $f(x) = a \in A$ such that $xH = aH$. Now consider the set C of cosets of H in G. We can define an operation $*$ on C by $xH * yH = f(x)yH$. I claim that $(C, *)$ is a loop — or rather, the reduct of a loop — and that G is its multiplication group.

We must first establish that $*$ is well-defined. Suppose $xH = x'H$ and $yH = y'H$. Then $f(x) = f(x')$, so $f(x)yH = f(x')y'H$ so $xH * yH = x'H * y'H$.

Now $(C, *)$ is the reduct of a quasigroup. For on the one hand, if we pick any xH, zH, then we may choose $y = f(x)^{-1}z$ and then we have

$$xH * yH = f(x)f(x)^{-1}zH = zH.$$

On the other hand we know that A is a stable transversal to H : hence for any y, $f(G)y$ is a transversal to H, and so for any z there exists x such that $f(x)yH = zH$, and hence $xH * yH = zH$.

Furthermore, $(C, *)$ has an identity, namely H, and is therefore a loop. For clearly $xH * H = f(x)H = xH$, so H is a right identity. In addition, $H * yH = f(h)yH$ for some $h \in H$. Now by Lemma 3.15, we must have $f(h) = 1_G$. Now $1_G yH = yH$, so H is a left identity.

So $(C, *)$ is the reduct of a loop.

It remains only to prove that $G \cong \mathcal{M}(C) = \langle \lambda_C, \rho_C \rangle \leq S_C$. So define a function $\theta : G \to S_C$ by the rule $[\theta x](zH) = xzH$. Now θ is a homomorphism, for clearly

$$[\theta x]([\theta y](zH)) = xyzH = [\theta xy](zH)$$

for all $zH \in C$.

Furthermore, θ is onto $\mathcal{M}(C)$. For choose any $xH \in C$, and consider that for each $zH \in C$ we have $\lambda_x H(zH) = xH * zH = f(x)zH = azH$ for some $a \in A$, and so $\lambda_x H(zH) = [\theta a](zH)$ for all $zH \in C$ and so $\lambda_x H = \theta a$ for some $a \in A$. Conversely, if we choose any $a \in A$ then we have $\theta a = \lambda_a H$. Hence we have $\theta A = \lambda_C$.

The proof that $\theta B = \rho_C$ is similar, but a little harder. Let g be the function from G to B such that $g(x)H = xH$. Choose any $xH \in C$, and consider that for each $zH \in C$ we have

$$\rho_x H(zH) = zH * xH = f(z)xH = f(z)g(x)H.$$

Now as A and B are H-connected, $f(z)g(x)H = g(x)f(z)H$ and so

$$\rho_x H(zH) = g(x)f(z)H = g(x)zH = bzH$$

for some $b \in B$, and so $\rho_x H(zH) = [\theta b](zH)$ for all $zH \in C$ and so $\rho_x H = \theta b$ for some $b \in B$. Conversely, if we choose any $b \in B$ then we have $\theta b = \rho_b H$. Hence we have $\theta B = \rho_C$.

So θ maps the generators of $G = \langle A, B \rangle$ onto the generators of $\mathcal{M}(C) = \langle \lambda_C, \rho_C \rangle$, and so $\theta G = \mathcal{M}(C)$.

It remains only to prove that θ is an isomorphism from G to $\mathcal{M}(C)$. Now let $k \in \ker \theta$. Then $\theta k = \iota_{S_C}$, so in particular $[\theta k](H) = H$, i.e. $kH = H$, so

$k \in H$. So $\ker\theta \leq H$, and as $\ker\theta$ is normal in G, $\ker\theta \trianglelefteq H$. But any normal subgroup of G contained in H is trivial by hypothesis; so $\ker\theta = \{1_G\}$, and so θ is an isomorphism as required. □

So putting the two theorems above together, we obtain the Niemenmaa-Kepka theorem:

THEOREM 3.20 *Let G be a group. Then $G \cong^{\phi} \mathcal{M}(L)$ for some loop L if and only if there exists $H \leq G$ with transversals A and B (not necessarily distinct) such that*

1. $[A, B] \leq H$.
2. $G = \langle A, B \rangle$.
3. *H contains no non-trivial normal subgroup of G.*

If these conditions hold then L is such that $H = \phi\mathcal{I}(L), A = \phi\lambda_G$, and $B = \phi\rho_G$ □

Obviously the possibilities opened out by the Niemenmaa-Kepka theorem have played an important role in reviving interest in loop theory and in particular the study of multiplication groups of loops. The other major recent theorem is Vesanen's.

3.4 Vesanen's theorem

THEOREM 3.21 (VESANEN'S THEOREM) *Let $\mathcal{M}(L)$ be solvable and finite. Then L is weakly solvable (see Section 4.5 for a definition of "weakly solvable").* □

I shall not attempt to given the full proof here, but shall sketch the ideas used, as they will recur in my own treatment of loops with solvable multiplication group.

The reasoning goes something like this: suppose that we could prove the theorem for finite simple loops. Then we could prove the theorem for finite loops in general, by induction on the order of the loop. For if L is not simple, then take any maximal normal subloop K of L. Then as the theorem holds for all finite simple groups (the base hypothesis), we have L/K solvable, and as $\mathcal{M}(K)$ is a homomorphic image of a subgroup of $\mathcal{M}(L)$, it is solvable and strictly smaller than $\mathcal{M}(L)$ — hence by the inductive hypothesis K is solvable. So L is solvable.

So it suffices to prove the theorem for finite simple loops. The argument goes like this. $M(L)$ is solvable. Take the sequence $\mathcal{M}(L), \mathcal{M}(L)', \mathcal{M}(L)''$.... One (exactly) of these will be non-trivial Abelian, and is a characteristic subgroup of $\mathcal{M}(L)$ — call it B. The order of B is divisible by some prime p. Let U be the subgroup of B generated by its elements of order p. This is also characteristic in $M(L)$, and non-trivial. Hence as L is simple we have

$U1_L = L$, and so $\mathcal{M}(L) = U\mathcal{I}(L)$. Pick V to be any non-trivial subgroup of U which is fixed by the conjugation actions of $\mathcal{M}(L)$ and which is minimal with respect to this property. As $\mathcal{M}(L) = U\mathcal{I}(L)$ and as U is Abelian, we have that V is a non-trivial normal subgroup of $\mathcal{M}(L)$ and so have $\mathcal{M}(L) = V\mathcal{I}(L)$.

Now the intersection of V with $\mathcal{I}(L)$ must be trivial. For the intersection is normal both in $\mathcal{I}(L)$ and of course in V as V is Abelian. Hence it is contained in $\mathcal{I}(L)$ and normal in $\mathcal{M}(L)$, and so by the Niemenmaa-Kepka theorem is trivial. So $\mathcal{M}(L) = V \rtimes^{\phi} \mathcal{I}(L)$. Now the kernel of ϕ is of course normal in $\mathcal{I}(L)$, and by definition its members commute with those of V. Hence $\ker \phi$ is normal in $\mathcal{M}(L)$ and so is trivial.

So to summarise: if L is finite simple and $\mathcal{M}(L)$ is solvable, then

$$\mathcal{M}(L) = V \rtimes^{\phi} \mathcal{I}(L),$$

where V is a finite dimensional vector space over F_p for some prime p, where ϕ gives a regular representation of $\mathcal{I}(L)$ in the linear group associated with V, and where the representation of $\mathcal{I}(L)$ fixes no proper non-trivial subspace of V.

To complete the theorem, we must prove that in such a case we must have V one-dimensional and $\mathcal{I}(L)$ trivial. Vesanen's proof relies on breaking the problem down into various different cases according to the value of p, and further exposition of the theorem here would not give the reader any particular insight into loop theory as such (though he or she would end up much better informed about general linear groups in particular).

Vesanen's theorem itself, together with adaptations of its reasoning, will later allow me to prove many interesting results about finite loops.

3.5 Isotopy

This subsection contains a brief review of the idea of isotopy: any results stated are well-known.

DEFINITION 3.22 *If $(X, *)$ is a quasigroup and (α, β, γ) is any ordered triple of bijective functions $X \leftrightarrow X$ then we may define a binary operation $\circ$ from $X \times X \rightarrow X$ given by $x \circ y = \gamma^{-1}(\alpha x * \beta y)$. Then the algebra $(X, \circ)$ is called an* **isotope** *of $(X, *)$ and the triple (α, β, γ) is said to be an* **isotopism** *from $(X, *)$ to $(X, \circ)$.*

THEOREM 3.23 *An isotope of a quasigroup is a quasigroup.* □

It is sensible to ask why we should want to consider the isotopes of a quasigroup.

- The concept of isotopy is a generalisation of isomorphy (except, trivially, that we are requiring that the two quasigroups have the same carrier set X). For if we have two quasigroups written with the same carrier set, and an isomorphism θ between them, then the triple (θ, θ, ι)

is an isotopism between them. Given the large number of morphically distinct quasigroups and loops even of small order (there are, for example, 23,750 anisomorphic loops of order 7, but these can be classified into "only" 563 isotopy classes) it is often more convenient to classify quasigroups and loops up to isotopism instead of isomorphism.

- Quasigroups and loops arise naturally in geometry, and in particular in the theory of 3-webs. Now when one finds "the" quasigroup of a 3-web, one may in fact equally well take any isotope of this quasigroup as "the" quasigroup of the 3-web. Thus consideration of isotopy classes arises naturally from the motivating subject matter of quasigroup theory.

- Isotopisms from loops to loops (**loop isotopisms**) preserve a considerable amount of algebraic structure. For example, let L_1, L_2 be isotopic loops. Then the following results hold.

    1. If L_1 is a group, then $L_1 \cong L_2$. This is, of course, why isotopy plays no part in group theory.
    2. $\mathcal{M}(L_1) \cong \mathcal{M}(L_2)$.
    3. $\mathcal{I}(L_1) \cong \mathcal{I}(L_2)$.
    4. $\mathcal{Z}(L_1) \cong \mathcal{Z}(L_2)$.
    5. The lattice of normal subloops of L_1 is isomorphic to the lattice of normal subloops of L_2..
    6. $N_\lambda(L_1) \cong N_\lambda(L_2)$.

7. $N_\mu(L_1) \cong N_\mu(L_2)$.

8. $N_\rho(L_1) \cong N_\rho(L_2)$.

(Here $N_\lambda(L), N_\mu(L), N_\rho(L)$ are the elements of L associating on the left, middle and right respectively).

However, some features of loops are not isotopy invariant: for example, the lattice of subloops of L_1 need not be isomorphic to the lattice of subloops of L_2, nor — rather surprisingly, given the results above — need it be true that $N(L_1) \cong N(L_2)$ — where $N(L) = N_\lambda(L) \cap N_\mu(L) \cap N_\rho(L)$ (see, for example [7]).

There are certain interesting loop varieties such if L_1, L_2 are isotopic loops then $L_1 \in \mathcal{V} \Leftrightarrow L_2 \in \mathcal{V}$ — that is, loop isotopy preserves the variety. These include groups and any group subvariety, Bol loops and Moufang loops. A large collection of such varieties may be identified as follows. Let $\mathcal{V}$ be any group variety. Then it's easy to check that the class

$$\mathcal{W} = \{L \in \mathcal{L} : \mathcal{M}(L) \in \mathcal{V}\}$$

is a loop variety. Now as isotopic loops have isomorphic multiplication groups, it follows that $L_1 \in \mathcal{W} \Leftrightarrow L_2 \in \mathcal{W}$. There are also varieties such that $L_1 \in \mathcal{V} \Rightarrow L_1 \cong L_2$ — in which case we say that $\mathcal{V}$ has the **isotopy-isomorphy** property. These include any group variety and commutative Moufang loops.

For my purposes, the most important result on isotopy is the following:

THEOREM 3.24 *Let* $(L_1, *)$ *and* $(L_2, \circ)$ *be two isotopic loops. Then* L_2 *is isomorphic to an isotope* $(L_3, .)$ *of* L_1 *with multiplication given by* $a.b = a/\!\!/y * x\backslash\!\!\backslash y$. $\square$

4 Loops and their multiplication groups

4.1 Characteristic subloops

DEFINITION 4.1 *Following group theory, we shall say that a subloop H of a loop L is* **characteristic** *in L if and only if it is fixed by every automorphism of L.*

Now in a group G, the inner mapping group $\mathcal{I}(G)$ is a group of automorphisms of G, and so if N is characteristic in G then $N \trianglelefteq G$. However, this is not necessarily true of $\mathcal{I}(L)$ in the case where L is not a group (though it may be), and so characteristic subloops of loops are not necessarily normal. The following is a smallest counterexample.

EXAMPLE 4.2

	1	2	3	4	5
1	1	2	3	4	5
2	2	1	5	3	4
3	3	5	4	2	1
4	4	3	1	5	2
5	5	4	2	1	3

Now the subloop $H = \{1, 2\}$ is clearly characteristic in L — it's the only order 2 subloop of L — but cannot be normal, as we know that normal subloops have order dividing the order of the loop. So in general, we can't expect characteristic subloops to be as well-behaved as are characteristic subgroups. We may, however, identify some characteristic subloops of loops which are necessarily normal.

THEOREM 4.3 *Let K be normal in L. Then K is a characteristic subloop if and only if the cosets of K in L are a characteristic congruence.*

PROOF: On the one hand, if the cosets are a characteristic congruence, then any automorphism permutes the cosets. But any automorphism of L must fix the identity, and so fixes the coset containing the identity, namely K.

On the other hand, suppose that K is characteristic, and choose any $\alpha \in \mathrm{Aut}(Q)$ and any coset xK of K in Q. Then

$$\alpha x K = \alpha x . \alpha K = \alpha x . K,$$

which is a coset of K. □

Hence from our discussion of characteristic congruences of quasigroups in the previous section, we immediately obtain the following result:

THEOREM 4.4 *Let N be a characteristic subgroup of $\mathcal{M}(L)$. Then $N1_L$ is a normal characteristic subloop of L* □

We observed in the context of quasigroups that given any automorphism $\alpha \in \mathrm{Aut}(L)$ this induces an automorphism $\overline{\alpha} \in \mathrm{Aut}(\mathcal{M}(L))$ given by letting

$\overline{\alpha}\lambda_x = \lambda_{\alpha x}$ and $\overline{\alpha}\rho_x = \rho_{\alpha x}$, and that the mapping $\alpha \mapsto \overline{\alpha}$ is an embedding of $\mathrm{Aut}(L)$ in $\mathrm{Aut}(\mathcal{M}(L))$. We might ask: can it be an isomorphism?

THEOREM 4.5 *Let L be a loop. Then* $\mathrm{Aut}(L) \cong \mathrm{Aut}(\mathcal{M}(L))$ *if and only if L is an Abelian group.*

PROOF: "Only if" is clear, since if L is an Abelian group then $L \cong \mathcal{M}(L)$.

"If" is only a little harder. Choose any $\alpha \in \mathrm{Aut}(L)$ and consider the induced automorphism $\overline{\alpha} \in \mathrm{Aut}(\mathcal{M}(L))$. Now $\overline{\alpha}(\mathcal{I}(L)) = \mathcal{I}(L)$. Intuitively this is clear: as α fixes 1_L, $\overline{\alpha}$ must fix $\mathcal{I}(L)$. For a rigorous proof, we use Bruck's original definition of $\mathcal{I}(L)$ (see [6]). That is: $\mathcal{I}(L)$ is that subgroup of $\mathcal{M}(L)$ generated by all elements of the form $\rho_{xy}^{-1}\rho_y\rho_x$ (which I'll call $\sigma_{x,y}$) and $\rho_{xy}^{-1}\lambda_x\rho_y$ (denoted by $\tau_{x,y}$). Now

$$\overline{\alpha}(\sigma_{x,y}) = \overline{\alpha}(\rho_{xy}^{-1}\rho_y\rho_x) = \rho_{\alpha x\alpha y}^{-1}\rho_{\alpha y}\rho_{\alpha x} = \sigma_{\alpha x,\alpha y},$$

and by similar reasoning $\overline{\alpha}(\tau_{x,y}) = \tau_{\alpha x,\alpha y}$. So $\overline{\alpha}$ maps the generators of $\mathcal{I}(L)$ onto the generators of $\mathcal{I}(L)$ and so $\overline{\alpha}(\mathcal{I}(L)) = \mathcal{I}(L)$ as required.

So suppose the mapping $\alpha \mapsto \overline{\alpha}$ is an isomorphism. Then as any induced automorphism must fix $\mathcal{I}(L)$, it follows that $\mathcal{I}(L)$ is characteristic in $\mathcal{M}(L)$, and hence normal. But we know that the only normal subgroup contained in $\mathcal{I}(L)$ is trivial. So $\mathcal{I}(L)$ is trivial, and so by [23] we know that L is an Abelian group. □

The results of the following two theorems should be intuitively acceptable to the reader:

THEOREM 4.6 *Let H be characteristic in L Then $\underline{H}$ is characteristic in L.*

PROOF: Let $\alpha \in \mathrm{Aut}(L)$. Then as H is characteristic in L and $\underline{H} \subseteq H$, we have $\alpha\underline{H} \subseteq H$ and as $\underline{H} \trianglelefteq L$ we have $\alpha\underline{H} \trianglelefteq L$. Hence $\underline{H}\alpha\underline{H} \subseteq H$ and $\underline{H}\alpha\underline{H} \trianglelefteq L$. So $\underline{H}\alpha\underline{H} \subseteq \underline{H}$, as $\underline{H}$ is the largest normal subloop of L in H. So $\alpha\underline{H} \subseteq \underline{H}$, for any $\alpha \in \mathrm{Aut}(L)$).

Conversely, by the forgoing, $\alpha^{-1}\underline{H} \subseteq \underline{H}$, so $\alpha\alpha^{-1}\underline{H} \subseteq \alpha\underline{H}$, i.e. $\underline{H} \subseteq \alpha\underline{H}$, so $\underline{H} = \alpha\underline{H}$, and so $\underline{H}$ is characteristic in L as required. □

THEOREM 4.7 *Let H be characteristic in L. Then $\overline{H}$ is characteristic in L.*

PROOF: The proof is dual to that above. Let $\alpha \in \mathrm{Aut}(L)$. Then as H is characteristic in L and $\overline{H} \supseteq H$, we have $\alpha\overline{H} \supseteq H$ and as $\overline{H} \trianglelefteq L$ we have $\alpha\overline{H} \trianglelefteq L$. Hence $\overline{H} \cap \alpha\overline{H} \supseteq H$ and $\overline{H} \cap \alpha\overline{H} \trianglelefteq L$. So $\overline{H} \cap \alpha\overline{H} \supseteq \overline{H}$, as $\overline{H}$ is the smallest normal subloop of L containing H. So $\alpha\overline{H} \supseteq \overline{H}$, for any $\alpha \in \mathrm{Aut}(L)$.

Conversely, by the forgoing, $\alpha^{-1}\overline{H} \supseteq \overline{H}$, so $\alpha\alpha^{-1}\overline{H} \supseteq \alpha\overline{H}$, i.e. $\overline{H} \supseteq \alpha\overline{H}$, so $\overline{H} = \alpha\overline{H}$, and so $\overline{H}$ is characteristic in L as required. □

I shall now investigate some particular characteristic subloops of loops.

4.2 The centre and nuclei

The results in this subsection are well-known, but will prove to be useful later on.

DEFINITION 4.8 *Let L be a loop. Then we define*

1. $N_\lambda(L) = \{a \in L : a.xy = ax.y \ \forall x, y \in L\}$.
2. $N_\rho(L) = \{a \in L : xy.a = x.ya \ \forall x, y \in L\}$.
3. $N_\mu(L) = \{a \in L : x.ay = xa.y \ \forall x, y \in L\}$.

It is trivial to check that these are characteristic subloops of L. They are known respectively as the **left nucleus**, **right nucleus**, *and* **middle nucleus** *of L. Then we may define the* **nucleus** *of L by*

$$N(L) = N_\lambda(L) \cap N_\mu(L) \cap N_\rho(L)$$

DEFINITION 4.9 *Let L be a loop. Then $\mathcal{Z}(L)$ — the* **centre** *of L — is defined by $\mathcal{Z}(L) = \{a \in N(L) : ax = xa \ \forall x \in L\}$.*

Of course, $\mathcal{Z}(L)$ is characteristic in L. Note that we could equally well define the centre of L by the Abelian law, saying that

$$\mathcal{Z}(L) = \{a \in L : ax.yz = ay.xz \wedge xa.yz = xy.az \wedge xy.za = xz.ya\}$$

Although this is more æsthetically satisfying, it is marginally harder to work with.

THEOREM 4.10 $\mathcal{Z}(L) = \mathcal{Z}(\mathcal{M}(L))1_L$.

PROOF: Let $z \in \mathcal{Z}(L)$. Then for any $x, y \in L$ we have

$$\lambda_z\lambda_x y = z.xy = zx.y = xz.y = x.zy = \lambda_x\lambda_z y,$$

so

$$\lambda_z\lambda_x = \lambda_x\lambda_z.$$

Similarly

$$\lambda_z\rho_x y = z.yx = zy.x = \rho_x\lambda_z y,$$

so $\lambda_z\rho_x y = \rho_x\lambda_z y$. So as $\mathcal{M}(L) = \langle\lambda_L, \rho_L\rangle$, we have $\lambda_z \in \mathcal{Z}(\mathcal{M}(L))$ and hence $z \in \mathcal{Z}(\mathcal{M}(L))1_L$.

Conversely, let $\zeta \in \mathcal{Z}(\mathcal{M}(L))$. Then

$$\zeta 1_L.x = \rho_x\zeta 1_L = \zeta\rho_x 1_L = \zeta(1_L.x) = \zeta x.$$

Similarly,

$$x.\zeta 1_L = \lambda_x\zeta 1_L = \zeta\lambda_x 1_L = \zeta(x.1_L) = \zeta x.$$

So putting these results together, we have $\zeta 1_L.x = x.\zeta 1_L$ for all $x \in L$.

Furthermore, we have

1. $(\zeta 1_L)(xy) = \zeta(xy) = \zeta\rho_y x = \rho_y\zeta x = (\zeta x)y = ((\zeta 1_L)x)y$. So $\zeta 1_L \in N_\lambda(L)$.

2. $(xy)\zeta 1_L = \zeta(xy) = \zeta\lambda_x y = \lambda_x\zeta y = x((\zeta 1_L)y) = x(y.\zeta 1_L)$. So $\zeta 1_L \in N_\rho(L)$.

3. $x((\zeta 1_L)y) = x(y.\zeta 1_L) = (xy)\zeta 1_L = (\zeta 1_L)(xy) = ((\zeta 1_L)x)y = (x.\zeta 1_L)y$.
So $\zeta 1_L \in N_\mu(L)$.

Hence $\zeta 1_L$ commutes with every $x \in \mathcal{M}(L)$ and $\zeta 1_L \in N(L)$. So $\zeta 1_L \in \mathcal{Z}(L)$ as required.

So $\mathcal{Z}(L) = \mathcal{Z}(\mathcal{M}(L))1_L$. □

COROLLARY 4.11 *Hence we have*

$$\langle \lambda_{\mathcal{Z}(L)}, \rho_{\mathcal{Z}(L)} \rangle \subseteq \mathcal{Z}(\mathcal{M}(L)) \subseteq \mathrm{cor}_{\mathcal{M}(L)}(\mathcal{Z}(L)) \subseteq \mathcal{Z}(\mathcal{M}(L))\mathcal{I}(L).$$

□

4.3 The lower central series

DEFINITION 4.12 *Let L be a loop and let $L = N_0 \supseteq N_1 \supseteq N_2 \ldots$ and let $N_i/N_{i+1} \subseteq \mathcal{Z}(L/N_{i+1})$ for all i. Then the series $N_0, N_1, N_2 \ldots$ is said to be a* **central series** *of L.*

DEFINITION 4.13 *A loop is said to be* **nilpotent** *if and only if it has a central series $N_0, N_1, N_2 \ldots$ such that $N_n = \{1_L\}$ for some n.*

It is then easy to prove the following well-known result:

THEOREM 4.14 *If $\mathcal{M}(L)$ is nilpotent then so is L.*

PROOF: For let $\mathcal{M}(L)$ have terminating central series $N_0, N_1, N_2 \ldots N_n$. Pick any i between 0 and $n-1$.

Let Θ be the usual homomorphism $\Theta : \mathcal{M}(L) \to \mathcal{M}(L/N_{i+1}1_L)$ defined by $\Theta\lambda_x = \lambda_{N_{i+1}x}$ and by $\Theta\rho_x = \rho_{N_{i+1}x}$. Let Δ then be the associated isomorphism from $\mathcal{M}(L)/\mathrm{cor}(N_{i+1}1_L)$ to $\mathcal{M}(L/N_{i+1}1_L)$ given by $\Delta(\mu\mathrm{cor}(N_{i+1}1_L)) = \Theta(\mu)$.

Now

$$N_i/N_{i+1} \subseteq \mathcal{Z}(\mathcal{M}(L)/N_{i+1})$$

by hypothesis. Now as

$$\mathrm{cor}(N_{i+1}1_L) \supseteq N_{i+1}$$

we have

$$N_i\mathrm{cor}(N_{i+1}1_L)/\mathrm{cor}(N_{i+1}1_L) \subseteq \mathcal{Z}(\mathcal{M}(L)/\mathrm{cor}(N_{i+1}1_L))$$

so then

$$\Delta(N_i\mathrm{cor}(N_{i+1}1_L)/\mathrm{cor}(N_{i+1}1_L)) \subseteq \Delta(\mathcal{Z}(\mathcal{M}(L)/\mathrm{cor}(N_{i+1}1_L)))$$

i.e.

$$\Theta(N_i) \subseteq \mathcal{Z}(\mathcal{M}(L/N_{i+1}1_L))$$

— as Δ is an isomorphism it necessarily maps the centre to the centre.

Hence the projection of $\Theta(N_i)$ into $L/N_{i+1}1_L$ is in the centre of $L/N_{i+1}1_L$. Now the elements of the projection of $\Theta(N_i)$ are given by

$$\Theta(N_i)1_{L/N_{i+1}1_L} = \{(\Theta\nu)N_{i+1}1_L : \nu \in N_i\}.$$

Now recalling that for any ν we have

$$(\Theta\nu)N_{i+1}1_L = \nu N_{i+1}1_L$$

we may rewrite this as

$$\Theta(N_i)1_{L/N_{i+1}1_L} = \{\nu N_{i+1}1_L : \nu \in N_i\}.$$

Now as $N_i \supseteq N_{i+1}$ we have

$$\bigcup\{\nu N_{i+1}1_L : \nu \in N_i\} = \{\nu 1_L : \nu \in N_i\} = N_i 1_L.$$

Hence $N_i 1_L / N_{i+1}1_L \subseteq \mathcal{Z}(L/N_{i+1})$. Hence the series $N_0 1_L \ldots N_n 1_L$ is a central series for L, and clearly if N_n is trivial then so is $N_n 1_L$. □

DEFINITION 4.15 *Let L be a loop and let $\Gamma_0 = L$ and then define inductively $\Gamma_{i+1} = [\mathcal{M}(L), \overline{M_L(\Gamma_i)}]1_L$, — where as usual by $\overline{M_L(\Gamma_i)}$ we mean the normal closure of $\langle \lambda_{\Gamma_i}, \rho_{\Gamma_i} \rangle$ in $\mathcal{M}(L)$. Then the series $\Gamma_0, \Gamma_1, \Gamma_2 \ldots$ is called the* **lower central series** *of L.*

THEOREM 4.16 *The lower central series of L is a central series of L.*

PROOF: Choose any $\mu \in \mathcal{M}(L)$ and any $x \in \Gamma_i$. Then certainly we have

$$[\mu, \lambda_x][\mathcal{M}(L), \mathcal{M}(\Gamma_i)] = [\mathcal{M}(L), \mathcal{M}(\Gamma_i)]$$

i.e.

$$\mu^{-1}\lambda_x^{-1}\mu\lambda_x[\mathcal{M}(L), \mathcal{M}(\Gamma_i)] = [\mathcal{M}(L), \mathcal{M}(\Gamma_i)]$$

so

$$\mu\lambda_x[\mathcal{M}(L), \mathcal{M}(\Gamma_i)] = \lambda_x\mu[\mathcal{M}(L), \mathcal{M}(\Gamma_i)].$$

So as we have

$$\mathrm{cor}(\Gamma_{i+1}) \supseteq [\mathcal{M}(L), \overline{M_L(\Gamma_i)}] \supseteq [\mathcal{M}(L), M_L(\Gamma_i)]$$

it follows that

$$\mu\lambda_x\mathrm{cor}(\Gamma_{i+1}) = \lambda_x\mu\mathrm{cor}(\Gamma_{i+1})$$

for any $\mu \in \mathcal{M}(L)$. Hence

$$\lambda_x\mathrm{cor}(\Gamma_{i+1}) \in \mathcal{Z}(\mathcal{M}(L)/\mathrm{cor}(\Gamma_{i+1})).$$

Similar reasoning applies to ρ_x so we conclude that

$$M_L(\Gamma_i)\mathrm{cor}(\Gamma_{i+1})/\mathrm{cor}(\Gamma_{i+1}) \subseteq \mathcal{Z}(\mathcal{M}(L)/\mathrm{cor}(\Gamma_{i+1}))$$

and so $\Gamma_i/\Gamma_{i+1} \subseteq \mathcal{Z}(L/\Gamma_{i+1})$ as required. □

We shall now justify the term "lower" central.

THEOREM 4.17 *Let $N_0, N_1, N_2 \ldots$ be a central series of L. Then for all i we have $\Gamma_i \subseteq N_i$.*

PROOF: We work, of course, by induction. The result clearly holds for $i = 0$, as $L \subseteq L$. Now suppose we have $\Gamma_i \subseteq N_i$.

As the series $N_0, N_1, N_2 \ldots$ is central we have $N_i/N_{i+1} \subseteq \mathcal{Z}(L/N_{i+1})$. Hence $M_L(N_i)\mathrm{cor}(N_{i+1})/\mathrm{cor}(N_{i+1}) \subseteq \mathcal{Z}(\mathcal{M}(L)/\mathrm{cor}(N_{i+1}))$.

So for any choice of $\gamma \in \mathcal{M}(L)$ and any $\mu \in N_i$ we have

$$[\gamma, \mu]\mathrm{cor}(N_{i+1}) = \gamma^{-1}\mu^{-1}\gamma\mu\mathrm{cor}(N_{i+1}) = \gamma^{-1}\gamma\mu^{-1}\mu\mathrm{cor}(N_{i+1}) = \mathrm{cor}(N_{i+1}).$$

Hence we have $[\gamma, \mu] \in \mathrm{cor}(N_{i+1})$, and so $[\mathcal{M}(L), M_L(N_i)] \subseteq \mathrm{cor}(N_{i+1})$. Now by hypothesis $\Gamma_i \subseteq N_i$, so we have $[\mathcal{M}(L), M_L(\Gamma_i)] \subseteq \mathrm{cor}(N_{i+1})$.

Hence as the core must be normal we have $\overline{[\mathcal{M}(L), M_L(\Gamma_i)]} \subseteq \mathrm{cor}(N_{i+1})$. But $\overline{[\mathcal{M}(L), M_L(\Gamma_i)]} = [\mathcal{M}(L), \overline{M_L(\Gamma_i)}]$. So $[\mathcal{M}(L), \overline{M_L(\Gamma_i)}] \subseteq \mathrm{cor}(N_{i+1})$. So we then have $[\mathcal{M}(L), \overline{M_L(\Gamma_i)}]1_L \subseteq \mathrm{cor}(N_{i+1})1_L$ — that is $\Gamma_{i+1} \subseteq N_{i+1}$ as required. Hence by induction the result follows. □

Later I shall thoroughly generalise the idea of nilpotence in loops and other algebras.

4.4 Commutator subloops

As with the centre, the following facts about the commutator are well-known, but as I shall make a great deal of use of them I shall give the definitions and proofs, which are in any case short.

DEFINITION 4.18 *If G is a group, its* **commutator subgroup** *or* **derived subgroup** *— written G' — is the subgroup generated by all elements $[g_1, g_2] = g_1^{-1}g_2^{-1}g_1g_2$ for any $g_1, g_2 \in G$.*

It is easy to see that this is a characteristic subgroup of G, and that this is the smallest normal subgroup of G such that G/G' is Abelian The concept of a commutator subgroup can be generalised to loops.

DEFINITION 4.19 *If L is a loop, then its* **derived subloop** *— written L' — is defined to be $\mathcal{M}(L)'1_L$.*

We have seen in the case of quasigroups that the projection of the commutator of $\mathcal{M}(Q)$ is indeed the smallest congruence on Q such having a quotient quasigroup which is an Abelian group. Obviously this holds for loops in particular.

There is another way to define L', namely $L' = \overline{\mathcal{I}(L)}1_L$, where $\overline{\mathcal{I}(L)}$ is the normal closure of $\mathcal{I}(L)$ in $\mathcal{M}(L)$.

THEOREM 4.20 *$L' = \overline{\mathcal{I}(L)}1_L$, where $\overline{\mathcal{I}(L)}$ is the normal closure of $\mathcal{I}(L)$ in $\mathcal{M}(L)$.*

PROOF: We know that L is Abelian if and only if $\mathcal{I}(L)$ is trivial. Moreover, we have mentioned that theorem of Bruck which states that $\mathcal{I}(L/K) \cong \mathcal{I}(L)/\mathrm{cor}(K)$. Now by definition $\overline{\mathcal{I}(L)}$ is the smallest normal subgroup of $\mathcal{M}(L)$ containing $\mathcal{I}(L)$, and so $\overline{\mathcal{I}(L)}1_L$ is indeed the commutator L'. □

COROLLARY 4.21 $\overline{\mathcal{I}(L)} = \mathrm{cor}_{\mathcal{M}(L)}(L')$

PROOF: For $\overline{\mathcal{I}(L)}$ is clearly the largest normal subgroup of $\mathcal{M}(L)$ contained in $\overline{\mathcal{I}(L)}\mathcal{I}(L) = \overline{\mathcal{I}(L)}$. □

4.5 Weak and strong solvability

DEFINITION 4.22 *A loop L will be called* **weakly solvable** *or* **solvable from the top down** *if and only if it is trivial or contains a normal subloop N such that L/N is Abelian and N is weakly solvable.*

DEFINITION 4.23 *A loop L will be called* **strongly solvable** *or* **solvable from the bottom up** *if and only if it is trivial or contains a normal subloop N such that L/N is strongly solvable and N is Abelian.*

Now in groups these two definitions coincide. In loops they do not.

EXAMPLE 4.24

	1	2	3	4	5	6	7	8	9	A	B	C
1	1	2	3	4	5	6	7	8	9	A	B	C
2	2	3	1	5	6	4	8	9	A	B	C	7
3	3	1	2	6	4	5	9	A	B	C	7	8
4	4	5	6	3	1	2	A	B	C	7	8	9
5	5	6	4	2	3	1	B	C	7	8	9	A
6	6	4	5	1	2	3	C	7	8	9	A	B
7	7	8	9	A	B	C	4	5	6	1	2	3
8	8	9	A	B	C	7	3	4	5	6	1	2
9	9	A	B	C	7	8	2	3	4	5	6	1
A	A	B	C	7	8	9	1	2	3	4	5	6
B	B	C	7	8	9	A	6	1	2	3	4	5
C	C	7	8	9	A	B	5	6	1	2	3	4

This has only four subloops: $\{1\}, J = \{1,2,3\}, K = \{1,2,3,4,5,6\}$ and the whole loop, L. Now K is normal in L and J is normal in K, and we have $L/K \cong K/J \cong C_2$ and $J \cong C_3$. So L is solvable from the top down. However, J is not normal in L and K is not Abelian, so L cannot be solvable from the bottom up.

DEFINITION 4.25 *We define a series $L^{(0)}, L^{(1)}, \ldots$ by*

1. $L^{(0)} = L$

2. $L^{(i+1)} = (L^{(i)})'$

THEOREM 4.26 *A loop L is weakly solvable if and only if there is some n for which $L^{(n)} = \{1_L\}$.* □

Equivalently, we have

THEOREM 4.27 *L is weakly solvable if and only if there exists a series $L = K_0 \trianglerighteq K_1 \trianglerighteq \ldots \trianglerighteq K_n = 1_L$ such that that $K^{(i)}/K^{(i+1)}$ is an Abelian group for every choice of i.* □

THEOREM 4.28 *Let L_1, L_2 be weakly solvable loops. Then $L_1 \times L_2$ is weakly solvable.* □

THEOREM 4.29 *Let L be a weakly solvable loop with $H \leq L$. Then H is weakly solvable.* □

THEOREM 4.30 *Let L be a weakly solvable loop with $K \trianglelefteq L$. Then L/K is weakly solvable.* □

All these last theorems about weak solvability follow from the fact that L' is the smallest normal subgroup of L such that L/L' is Abelian. The whole subject of weak solvability will be treated in depth later, when these theorems will be proved in a more general context.

4.6 The Frattini subloop and its variations

DEFINITION 4.31 *Let L be a loop. Then the* **Frattini subloop** *of L — denoted by $\Phi(L)$ — is defined by*

$$\Phi(L) = L \bigcap \{M \leq L : M \textit{ is maximal in } L\}$$

In fact it is clear that we can make such a definition for any algebraic structure.

DEFINITION 4.32 *Let L be a loop. Then x is a* **non-generator** *of L if and only if for any $T \subseteq L$, we have $\langle T, x\rangle = L \Rightarrow \langle T \rangle = L$.*

It is well-known that the Frattini subalgebra of an algebra is precisely its set of non-generators, and that it is characteristic in the algebra.

Now in a group, the Frattini subgroup will be normal: in a loop this is not necessarily the case. See example 4.2 for a counterexample. Hence it is reasonable to make the following definitions.

DEFINITION 4.33 *Let L be a loop. Let the* **lower Frattini subloop** *of L — denoted by $\underline{\Phi}(L)$ — be the largest normal subloop of L contained in $\Phi(L)$, and let the* **upper Frattini subloop** *of L — denoted by $\overline{\Phi}(L)$ — be the normal closure of $\Phi(L)$.*

DEFINITION 4.34 *Let L be a loop. Then the* **cosocle** *of L — denoted by* Cosoc(L) *— is defined by*

$$\mathrm{Cosoc}(L) = L \bigcap \{N \trianglelefteq L : N \textit{ is maximal normal in } L\}.$$

Now as any automorphism of L permutes the maximal normal subloops of L amongst themselves, it is easy to see that $\mathrm{Cosoc}(L)$ is characteristic in L.

THEOREM 4.35 *Let L be a loop. Then $\underline{\Phi}(L) \subseteq \mathrm{Cosoc}(L)$*

PROOF: For let K be any maximal normal subloop of L. Then $K\mathrm{Cosoc}(L) \trianglelefteq L$. Now suppose $K\underline{\Phi}(L) = L$. Then we would have $\langle K, \underline{\Phi}(L) \rangle = L$. But $\underline{\Phi}(L) \subseteq \Phi(L)$, and so we should have $\langle K \rangle = L$ and hence $K = L$, contradicting our choice of K. Hence we have $K \subseteq K\underline{\Phi}(L) \lhd L$. Hence $K = K\underline{\Phi}(L)$ and so $\underline{\Phi}(L) \subseteq K$.

So $\underline{\Phi}(L)$ is contained in every maximal normal subloop of L, and so is contained in $\mathrm{Cosoc}(L)$ as required. □

Hence if G is a group, then as $\underline{\Phi}(G) = \Phi(G)$ we have $\Phi(G) \subseteq \mathrm{Cosoc}(G)$. However, this does not hold in general for loops.

Example 4.36

	1	2	3	4	5	6	7	8	9	A
1	1	2	3	4	5	6	7	8	9	A
2	2	1	4	5	3	7	6	9	A	8
3	3	4	5	2	1	8	9	A	7	6
4	4	5	1	3	2	9	A	6	8	7
5	5	3	2	1	4	A	8	7	6	9
6	6	7	8	9	A	1	2	3	4	5
7	7	6	9	A	8	2	1	4	5	3
8	8	9	A	7	6	3	4	5	2	1
9	9	A	6	8	7	4	5	1	3	2
A	A	8	7	6	9	5	3	2	1	4

Now this loop L has subloops

$$\{1\}; \{1,2\}; \{1,6\}; \{1,7\}; \{1,2,6,7\}; \{1,2,3,4,5\} \text{ and } L.$$

Of these, $\{1,6\}$ and $\{1,2,3,4,5\}$ are maximal normal, having intersection $\mathrm{Cosoc}(L) = \{1\}$, whereas $\{1,2,6,7\}$ and $\{1,2,3,4,5\}$ are maximal, having intersection $\Phi(L) = \{1,2\}$.

4.7 Maximal normal p-subloops

Definition 4.37 *Let p be any prime number. A quasigroup Q is said to be a* **p-quasigroup** *if and only if $|Q| = p^m$ for some m. Similarly, if p is any* *prime and Q is any quasigroup, a subquasigroup P of a quasigroup Q is said to be a* **p-subquasigroup** *if and only if $|P| = p^n$ for some n.*

THEOREM 4.38 *Let L be a loop. Let P_1, P_2 be normal p-subquasigroups of L. Then $P_1P_2 = \{p_1p_2 : p_1 \in P_1, p_2 \in P_2\}$ is a normal p-subquasigroup of L, and similarly $P_1 \backslash\backslash P_2$ and $P_1 /\!/ P_2$ are normal p-subquasigroups of L.*

PROOF: We shall just prove the first assertion, as the other proofs are similar. We know that $P_1P_2 \trianglelefteq L$. Now $P_1P_2 = \{p_1P_2 : p_1 \in P_1\}$, and of course each coset is a power of p by choice of P_2. So we must count the cosets. Now trivially the mapping θ from P_1 to L/P_2 given by $\theta p_1 = p_1P_2$ is a homomorphism. Now $|\theta P_1| = |\{p_1P_2 : p_1 \in P_1\}|$, and so by Lagrange's Theorem for normal subquasigroups and our choice of P_1, the result follows. □

DEFINITION 4.39 *A subloop $P_1 \leq L$ is said to be a* **maximal normal p-subloop** *if and only if*

1. $P_1 \trianglelefteq L$
2. $|P_1| = p^n$ *for some n.*
3. *If $P_2 \trianglelefteq L$ and $|P_2| = p^m$ for some m, then $|P_2| \leq |P_1|$.*

COROLLARY 4.40 *In a finite loop L, for any prime p there is exactly one maximal normal p-subloop of L, which is therefore characteristic in L.*

Given this, it is reasonable to make the following definition:

DEFINITION 4.41 *Let $N_p(L)$ be the maximal normal p-subloop of L.*

THEOREM 4.42 *Let L be a finite loop. Then $N_p(L)$ contains every normal p-subloop of L.*

PROOF: By Theorem 4.38, for any normal p-subloop K of L, we have that $KN_p(L)$ is a normal p-subloop. Now clearly $N_p(L) \subseteq KN_p(L)$ and so by maximality of $N_p(L)$ we have $N_p(L) = KN_p(L)$. Hence $K \subseteq N_p(L)$. □

THEOREM 4.43 *Let L be a finite loop. Then $(N_p(\mathcal{M}(L)))1_L \subseteq N_p(L)$.*

PROOF: We know that $(N_p(\mathcal{M}(L)))1_L \trianglelefteq L$, as $N_p(\mathcal{M}(L)) \trianglelefteq \mathcal{M}(L)$. Further, by the Orbit-Stabilizer Theorem, $(N_p(\mathcal{M}(L)))1_L$ must be a p-subloop. Hence by Theorem 4.42 we have $(N_p(\mathcal{M}(L)))1_L \subseteq N_p(L)$. □

THEOREM 4.44 *Let G be a finite group. Then $(N_p(\mathcal{M}(G)))1_G = N_p(G)$.*

PROOF: For the set $\{\lambda_x : x \in N_p(G)\}$ is the left regular representation of $N_p(G)$, and so a p-subgroup of $\mathcal{M}(G)$. Furthermore, as $\mu_{y,z}^{-1}\lambda_x\mu_{y,z} = \lambda_{yzy^{-1}}$ it is normal. Hence by Theorem 4.42 we have

$$\{\lambda_x : x \in N_p(G)\} \subseteq N_p(\mathcal{M}(G))$$

and so $N_p(G) \subseteq (N_p(\mathcal{M}(G)))1_G$. By the previous theorem we have

$$(N_p(\mathcal{M}(G)))1_G \subseteq N_p(G),$$

so we have equality as required. □

4.8 Multiplication groups of groups

Note that the multiplication group of a group G is often called the **holomorph** of G in group theory.

There are two interesting ways to analyse the structure of $\mathcal{M}(G)$. Both depend on noting that for any $\phi \in \mathcal{M}(G)$ we can choose $g_1, g_2 \in G$ such that for every $x \in G$ we have $\phi(x) = g_1 x g_2$. So if we define a function $\theta : G \times G \to \mathcal{M}(G)$ by $\theta(g,h)(x) = gxh^{-1}$ it is certainly onto $\mathcal{M}(G)$. Furthermore, θ is a homomorphism.

So

$$\ker\theta = \{(g,h) : gxh^{-1} = x \;\forall\; x \in G\}.$$

Now in particular this requires $g1_G h^{-1} = 1_G$, so $gh^{-1} = 1_G$ so $g = h$. So

$$\ker\theta = \{(g,g) : gxg^{-1} = x \;\forall\; x \in G\}.$$

So $\ker\theta = \{(g,g) : g \in \mathcal{Z}(G)\}$, and so $\mathcal{M}(G) = (G \times G)/\ker\theta$, with $\ker\theta$ isomorphic to $\mathcal{Z}(G)$.

Alternatively, we can reason as follows. Since for any $\phi \in \mathcal{M}(G)$ we can choose $g_1, g_2 \in G$ such that for every $x \in G$ we have $\phi(x) = g_1 x g_2$, we can equally well choose $h_1, h_2 \in G$ such that $\phi(x) = h_2^{-1} h_1 x h_2$, by choosing $h_1 = g_2 g_1$ and $h_2 = g_2$.

Hence if we define the function $\kappa : G \to S_G$ by letting $\kappa_g x = g^{-1}xg$, we can write any $\phi \in \mathcal{M}(G)$ as $\phi = \kappa_h \lambda_g$ for some $g, h \in G$. Now

$$\kappa_h \lambda_g(x) = h^{-1}gxh = h^{-1}ghh^{-1}xh = \lambda_{\kappa_h g}\kappa_h(x).$$

Now as $\kappa_G = \mathcal{I}(G)$ and by Cayley's theorem λ_G is (isomorphic to) G, it follows that $\mathcal{M}(G)$ is (isomorphic to) a semidirect product of G with $\mathcal{I}(G)$. Hence, incidentally, λ_G is normal in $\mathcal{M}(G)$. Similar results hold for ρ_G

It follows that as G is isomorphic to a subgroup of $\mathcal{M}(G)$ and $\mathcal{M}(G)$ is isomorphic to a homomorphic image of two direct products of G, that $\mathcal{M}(G)$ and G belong to exactly the same varieties.

By either of the analyses of $\mathcal{M}(G)$ given above, we immediately obtain the order formula

$$|\mathcal{M}(G)||\mathcal{Z}(G)| = |G|^2.$$

We may use this to put restrictions on the order of $\mathcal{M}(G)$ on the hypothesis that G is non-Abelian.

THEOREM 4.45 *If G is non-Abelian then $|\mathcal{M}(G)|$ is divisible by the square of some compound number.*

PROOF: First of all, notice that

$$|\mathcal{M}(G)||\mathcal{Z}(G)| = |G|^2$$

implies that

$$|\mathcal{M}(G)| = |\mathcal{Z}(G)||\mathcal{I}(G)|^2.$$

Now if G is non-Abelian, then $|\mathcal{I}(G)| > 1$. Furthermore, we can't have $|\mathcal{I}(G)| = p$ for some prime p, for then $\mathcal{I}(G)$ would be cyclic and hence G would be Abelian - a contradiction. □

THEOREM 4.46 *If* $|\mathcal{M}(G)| = p^4$ *for some prime* p *then* G *is Abelian.*

PROOF: For then by the order formula $|\mathcal{I}(G)|^2$ divides p^4, so there are three possible cases:

1. $|\mathcal{I}(G)| = 1$. But then G is certainly Abelian.

2. $|\mathcal{I}(G)| = p$. But then $\mathcal{I}(G)$ is cyclic and so G is Abelian.

3. $|\mathcal{I}(G)| = p^2$. But then as (by the order formula) $|\mathcal{Z}(G)||\mathcal{I}(G)|^2 = p^4$, we have $|\mathcal{Z}(G)| = 1$. Now $|G| = |\mathcal{Z}(G)||\mathcal{I}(G)|$, so we have $|G| = p^2$. But then G has non-trivial centre — a contradiction.

□

THEOREM 4.47 *If* $|\mathcal{M}(G)| = p^4 \times q_1 \times \dots q_n$, *with* p *and the* q_i *distinct primes and* $1 \leq n$, *then* G *is Abelian.*

PROOF: Suppose otherwise. By the order formula we must have $|\mathcal{I}(G)| = p^2$. Then $|\mathcal{Z}(G)| = q_1 \times \dots q_n$, and so $|G| = p^2 \times q_1 \times \dots q_n$.

Now, what is the class equation of G? We have exactly $|\mathcal{Z}(G)|$ conjugacy classes of order 1: hence the remaining conjugacy classes — some must remain, as by hypothesis $|\mathcal{Z}(G)| < |G|$ — must have order greater than one. By the orbit-stabiliser theorem they must have order dividing $|\mathcal{I}(G)|$. Hence as their order is greater than 1 they must each have order divisible by p.

Hence p divides $|G| - |\mathcal{Z}(G)| = (|\mathcal{I}(G)| - 1) \times |\mathcal{Z}(G)| = (p^2 - 1) \times q_1 \times \ldots q_n$. But this is clearly impossible, so we have a contradiction. □

Hence the smallest order possible by these criteria for the multiplication group of a non-Abelian group is $32 = |\mathcal{M}(Q_8)|$. The next largest possible is $36 = |\mathcal{M}(S_3)|$. Next are $64 = |\mathcal{M}(C_2 \times Q_8)|$ and $72 = |\mathcal{M}(C_2 \times S_3)|$. Next is 100. Now for $|\mathcal{M}(G)| = 100$ we must have G with order 10 and trivial centre: hence its class equation must be $1+5+2+2 = 10$. Now this describes the fifth dihedral group. In fact, in general we have $|\mathcal{M}(D_{2n+1})| = (4n+2)^2$, as odd dihedral groups have trivial centre, so, for example, we have $|\mathcal{M}(D_7)| = 196$.

4.9 Multiplication groups of loops

Intriguingly there is one claim which we can make specifically about multiplication groups of loops which specifically are not groups. For as we have seen in the Niemenmaa and Kepka theorem, $\lambda_x^{-1}\rho_z^{-1}\lambda_x\rho_z \in \mathcal{I}(L)$ for any $x, z \in L$. Now for $\lambda_x^{-1}\rho_z^{-1}\lambda_x\rho_z$ to be trivial for all $x, z \in L$ we should require that $\lambda_x^{-1}\rho_x^{-1}\lambda_x\rho_z y = y$ for all $x, y, z \in L$, i.e. $\lambda_x\rho_z y = \rho_z\lambda_x y$ i.e. $x.yz = xy.z$ for all $x, y, z \in L$, in which case the loop, being associative, would be a group. So we have the following theorem:

THEOREM 4.48 *If L is not a group, then the intersection of $\mathcal{M}(L)'$ and $\mathcal{I}(L)$ is non-trivial.* □

This is not necessarily true of loops which are groups. Consider for example a non-Abelian group G of order p^3 for some odd prime p. Then we must have $\mathcal{Z}(G) = G'$. From our analysis of holomorphs in the previous subsection, it is then evident that $\mathcal{Z}(\mathcal{M}(G)) = \mathcal{M}(G)'$. But of course the intersection of $\mathcal{I}(G)$ with $\mathcal{Z}(\mathcal{M}(G))$ is trivial.

Now since so much can be said about multiplication groups of groups, this will sometimes give us an opportunity to carry out a proof by the cases "L is a group" and "L is not a group". Here is a simple example.

THEOREM 4.49 *Let $\mathcal{M}(L)$ be meta-Abelian. Then there is $N \trianglelefteq L$ such that L/N is non-trivial Abelian.*

PROOF: For on the one hand, if L is a group then it belongs to exactly the same varieties as its holomorph. Hence L is meta-Abelian and we're done.

On the other hand, suppose that L is not a group. We know that $\mathcal{M}(L)'1_L$ is the commutator of L — hence if we can show that this subloop is not the whole of L then we are done. So suppose that $\mathcal{M}(L)'1_L = L$. Then we have $\mathcal{M}(L)'\mathcal{I}(L) = \mathcal{M}(L)$. As L is not a group the intersection of $\mathcal{M}(L)'$ and $\mathcal{I}(L)$ is non-trivial. It is normalised by $\mathcal{I}(L)$ because it is the intersection of $\mathcal{I}(L)$ with a normal subgroup of $\mathcal{M}(L)$ and it is normalised by $\mathcal{M}(L)'$ because $\mathcal{M}(L)'$ is Abelian. Hence it is a non-trivial normal subgroup of $\mathcal{M}(L)$ contained in $\mathcal{I}(L)$, contradicting Niemenmaa and Kepka. □

We shall use this method again later.

DEFINITION 4.50 *Let G be a group. I shall say that a group is* **innocent** *if and only if for all $N \lhd G$, the quotient group G/N is not the multiplication group of a loop. The trivial group is not innocent.*

Clearly a group must be insoluble to be innocent. In particular, no Abelian group is innocent.

THEOREM 4.51 *Let G be a group such that $G/\mathcal{Z}(G)$ is innocent. Then G is not the multiplication group of a loop.*

PROOF: For suppose that G is the multiplication group of some loop. Then so is $G/\text{cor}(\mathcal{Z}(G))$. But as $\mathcal{Z}(G) \subseteq \text{cor}(\mathcal{Z}(G))$ and $G/\mathcal{Z}(G)$ is innocent, we must have $\text{cor}(\mathcal{Z}(G)) = G$. But then we have $\mathcal{Z}(L) = L$, so L is Abelian, so G is also Abelian and so far from innocent — a contradiction. □

Now as we know that for $q \neq 9$ we have $PSL(2, q)$ simple and not the multiplication group of a loop (and therefore innocent), we must also have $SL(2, q)$ not the multiplication group of a loop (for $q \neq 9$). Indeed, it is clear from the definition and theorem that $SL(2, q)$ must itself be innocent (for $q \neq 9$ — it is certainly not innocent when $q = 9$), inasmuch as every $N \lhd SL(2, q)$ must lie in the centre of $SL(2, q)$ and that we then have

$$\mathcal{Z}(SL(2, q)/N) = \mathcal{Z}(SL(2, q))/N.$$

THEOREM 4.52 *Let G be a group having a normal subgroup N such that N*

is cyclic and G/N is innocent. Then G is not the multiplication group of a loop.

PROOF: For suppose otherwise. Again, as $G/\text{cor}(N)$ is the multiplication group of a loop, and G/N is innocent, it follows that $\text{cor}(N) = G$. Now as N is normal in G and cyclic, any subgroup of N is characteristic in G. Hence $N \cap \mathcal{I}(L) = \{1_L\}$ by Niemenmaa and Kepka.

Then G $= N \rtimes^{\phi} \mathcal{I}(L)$. Hence $\mathcal{I}(L)$ is innocent and so non-Abelian. Hence ϕ has non-trivial kernel. But clearly the kernel of ϕ is centralised by N and normalised by $\mathcal{I}(L)$. Hence it is normal in G and contained in $\mathcal{I}(L)$, contradicting Niemenmaa and Kepka. □

DEFINITION 4.53 *The* **socle** *of a loop, written* $\text{Soc}(L)$, *is the product of the minimal normal subgroups of that loop.*

THEOREM 4.54 *Let $\mathcal{M}(L)$ be the direct product of A and B with*

$$\gcd(|A|, |\text{Soc}(B)|) = \gcd(|\text{Soc}(A)|, |B|) = 1$$

Then L is the direct product of $A1_L$ and $B1_L$, and $A \cong \mathcal{M}(A1_L)$ and $B \cong \mathcal{M}(B1_L)$.

PROOF: We show first that $A = \text{cor}(A1_L)$.

Consider that since $A \subseteq \text{cor}(A1_L)$, it follows that for any $\alpha\beta \in \text{cor}(A1_L)$ (taking $\alpha \in A$ and $\beta \in B$) we must also have $\beta \in \text{cor}(A1_L)$. Hence if

$A \subset \operatorname{cor}(A1_L)$ then the intersection of $\operatorname{cor}(A1_L)$ and B must be some non-trivial normal subgroup of $\mathcal{M}(L)$, and hence contains a minimal normal subgroup of $\mathcal{M}(L)$ which I shall call K. Now as $\gcd(|A|, |\operatorname{Soc}(B)|) = 1$ we have $\gcd(|A|, |K|) = 1$ so $\gcd(|A1_L|, |K1_L|) = 1$. As $K \subseteq \operatorname{cor}(A1_L)$ we have $K1_L \subseteq A1_L$. It follows that $K1_L = \{1_L\}$. So $K \subseteq \mathcal{I}(L)$, contradicting the Niemenmaa-Kepka theorem.

So we must have $A = \operatorname{cor}(A1_L)$. Similarly, $B = \operatorname{cor}(B1_L)$. Hence $A1_L \cap B1_L = \{1_L\}$, so $\mathcal{M}(L) \cong \mathcal{M}(A1_L) \times \mathcal{M}(B1_L)$, and then clearly $A \cong \mathcal{M}(A1_L)$ and $B \cong \mathcal{M}(B1_L)$. □

DEFINITION 4.55 *For ease of exposition we shall introduce a function π from the class of all finite loops to the set of non-negative whole numbers given by setting $\pi(L) = n$ if and only if $|L|$ is the product of exactly n (not necessarily distinct) prime numbers (we may take π of the trivial loop to be 0 if required).*

THEOREM 4.56 *If $\pi(\mathcal{M}(L)) \leq 3$, then L is an Abelian loop.*

PROOF: Suppose otherwise. Then as $\mathcal{I}(L)$ cannot be cyclic [23] we must have $\pi(\mathcal{I}(L)) = 2$. But then L having prime order is simple, and by hypothesis non-Abelian. But this contradicts Vesanen's theorem, as there is no insoluble group G having $\pi(G) \leq 3$ □

Now consider the case where $\mathcal{M}(L)$ is non-Abelian and $\pi(\mathcal{M}(L)) = 4$ This can certainly happen. For example, if G is a non-Abelian group of order pq — with p, q prime — then $|\mathcal{M}(G)| = p^2q^2$. There are no other examples amongst groups. However, there are plenty of loops which are not groups and which have multiplication groups with order the product of four primes.

Example 4.57 *The loop below has* $|\mathcal{M}(L)| = 2^3 \times 3$.

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	4	3	6	5
3	3	4	5	6	1	2
4	4	3	6	5	2	1
5	5	6	1	2	4	3
6	6	5	2	1	3	4

Example 4.58 *The loop below has* $|\mathcal{M}(L)| = 3^4$.

	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9
2	2	3	1	5	6	4	8	9	7
3	3	1	2	6	4	5	9	7	8
4	4	5	6	7	8	9	1	2	3
5	5	6	4	8	9	7	2	3	1
6	6	4	5	9	7	8	3	1	2
7	7	8	9	1	2	3	5	6	4
8	8	9	7	2	3	1	6	4	5
9	9	7	8	3	1	2	4	5	6

I shall now look at length at the case in which $\pi(\mathcal{M}(L)) = 4$. There is a boring case in which $M(L)$ is Abelian. This needs no analysis. The only simple candidate would be the group A_5, which is known not to be the multiplication loop of a group . So we only need to think about groups which are solvable. The analysis will use Vesannen's theorem to help find the structure of the loop.

So let $|\mathcal{M}(L)| = pqrs$ with p, q, r, s (not necessarily distinct) primes, and suppose that $\mathcal{M}(L)$ is neither Abelian nor simple. As $\mathcal{M}(L)$ is not Abelian, $\mathcal{I}(L)$ is neither trivial nor cyclic. As $\mathcal{M}(L)$ is not simple it is solvable, so by Vesanen's theorem L is solvable. So L cannot have prime order without being a cyclic group of that order, in which case L and $\mathcal{M}(L)$ are Abelian — a contradiction.

Hence (without loss of generality) we may take $|L| = ps$ and $|\mathcal{I}(L)| = qr$.

As L is solvable and by hypothesis non-Abelian, it has a commutator L' of order (without loss of generality) p, with $L' \cong C_p$. So $L/L' \cong C_s$ and so $\mathcal{M}(L)/\mathrm{cor}(L') \cong C_s$ and so $|\mathrm{cor}(L')| = pqr$ and $\mathcal{M}(L) \cong \mathrm{cor}(L') \rtimes^{\phi} C_s$

Now if we had $\ker\phi = C_s$ then we'd have $\mathcal{M}(L) \cong \mathrm{cor}(L') \times C_s$. Then as $\mathrm{cor}(L') \cap C_s = \{\iota\}$ we would have $L' \cap C_s 1_L = \{1_L\}$. So then $L \cong L' \times C_s 1_L$. As L is solvable and L' and $C_s 1_L$ are of prime order, they must be cyclic groups. So L, and hence $\mathcal{M}(L)$, would be Abelian — a contradiction. Hence $\ker\phi$ is trivial.

So $\mathcal{M}(L) \cong \mathrm{cor}(L') \rtimes^{\phi} C_s$ with $\ker\phi$ trivial. We turn now to the structure of $\mathrm{cor}(L')$.

Suppose first that $\mathrm{cor}(L')$ is Abelian. Then its Sylow q and r subgroups are normal, hence characteristic, in $\mathrm{cor}(L')$. Hence they are normal in $\mathcal{M}(L)$. Now as they lie in $\mathrm{cor}(L')$ they must have non-trivial projections in L', which has order p. Hence $p = q = r$.

So then $\mathrm{cor}(L') \cong C_p \times C_p \times C_p$ or $C_p \times C_{p^2}$ or C_{p^3}. But recall that $\mathcal{I}(L) \subseteq \mathrm{cor}(L')$. Now in the case $\mathrm{cor}(L') \cong C_p \times C_{p^2}$, recall that $\mathcal{I}(L)$ must not be cyclic: but there is only one non-cyclic subgroup of $C_p \times C_{p^2}$, which is therefore characteristic in $\mathrm{cor}(L')$. Similarly in C_{p^3} every subgroup of $\mathrm{cor}(L')$ is characteristic in $\mathrm{cor}(L')$ (besides being cyclic!) and so is normal in $\mathcal{M}(L)$. So in these cases $\mathcal{I}(L)$ would be a normal subgroup of $\mathcal{M}(L)$, contradicting Niemenmaa and Kepka.

So in the case where $\mathrm{cor}(L')$ is Abelian we must have

$$\mathcal{M}(L) \cong (C_p \times C_p \times C_p) \rtimes^{\phi} C_s.$$

Consider now the cases where $\mathrm{cor}(L')$ is not Abelian. I shall aim to show that $\mathrm{cor}(L')' \cong C_p \times C_p$.

As $\mathrm{cor}(L')$ is solvable we have $1 < |\mathrm{cor}(L')'| < pqr$. As $\mathrm{cor}(L')'$ is characteristic in $\mathrm{cor}(L')$ it is normal in $\mathcal{M}(L)$ and so has projection L'. Hence p divides $|\mathrm{cor}(L')'|$. So (without loss of generality) we may say that $|\mathrm{cor}(L')'| = p$ or pq. In the case that $\mathrm{cor}(L')' \cong C_p \times C_p$ we are finished. Otherwise $\mathrm{cor}(L')'$ must contain a non-trivial subgroup of prime order characteristic in $\mathrm{cor}(L')'$, hence characteristic in $\mathrm{cor}(L')$ and so normal in $\mathcal{M}(L)$. As it lies in $\mathrm{cor}(L')$ it must have projection L' and so has order p. I shall call this subgroup P.

Now as P and $\mathrm{cor}(L')$ have the same projection, we have

$$P\mathcal{I}(L) = \mathrm{cor}(L')\mathcal{I}(L)$$

and so

$$P\mathcal{I}(L) = \mathrm{cor}(L').$$

Now by the order of P we must have

$$P \cap \mathcal{I}(L) = \{\iota\}$$

and so

$$\mathrm{cor}(L') = P \rtimes^{\psi} \mathcal{I}(L).$$

Now as p is prime $\mathrm{Aut}(P)$ is cyclic. But we know that $\mathcal{I}(L)$ cannot be cyclic. Hence $\ker\psi$ is non-trivial. Now if $\ker\psi \cong C_q \times C_q$ then $\mathrm{cor}(L')$ is Abelian — a case dealt with above. So consider the cases where it is not. Then $\ker\psi$ contains a normal subgroup of order (without loss of generality) q, which I shall call Q. Furthermore, as the elements of $\ker\psi$ commute with the elements of P we have $Q \trianglelefteq \mathrm{cor}(L')$. Now if $q = p$ then we are done. So we suppose that $q \neq p$ and look for a contradiction.

If Q is the only normal subgroup of order q in $\mathrm{cor}(L')$ then it is characteristic in $\mathrm{cor}(L')$ and so normal in $\mathcal{M}(L)$. But $Q \subseteq \mathcal{I}(L)$, contradicting Niemenmaa and Kepka. If $\mathrm{cor}(L')$ has another normal subgroup of order q — call it Q^* — then as $|\mathrm{cor}(L')| = pq^2$ with $q \neq p$ the product QQ^* is the unique Sylow q-subgroup of $\mathrm{cor}(L')$ and so is characteristic in $\mathrm{cor}(L')$ and so is normal in $\mathcal{M}(L)$. But then we have $|\mathcal{I}(L)| = q^2$ and so $\mathcal{I}(L) = QQ^* \trianglelefteq \mathcal{M}(L)$, contradicting Niemenmaa and Kepka. This completes the proof.

To summarise what we have achieved so far: Suppose $\mathcal{M}(L)$ has order the product of four primes, and is non-Abelian. Then we may write

$$\mathcal{M}(L) = ((P \times Q) \rtimes^{\phi} R) \rtimes^{\theta} S)$$

with $\mathcal{I}(L) = QR$, with $\mathrm{cor}(L') = PQR$, with $|P| = |Q|$, and with $\ker\theta$ trivial. Moreover, either $\ker\phi$ is trivial, or

$$PQR \cong C_p \times C_p \times C_p.$$

We may go a little further. Consider the case where $p = r$. Then clearly not only do the elements of Q commute with the elements of P, but also of R, since we have by hypothesis $|QR| = p^2$. Hence Q lies in the centre of PQR. If PQR were non-Abelian, then we would have to conclude that Q was the centre of PQR, making it a characteristic subgroup of PQR, hence normal in $\mathcal{M}(L)$, contradicting Niemenmaa and Kepka, since Q lies in $\mathcal{I}(L)$. Hence in such cases we have $PQR \cong C_p \times C_p \times C_p$. Examples of loops with such multiplication groups have been given above.

Now let us consider the case where $r \neq p$. Up until a certain point, we must also treat separately the cases $s = p$ and $s \neq p$.

First, suppose that $s = p$. Then consider that R is a Sylow r-subgroup of PQR. Hence if we take any $\sigma \in S$ such that $\iota_{\mathcal{M}(L)} \neq \sigma$, then $\sigma^{-1}R\sigma = \pi^{-1}R\pi$ for some $\pi \in PQ$. So $\langle \sigma\pi^{-1} \rangle$ normalises R. Now $\sigma\pi^{-1}$ is a non-trivial element of PQS, which by hypothesis has order p^3. PQS cannot be Abelian, for that would leave Q normal in $\mathcal{M}(L)$. So every non-trivial element of PQS — and in particular $\sigma\pi^{-1}$ — must have order p. Now as $\sigma \neq \iota_{\mathcal{M}(L)}$, we must have $\langle \sigma\pi^{-1} \rangle \cap PQR = \{\iota_{\mathcal{M}(L)}\}$. Hence we can, and will, choose $S = \langle \sigma\pi^{-1} \rangle$.

We can then write $\mathcal{M}(L) = (P \times Q) \rtimes^{\psi} (R \rtimes^{\zeta} S)$. We shall now set about proving the same thing in the case where $s \neq p$.

Again, we observe that R is a Sylow r-subgroup of PQR, and so has either p or p^2 conjugate subgroups in PQR. Now as $s \neq p$, the Orbit-Stabiliser Theorem tells us that S must normalise at least one of these — so there is some γ such that for all $\sigma \in S$ we have $\sigma^{-1}\gamma^{-1}R\gamma\sigma = \gamma^{-1}R\gamma$. But then of course we have $\gamma\sigma^{-1}\gamma^{-1}R\gamma\sigma\gamma^{-1} = R$. Hence we can, and will, choose $S = \langle\gamma\sigma\gamma^{-1}\rangle$.

So again, we can write $\mathcal{M}(L) = (P \times Q) \rtimes^{\psi} (R \rtimes^{\zeta} S)$. What follows then applies equally to the cases $s = p$ and $s \neq p$.

Notice first of all that R normalises Q but does not centralise it (or we should have QR cyclic) , and that S does not normalise Q, for this would make Q normal in $\mathcal{M}(L)$, contradicting Niemenmaa and Kepka. It follows that the kernel of ψ must be trivial.

Now we shall think about ζ. By Maschke's theorem, as R normalises Q it must normalise some other subgroup of $P \times Q$ — call it P'. Now R cannot centralise P', for then Q would be the only subgroup of $P \times Q$ which was normalised but not centralised by R, and so would be characteristic in PQR, normal in $\mathcal{M}(L)$ and in contradiction of Niemenmaa and Kepka (as usual).

Hence R normalises but does not centralise both P' and Q. So by appropriate choice of bases, ψ maps R onto matrices of the form λI in $GL(2,p)$. Since we know that the kernel of ψ is trivial, it follows that RS is Abelian.

Hence in these two cases we may write $\mathcal{M}(L) = (P \times Q) \rtimes^{\psi} (R \times S)$.

To summarise

THEOREM 4.59 *Let $\mathcal{M}(L)$ be non-Abelian and have order the product of four* *primes. Then we can write*

$$\mathcal{M}(L) = (P \times Q) \rtimes^{\phi} R) \rtimes^{\theta} S$$

with $\mathcal{I}(L) = QR$, *with* $\mathrm{cor}(L') = PQR$, *with* $|P| = |Q|$, *and with* $\ker\theta$ *trivial. Either* $\ker\phi$ *is trivial, or* $PQR \cong C_p \times C_p \times C_p$.

Moreover, if $|R| = |P|$ *then we have*

$$\mathcal{M}(L) = (P \times Q \times R) \rtimes^{\psi} S$$

and if $|R| \neq |P|$ *then we have*

$$\mathcal{M}(L) = (P \times Q) \rtimes^{\psi} (R \times S)$$

in both cases with the kernel of ψ *trivial.* □

Various lemmas in this proof might be approached by other methods, such as those found in [12] and [16].

THEOREM 4.60 *Let* L *be a finite non-Abelian loop. Then there is some prime* p *such that* p^2 *divides* $|\mathcal{M}(L)|$.

PROOF: If $\mathcal{M}(L)$ is not solvable then 4 divides $|\mathcal{M}(L)|$ and we are done. So we need only treat the case where $\mathcal{M}(L)$ is solvable. We shall suppose that $|\mathcal{M}(L)|$ is square-free (i.e. it does not have a square greater than 1 as a factor) and argue for a contradiction.

We shall now construct inductively a series $L_0, L_1 \ldots$ of non-Abelian loops such that for each L_i in the series we have

- L_i is non-Abelian
- $\mathcal{M}(L_i)$ is solvable
- $|\mathcal{M}(L_i)|$ is square-free

First, we set $L_0 = L$. Clearly this has all three required properties.

Now given that L_i has these three properties we construct L_{i+1} as follows. Let B_i be the Abelian non-trivial member of the series $\mathrm{cor}(L_i')$, $\mathrm{cor}(L_i')'$, $\mathrm{cor}(L_i')''$... Note that by hypothesis $\mathcal{M}(L_i)$ is solvable and L_i is non-Abelian (so $\mathrm{cor}(L_i')$ is non-trivial), and so such a B_i can indeed be found. Then choose any prime q_i dividing $|B_i|$. As B_i is Abelian, it has a normal subgroup of order q_i, which I shall call Q_i By hypothesis, B_i, being a subgroup of $\mathcal{M}(L_i)$, must have square-free order. Hence Q_i is a Sylow q_i-subgroup of B_i, and so is characteristic in B_i which is characteristic in $\mathrm{cor}(L_i')$ which is normal in $\mathcal{M}(L_i)$. Hence $Q_i \trianglelefteq \mathcal{M}(L_i)$.

Now if L_i/Q_i1 is non-Abelian, we set $L_{i+1} = L_i/Q_i1$. If it is Abelian, then we stop: L_i is the last member of the series. Hence if we construct L_{i+1} at all, it will be non-Abelian, and as $\mathcal{M}(L_{i+1}) \cong \mathcal{M}(L_i)/\mathrm{cor}(Q_i1)$, the properties of being solvable and having square-free order will be inherited by $\mathcal{M}(L_{i+1})$ from $\mathcal{M}(L_i)$. So by induction every member of the series will have the three required properties.

Now as L is finite, this proceedure must terminate. Hence the series terminates with a non-Abelian loop which I shall call L_k, such that $\mathcal{M}(L_k)$

has square-free order and contains a normal subgroup Q_k of prime order such that L_k/Q_k1 is Abelian.

As L_k is non-Abelian L'_k is non-trivial. As L_k/Q_k1 is Abelian we have $L'_k \subseteq Q_k1$. So as Q_k1 has prime order we have that $L'_k = Q_k1$. Hence $\mathrm{cor}(L'_k) = Q_k\mathcal{I}(L_k)$, and indeed as Q_k has prime order we have $\mathrm{cor}(L'_k) = Q_k \rtimes^{\phi} \mathcal{I}(L_k)$. Now $\mathrm{Aut}(Q_k)$ and its subgroups are cyclic, but $\mathcal{I}(L_k)$ cannot be cyclic. Hence $\ker\phi$ is non-trivial.

Now $\ker\phi \trianglelefteq \mathcal{I}(L_k)$ and the elements of $\ker\phi$ commute with the elements of Q_k. Hence $\ker\phi \trianglelefteq \mathrm{cor}(L'_k)$. But $\ker\phi$ cannot be characteristic in $\mathrm{cor}(L'_k)$, for then it would be normal in $\mathcal{M}(L_k)$, contradicting Niemenmaa and Kepka. Hence there is $\alpha \in \mathrm{Aut}(\mathrm{cor}(L'_k))$ such that $\ker\phi \neq \alpha\ker\phi$. Now the subgroup $(\ker\phi)(\alpha\ker\phi)$ must have order divisible by the square of some prime, and so $|\mathcal{M}(L_k)|$ cannot be square-free — a contradiction.

This completes the proof. □

THEOREM 4.61 *Let $\mathcal{M}(L)$ be a solvable group with $\pi(\mathcal{M}(L)) = 5$. Then L is meta-Abelian.*

PROOF: Suppose otherwise. We know that for any non-Abelian loop we have $\pi(\mathcal{I}(L)) \geq 2$. If we had $\pi(\mathcal{I}(L)) \geq 3$ then we should have $\pi(L) \leq 2$ and so as L is solvable it would be meta-Abelian. Hence we need only consider the case $\pi(\mathcal{I}(L)) = 2$.

So as L is solvable but not meta-Abelian, its structure is clear. By Vesanen's theorem it's solvable, so we must have $L_2 \trianglelefteq L_1 \trianglelefteq L$ such that $L/L_1, L_1/L_2$ and L_2 are cyclic groups of prime order and such that neither L_1 nor L/L_2 is Abelian (in the case that L_2 is normal in L at all).

As L/L_1 is a cyclic group of prime order, we have $\pi(\mathcal{M}(L/L_1)) = 1$ and hence $\pi(\mathrm{cor}(L_1)) = 4$. Now as L_1 is non-Abelian, we also have $(\pi(\mathcal{M}(L_1)) = 4$. So we must have

$$\mathrm{cor}(L_1) = \langle \lambda_{L1}, \rho_{L1} \rangle \cong \mathcal{M}(L_1)$$

(by the obvious isomorphism).

Now $\mathrm{cor}(L_1)' \trianglelefteq \mathcal{M}(L)$, as it is a characteristic subgroup of a normal subgroup of $\mathcal{M}(L)$. Hence $\mathrm{cor}(L_1)'1_L \trianglelefteq L$. Now we know that as L_1 is solvable we have $\mathcal{M}(L_1)'1_L \subset L_1$. Hence $\mathrm{cor}(L_1)'1_L$ is a proper subloop of L_1 which is normal in L. As L_1 is non-Abelian meta-Abelian we have $\mathrm{cor}(L_1)'1_L = L_2$, and so $\mathrm{cor}(L_1)' \subseteq \mathrm{cor}(L_2)$. Now as L/L_2 is non-Abelian we must have $\pi(L/L_2) = 4$ and so $\pi(\mathrm{cor}(L_2)) = 1$. Hence $\pi(\mathrm{cor}(L_1)') \leq 1$.

We now have two cases to consider, both of which will lead to a contradiction:

1. L_1 is a group. In this case, it's of the form $C_p \rtimes^\theta C_q$ with p, q prime and $\ker\theta$ trivial. Hence $\mathcal{M}(L_1) \cong (C_p \rtimes^\theta C_q) \times (C_p \rtimes^\theta C_q)$ and so $\mathcal{M}(L_1)' \cong C_p \times C_p$. Hence $\pi(\mathrm{cor}(L_1)') = 2$ — a contradiction.

2. L_1 is not a group. Hence for some $x, y \in L_1$ we have $[\lambda_x, \rho_y] \neq \iota_{\mathcal{M}(L)}$.

Hence $\pi(\mathcal{M}(L_1)' \cap \mathcal{I}(L_1)) \geq 1$ Now by Niemenmaa and Kepka we can't have $\mathcal{M}(L_1)' \subseteq \mathcal{I}(L_1)$. So we have $\pi(\mathcal{M}(L_1)') > 1$ and so as $\mathcal{M}(L_1) \cong \mathrm{cor}(L_1)$ we have $\pi(\mathrm{cor}(L_1)') > 1$ — a contradiction.

This completes the proof. □

Now consider the case where $\pi(\mathcal{M}(L)) = 5$ and $\mathcal{M}(L)$ is not solvable. There are two cases.

First, suppose $\mathcal{M}(L)$ is simple. Then by the classification theorem for simple finite groups, we can see that the only possible candidates would be of the form $PSL(2,q)$. However, we have already mentioned that by a theorem of Vesanen, the only group of this form which is a multiplication group of a loop is $PSL(2,9)$. However, $\pi(PSL(2,9)) \neq 5$. This disposes of the simple case.

There remains the case where $\mathcal{M}(L)$ is neither solvable nor simple — in which case it is either of the form $C_p \rtimes A_5$ or $A_5 \rtimes C_p$. In the first case, as A_5 is simple and not the multiplication group of a loop, it is innocent, and so we may apply Theorem 4.52. In the second case, the automorphism group of A_5 consists of a semidirect product of its inner automorphisms with C_2. Hence either $\mathcal{M}(L)$ has non-trivial centre — and we can apply theorem 4.51 — or we have $p = 2$. In this case we have $\mathcal{M}(L) \cong S_5$, which is indeed the multiplication group of a loop. Hence:

THEOREM 4.62 *If $\pi(\mathcal{M}(L)) = 5$ then $\mathcal{M}(L) \cong S_5$ or L is meta-Abelian.* □

5 Generalising solvability

The standard idea of solvability has proved of great interest in group theory. It seems reasonable to try to generalise the concept and see if we still get something equally interesting and useful.

It is clear that there is no single way to generalise a mathematical idea. I shall put forward a scheme applying to loops and other algebras with similar nice properties, in which there are a whole range of different "flavours" of solvability. There is another generalisation used in universal algebra, in which the concept of solvability may be defined for any variety, but in which there is no choice of flavours. It would be foolish to ask which of these is correct. (In loop theory, however, the one will incorporate the other as a special case).

What we would ask, then of a generalised idea of solvability is the following: that it should be rich in deductions; that it should agree with the classical theory of solvability (in that it will emerge as a natural consequence of the new theory that classically solvable loops and groups are still in some way solvable under the new theory); that the most basic results on solvability generalise to the new theory; and that the generalisation be natural.

Even theories with the specific aim of generalising solvability in loops may differ, according to what we take to be the essential features that make the classical theory work, and which bits of the theory we want to keep working after the generalisation. The first generalisation of solvability and nilpotence for loops was given by Bruck [6], following ideas in group theory put forward by Philip Hall, and is clearly inspired by the observation that *in groups, the centre is a characteristic (and hence normal) subgroup* . The following definitions are copied more or less from Bruck's paper. I have elided some of his explanatory comments, and have brought his notation in line with my own where possible:

DEFINITION 5.1 *Let the statement "the element a of a loop L has property π with respect to L (which we shall abbreviate to "$a\pi L$") be a predicate. Then π will be called a* **characteristic property** *of loops if and only if it possesses the following properties for every loop L:*

- $1_L \pi L$
- *If $a \in H \leq L$ and $a\pi L$ then $a\pi H$*
- *If ϕ is an isomorphism from L onto ϕL, then $a\pi L \Rightarrow (\phi a)\pi(\phi L)$*

DEFINITION 5.2 *For any loop L, let $L_\pi = \{x \in L : x\pi L\}$. If $L_\pi \leq L$, there exists a largest normal subloop of L contained in L_π, which we shall denote by $Z_\pi(L)$ and call the* **π-centre** *of L*

DEFINITION 5.3 *If π is a characteristic property of loops, then we shall say that a loop L is π-admissible if and only if*

1. *$L_\pi \leq L$ (so the π-centre of L exists)*

2. For any $K \trianglelefteq L$, the previous condition holds for L/K

3. For each $N \trianglelefteq L$ there exists a non-empty set $S(N) \subseteq N$ such that for any $K \trianglelefteq L$ we have $NK/K \in Z_\pi(L/K) \Leftrightarrow S(N) \subseteq K$

4. If $M, N \trianglelefteq L$ and $M \subseteq N$ then $S(M) \subseteq S(N)$

5. Conditions 1 to 4 hold for every subloop of L

DEFINITION 5.4 *Let the function S be as above. Then for any $N \trianglelefteq L$ we define $[N, L]_\pi = \bigcap\{J \trianglelefteq L : S(N) \trianglelefteq J\}$. The subloop $[L, L]_\pi$ we call the* **π-derived loop** *of L.*

Anyone familiar with solvability and nilpotence in groups will see where these definitions are tending, and should be able to see how Bruck will define π-solvability and π-nilpotence for π-admissible loops.

As Bruck makes good use of this generalisation in the rest of his paper, the generalisation may be said to be rich in deductions; it certainly incorporates the classical idea of solvability; and certainly the constraints on π ensure that many of the basic results on classical solvability generalise to π-solvability. So it meets three of my criteria for a good generalisation. It falls down on the fourth criterion. Nobody, I think, could call the set of conditions above "natural": the conditions on π seem to have been carefully chosen so as to achieve the required results, rather than occurring naturally. Also, these conditions are quite stringent, and make it hard to find suitable π, although as I've remarked, given a suitable π Bruck can indeed get interesting results.

Of course, I prefer my own generalisation (it may be a hideous child, but it looks just like me ...) Bruck's generalisation, as I said, seems to be inspired by the observation that the centre of a group is a characteristic subgroup. My version is based on the observation that Abelian groups are a subvariety of groups.

5.1 $\mathcal{V}$-solvability and $\mathcal{S}$-solvability

THEOREM 5.5 *Let A be an algebra and let $\mathcal{V}$ be a variety of the same type. Then there exists a congruence $\sim_{\mathcal{V}}$ on A, called the* **$\mathcal{V}$-commutator**, *such that for any congruence $\sim$ we have $\sim_{\mathcal{V}} \subseteq \sim$ if and only if $A/\sim$ belongs to $\mathcal{V}$. The $\mathcal{V}$-commutator is characteristic (that is, any automorphism of A permutes the congruence classes).* □

LEMMA 5.6 *Let A be an algebra and let $\mathcal{V}, \mathcal{W}$ be varieties with $\mathcal{V} \subseteq \mathcal{W}$. Then $\sim_{\mathcal{V}} \supseteq \sim_{\mathcal{W}}$.*

PROOF: As $L/\sim_{\mathcal{V}}$ belongs to $\mathcal{V}$ then it also belongs to $\mathcal{W}$. Hence $\sim_{\mathcal{V}} \supseteq \sim_{\mathcal{W}}$ as required. □

DEFINITION 5.7 *Let $\mathcal{V}_0 \subseteq \mathcal{V}_1 \subseteq \ldots$ be an ascending chain of varieties. Let $\mathcal{S} = \bigcup_i \{\mathcal{V}_i\}$. Then $\mathcal{S}$ will be called a* **limit variety**.

We have defined the class operators $\mathbf{H}, \mathbf{S}$ and $\mathbf{P}$ in the Introduction. It is easy to show by construction that limit varieties are not closed under $\mathbf{P}$

and so are not generally varieties (of course, every variety is a limit variety). However, we may substitute for $\mathbf{P}$ the operator $\mathbf{P}_{\text{fin}}$, defined by saying that $\mathbf{P}_{\text{fin}}\mathcal{C}$ is the class of all algebras isomorphic to finite direct products of algebras in $\mathcal{C}$

THEOREM 5.8 *Clearly $\mathcal{S}$ is closed under $\mathbf{H}, \mathbf{S}$ and $\mathbf{P}_{\text{fin}}$* □

THEOREM 5.9 *The intersection of two limit varieties is a limit variety.*

PROOF: For let $\mathcal{S}$ be the limit of $\mathcal{V}_0 \subseteq \mathcal{V}_1 \subseteq \ldots$ and let $\mathcal{T}$ be the limit of $\mathcal{W}_0 \subseteq \mathcal{W}_1 \subseteq \ldots$. Then consider the chain $\mathcal{V}_0 \cap \mathcal{W}_0 \subseteq \mathcal{V}_1 \cap \mathcal{W}_1 \subseteq \ldots$. Now on the one hand if $A \in \mathcal{V}_i \cap \mathcal{W}_i$ then $A \in \mathcal{S}$ and $A \in \mathcal{T}$, so $A \in \mathcal{S} \cap \mathcal{T}$.

On the other hand, suppose $A \in \mathcal{S} \cap \mathcal{T}$. Then $A \in V_i$ and $A \in \mathcal{W}_j$ for some particular i, j. Hence $A \in \mathcal{V}_{\max\{i,j\}}$ and $A \in \mathcal{W}_{\max\{i,j\}}$. Hence $A \in \mathcal{V}_{\max\{i,j\}} \cap \mathcal{W}_{\max\{i,j\}}$, and of course the intersection of two varieties is a variety.

So $\mathcal{S} \cap \mathcal{T} = \bigcup_i \{\mathcal{V}_i \cap \mathcal{W}_i\}$. □

THEOREM 5.10 *Let A be an algebra such that any descending chain in the lattice of characteristic congruences on A has a least element, and let $\mathcal{S}$ be a limit variety. Then there is a unique congruence $\sim_{\mathcal{S}}$ on A such that $\sim_{\mathcal{S}} \ \subseteq \ \sim$ if and only if $A/\sim \ \in \mathcal{S}$.*

PROOF: Let $\mathcal{S}$ be the union of the chain of congruences $\sim_{\mathcal{V}_0} \ \supseteq \ \sim_{\mathcal{V}_1} \ \supseteq \ldots$ in Con(A). This is indeed a chain by the previous lemma. Furthermore, this has a least element $\min_i\{\sim_{\mathcal{V}_i}\}$ because of the minimum condition. Now if $A/\sim\ \in \mathcal{S}$ then $A/\sim\ \in \mathcal{V}_k$ for some k. Hence $\sim\ \supseteq\ \sim_{\mathcal{V}_k}\ \supseteq\ \min_i\{\sim_{\mathcal{V}_i}\}$. So $A/\sim\ \in \mathcal{S} \Rightarrow\ \sim\ \supseteq \min_i\{\sim_{\mathcal{V}_i}\}$.

On the other hand, let $\sim\ \supseteq \min_i\{\sim_{\mathcal{V}_i}\}$. Then as $A/\min_i\{\sim_{\mathcal{V}_i}\} \in \mathcal{V}_k$ for some k, and $\mathcal{V}_k$ is a variety, we have $A/\sim\ \in \mathcal{V}_k$ and so in $\mathcal{S}$.

Hence we can define $\sim_{\mathcal{S}}$ to be $\min_i\{\sim_{\mathcal{V}_i}\}$. □

THEOREM 5.11 *Let A be an algebra and let $\mathcal{S}, \mathcal{T}$ be limit varieties with $\mathcal{S} \subseteq \mathcal{T}$. Then $\sim_{\mathcal{S}}\ \supseteq\ \sim_{\mathcal{T}}$.*

PROOF: As $A/\sim_{\mathcal{S}}$ belongs to $\mathcal{S}$ then it also belongs to $\mathcal{T}$. Hence $\sim_{\mathcal{S}}\ \supseteq\ \sim_{\mathcal{T}}$ as required. □

Now this being so, we could then adapt all our results to consider limits of chains of limit varieties and so forth. It is not clear that there is any interest in doing this, but it may as well be noted. It is more interesting to observe that we may adapt our results to pseudovarieties.

DEFINITION 5.12 *A* **pseudovariety** *is a class of finite algebras closed under* **H**, **S** *and* $\mathbf{P}_{\text{fin}}$.

Now the general form of a pseudovariety is well-known. For algebras of finite type, any pseudovariety $\mathcal{S}$ must consist precisely of the finite algebras contained in the limit of some chain of varieties $\mathcal{V}_0 \subseteq \mathcal{V}_1 \subseteq \ldots$. So if A is a finite algebra of finite type, then we may note that as A is finite, $A/\sim$ belongs to $\mathcal{S}$ if and only if $A/\sim$ belongs to $\bigcup_i\{\mathcal{V}_i\}$. Hence we can define the $\mathcal{S}$-commutator of A simply by setting $\sim_{\mathcal{S}}\ = \min_i\{\sim_{\mathcal{V}_i}\}$ as before, and as before we have $\sim_{\mathcal{S}}$ is a characteristic congruence on A with $\sim_{\mathcal{S}}\ \subseteq\ \sim$ if and only if $A/\sim\ \in \mathcal{S}$

In the case of pseudovarieties at least we needn't study limits of chains of pseudovarieties.

THEOREM 5.13 *Let $\mathcal{S}_0 \subseteq \mathcal{S}_1 \subseteq \ldots$ be a chain of pseudovarieties for a finite type (that is, there are only finitely many operations in the type. Then $\bigcup_i\{\mathcal{S}_i\}$ is a pseudovariety.* □

It is then clear from the foregoing discussion that:

THEOREM 5.14 *If L is a loop and $\mathcal{S}$ is a variety — or if L is a loop with the minimum condition on its lattice of characteristic congruences and $\mathcal{S}$ is a limit variety — or if L is a finite loop and $\mathcal{S}$ is a pseudovariety — then there is a unique smallest normal subloop $L^{\mathcal{S}}$ of L such that $L/L^{\mathcal{S}} \in \mathcal{S}$. Now $L^{\mathcal{S}}$ is characteristic in L, and for any $N \trianglelefteq L$ we have $L^{\mathcal{S}} \subseteq N$ if and only if L/N also belongs to $\mathcal{S}$.*

So for example if $\mathcal{S}$ is the variety of Abelian groups then $L^{\mathcal{S}} = L'$. Hence it is reasonable to make the following definition.

Definition 5.15 *Let L and $\mathcal{S}$ be as above, and define a series inductively by the rules $L_0 = L$ and $L_{i+1} = L_i^{\mathcal{S}}$. Then L is said to be* $\mathcal{S}$-**solvable** *if and only if there is some n such that $L_n = \{1_L\}$.*

Definition 5.16 *Let L be a $\mathcal{S}$-solvable loop, and let the series $L_0, L_1 \dots$ be defined as above. Then the* $\mathcal{S}$-**height** *of L is defined to be the smallest n such that $L_n = \{1_L\}$.*

Note that while every L_i must be characteristic in L, it is not obvious that it must be normal in L. I should guess that a counterexample exists. However in the group case any characteristic subgroup is normal.

We can easily produce generalisations of well-known results on (standard) solvability in groups to $\mathcal{S}$-solvability in loops.

Definition 5.17 *Let L and $\mathcal{S}$ be as above. An* $\mathcal{S}$-**series** *for L is a series $N_0 \supseteq N_2 \supseteq \dots N_n$ such that*

- $N_0 = L$
- $N_{i+1} \trianglelefteq N_i$ *for all i.*
- N_i/N_{i+1} *belongs to $\mathcal{S}$ for all i*
- $N_n = \{1_L\}$

Theorem 5.18 *L is $\mathcal{S}$-solvable if and only if L has an $\mathcal{S}$-series.*

PROOF: To prove the "if" part, let the series $N_0 \supseteq N_1 \supseteq \dots N_n$ be an $\mathcal{S}$-series for L and define the usual series $L_0 = L$ and $L_{i+1} = L_i^{\mathcal{S}}$. Observe that if $L_i \leq N_i$ then as N_i/N_{i+1} is of variety $\mathcal{S}$, so is L_iN_{i+1}/N_{i+1}, which is isomorphic to $L_i/(L_i \cap N_{i+1})$. Hence $L_i^{\mathcal{S}} \trianglelefteq L_i \cap N_{i+1}$ and so $L_i^{\mathcal{S}} \leq N_{i+1}$. Now by definition $L_i^{\mathcal{S}} = L_{i+1}$ and so $L_{i+1} \leq N_{i+1}$. So by induction $L_i \leq N_i$ for all i. So in particular $L_n = \{1_L\}$, so L is $\mathcal{S}$-solvable.

To see that the converse holds, observe that if the series $L_0, L_1, \dots$ terminates, then it's an $\mathcal{S}$-series. □

THEOREM 5.19 *Let L be $\mathcal{S}$-solvable and let $K \trianglelefteq L$. Then L/K is $\mathcal{S}$-solvable.*

PROOF: Consider the series $L_0K/K \supseteq \dots L_nK/K$, where the series $L_0, L_1 \dots$ is defined as before and with $L_n = \{1_L\}$. Then for any i we have $L_{i+1}K/K \trianglelefteq L_iK/K$. Now,

$$\begin{aligned}&(L_iK/K)/(L_{i+1}K/K)\\ &\cong (L_iK)/(L_{i+1}K)\\ &= (L_iL_{i+1}K)/L_{i+1}K\\ &\cong L_i/(L_i \cap (L_{i+1}K));\end{aligned}$$

now as $L_i \supseteq L_{i+1}$ we have $L_i \cap (L_{i+1}K) \supseteq L_{i+1}$. Hence $L_i/(L_i \cap (L_{i+1}K))$ belongs to $\mathcal{S}$, and so for any i we have $(L_iK/K)/(L_{i+1}K/K)$ belonging to $\mathcal{S}$. Hence $L_0K/K \supseteq \dots L_nK/K$ is an $\mathcal{S}$-series for L/K and so by the previous theorem L/K is $\mathcal{S}$-solvable as required. □

THEOREM 5.20 *Let L be $\mathcal{S}$-solvable and let $H \leq L$. Then H is $\mathcal{S}$-solvable.*

PROOF: We work by induction. Suppose that $H_i \leq L_i$ — which is certainly true in the case $i = 0$. Then

$$H_i/(L_{i+1} \cap H_i) \cong H_i L_{i+1}/L_{i+1} \leq L_i/L_{i+1},$$

which of course belongs to $\mathcal{S}$. Hence as varieties are preserved by taking subalgebras and isomorphic images, $H_i/(L_{i+1} \cap H_i)$ also belongs to $\mathcal{S}$. Hence $H_i^{\mathcal{S}} \leq L_{i+1} \cap H_i$ and so $H_i^{\mathcal{S}} \leq L_{i+1}$. By definition, $H_i^{\mathcal{S}} = H_{i+1}$ and so $H_{i+1} \leq L_{i+1}$. Hence by induction we have $H_i \leq L_i$ for all i. Hence if $L_n = \{1_L\}$ for some n, then $H_n = \{1_L\}$ also. □

THEOREM 5.21 *Let L and M be $\mathcal{S}$-solvable loops. Then $L \times M$ is also $\mathcal{S}$-solvable.*

PROOF: Consider the series $(L_0, M_0) \supseteq (L_1, M_1) \supseteq \ldots$ Clearly each subloop is normal in the one that precedes it. As L and M are $\mathcal{S}$-solvable, there is certainly some n such that $(L_n, M_n) = \{1_{L \times M}\}$. Now

$$(L_i, M_i)/(L_{i+1}, M_{i+1}) \cong L_i/L_{i+1} \times M_i/M_{i+1}.$$

We know that L_i/L_{i+1} and M_i/M_{i+1} belong to $\mathcal{S}$. Hence as varieties are preserved by taking direct products, this product must belong to $\mathcal{S}$, and so $(L_i, M_i)/(L_{i+1}, M_{i+1})$ belongs to $\mathcal{S}$ also. Hence the series

$$(L_0, M_0) \supseteq (L_1, N_1) \supseteq \ldots \supseteq (L_n, M_n)$$

is an $\mathcal{S}$-series for the loop $L \times M$. Hence $L \times M$ is $\mathcal{S}$-solvable as required. □

It is evident from the three preceding theorems that for any $\mathcal{S}$ the $\mathcal{S}$-solvable loops — or if $\mathcal{S}$ is a pseudovariety, the finite $\mathcal{S}$-solvable loops — are themselves closed under $\mathbf{H}, \mathbf{S}$ and $\mathbf{P}_{\text{fin}}$. Hence if $\mathcal{S}$ is a pseudovariety then the finite $\mathcal{S}$-solvable loops themselves form a pseudovariety.

Let us examine then the case where $\mathcal{S}$ is a limit variety. Then the $\mathcal{S}$-solvable loops do not generally form a variety, even in the case where $\mathcal{S}$ is itself a variety. For suppose we have a set $\mathcal{C}$ of $\mathcal{S}$-solvable loops such that for any n we have some L in $\mathcal{C}$ with $\mathcal{S}$-height greater than n. Of course $\mathcal{C}$ must be an infinite set. Then the direct product of the loops in $\mathcal{C}$ is not $\mathcal{S}$-solvable.

Let us consider, for any given n, the $\mathcal{S}$-solvable loops with $\mathcal{S}$-height less than n. It is clear from the preceding theorems that, where L and M are $\mathcal{S}$-solvable, we have the following:

- If $K \trianglelefteq L$ then the $\mathcal{S}$-height of L/K is at most the $\mathcal{S}$-height of L
- If $H \leq L$ then the $\mathcal{S}$-height of $H \leq$ the $\mathcal{S}$-height of L
- The $\mathcal{S}$-height of $L \times M$ is the maximum of the $\mathcal{S}$-heights of L and M.

It follows that the class of $\mathcal{S}$-solvable loops of height less than a given n is closed under $\mathbf{H}, \mathbf{S}$ and $\mathbf{P}$ and hence is a variety.

If we denote by $\mathcal{V}_i$ the variety of loops which are $\mathcal{S}$-solvable with $\mathcal{S}$-height at most i, then it is clear that $\mathcal{V}_0 \subseteq \mathcal{V}_1 \subseteq \ldots$ and that the class of $\mathcal{S}$-solvable groups is precisely $\bigcup_i\{\mathcal{V}_i\}$. Hence the class of $\mathcal{S}$-solvable loops is a limit variety.

THEOREM 5.22 *Let $\mathcal{S}$ be a limit variety. Then the class of quasigroups having $\mathcal{S}$-solvable multiplication groups is a limit variety.*

PROOF: Let Q be a quasigroup having $\mathcal{S}$-solvable multiplication group and let $\sim$ be any congruence on Q. Then $\mathcal{M}(Q/\sim) \cong \mathcal{M}(Q)/\mathrm{cor}(\sim)$. Now as $\mathcal{S}$-solvability is preserved by $\mathbf{H}$, this is $\mathcal{S}$-solvable. Hence having $\mathcal{S}$-solvable multiplication group is preserved by $\mathbf{H}$.

Similarly, we know that if $H \leq Q$ then $\mathcal{M}(H)$ is a homomorphic image of the subalgebra $\langle \lambda_H, \rho_H \rangle$ of $\mathcal{M}(Q)$. Now as $\mathcal{S}$-solvability is preserved by $\mathbf{H}$, and $\mathbf{S}$, this is $\mathcal{S}$-solvable. Hence having $\mathcal{S}$-solvable multiplication group is preserved by $\mathbf{S}$.

Now let Q_1 and Q_2 be two quasigroups with $\mathcal{S}$-solvable multiplication groups. Then $\mathcal{M}(Q_1 \times Q_2) \cong \mathcal{M}(Q_1) \times \mathcal{M}(Q_2)$. Now as $\mathcal{S}$-solvability is preserved by $\mathbf{P}_{\text{fin}}$, this is $\mathcal{S}$-solvable. Hence having $\mathcal{S}$-solvable multiplication group is preserved by $\mathbf{P}_{\text{fin}}$.

It is clear again that the class of quasigroups with $\mathcal{S}$-solvable multiplication groups with $\mathcal{S}$-heightat most n for given n is a variety, and that the class of quasigroups with $\mathcal{S}$-solvable multiplication groups is then the limit of the chain of such classes. □

THEOREM 5.23 *Similarly, if $\mathcal{S}$ is a pseudovariety then the class of finite* *quasigroups with $\mathcal{S}$-solvable multiplication groups is a pseudovariety.* □

THEOREM 5.24 *Let $\mathcal{V}$ be a group variety, and let*

$$\mathcal{W} = \{Q \in \mathcal{Q} : \mathcal{M}(Q) \in \mathcal{V}\}.$$

Then for any quasigroup Q, $\sim_{\mathcal{W}}$ is the projection of $\mathcal{M}(Q)^{\mathcal{V}}$ onto Q. □

Similar theorems hold for pseudovarieties and limit varieties.

THEOREM 5.25 *Let L be a loop and let $\mathcal{S}$ and $\mathcal{T}$ be limit varieties with $\mathcal{S} \subseteq \mathcal{T}$ — or let L be a finite loop and $\mathcal{S}$ and $\mathcal{T}$ be two pseudovarieties with $\mathcal{S} \subseteq \mathcal{T}$. Then if L is $\mathcal{S}$-solvable it is also $\mathcal{T}$-solvable.*

PROOF: Let $L_0 \supseteq L_1 \supseteq \ldots \supseteq L_n = \{1_L\}$ be the usual series for $\mathcal{S}$. Then L_i/L_{i+1} belongs to $\mathcal{S}$ and hence to $\mathcal{T}$. Hence $L_0 \supseteq \ldots \supseteq L_n$ is a $\mathcal{T}$-series. Hence L is $\mathcal{T}$-solvable. □

THEOREM 5.26 *Let L be a loop and let $\mathcal{S}$ and $\mathcal{T}$ be limit varieties. Then if $L^{\mathcal{S}}$ and $L^{\mathcal{T}}$ are defined, $\mathcal{L}^{\mathcal{S} \cap \mathcal{T}} = L^{\mathcal{S}} L^{\mathcal{T}}$.* □

THEOREM 5.27 *Let G be any group and let $\mathcal{S}$ be a limit variety — or let G be a finite group and let $\mathcal{S}$ be a pseudovariety. Then G is $\mathcal{S}$-solvable if and only if $\mathcal{M}(G)$ is $\mathcal{S}$-solvable .*

PROOF: G is isomorphic to a subgroup λ_G of $\mathcal{M}(G)$ and $\mathcal{M}(G)$ is isomorphic to a homomorphic image of $G \times G$. Hence as the property of being $\mathcal{S}$-solvable is closed under $\mathbf{H}$, $\mathbf{S}$ and $\mathbf{P}_{\text{fin}}$ the result follows. □

Finally in this section, here are a couple of results relating to isotopy.

THEOREM 5.28 *Let $\mathcal{V}$ be a variety preserved by loop isotopy. Then if $(L_1, *)$ is isotopic to $(L_2, \circ)$ then $L_1/L_1^{\mathcal{V}}$ is isotopic to $L_2/L_2^{\mathcal{V}}$*

PROOF: As stated in Section 3, we may take the isotopy to be of the form $a \circ b = a/\!\!/y * x\backslash\!\!\backslash b$. It then follows that L_2 has the element $x * y$ as its identity element, and that $xy * L_1^{\mathcal{V}}$ is a normal subloop of L_2. Now the isotopy $a \circ b = a/\!\!/y * x\backslash\!\!\backslash b$ induces an isotopy between $L_1/L_1^{\mathcal{V}}$ and $L_2/xy * L_1^{\mathcal{V}}$, so as $\mathcal{V}$ is preserved by loop isotopy, we must have $L_2^{\mathcal{V}} \subseteq xy * L_1^{\mathcal{V}}$: and by considering the inverse isotopism we obtain equality, giving the desired result. □

Hence we immediately have:

COROLLARY 5.29 *Let $\mathcal{V}$ be a variety with the isotopy-isomorphy property. Then if L_1 is isotopic to L_2 then $L_1/L_1^{\mathcal{V}} \cong L_2/L_2^{\mathcal{V}}$* □

5.2 Generalising Fitting's theorem

THEOREM 5.30 *Let L be a finite loop and $\mathcal{S}$ be a pseudovariety. Then L is $\mathcal{S}$-solvable if and only if every factor loop of L is in $\mathcal{S}$.*

PROOF: Being finite, L of course has a composition series

$$L = K_0 \rhd K_1 \rhd \ldots \rhd K_n = \{1_L\}$$

Now if L is $\mathcal{S}$-solvable, then so is K_i for each $0 \leq i < n$, by virtue of being a subloop, and then as K_i/K_{i+1} is a homomorphic image of K_i, it must also be $\mathcal{S}$-solvable. But as this is a composition series, K_{i+1} is maximal normal in K_i and so K_i/K_{i+1} is simple. Hence being simple and $\mathcal{S}$-solvable it must lie in $\mathcal{S}$.

Conversely, suppose that each of the factor groups lies in $\mathcal{S}$. Then the composition series is an $\mathcal{S}$-series for L. □

This suggests the following incidental theorem:

THEOREM 5.31 *Let L be a finite loop which is $\mathcal{S}$-solvable . Then $L^{\mathcal{S}}$ is contained in the cosocle of L.* □

We may also now easily generalise Fitting's theorem:

THEOREM 5.32 (FITTING'S THEOREM) *Let L be a finite loop and $\mathcal{S}$ be a pseudovariety. Then L contains a unique largest normal $\mathcal{S}$-solvable subloop, which of course is characteristic.*

PROOF: For let J and K be two normal $\mathcal{S}$-solvable subloops. We wish to show that JK is $\mathcal{S}$-solvable . Consider then that $K \trianglelefteq JK$, and that $JK/K = J/(J \cap K)$. Now $J/(J \cap K)$ is a homomorphic image of J — which by hypothesis is $\mathcal{S}$-solvable — and so is $\mathcal{S}$-solvable, and so all its factor groups lie in $\mathcal{S}$. Also, all the factor groups of K lie in $\mathcal{S}$, as by hypothesis K is $\mathcal{S}$-solvable.

So all the factor groups of JK/K and of K lie in $\mathcal{S}$. It follows that all the factor groups of JK lie in $\mathcal{S}$ and so the result follows. □

5.3 An alternative generalisation

Another way to reach essentially the same generalisation is to begin by observing that many of the basic theorems on solvability follow from certain attractive properties of L'. This motivates the following definition:

DEFINITION 5.33 *Let Θ be a function mapping each loop in $\mathcal{L}$ — the variety of loops — to one of its normal subloops, and such that*

1. *For any $L \in \mathcal{L}$ and any homomorphism $\phi : L \to \phi L$ we have $\phi\Theta L = \Theta\phi L$.*
2. *For any $L \in \mathcal{L}$ and any $H \leq L$ we have $\Theta L \supseteq \Theta H$ — or more precisely, ΘL contains the natural inclusion of ΘH in L.*
3. *For any set $\mathcal{P} \subseteq \mathcal{L}$ we have $\prod_{L\in\mathcal{P}} \Theta L \supseteq \Theta \prod_{L\in\mathcal{P}} L$ — or to be precise, the natural inclusion of $\prod_{L\in\mathcal{P}} \Theta L$ in $\prod_{L\in\mathcal{P}} L$ contains $\Theta \prod_{L\in\mathcal{P}} L$.*

Then we shall say that a loop L is Θ-solvable if and only if there is some n such that $\Theta^n L$ is the trivial loop.

It is clear that for any loop variety $\mathcal{V}$, the mapping $\Theta_{\mathcal{V}}$ given by $\Theta_{\mathcal{V}} L = L^{\mathcal{V}}$ is just such a function, and so L is $\mathcal{V}$-solvable if and only if L is $\Theta_{\mathcal{V}}$-solvable.

I can also give a reverse construction, giving for each Θ a variety $\mathcal{V}_\Theta$ such that $\Theta L = L^{\mathcal{V}_\Theta}$, so demonstrating that L is Θ-solvable if and only if L is $\mathcal{V}_\Theta$-solvable.

LEMMA 5.34 *Let Θ be a function as described above. Then the set*

$$\mathcal{V}_\Theta = \{L \in \mathcal{L} : \Theta L = \{1_L\}\}$$

is a loop variety. □

From which we may deduce:

THEOREM 5.35 *For any loop L we have $\Theta L = L^{\mathcal{V}_\Theta}$*

PROOF: On the other hand, consider that for any loop L we have

$$\Theta(L/\Theta L) = \Theta L/\Theta L,$$

by condition 1 on Θ, and so $L/\Theta L \in \mathcal{V}_\Theta$. Hence $L^{\mathcal{V}_\Theta} \subseteq \Theta L$. On the other hand, consider that $L/L^{\mathcal{V}_\Theta} \in \mathcal{V}_\Theta$, so $\Theta(L/L^{\mathcal{V}_\Theta})$ is the identity $L^{\mathcal{V}_\Theta}/L^{\mathcal{V}_\Theta}$ by definition of $\mathcal{V}_\Theta$. But we also know, by condition 1 on Θ, that

$$\Theta(L/L^{\mathcal{V}_\Theta}) = ((\Theta L)(L^{\mathcal{V}_\Theta}))/L^{\mathcal{V}_\Theta}.$$

We conclude that $(\Theta L)(L^{\mathcal{V}_\Theta}) = L^{\mathcal{V}_\Theta}$ and so that $\Theta L \subseteq L^{\mathcal{V}_\Theta}$.

Hence for any L we have $\Theta L = L^{\mathcal{V}_\Theta}$ as required. □

It is easy to alter this theorem so that it deals with finite loops and pseudovarieties.

It is clear that solvability may be defined on groups and loops because we have a correspondence in loop theory between congruences of a loop and normal substructures. No other particular properties of a loop were used. It follows that the results above generalise to all such algebras. The most important example is the variety of rings.

5.4 Note on the algebra of varieties

Briefly, if $\mathcal{V}, \mathcal{W}$ are loop varieties then the class

$$\mathcal{V}\mathcal{W} = \{L \in \mathcal{L} : \exists N \trianglelefteq L : N \in \mathcal{V} \wedge L/N \in \mathcal{W}\}$$

is also a loop variety, moreover, this multiplication is associative. Then we may define $\mathcal{V}$ solvability by saying that a loop is $\mathcal{V}$-solvable of height n if and only if it is in $\mathcal{V}^n$.

In Section 6, we shall develop a rather similar algebra, so it may be worth the reader's while to try and prove the claims about $\mathcal{V}\mathcal{W}$ made above.

This may remind the reader of the algebra of group varieties put forward by Hannah Neumann [21]. Indeed, in the group case they are identical, since generalised solvability in groups is the same from the top down as from the bottom up.

6 Generalising nilpotence

I shall now take a similar look at nilpotence. I shall do so first in the loop case and then look at the more general algebraic case.

DEFINITION 6.1 *Let X be a function mapping each loop in $\mathcal{L}$ to one of its normal subloops, and such that*

1. *For any $L \in \mathcal{L}$ and any homomorphism $\phi : L \to \phi L$ we have $\phi XL \subseteq X\phi L$.*
2. *For any $L \in \mathcal{L}$ and any $H \leq L$ we have $H \cap XL \subseteq XH$ — or more precisely, $H \cap XL$ lies in the natural inclusion of XH in L.*
3. *For any set $\mathcal{P} \subseteq \mathcal{L}$ we have $\prod_{L\in\mathcal{P}} XL \subseteq X\prod_{L\in\mathcal{P}} L$ — or more precisely, the natural inclusion of $\prod_{L\in\mathcal{P}} XL$ in $\prod_{L\in\mathcal{P}} L$ lies in $X\prod_{L\in\mathcal{P}} L$.*

Then X will be called a **loop centroid***, or, since we are going to be working in the variety of loops, we may just refer to such a function as a* **centroid** *where there is no ambiguity.*

EXAMPLE 6.2 *Let $\mathcal{V}$ be any loop variety, and set*

$$QL = \bigcup\{N \trianglelefteq L : N \in \mathcal{V}\}.$$

Then Q is a centroid.

EXAMPLE 6.3 *The function $\mathcal{Z}$ sending L to $\mathcal{Z}(L)$ is a centroid.*

Note also that for any centroid X, we must have XL characteristic in L as a trivial consequence of condition 1. It seems (what a surprise!) that centroids are a good generalisation of the idea of the centre of a loop. Hence the following definition.

DEFINITION 6.4 *A series $L = K_0 \supseteq K_1 \supseteq K_2 \supseteq \ldots$ of normal subloops of L is said to be an* X-**central series** *if and only if $K_i/K_{i+1} \subseteq X(L/K_{i+1})$ for all i.*

So again by analogy we may define X-nilpotence as a generalisation of nilpotence:

DEFINITION 6.5 *A loop L will be said to be* X-**nilpotent** *if and only if it has an X-central series $L = K_0 \supseteq K_1 \supseteq K_2 \supseteq \ldots \supseteq K_n = \{1_L\}$.*

Then we produce the equivalent of the upper central series.

DEFINITION 6.6 *The* **upper** X-**central series** *of a loop L is defined inductively as follows*

- $J_1 = \{1_L\}$
- $J_{i+1} = \{x \in L : xJ_i \in X(L/J_i)\}$

THEOREM 6.7 *A loop L has an X-central series*

$$L = K_0 \supseteq K_1 \supseteq K_2 \supseteq \ldots \supseteq K_n = \{1_L\}$$

if and only if the n^{th} subloop in the upper central series equals L. □

The proof follows the proof for classical nilpotence in groups so closely that it may as well be omitted. We may use this to give a generalised definition of the class of a nilpotent group:

DEFINITION 6.8 *Let L be a loop with the n^{th} subloop in the upper central series equal to L, and such that n is the smallest natural number with this property. Then we shall say that L is* **X-nilpotent of length** *n.*

I substitute the word "length" for the word "class" used in the classical theory of nilpotence to avoid confusion, as we are already making some use of the word "class" in its set-theoretic sense.

Now let's construct a lower central series.

Let $\mathcal{N}_0$ be the trivial variety, and inductively define

$$\mathcal{N}_{i+1} = \{L \in \mathcal{L} : L/XL \in \mathcal{N}_i\}.$$

Then for any i the class $\mathcal{N}_i$ is the variety of loops which are X-nilpotent of length at most i. If this is not apparent (and indeed I have given no proof as yet that such loops do indeed form a variety) the proof will appear later when I deal with the algebra of centroids.

Then the **lower X-central series** will be defined to be the normal series $L^{\mathcal{N}_0}, L^{\mathcal{N}_1}, L^{\mathcal{N}_2}, \ldots$

THEOREM 6.9 *The lower X-central series is, indeed, an X-central series.*

PROOF: As $L/L^{\mathcal{N}_{i+1}} \in \mathcal{N}_{i+1}$ we have

$$(L/L^{\mathcal{N}_{i+1}})/X(L/L^{\mathcal{N}_{i+1}}) \in \mathcal{N}_i.$$

So $X(L/L^{\mathcal{N}_{i+1}}) \supseteq (L/L^{\mathcal{N}_{i+1}})^{\mathcal{N}_i}$. Now as $L^{\mathcal{N}_{i+1}} \subseteq L^{\mathcal{N}_i}$ we have

$$(L/L^{\mathcal{N}_{i+1}})^{\mathcal{N}_i} = L^{\mathcal{N}_i}/L^{\mathcal{N}_{i+1}}.$$

So

$$X(L/L^{\mathcal{N}_{i+1}}) \supseteq L^{\mathcal{N}_i}/L^{\mathcal{N}_{i+1}}$$

as required. □

6.1 Algebra of loop centroids

In this subsection I shall develop just enough of an algebra of loop centroids to show the algebra of centroids relates to X-nilpotence, and how generalised nilpotence may be related to generalised solvability in loops. The same algebra will be treated much more thoroughly, in a more abstract setting, in the following subsection.

THEOREM 6.10 *Let X, Y be centroids. Then $X \wedge Y$ — defined by letting $(X \wedge Y)(L) = X(L) \cap Y(L)$ — is also a centroid.*

PROOF: We shall just check the conditions for being a centroid one by one.

First, note that if ϕ is a homomorphism $L \to \phi L$ then

$$\phi((X \wedge Y)(L)) \subseteq \phi X(L) \cap \phi Y(L) \subseteq X(\phi L) \cap Y(\phi L) = (X \wedge Y)(\phi L).$$

Secondly,

$$H \cap (X \wedge Y)L = H \cap X(L) \cap Y(L) \subseteq H \cap X(L) \subseteq X(H).$$

On similar grounds,

$$H \cap (X \wedge Y)L \subseteq Y(H).$$

So

$$H \cap (X \wedge Y)L \subseteq X(H) \cap Y(H) = (X \wedge Y)(H).$$

as required.

Thirdly,

$$\begin{aligned}\coprod_{L \in \mathcal{P}} (X \wedge Y)(L) &= \coprod_{L \in \mathcal{P}} X(L) \cap Y(L) \\ &\subseteq \coprod_{L \in \mathcal{P}} X(L) \cap \coprod_{L \in \mathcal{P}} Y(L) \\ &\subseteq X(\coprod_{L \in \mathcal{P}} L) \cap Y(\coprod_{L \in \mathcal{P}} L) \\ &= (X \wedge Y)(\coprod_{L \in \mathcal{P}} L)\end{aligned}$$

as required. □

There is another more interesting way of combining centroids.

DEFINITION 6.11 *Let X and Y be centroids. Then we define their* **centroid product**, *written $X * Y$, by*

$$(X * Y)(L) = \{q \in L : qX(L) \in Y(L/X(L))\}.$$

The reader is advised to think about the following theorem carefully before — or instead of — reading the proof, since it is quite easy to grasp the theorem intuitively.

THEOREM 6.12 *Let X and Y be centroids. Then $X * Y$ is a centroid.*

PROOF: As in the last proof, we shall work our way carefully through the conditions for a function to be a centroid.

First of all, let ϕ be a homomorphism $L \to \phi L$. Then by definition $q \in (X * Y)(L)$ if and only if $qX(L) \in Y(L/X(L))$. Now let θ be the homomorphism from $L/X(L) \to \phi L/X(\phi L)$ given by sending $xX(L)$ to $(\phi x)X(\phi L)$. Then if $qX(L) \in Y(L/X(L))$ then $\theta qX(L) \in \theta Y(L/X(L))$, i.e.

$$(\phi q)X(\phi L) \in \theta Y(L/X(L)) \subseteq Y(\theta(L/X(L))) = Y(\phi L/X(\phi L))$$

So $\phi q \in (X * Y)(\phi L)$. So we have

$$\phi((X * Y)(L)) \subseteq (X * Y)(\phi L)$$

as required.

Secondly, let $H \leq L$. Now from the definition

$$H \cap (X * Y)(L) = \{q \in H : qX(L) \in Y(L/X(L))\}.$$

So let $q \in H \cap (X * Y)(L)$. Then

$$qX(L) \in HX(L)/X(L) \cap Y(L/X(L)),$$

and so using condition 2 for centroids we have $qX(L) \in Y(HX(L)/X(L))$. So let θ be the homomorphism from $HX(L)/X(L) \to H/X(H)$ given by sending $hX(L)$ to $hX(H)$. Then for q as given,

$$qX(H) = \theta(qX(L)) \in \theta(Y(HX(L)/X(L))$$

$$\subseteq Y(\theta(HX(L)/X(L))) = Y(H/X(H)).$$

So $q \in (X * Y)(H)$ as required.

Thirdly, consider that by definition

$$\prod_{L\in\mathcal{P}} (X * Y)(L) = \prod_{L\in\mathcal{P}} \{q \in L : qX(L) \in Y(L/X(L))\}.$$

Now this is just

$$\{q \in \prod_{L\in\mathcal{P}} L : q \prod_{L\in\mathcal{P}} X(L) \in (\prod_{L\in\mathcal{P}} Y(L))/(\prod_{L\in\mathcal{P}} X(L)))\},$$

which by condition 3 is a subset of

$$\{q \in \prod_{L\in\mathcal{P}} L : q \prod_{L\in\mathcal{P}} X(L) \in (Y(\prod_{L\in\mathcal{P}} L))/(\prod_{L\in\mathcal{P}} X(L)))\}.$$

So define

$$\theta : (\prod_{L\in\mathcal{P}} L)/(\prod_{L\in\mathcal{P}} X(L)) \to (\prod_{L\in\mathcal{P}} L)/X(\prod_{L\in\mathcal{P}} L)$$

to be the homomorphism which maps $x \prod_{L\in\mathcal{P}} X(L)$ to $xX(\prod_{L\in\mathcal{P}} L)$. Then since we have

$$q \prod_{L\in\mathcal{P}} X(L) \in Y((\prod_{L\in\mathcal{P}} L)/(\prod_{L\in\mathcal{P}} X(L)))$$

then by applying θ to both sides of this we obtain

$$\theta(q\prod_{L\in\mathcal{P}} X(L)) \in \theta(Y((\prod_{L\in\mathcal{P}} L)/(\prod_{L\in\mathcal{P}} X(L))))$$

so using condition 1 and applying θ we get

$$qX(\prod_{L\in\mathcal{P}} L) \in Y((\prod_{L\in\mathcal{P}} L)/X(\prod_{L\in\mathcal{P}} L))$$

as required.

So $(X * Y)$ is a centroid. $\square$

THEOREM 6.13 *Let X, Y, Z be centroids. Then $X * (Y * Z) = (X * Y) * Z$.*

PROOF: For

$$(X * (Y * Z))(L) = \{q \in L : qX(L) \in (Y * Z)(L/X(L))\}$$

$$= \{q \in L : qX(L)Y(L/X(L)) \in Z((L/X(L))/Y(L/X(L)))\}.$$

Now from the definition of the centroid product we have

$$Y(L/X(L)) = ((X * Y)(L))/X(L).$$

So substituting this, we get

$$(X * (Y * Z))(L) =$$

$$\{q \in L : qX(L)(((X*Y)(L))/X(L)) \in Z((L/X(L))/(((X*Y)(L))/X(L)))\}.$$

Then applying the third isomorphism theorem we have

$$(X * (Y * Z))(L) =$$

$$\{q \in L : q(X * Y)(L) \in Z(L/(X * Y)(L))\} = ((X * Y) * Z)(L)$$

as required. □

THEOREM 6.14 *Let X, Y, Z be centroids. Then* $(X \wedge Y) * Z \subseteq (X * Z) \wedge (Y * Z)$

— That is to say, for all $L \in \mathcal{L}$ we have $((X \wedge Y) * Z)(L) \subseteq ((X * Z) \wedge (Y * Z))(L)$

PROOF: Let

$$((X \wedge Y) * Z)(L) = \{q \in L : q(X \wedge Y)(L) \in Z(L/(X \wedge Y)(L))\}.$$

Now let θ be the homomorphism $L/(X \wedge Y)(L) \to L/X(L)$ given by sending $x(X \wedge Y)(L)$ to $xX(L)$. Then if $q \in ((X \wedge Y) * Z)(L)$ then $q(X \wedge Y)(L) \in Z(L/(X \wedge Y)(L))$ so $\theta(q(X \wedge Y)(L)) \in \theta(Z(L/(X \wedge Y)(L)))$. So using condition 1 and applying θ, we get $qX(L) \in Z(L/X(L))$, i.e. $q \in (X * Z)(L)$. By similar reasoning, $q \in (Y * Z)(L)$. Hence $((X \wedge Y) * Z)(L) \subseteq (X * Z)(L) \cap (Y * Z)(L) = ((X * Z) \wedge (Y * Z))(L)$ as required. □

THEOREM 6.15 $X * (Y \wedge Z) = (X * Y) \wedge (X * Z)$

PROOF: For $(X * (Y \wedge Z))(L) = \{q \in L : qX(L) \in (Y \wedge Z)(L/X(L))\} = \{q \in L : qX(L) \in Y(L/X(L)) \cap Z(L/X(L))\} = \{q \in L : qX(L) \in Y(L/X(L))\} \cap \{q \in L : qX(L) \in Z(L/X(L))\} = (X * Y)(L) \cap (X * Z)(L) = ((X * Y) \wedge (X * Z)(L))$ as required. □

Let O be the centroid mapping every loop to itself and

Let E be the centroid mapping every loop L to $\{1_L\}$.

THEOREM 6.16 *For any centroid X we have*

- $O * X = O = X * O$
- $E * X = X = X * E$
- $O \wedge X = X = X \wedge O$
- $E \wedge X = E = X \wedge E$

□

DEFINITION 6.17 *If X is a centroid, it is convenient to define X^{*n} inductively by the rules*

- $X^{*0} = E$
- $X^{*i+1} = X * X^{*i}$

Now we may associate centroids with varieties in the following manner. First, observe that:

THEOREM 6.18 *Let X be a centroid and let $\mathcal{V}$ be a variety. Then the class*

$$\{L \in \mathcal{L} : L/X(L) \in \mathcal{V}\}$$

is a variety. □

This may be proved trivially from the behaviour of centroids and the behaviour of $\mathcal{V}$-commutators. In particular, this holds where $\mathcal{V}$ is the trivial variety.

COROLLARY 6.19 *Let X be a centroid. Then the class*

$$\mathcal{V}_X = \{L \in \mathcal{L} : L = X(L)\}$$

is a variety. □

I shall call such varieties **centroid varieties**. Putting these last two results together, we have the following result:

COROLLARY 6.20 *Let X and Y be centroids. Then*

$$\mathcal{V}_{X*Y} = \{L \in \mathcal{L} : L/X(L) \in \mathcal{V}_Y\}.$$

□

It is now easy to see, from the definition of X-nilpotence and from my remarks on the upper X-central series, that if X is a centroid then the class of loops which are X-nilpotent of length $\leq i$ is just the centroid variety $\mathcal{V}_{X^{*i}}$. The generalisations of the classical result on homomorphic images, subgroups and direct products of nilpotent groups then follow without a fight.

Note that as a corollary to the last corollary we have

COROLLARY 6.21 *Let X, Y be centroids. Then $\mathcal{V}_{X*Y} \subseteq \mathcal{V}_X\mathcal{V}_Y$ — the usual varietal product of $\mathcal{V}_X$ and $\mathcal{V}_Y$.* □

This follows from the fact that $X(L) \in \mathcal{V}_X$ for any centroid X and $L \in \mathcal{L}$. It follows immediately from the definitions that

COROLLARY 6.22 *Let $L \in \mathcal{L}$ be X-nilpotent. Then L is $\mathcal{V}_X$-solvable.* □

6.2 Centroids in any variety

The astute reader will have noticed that apart from the results connecting nilpotence to strong solvability, we don't need centroids to be subalgebras: it is enough that they be congruences. We may therefore generalise the ideas of centroids and X-nilpotence still further.

6.3 The lattice of characteristic congruences

The reader should be aware that to each algebra A we may asign a set of congruences $\mathrm{Con}(A)$ with lattice operations $\wedge$ and $\vee$. The basic definitions and results can be found in any volume on Universal Algebra and so will not be repeated here.

In what follows I shall write $C[a]$ for the class of a under the congruence C, rather than $[a]_C$ as has been my usual practice. This makes the algebra — slightly — clearer.

Just as in group theory, where one writes HN/N to denote the subgroup of G/N consisting of the cosets of N containing the elements of H, so if $H \leq A$ for some algebra A, and C is a congruence on A, I shall write

$C[H]/C$ to denote the subalgebra $\{C[h] : h \in H\}$ of A/C. The reader will then for example recognise $C[H]/C \cong H/((H \times H) \cap C)$ as a form of the second isomorphism theorem (the reader may think that this is the third isomorphism theorem — there is some debate on the subject — but for the purposes of this thesis it's the second).

If R, S are congruences on A, B respectively, then by $R \times S$ I mean the relation given by

$$(R \times S)[(x, y)] = \{(a, b) \in A \times B : a \in R[x] \wedge b \in S[y]\}.$$

It is trivial to see that this must be a congruence on $A \times B$. This definition extends naturally to infinite direct products.

In the case of quasigroups I have earlier in this thesis proposed a definition which can be applied more generally.

DEFINITION 6.23 *Let A be an algebra and let $X \in \mathrm{Con}(A)$. Then we shall say that X is a* **characteristic congruence** *if and only if for all $\alpha \in \mathrm{Aut}(A)$ and all $a \in A$ we have $\alpha[a] = [\alpha a]$*

DEFINITION 6.24 *The set of characteristic congruences of A will be called* $\mathrm{CCon}(A)$.

It is then easy to check the following:

THEOREM 6.25 $\mathrm{CCon}(A)$ *is a complete sublattice of* $\mathrm{Con}(A)$ □

Furthermore we have the following theorem:

THEOREM 6.26 *Let A be an algebra, let $R \in \mathrm{CCon}(A)$ and let S be a member of $\mathrm{CCon}(A/R)$. Then the congruence T on A given by $x \sim_T y$ if and only if $R[x] \sim_S R[y]$ is characteristic.*

PROOF: For as R is characteristic every automorphism of A induces an automorphism on A/R, which as S is characteristic fixes T. □

6.4 Characteristic functions

DEFINITION 6.27 *Let $\mathcal{A}$ be a variety. A function F which maps each $A \in \mathcal{A}$ to some element of $\mathrm{Con}(A)$ and having the property that for any isomorphism ϕ from A onto ϕA we have $\phi F A = F \phi A$ will be called a* **characteristic function** *of the variety $\mathcal{A}$. The class of such functions will be called $\mathrm{CFun}(\mathcal{A})$.*

It is clear from the definition that as characteristic functions must be preserved by automorphisms, we must in fact have $FA \in \mathrm{CCon}(\mathcal{A})$ for all $F \in \mathrm{CFun}(\mathcal{A})$ and $A \in \mathcal{A}$.

From the remarks and theorems in the previous subsection, we may fit out the set $\mathrm{CFun}(\mathcal{A})$ with three operations and an ordering.

DEFINITION 6.28 *Let $X, Y \in \mathrm{CFun}(\mathcal{A})$. Then*

- *$X \wedge Y$ is defined by $(X \wedge Y)A = XA \wedge YA$, where on the right hand side of the equation, the symbol $\wedge$ denotes the lattice operation on* $\mathrm{CCon}(\mathcal{A})$

- *$X \vee Y$ is defined by $(X \vee Y)A = XA \vee YA$, using a similar convenient abuse of notation.*

- *We then of course have an ordering given by $X \leq Y$ if and only if $XA \subseteq YA$ for all $A \in \mathcal{A}$*

- *$(F * G)$ — the* **extension product of** X **by** Y *is defined by saying that for each $a \in \mathcal{A}$ the congruence $(X * Y)A$ is the kernel of the natural homomorphism from A to $(A/XA)/Y(A/XA)$ — that is,*

$$(X * Y)[a] = \{q \in A : XA[q] \in Y(A/XA)[XA[a]]\}.$$

Although the class with the three operations is strictly speaking too big to be an algebra, this presents no particular problems and so I shall treat it as one. The $\wedge$ and $\vee$ operations behave like lattice operations, the ordering behaves like a lattice ordering, and the operation $*$, as we shall demonstrate, behaves like a semigroup:

THEOREM 6.29 *Let $X, Y, Z \in$ $\mathrm{CFun}(\mathcal{A})$.. Then $X * (Y * Z) = (X * Y) * Z$*

PROOF: By definition

$$((X * (Y * Z))A)[a] =$$

$$\{q \in A : (Y(A/XA))[XA[q]] \in (Z((A/XA)/Y(A/XA)))[Y(A/XA)[XA[a]]\}.$$

Now by definition of the extension product there's an isomorphism defined $(A/XA)/Y(A/XA) \to A/(X*Y)A$ given by

$$(Y(A/XA))[XA[p]] \mapsto ((X*Y)A)[p].$$

So as the functions are characteristic, the set above is just

$$\{q \in A : ((X*Y)A)[q] \in Z(A/(X(X*Y)A))[((X*Y)A)[a]]\}$$

which is equal to $(((X*Y)*Z)A)[a]$ by definition. □

Note also that:

THEOREM 6.30 $X \leq X*Y$ □

Moreover, note that we can regard $(\mathrm{CFun}(\mathcal{A}), \wedge, \vee)$ as being isomorphic to a "subalgebra" of the "lattice" $\prod_{A \in \mathcal{A}} \mathrm{CCon}(\mathcal{A})$. Hence it will obey the same lattice laws as as $\mathrm{CCon}(\mathcal{A})$ and so as $\mathrm{Con}(\mathcal{A})$ — for example, if $\mathcal{A}$ is congruence modular, then $(\mathrm{CFun}(\mathcal{A}), \wedge, \vee)$ is modular.

Our "algebra" also has two obvious constants:

DEFINITION 6.31 *Let $O_{\mathcal{A}}$ be the characteristic function of $\mathcal{A}$ mapping every $A \in \mathcal{A}$ to the complete congruence on A and let $E_{\mathcal{A}}$ be the characteristic function of $\mathcal{A}$ mapping every $A \in \mathcal{A}$ to the trivial congruence on A.*

Clearly $O_{\mathcal{A}}$ is the bottom and $E_{\mathcal{A}}$ the top of the "lattice" $(\mathrm{CFun}(\mathcal{A}), \wedge, \vee)$. Moreover:

Theorem 6.32 *For any* $X \in \mathrm{CFun}(\mathcal{A})$ *we have*

- $O_{\mathcal{A}} * X = O_{\mathcal{A}} = X * O_{\mathcal{A}}$
- $E_{\mathcal{A}} * X = X = X * E_{\mathcal{A}}$
- $O_{\mathcal{A}} \wedge X = X = X \wedge O_{\mathcal{A}}$
- $E_{\mathcal{A}} \wedge X = E_{\mathcal{A}} = X \wedge E_{\mathcal{A}}$

□

6.5 Some interesting subsets of CFun($\mathcal{A}$)

Most characteristic functions are not at all interesting. Usually we only concern ourselves with those characteristic functions — such as that mapping a group to its centre — which have useful and agreeable properties. In an abstract setting, such properties must needs be defined abstractly. There are six of particular interest.

Definition 6.33 *Let* $\mathcal{A}$ *be a variety. We define the properties H1, H2, S1, S2, P1, P2 as follows:*

1. *H1(X): For any* $A \in \mathcal{A}$ *and homomorphism* ϕ *from* A *to* ϕA *we have* $\phi X A \supseteq X \phi A$
2. *H2(X): For any* $A \in \mathcal{A}$ *and homomorphism* ϕ *from* A *to* ϕA *we have* $\phi X A \subseteq X \phi A$

3. *S1(X): For any $A \in \mathcal{A}$ and $H \leq A$ we have $(H \times H) \cap XA \supseteq XH$*

4. *S2(X): For any $A \in \mathcal{A}$ and $H \leq A$ we have $(H \times H) \cap XA \subseteq XH$*

5. *P1(X): For any collection A_Λ of algebras in $\mathcal{A}$ we have*

$$\prod_{\lambda \in \Lambda} XA_\lambda \supseteq X \prod_{\lambda \in \Lambda} A_\lambda$$

6. *P2(X): For any collection A_Λ of algebras in $\mathcal{A}$ we have*

$$\prod_{\lambda \in \Lambda} XA_\lambda \subseteq X \prod_{\lambda \in \Lambda} A_\lambda$$

DEFINITION 6.34 *Suppose X satisfies $H2, S2, P2$. Then X will be called an* **$\mathcal{A}$-centroid**, *or, where the variety we are using is clear and there is no ambiguity, we shall just call such a function a* **centroid**.

Using the condition H2 it is easy to see that for any centroid X and algebra A the congruence XA is a characteristic congruence.

THEOREM 6.35 *Let X, Y be $\mathcal{A}$-centroids. Then $X * Y$ is an $\mathcal{A}$-centroid.*

PROOF: We shall work through the conditions for a function to be a centroid one by one. In each case, to show the desired inclusion we shall demonstrate it for an arbitrary algebra $A \in \mathcal{A}$.

Firstly, let $\phi : A \to \phi A$ be a homomorphism. Then

$$((X * Y)A[a]) = \{q \in A : XA[q] \in Y(A/XA)[XA[a]]\}.$$

Now let $\theta : A/XA \to \phi A/X\phi A$ be the homomorphism given by $XA[p] \mapsto X\phi A[\phi p]$. Then

$$\{q \in A : XA[q] \in Y(A/XA)[XA[a]]\}$$

$$\subseteq \{q \in A : \theta XA[q] \in \theta Y(A/XA)[XA[a]]\}$$

$$\subseteq \{q \in A : X\phi A[\phi q] \in Y(\phi A/X\phi A)[X\phi A[\phi a]]\}$$

$$= \{q \in A : \phi q \in ((X * Y)\phi A)[\phi a]\}$$

as required.

Secondly, let $h \in H \leq A$, and let $q \in ((H \times H) \cap ((X * Y)A))[h]$ — that is, $q \in H$ and $XA[q] \in Y(A/XA)[h]$. Then

$$XA[q] \in ((XA[H]/XA \times XA[H]/XA) \cap Y(A/XA)) \subseteq Y(XA[H]/XA)$$

by condition S2. So let

$$\theta : XA[H]/XA \to H/XH$$

be the homomorphism given by

$$XA[p] \mapsto XH[h].$$

Then

$$XH[q] = \theta XA[q] \in \theta Y(XA[H]/XA) \subseteq Y(H/XH)$$

as required.

Thirdly, we wish to prove that

$$\prod_{\lambda\in\Lambda}(X*Y)A_\lambda \subseteq (X*Y)\prod_{\lambda\in\Lambda} A_\lambda$$

. For concision, I shall write $\prod A$ for $\prod_{\lambda\in\Lambda} A_\lambda$. Let $\theta : \prod A/\prod XA \to \prod A/X\prod A$ be the homomorphism given by $\prod XA[p] \mapsto X\prod A[p]$. Now

$$(\prod((X*Y)A)[x] = \{q \in \prod A : \prod XA[q] \in (\prod Y(A/XA))[\prod XA[x]]\}$$

which by condition P2 is a subset of

$$\{q \in \prod A : \prod XA[q] \in (Y(\prod A/XA))[\prod XA[x]]\}$$

which is a subset of

$$\begin{aligned}
&\{q \in \prod A : \prod XA[q] \in (Y(\prod A/\prod XA))[\prod XA[x]]\} \\
&\subseteq \{q \in \prod A :\ \theta(\prod XA[q]) \in \theta((Y(\prod A/\prod XA))[\prod XA[x]])\} \\
&= \{q \in \prod A : X\prod A[q] \in (Y(\prod A/X\prod A))[X\prod A[x]]\} \\
&= ((X*Y)(\prod A))[x]
\end{aligned}$$

as required. □

The astute reader may consider how these proofs may be modified for functions obeying H1, S1, P1, observing that these are the generalised form of commutoids.

We may put a partial order on $\mathcal{A}$-centroids by saying that $X \subseteq Y$ if and only if $XA \subseteq YA$ for all $A \in \mathcal{A}$. In the same way, we shall say that that $X = Y$ if and only if $XA = YA$ for all $A \in \mathcal{A}$.

DEFINITION 6.36 *Let X, Y be centroids. Then $X \wedge Y$ is defined by*

$$(X \wedge Y)(A) = XA \cap YA.$$

THEOREM 6.37 *Let X, Y be centroids. Then $X \wedge Y$ is a centroid.* □

Now obviously from the definition of $\wedge$ every subset of $\mathrm{Cent}(\mathcal{A})$ has an infimum, and so we can define an operation $\vee$ by the rule $X \vee Y = \bigwedge\{Z \in \mathrm{Cent}(\mathcal{A}) : X, Y \subseteq Z\}$ — and similarly define the suprema of infinite sets of centroids, if so we please. However, we sha'n't make much use of this operation. It should be noted that unlike the operations $\wedge$ and $*$, this operation is not "inherited" from the algebra of characteristic functions.

DEFINITION 6.38 *The set of $\mathcal{A}$-centroids, together with the operations $*$, $\wedge$ and $\vee$ will be called* $\mathrm{Cent}(\mathcal{A})$ — *the* **centroid algebra of the variety $\mathcal{A}$**.

THEOREM 6.39 *Let $X \subseteq X', Y \subseteq Y'$. Then $X * Y \subseteq X' * Y'$.*

PROOF: As $X \subseteq X'$, by considering the obvious homomorphism defined $A/XA \to A/X'A$ we can see that as Y is a centroid we have $X * Y \subseteq X' * Y$, and then clearly as $Y \subseteq Y'$ we have $X * Y \subseteq X' * Y'$ as required. □

Now this allows us to say *something* about $X \vee Y$.

COROLLARY 6.40 $X \vee Y \subseteq (X * Y) \wedge (Y * X)$. □

THEOREM 6.41 *Let $X, Y, Z \in \mathrm{Cent}(\mathcal{A})$ be centroids. Then*

$$(X \wedge Y) * Z \subseteq ((X * Z) \wedge (Y * Z))$$

PROOF: Let θ be the homomorphism $A/(X \wedge Y)A \to A/XA$ given by sending $((X \wedge Y)A)[p]$ to $XA[p]$. Now if

$$((X \wedge Y)A)[q] \in Z(A/((X \wedge Y)A))[((X \wedge Y)A)[a]]$$

then

$$\theta(((X \wedge Y)A)[q]) \in \theta(Z(A/((X \wedge Y)A))[((X \wedge Y)A)[a]])$$

and so $XA[q] \in (Z(A/XA))[XA[a]]$; so $q \in ((X * Z)A)[a]$. By similar reasoning $q \in ((Y * Z)A)[a]$. Hence

$$((X \wedge Y) * Z)A \subseteq ((X * Z) \wedge (Y * Z))A$$

as required. □

THEOREM 6.42 *$(X * (Y \wedge Z) = (X * Y) \wedge (X * Z)$.* □

DEFINITION 6.43 *For every centroid $X \in \mathrm{Cent}(\mathcal{A})$ there is a* **variety associated with** X *— denoted by $\mathcal{V}_X$ — given by*

$$\mathcal{V}_X = \{A \in \mathcal{A} : XA = O_{\mathcal{A}}A\}.$$

It is trivial to check that this is in fact a variety.

The definition of, and results on, X-nilpotence then follow easily. In particular, if we have a variety in which for every algebra we have a one-to-one correspondence between normal subalgebras and congruences, then we may say that any X-nilpotent algebra in the variety is strongly $\mathcal{V}_X$-solvable.

6.6 Examples

It is particularly easy to calculate the centroid algebras of "small" group subvarieties.

Example 6.44

Consider the variety $\mathcal{V}(C_p)$ generated by the cyclic group C_p. Suppose that $X \in \text{Cent}(\mathcal{V}(C_p))$ and that $X \neq E$. Then XG is non-trivial for some $G \in \mathcal{V}(C_p)$. So XG contains a subgroup isomorphic to C_p, so $XC_p = C_p$. Hence $X = O$. So $\text{Cent}(\mathcal{V}(C_p))$ has a multiplication table which looks like this:

	E	O
E	E	O
O	O	O

Example 6.45

Consider the variety $\mathcal{V}(C_p \times C_q)$ generated by the group $C_p \times C_q$. By similar reasoning to that in the last example, $\text{Cent}(\mathcal{V}(C_p \times C_q))$ has just four centroids:

- $E : E(G) = 1_G$
- $P : P(G) = \{g \in G : o(g) = p\}$
- $Q : Q(G) = \{g \in G : o(g) = q\}$
- $O : O(G) = G$

with a multiplication table which looks like this:

	E	P	Q	O
E	E	P	Q	O
P	P	P	O	O
Q	Q	O	Q	O
O	O	O	O	O

Example 6.46

Consider the variety $\mathcal{V}(C_p \rtimes^\theta C_q)$ — where θ has trivial kernel. We may establish what the centroids are as follows.

First, consider that if for some centroid X and some group G in the variety we have XG containing some non-central element of order q, then we must have $X(C_p \rtimes^\theta C_q) = C_p \rtimes^\theta C_q$ and so $X = O$.

Now suppose that for some G we have XG containing a central element of order q. Then clearly $X(C_q) = C_q$. Now in any group in the variety, the central elements of order q "split" — i.e. if $g \in Z(G)$ has order q, then we may write $G \cong \langle g \rangle \times H$. So as the centroid of the product is the product of the centroids, XG must contain the central elements of order q for any G in the variety.

Similar remarks apply to the central elements of order p.

Finally, suppose that for some G, XG contains a non-central element of order p. Then $X(C_p \rtimes^\theta C_q)$ contains a non-central element of order p. Hence as $C_p \rtimes^\theta C_q$ generates the variety, and every element of order p in any group in the variety is thus "descended" from the elements of order p in $C_p \rtimes^\theta C_q$, it follows that X must then contain every element of order p in any group of the variety.

It follows that the variety has seven distinct centroids.

- $E : E(G) = 1_G$
- $P : P(G) = \{g \in Z(G) : o(g)|p\}$
- $Q : Q(G) = \{g \in Z(G) : o(g)|q\}$
- Z : the centre of the group
- $S : S(G) = \{g \in G : o(g)|p\}$
- $T : T(G) = Z(G)S(G)$
- $O : O(G) = G$

with a multiplication table like this:

	E	P	Q	Z	S	T	O
E	E	P	Q	Z	S	T	O
P	P	P	Z	Z	S	T	O
Q	Q	Z	Q	Z	T	T	O
Z	Z	Z	Z	Z	T	T	O
S	S	S	O	O	S	O	O
T	T	T	O	O	T	O	O
O	O	O	O	O	O	O	O

Example 6.47

The centroid algebra of the variety which is generated by C_{p^n} has members $A_0 \dots A_n$ given by $A_i(G) = \{g \in G : o(g) \text{ divides } p^i\}$ and operations such that $A_i \wedge A_j = A_{min(i,j)}$, $A_i \vee A_j = A_{max(i,j)}$, and $A_i * A_j = A_{min(i+j,n)}$.

From the above examples it is evident that groups with intuitively "similar" structures (and which therefore generate "similar" varieties) will have isomorphic centroid algebras. Observe also the relationships between the various examples of centroid algebras given above.

6.7 Congruences on centroid algebras

Let us consider congruences on centroid algebras, especially Cent($\mathcal{L}$) and similar centroid algebras. First consider the general case.

Let $\mathcal{A}$ be a variety, and let $\sim$ be a congruence on Cent($\mathcal{A}$). Then there are two interesting congruence classes — the **ideal** given by $[O_{\mathcal{A}}]$ and the **kernel** given by $[E_{\mathcal{A}}]$. As $O_{\mathcal{A}}$ and $E_{\mathcal{A}}$ are both idempotents of $\mathrm{Cent}(\mathcal{A})$, both of these are subalgebras.

Now consider that for every subvariety $\mathcal{B}$ of $\mathcal{A}$ there is a congruence $\sim_{\mathcal{B}}$ on $\mathrm{Cent}(\mathcal{A})$ given by $\mathcal{B}[X] = \{Z \in \mathrm{Cent}(\mathcal{A}) : ZA = XA \ \forall A \in \mathcal{B}\}$ — that is, two centroids are $\mathcal{B}$-equivalent if and only if they are the same when their domain is restricted to $\mathcal{B}$. It is trivial to verify that this is indeed a congruence. Clearly $\mathrm{Cent}(\mathcal{A})/\sim_{\mathcal{B}}$ is (isomorphic to) a subalgebra of $\mathrm{Cent}(\mathcal{B})$.

With such a congruence, the subalgebra $\mathcal{B}[O_{\mathcal{A}}]$ has a complete lattice structure and so in particular has a least element $\bigwedge \mathcal{B}[O_{\mathcal{A}}]$.

Now let's return to $\mathrm{Cent}(\mathcal{L})$.

THEOREM 6.48 *Let $\mathcal{B}$ be a subvariety of $\mathcal{L}$, and let $\sim_{\mathcal{B}}$ be defined as above. Then*

1. $\mathcal{B}[O_{\mathcal{L}}] = \{X \in \mathrm{Cent}(\mathcal{L}) : \mathcal{V}_X \cap \mathcal{B} = \mathcal{B}\}$

2. $\mathcal{B}[E_{\mathcal{L}}] = \{X \in \mathrm{Cent}(\mathcal{L}) : \mathcal{V}_X \cap \mathcal{B} = \mathcal{E}\}$

(Here $\mathcal{E}$ denotes the trivial loop variety).

PROOF: The first of these assertions is trivial to prove. For the second, consider on the one hand that if XL is trivial for all $L \in \mathcal{B}$ then the only member of $\mathcal{B}$ for which $XL = L$ is the trivial algebra. Hence $\mathcal{V}_X \cap \mathcal{B} = \mathcal{E}$.

On the other hand, if XL is not trivial for some $A \in \mathcal{B}$ then as for any L we have $X(X(L)) = XL$ it follows that XL is a non-trivial member of $\mathcal{V}_X$. But as $\mathcal{B}$ is a variety, and $XL \leq L \in \mathcal{B}$, we have $XL \in \mathcal{B}$. Hence XL is a non-trivial member of both $\mathcal{V}_X$ and $\mathcal{B}$. Hence $\mathcal{V}_X \cap \mathcal{B} \neq \mathcal{E}$. □

6.8 Cent($\mathcal{L}$) has no zero divisors

In this subsection I shall show that Cent($\mathcal{L}$) has no zero divisors. (The proof will work for a large class of other varieties).

Now $X * Y = O_{\mathcal{L}}$ if and only if $L/XL \in \mathcal{V}_Y$ for all $L \in \mathcal{L}$, which is of course equivalent to the requirement that $L^{\mathcal{V}_Y} \subseteq XL$ for any L. Now if we denote the free loop with generating set of cardinality c by $F_c(\mathcal{L})$, then as every loop is the homomorphic image of some such loop it is then only necessary and sufficient that we have $F_c(\mathcal{L})^{\mathcal{V}_Y} \subseteq XF_c(\mathcal{L})$ for all cardinal numbers c — as may be seen by reference to our results on commutators and our definition of centroids. Now we may rule out such a possibility, as will be shown. The following line of reasoning was motivated by the observation that the centre of a free group is either the whole of the free group (if it has one generator) or trivial (if it has more than one generator).

For consistency of notation, the free loop of cardinality 0 will be taken to be the trivial loop.

LEMMA 6.49 *Let $X \in$ Cent($\mathcal{L}$), let c be any infinite cardinal number. Then*

$XF_c(\mathcal{L})$ is either trivial or the whole of $F_c(\mathcal{L})$

PROOF: For $XF_c(\mathcal{L})$, being a subloop of a free loop, is itself free, so we have $XF_c(\mathcal{L}) \cong F_d(\mathcal{L})$, for some cardinal d. As c is infinite, we must have $d \leq c$. Now if $0 < d < c$ then it is easy to see that $XF_c(\mathcal{L})$ cannot be characteristic in $F_c(\mathcal{L})$, and so can't be a centroid — a contradiction. Hence we have $d = 0$ or $d = c$. Now if $d = 0$ then we are done.

So suppose that $d = c$. By condition S2 for centroids we have $XXL = XL$ for any loop L. So $XXF_c(\mathcal{L}) = XF_c(\mathcal{L})$. But by the hypothesis that $d = c$ we have $XF_c(\mathcal{L}) \cong F_c(\mathcal{L})$. So by condition H2 on centroids we have $XF_c(\mathcal{L}) = F_c(\mathcal{L})$ as required. □

COROLLARY 6.50 *Hence if $X \neq O_{\mathcal{L}}$ then there is some cardinal $r(X)$ such that $XF_{r(X)}(\mathcal{L})$ is trivial, and furthermore — by condition S2 on centroids and the last lemma — for all $n \geq r(X)$ we also must have $XF_n(\mathcal{L})$ trivial.* □

Now this allows us to produce the following theorem.

THEOREM 6.51 Cent$(\mathcal{L})$ *has no zero divisors.*

PROOF: Let $X, Y \neq O_{\mathcal{L}}$, and let the cardinals $r(X)$ and $r(Y)$ be as defined in the previous corollary. Choose $r = \max(r(X), r(Y))$. Then we have $XF_r(\mathcal{L})$ and $YF_r(\mathcal{L})$ both trivial, and so $(X * Y)F_r(\mathcal{L})$ is trivial. Hence $(X * Y) \neq O_{\mathcal{L}}$ as required. □

COROLLARY 6.52 *$O_{\mathcal{L}}$ and $E_{\mathcal{L}}$ are the only loop centroids which are also generalised commutators, or which contain generalised commutators.* □

COROLLARY 6.53 *There is no $O_{\mathcal{L}} \neq X \in \mathrm{Cent}(\mathcal{L})$ such that every $L \in \mathcal{L}$ is X-nilpotent.*

PROOF: For if every loop was X-nilpotent then every non-trivial loop would have non-trivial X. But from the reasoning above we see that this is the case only for $O_{\mathcal{L}}$. □

The fact that $\mathrm{Cent}(\mathcal{L})$ has no zero divisors is not as useful as we should like. In a ring structure, we could immediately conclude that the ring was left and right cancellative: in $\mathrm{Cent}(\mathcal{L})$ we lack both subtraction and right distribution, so the proof wouldn't work.

Despite initial difficulties in tackling the subject of centroid algebras and related characteristic algebras, their wide applicability, their basis in group theoretic practice, and the uses Bruck managed to find for similar generalizations, suggests that there may be considerable insight gained from further study in this direction.

References

[1] A. A. Albert: Quasigroups I, *Trans. Amer. Math. Soc.* **54** (1943), 507-519

[2] A. A. Albert: Quasigroups II, *Trans. Amer. Math. Soc.* **55** (1944), 401-419

[3] R. Baer: The homomorphism theorems for loops, *Amer. J. Math.* **67** (1945), 450-460

[4] G. Birkhoff: On the structure of abstract algebras, *Proc. Cambridge Phil. Soc.* **31** (1935), 433-454

[5] R. H. Bruck: Some results in the theory of quasigroups, *Trans. Amer. Math. Soc.* **55** (1944), 19-42

[6] R. H. Bruck: Contributions to the theory of loops, *Trans. Amer. Math. Soc.* **60** (1946), 245-354

[7] R. H. Bruck: *A Survey of Binary Systems*, Springer-Verlag (1959)

[8] O. Chein, H. O. Pflugfelder, J. D. H. Smith: *Quasigroups and loops: theory and applications* Heldermann Verlag (1990)

[9] P. M. Cohn: *Universal Algebra*, Harper & Row (1965)

[10] P. Csörgö, M. Niemenmaa: Solvability conditions for loops and groups, *J. Algebra* 232 (2000) 336-342

[11] K. Doerk, T. Hawkes: *Finite Soluble Groups*, de Gruyter (1992)

[12] A. Drápal: Orbits of inner mapping groups *Monatschefte für Mathematik* **134** (2002)

[13] A. Drápal, T. Kepka: Alternating groups and latin squares, *Europ. J. Combinatorics* **10** (1989) 175-180

[14] H. Fitting: Beiträge zur Theorie der Gruppen endlicher Ordnung, *Jber. Deutchen Math. Verein.* **48** (1938), 77-141

[15] T. Ihringer: On multiplication groups of quasigroups, *Europ. J. Combinatorics* **5** (1984), 137-141

[16] T. Kepka, M. Niemenmaa: On connected transversals to abelian subgroups in finite groups, *Bull. London Math. Soc.* **24** (1992), 343-346.

[17] M. Hall: *The Theory of Groups*, Macmillan (1959)

[18] P. Hall: A contribution to the theory of groups of prime-power order, *Proc. Lond. Math. Soc* **36** (1934), 29-95

[19] R. McKenzie, G. McNulty, W. Taylor: *Algebras, Lattices, Varieties*, Wadsworth & Brooks / Cole (1987)

[20] R. Moufang: Zur Struktur von Alternativkörpern, *Math. Ann.* **110** (1935), 509-522

[21] H. Neumann: *Varieties of Groups*, Springer-Verlag (1967)

[22] M. Niemenmaa: On the structure of the inner mapping groups of loops, *Comm. Alg.* **24(1)** (1996), 135-142

[23] M. Niemenmaa, T. Kepka: On loops with cyclic inner mapping groups, *Arch. Math.* **60** (1993), 233 - 236

[24] M. Niemenmaa, T. Kepka: On multiplication groups of loops, *J. Algebra* **135** (1990), 112-122

[25] M. Niemenmaa, A. Vesanen: From geometries to loops and groups, *Groups — Korea '94*, de Gruyter (1995) 257-261

[26] H. O. Pflugfelder: *Quasigroups and loops: introduction*, Heldermann Verlag (1990)

[27] A. Vesanen: Solvable loops and groups, *J. Algebra* **180** (1996) 862-876

[28] A. Vesanen: The group PSL(2,q) is not the multiplication group of a loop, *Comm. Algebra* **22** (1994) 1177-1195