

MOUFANG LOOPS OF CLASS 2 AND CUBIC FORMS

TIM HSU

ABSTRACT. We classify finite Moufang loops which are centrally nilpotent of class 2 in terms of certain cubic forms, concentrating on *small Frattini Moufang loops*, or SFML's, which are Moufang loops L with a central subgroup Z of order p such that L/Z is an elementary abelian p -group. (For example, SFM 2-loops are precisely the class of *code loops*, in the sense of Griess.)

More specifically, we first show that the nuclearly-derived subloop (normal associator subloop) of a Moufang loop of class 2 has exponent dividing 6. It follows that the subloop of elements of p -power order is associative for $p > 3$. Next, we show that if L is an SFML, then L/Z has the structure of a vector space with a symplectic cubic form. We then show that every symplectic cubic form is realized by some SFML, and that two SFML's are isomorphic in a manner preserving the central subgroup Z if and only if their symplectic cubic spaces are isomorphic up to scalar multiple. Consequently, we also obtain an explicit characterization of isotopy in SFM 3-loops. Finally, we extend many of our results to all finite Moufang loops of class 2.

1. INTRODUCTION

The loops characterized by the near-associativity property $(xy)(zx) = x((yz)x)$ are known as *Moufang loops* (see Pflugfelder [24, Ch. IV]). Many aspects of group theory may be generalized to Moufang loops, and among these aspects is the theory of *central nilpotence* (Bruck [6, Ch. VI]), the loop generalization of nilpotence in groups. In fact, centrally nilpotent Moufang loops provide many of the basic examples of finite Moufang loops; see, for instance, Bruck [6, Ch. VIII, Thm. 10.1], Chein [7, II.4], Pflugfelder [24, Ch. IV], and Smith [29, p. 181]. See also Glauberman and Wright [14, 15], who extended many of the standard theorems about finite nilpotent groups to finite centrally nilpotent Moufang loops.

One class of centrally nilpotent Moufang loops which has particularly interesting applications to finite group theory is the class of *code loops*. The first code loop to be recognized as such was the *Parker loop* (named after its discoverer R. A. Parker), which played a key role in Conway's construction of the Monster finite simple group [10]. Subsequently, Griess [16] defined code loops to be certain central extensions of doubly even codes, providing the first published proof of their existence, and then went on [17] to use code loops to construct 2-local subgroups of several other sporadic groups. For more on code loops and finite groups, including further references, see Griess [17, 18, 19] and Richardson [26].

This paper was motivated by the problem of gaining a better understanding of code loops and other similar Moufang loops, in order to compute inside the

Date: May 4, 1998; revised September 22, 1998.

1991 Mathematics Subject Classification. Primary 20N05; Secondary 20D15, 20D08.

Key words and phrases. Centrally nilpotent Moufang loops of class 2, Moufang p -loops, small Frattini Moufang loops, code loops, cubic forms.

Monster more efficiently, and to understand Conway’s construction of the Monster in a more general setting. The main point of this paper is that such loops may be understood quite effectively in terms of the relatively familiar language of symplectic cubic forms. (For general information about cubic forms, see Aschbacher [2].) We eventually hope to use this analysis and similar ideas to investigate the Monster and related groups. In particular, in [20], we give some short explicit constructions of code loops, including a Turyn-type construction for the Parker loop; and in the future, we hope to use the framework established here to generalize Conway’s construction of the Monster to other groups.

Main results. For the convenience of the reader, we now summarize our main results. (The reader who is unfamiliar with the notation and terminology used here may first wish to read Section 2.)

Let L be a Moufang loop which is centrally nilpotent of class 2, that is, a Moufang loop L such that the quotient of L by its center $Z(L)$ is an abelian group; and let L_p be the set of all elements of L whose order is a power of p . Recall that the nuclearly-derived subloop, or normal associator subloop, of L , which we denote by L^* , is the smallest normal subloop of L such that L/L^* is associative (is a group). Recall also that the torsion subloop (subloop of finite order elements) of L is isomorphic to the (restricted) direct product of the subloops L_p , where p runs over all primes (Thm. 6.2 of Bruck [5], our Theorem 3.7, or in the finite case, Cor. 1 of Glauberman and Wright [15]).

In Section 3, we show that the commutator and associator functions are symplectic and skew-symmetric functions on $L/Z(L) \times L/Z(L)$ and $L/Z(L) \times L/Z(L) \times L/Z(L)$, respectively; that the two functions are related by polarization; and that the associator function is multilinear (Theorem 3.3). As a consequence, we observe:

Theorem A. *Let L be a Moufang loop which is centrally nilpotent of class 2. Then L^* (as defined above) has exponent dividing 6. In particular, for $p > 3$, L_p (as defined above) is associative (is a group).*

Compare the result of Bruck [6, VIII.2] that the cube of every associator of a commutative Moufang loop is trivial. (In fact, to prove Theorem A, we use another case of the same formulas Bruck used to obtain that result.) We also note that Theorem A is, in some sense, the best possible result of this type, since Example 3 of VII.5 of Bruck [6] gives a construction of nonassociative finite Moufang p -loops of class 3 for all $p > 2$.

In Sections 4–6, we focus on *small Frattini Moufang loops* (also known as SFM loops, or SFML’s), which are Moufang p -loops L with a central subgroup Z of order p such that $C \cong L/Z$ is an elementary abelian group. (Note that we often think of Z and C as part of the structure of L .) SFML’s are a class of Moufang loops often found “in nature.” For instance, every extraspecial Moufang loop (Definition 4.1) is an SFML, as is every code loop. (In fact, it follows from results of Chein and Goodaire [8] that the SFM 2-loops are precisely the class of code loops.)

The key to our central result on SFML’s (Theorem B) is the fact that L gives C the structure of a *symplectic cubic space*, that is, a vector space over \mathbf{F}_p with an attached *symplectic cubic form*. In these terms, the relationship between SFML’s and cubic forms can be stated as:

Theorem B. *Every symplectic cubic space can be realized by some SFML in the manner described above. Furthermore, let L and M be SFML’s, with distinguished central subgroups Z_L and Z_M , and associated symplectic cubic spaces C_L and C_M .*

Then there is an isomorphism $\varphi : L \rightarrow M$ such that $\varphi(Z_L) = Z_M$ if and only if C_L and C_M are isomorphic up to scalar multiple (action of $\text{Aut}(Z_L) = \text{Aut}(Z_M)$).

The proof of Theorem B has two main parts. First, in Section 4, we define the *Frattini extension* of a symplectic cubic space (Definition 4.9), and show that SFML's are precisely the Frattini extensions of symplectic cubic spaces (Theorem 4.10). Then, in Section 5, we show that every symplectic cubic space has a unique Frattini extension (Theorems 5.1 and 5.6), which implies Theorem B.

Note that once we have Theorem 4.10, the most significant part of Theorem B is Theorem 5.6, a result which can also be obtained from work done independently by Johnson [21] (see Remark 5.8). However, we believe that our proof of Theorem 5.6 is still of independent interest, both because of its relative simplicity, and because of its explicit emphasis on what we call the *centrally twisted product*. See Remark 5.7 for details.

Now, as mentioned above, every SFM 3-loop L is a Frattini extension of a symplectic cubic space $(C, \sigma(c), \chi(c, d), \alpha(c, d, e))$ over \mathbf{F}_3 . For any $k \in C$, define the *adjoint translate* $\text{ad}_k(C)$ of C to be the symplectic cubic space $(C, \sigma(c), \chi(c, d) + \alpha(c, k, d), \alpha(c, d, e))$. A straightforward application of Theorem B then gives the following characterization of isotopy in SFM 3-loops (Section 6).

Theorem C. *Let L be the Frattini extension of a symplectic cubic space $(C, \sigma, \chi, \alpha)$ over \mathbf{F}_3 . Then every loop-isotope of L is isomorphic to the Frattini extension of an adjoint translate of C . In particular, σ and α are isotopy invariants of L ; that is, if M is a loop-isotope of L , then there is some isotopy from L to M which preserves both σ and α .*

We conclude (Section 7) by describing how most of our results, including much of Theorem B, may be extended to finite Moufang loops of class 2 in general. In particular, we give a construction of any finite Moufang loop of class 2, and we indicate how to generalize Theorem C to the case of Moufang loops of class 2 and exponent 3.

Previous related work. The associator and commutator calculus of loops, especially Moufang loops, has a history dating back at least to Bruck [6]. For a cohomological interpretation, see Eilenberg and MacLane [12], and for a detailed investigation of the commutative case, see Smith [28].

Several special cases of this paper are already well-known. Specifically, Commutative Moufang loops have been studied in terms of associator calculus and trilinear forms by, for instance, Bénéteau [3, IV.3], Bruck [4], Chein [7, II.4], and Ray-Chaudhuri and Roth [25]; and code loops have been classified in terms of associators and commutators by Chein and Goodaire [8, Thm. 2].

It should also be noted that *all* loops of class 2 have been classified in terms of their commutator, associator, and “power map” functions by Johnson [21]. The main difference between that work and this paper is that by specializing to the case of Moufang loops, we are able to get more “invariant” results (Theorems B and C) in a more familiar setting (cubic forms). See Remark 5.8 for a more detailed statement of Johnson's results.

2. BACKGROUND AND NOTATION

First, we set some conventions and notation to be used throughout.

Notation. Let p be a prime. \mathbf{F}_p denotes the field of order p , and \mathbf{F}_p^\times its nonzero elements. Following group-theoretic custom, unless otherwise specified, we think of \mathbf{F}_p as the group of order p , and \mathbf{F}_p^\times as the automorphism group of \mathbf{F}_p . In this context, we identify the vector space \mathbf{F}_p^k with the elementary abelian p -group of rank k , and we write vector addition in \mathbf{F}_p^k multiplicatively, with the zero vector written as 1.

If a, b, c, \dots are elements or subsets of a loop (resp. vector space), $\langle a, b, c, \dots \rangle$ denotes the subloop (resp. subspace) generated by a, b, c, \dots .

For those less familiar with loop theory, and for the purpose of establishing notation and terminology, we also review some definitions and results of loop theory, using Pflugfelder [24], Bruck [6], and Chein, Pflugfelder, and Smith [9] as our standard sources.

Definition 2.1. A *loop* is a set L with a binary operation (written as juxtaposition) and an element $1 \in L$ such that for all $a \in L$, the maps $x \mapsto xa$ and $x \mapsto ax$ are bijections from L to itself, and $1a = a1 = a$. An *inverse property loop*, or IP loop, is a loop with unique two-sided inverses. (Note that the term “inverse” means that $a^{-1}(ax) = (xa)a^{-1} = x$.)

Many concepts of group theory may be generalized to loop theory; we highlight the following ones.

Definition 2.2. For elements γ, δ , and ϵ of a loop L , we define the *commutator* $[\gamma, \delta]$ and the *associator* $[\gamma, \delta, \epsilon]$ to be the (unique) elements of L such that

$$(2.1) \quad \gamma\delta = (\delta\gamma)[\gamma, \delta],$$

$$(2.2) \quad (\gamma\delta)\epsilon = (\gamma(\delta\epsilon))[\gamma, \delta, \epsilon].$$

If L is an IP loop, we also have

$$(2.3) \quad [\gamma, \delta] = (\delta\gamma)^{-1}(\gamma\delta),$$

$$(2.4) \quad [\gamma, \delta, \epsilon] = (\gamma(\delta\epsilon))^{-1}((\gamma\delta)\epsilon),$$

$$(2.5) \quad \gamma(\delta\epsilon) = ((\gamma\delta)\epsilon)[\gamma, \delta, \epsilon]^{-1}.$$

(The inexperienced reader should note the inverse in the last formula.)

Definition 2.3. Let L be a loop. The *nucleus* of L (denoted by $N(L)$) is the set of all $z \in L$ such that $[z, x, y] = [x, z, y] = [x, y, z] = 1$ for all $x, y \in L$; and the *center* of L (denoted by $Z(L)$) is defined to be the set of all $z \in N(L)$ such that $[z, x] = 1$ for all $x, y \in L$.

If L is a loop, it can be shown (see Pflugfelder [24, I.3]) that $N(L)$ is a subgroup of L , and that $Z(L)$ is an abelian subgroup of $N(L)$.

Definition 2.4. A *normal* subloop of a loop L is any subloop of L which is the kernel of some homomorphism from L to a loop.

For instance, any *central subgroup* (subgroup of $Z(L)$) of a loop L is normal in L (Pflugfelder [24, I.7]).

Definition 2.5. Let L be a loop. We define the *centrally-derived subloop* (or normal commutator-associator subloop) of L to be the smallest normal subloop $L' \triangleleft L$ such that L/L' is an abelian group. Similarly, we define the *nuclearly-derived subloop* (or normal associator subloop) of L to be the smallest normal subloop $L^* \triangleleft L$ such that L/L^* is associative (is a group).

See Bruck [6, Ch. VI] for a proof that L' and L^* are well-defined. Note that it follows from the isomorphism theorems for loops (see Pflugfelder [24, I.7]) that L' (resp. L^*) is the smallest normal subloop of L containing all $[\gamma, \delta]$ and $[\gamma, \delta, \epsilon]$ (resp. all $[\gamma, \delta, \epsilon]$), where γ, δ, ϵ run over all elements of L .

We will use Bruck's theory of central nilpotence [6, Ch. VI], as described in Definitions 2.6–2.7 and Theorem 2.8.

Definition 2.6. Let L be a loop. The *upper central series* $\{Z_i\}$ of L is defined by letting $Z_0 = 1$ and letting Z_{i+1} be the unique subloop of L containing Z_i such that $Z_{i+1}/Z_i = Z(L/Z_i)$. We say that L is *centrally nilpotent of class n* , or simply of class n , if there exists n such that $Z_n = L$ and $Z_{n-1} \neq L$.

For instance, L is of class 2 if and only if $L/Z(L)$ is an abelian group and L is not, that is, if and only if $1 < L' \leq Z(L)$.

Definition 2.7. The *Frattini subloop* $\Phi(L)$ of a loop L is defined to be the set of *non-generators* of L , that is, the set of all $x \in L$ such that for any subset S of L , $L = \langle x, S \rangle$ implies $L = \langle S \rangle$.

Theorem 2.8. *Let L be a finite centrally nilpotent loop. Then $\Phi(L) \triangleleft L$, and $L/\Phi(L)$ is the direct product of groups of prime order.*

Proof. This follows immediately from Thms. 2.1 and 2.2 of Ch. VI of Bruck [6]. \square

We are particularly interested in loops of the following type.

Definition 2.9. A loop L is said to be *Moufang* if any, and therefore all (see Pflugfelder [24, Ch. IV]), of the following identities hold for all $\gamma, \delta, \epsilon \in L$:

$$(2.6) \quad ((\delta\gamma)\epsilon)\gamma = \delta(\gamma(\epsilon\gamma)),$$

$$(2.7) \quad ((\gamma\delta)\gamma)\epsilon = \gamma(\delta(\gamma\epsilon)),$$

$$(2.8) \quad (\gamma(\delta\epsilon))\gamma = (\gamma\delta)(\epsilon\gamma) = \gamma((\delta\epsilon)\gamma).$$

Definition 2.10. The *Moufang center* of a Moufang loop L , denoted by $C(L)$, is defined to be the set of all $z \in L$ such that $[z, x] = 1$ for all $x \in L$.

Let L be a Moufang loop. Clearly, $Z(L) = N(L) \cap C(L)$. Furthermore, it can also be shown (see Pflugfelder [24, Thm. IV.3.10]) that $C(L)$ is a subloop of L .

Moufang loops are IP loops (see Pflugfelder [24, Thm. IV.1.4]) and have many near-associativity properties, such as the following consequence of *Moufang's theorem* (see Pflugfelder [24, Ch. IV]).

Theorem 2.11. *Let L be a Moufang loop. Then L is di-associative; that is, for $x, y \in L$, $\langle x, y \rangle$ is associative. In particular, L is power-associative; that is, x^n is well-defined.* \square

We will also use the Lagrangian property of di-associative loops (Bruck [6, Thm. V.1.2]), stated as:

Theorem 2.12. *Let L be a finite di-associative (e.g., Moufang) loop. Then the order of any element of L divides the order of L .* \square

Definition 2.13. Let L be a power-associative loop, and let p be a prime. We say that L is a *p -loop* if every element of L has order a power of p .

Let L be a di-associative loop. Because of Theorem 2.12, if L has order a power of p , then L is a finite p -loop. Conversely, if L is a finite centrally nilpotent p -loop, the isomorphism theorems for loops imply that the order of L is a power of p . Therefore, since most of the loops we consider are finite centrally nilpotent Moufang loops, we will usually treat the concepts of having order a power of p and being a finite p -loop as interchangeable. (In fact, all finite Moufang p -loops are centrally nilpotent; see Glauberman [14, Thm. 4] and Glauberman and Wright [15].)

Finally, we define one last important concept of loop theory.

Definition 2.14. A triple (U, V, W) of bijections from a loop L to a loop M (whose operation is denoted by \circ) is called an *isotopism* if, for all $x, y \in L$, $(xU) \circ (yV) = (xy)W$. If an isotopism exists from L to M , we say that M is an *isotope* of L , or that L and M are *isotopic*.

It is worth noting that isotopy plays no role in group theory because every loop-isotope of a group G is isomorphic to G (see Pflugfelder [24, Cor. III.2.3]). More generally, any loop which is isomorphic to all of its loop-isotopes is called a G -loop. See Pflugfelder [24, Ch. III] for more on isotopy.

3. MOUFANG LOOPS OF CLASS 2

We first quote the following result, due to Bruck.

Proposition 3.1. *Let L be a Moufang loop such that $[[\gamma, \delta, \epsilon], \gamma] = 1$ for all $\gamma, \delta, \epsilon \in L$. Then for all $\gamma, \delta, \epsilon \in L$, $[\gamma, \delta, \epsilon]$ is central in $\langle \gamma, \delta, \epsilon \rangle$, and the following identities hold for all $n \in \mathbf{Z}$:*

$$(3.1) \quad [\gamma, \delta, \epsilon] = [\delta, \epsilon, \gamma] = [\delta, \gamma, \epsilon]^{-1}$$

$$(3.2) \quad [\gamma^n, \delta, \epsilon] = [\gamma, \delta, \epsilon]^n$$

$$(3.3) \quad [\gamma\delta, \epsilon] = [\gamma, \epsilon][[\gamma, \epsilon], \delta][\delta, \epsilon][\gamma, \delta, \epsilon]^3$$

Note that part of the statement of (3.3) is that the right hand side gives the same result, no matter how the terms are associated.

Proof. This follows from Lemma VII.5.5 of Bruck [6]. □

For the rest of this section, let L be a Moufang loop with a fixed central subgroup Z such that $C \cong L/Z$ is an abelian group. Clearly, such a loop is centrally nilpotent of class 2, and conversely, for any Moufang loop L of class 2, we may take $Z = Z(L)$. By convention, the letters γ, δ, ϵ , and φ refer to elements of L , and their images in the quotient C are denoted by c, d, e , and f , respectively.

Definition 3.2. We define functions $\chi : C \times C \rightarrow Z$ and $\alpha : C \times C \times C \rightarrow Z$ by the following formulas.

$$(3.4) \quad \chi(c, d) = [\gamma, \delta],$$

$$(3.5) \quad \alpha(c, d, e) = [\gamma, \delta, \epsilon].$$

Note that χ and α are well-defined because for any $z \in Z$, $[\gamma z, \delta, \epsilon] = [\gamma, \delta, \epsilon]$, and so on.

The following theorem says that the functions χ and α are “symplectic” ((3.6) and (3.10)), “skew-symmetric” ((3.7) and (3.11)), “power-multilinear” ((3.8) and (3.12)), and related by “polarization” (3.9); and furthermore, that α is multilinear (3.13).

Theorem 3.3. *For all $c, d, e, f \in C$ and all $n \in \mathbf{Z}$, we have:*

$$(3.6) \quad \chi(c, c) = 1,$$

$$(3.7) \quad \chi(c, d) = \chi(d, c)^{-1},$$

$$(3.8) \quad \chi(c^n, d) = \chi(c, d)^n,$$

$$(3.9) \quad \chi(cd, e) = \chi(c, e)\chi(d, e)\alpha(c, d, e)^3,$$

and

$$(3.10) \quad \alpha(c, d, d) = \alpha(d, c, d) = \alpha(d, d, c) = 1,$$

$$(3.11) \quad \alpha(c, d, e) = \alpha(d, c, e)^{-1} = \alpha(d, e, c),$$

$$(3.12) \quad \alpha(c^n, d, e) = \alpha(c, d, e)^n,$$

$$(3.13) \quad \alpha(cd, e, f) = \alpha(c, e, f)\alpha(d, e, f).$$

Proof. We first note that (3.6) and (3.7) are easy, (3.9) follows from (3.3) and the fact that L' is central, (3.10) follows from di-associativity, (3.11) follows from (3.1), and (3.12) follows from (3.2). Furthermore, (3.9), (3.10), and (3.12) imply

$$(3.14) \quad \begin{aligned} \chi(c^{n+1}, d) &= \chi(c^n, d)\chi(c, d)\alpha(c^n, c, d)^3 \\ &= \chi(c^n, d)\chi(c, d), \end{aligned}$$

so (3.8) follows by induction on positive and negative n .

It remains to prove (3.13). Now, this formula is essentially proved (though not stated in full generality) in Chein and Goodaire [8, Thm. 2]. However, to be more self-contained, and to show how (3.13) follows from the ‘‘pentagonal’’ relation of the theory of monoidal categories (MacLane [23, Ch. VII]) and skew-symmetry (3.11), we present the following proof.

First, by definition,

$$(3.15) \quad \alpha(cd, e, f) = ((\gamma\delta)(\epsilon\varphi))^{-1}(((\gamma\delta)\epsilon)\varphi),$$

and

$$(3.16) \quad \begin{aligned} ((\gamma\delta)\epsilon)\varphi &= (\gamma(\delta\epsilon))\varphi \cdot \alpha(c, d, e) \\ &= \gamma((\delta\epsilon)\varphi) \cdot \alpha(c, d, e)\alpha(c, de, f) \\ &= \gamma(\delta(\epsilon\varphi)) \cdot \alpha(c, d, e)\alpha(c, de, f)\alpha(d, e, f) \\ &= (\gamma\delta)(\epsilon\varphi) \cdot \alpha(c, d, e)\alpha(c, de, f)\alpha(d, e, f)\alpha(c, d, ef)^{-1}, \end{aligned}$$

which means that

$$(3.17) \quad \alpha(cd, e, f) = \alpha(c, d, e)\alpha(c, de, f)\alpha(d, e, f)\alpha(c, d, ef)^{-1}.$$

We claim that (3.13) is a consequence of (3.17) (which is essentially the pentagonal relation) and skew-symmetry (3.11).

To prove this claim, by substituting first $c = w$, $d = x$, $e = y$, and $f = z$, and then $c = x$, $d = y$, $e = z$, and $f = w$, into (3.17), we get

$$(3.18) \quad \alpha(wx, y, z) = \alpha(w, x, y)\alpha(w, xy, z)\alpha(x, y, z)\alpha(w, x, yz)^{-1},$$

$$(3.19) \quad \alpha(xy, z, w) = \alpha(x, y, z)\alpha(x, yz, w)\alpha(y, z, w)\alpha(x, y, zw)^{-1}.$$

Since skew-symmetry implies $\alpha(w, xy, z) = \alpha(xy, z, w)$, we may substitute the right-hand side of (3.19) for the second term in the right-hand side of (3.18). Applying

skew-symmetry to collect terms, and keeping in mind that $zw = wz$, since w and z are elements not of L but of its commutative quotient C , we obtain

$$(3.20) \quad \alpha(wx, y, z) = \alpha(wz, y, x)\alpha(w, x, y)\alpha(w, y, z)\alpha(x, y, z)^2.$$

We call (3.20) the *exchange identity*, since it implies that we may exchange the x and the z in $\alpha(wx, y, z)$ at the cost of adding the other terms on the right-hand side of (3.20).

Using the exchange identity and skew-symmetry, we see that

$$(3.21) \quad \begin{aligned} \alpha(c, de, f) &= \alpha(de, f, c) \\ &= \alpha(dc, f, e)\alpha(d, e, f)\alpha(d, f, c)\alpha(e, f, c)^2 \\ &= \alpha(cd, e, f)^{-1}\alpha(d, e, f)\alpha(c, d, f)\alpha(c, e, f)^2. \end{aligned}$$

Applying exchange and skew-symmetry again, we have

$$(3.22) \quad \begin{aligned} \alpha(c, d, ef)^{-1} &= \alpha(ef, d, c) \\ &= \alpha(ec, d, f)\alpha(e, f, d)\alpha(e, d, c)\alpha(f, d, c)^2 \\ &= \alpha(ce, f, d)^{-1}\alpha(d, e, f)\alpha(c, d, e)^{-1}\alpha(c, d, f)^{-2}, \end{aligned}$$

and applying exchange and skew-symmetry to the first term of the last expression in (3.22), we have

$$(3.23) \quad \begin{aligned} \alpha(c, d, ef)^{-1} &= \alpha(cd, f, e)^{-1}\alpha(c, e, f)^{-1}\alpha(c, f, d)^{-1}\alpha(e, f, d)^{-2} \\ &\quad \cdot \alpha(d, e, f)\alpha(c, d, e)^{-1}\alpha(c, d, f)^{-2}, \\ &= \alpha(cd, e, f)\alpha(c, d, e)^{-1}\alpha(c, d, f)^{-1}\alpha(c, e, f)^{-1}\alpha(d, e, f)^{-1}. \end{aligned}$$

Finally, substituting (3.21) and (3.23) into (3.17), we get

$$(3.24) \quad \begin{aligned} \alpha(cd, e, f) &= \alpha(c, d, e) \\ &\quad \cdot \alpha(cd, e, f)^{-1}\alpha(d, e, f)\alpha(c, d, f)\alpha(c, e, f)^2 \\ &\quad \cdot \alpha(d, e, f) \\ &\quad \cdot \alpha(cd, e, f)\alpha(c, d, e)^{-1}\alpha(c, d, f)^{-1}\alpha(c, e, f)^{-1}\alpha(d, e, f)^{-1} \\ &= \alpha(c, e, f)\alpha(d, e, f), \end{aligned}$$

and the theorem follows. \square

Remark 3.4. Just as (3.17) is essentially the “pentagonal” relation from the theory of monoidal categories, (3.9) is a version of the “hexagonal” relation from the theory of symmetric monoidal categories (MacLane [23, Ch. VII]). We also note that the pentagonal and hexagonal relations are crucial to Johnson’s work on loops of class 2. See Remark 5.8 for details.

In the rest of this section, we describe some of the consequences of Theorem 3.3.

Theorem 3.5. *For $c, d, e \in C$ such that $c^k = d^m = e^n = 1$, the order of $\chi(c, d)$ divides $\gcd(k, m)$, and the order of $\alpha(c, d, e)$ divides $\gcd(k, m, n)$.*

Proof. From (3.8), we have

$$(3.25) \quad \chi(c, d)^k = \chi(c^k, d) = \chi(1, d) = 1,$$

and our commutator claim follows by skew-symmetry. The same proof works for our associator claim. \square

For a prime p , define L_p to be the set of all $x \in L$ such that the order of x is a power of p . In the next two theorems (Theorems 3.6 and 3.7) we recover the class 2 case of results of Bruck [5, Thm. 6.2] and Glauberman and Wright [15, Cor. 1].

Theorem 3.6. *L_p is a subloop of L .*

Proof. For $\gamma, \delta \in L_p$, let q be the greater of the orders of γ and δ , and let $r = q(q-1)/2$. Then, using di-associativity and the definition of χ , we have

$$(3.26) \quad (\gamma\delta)^q = \gamma^q \delta^q \chi(d, c)^r = \chi(d, c)^r,$$

and the theorem follows from Theorem 3.5. \square

Theorem 3.7. *Let T be the set of all elements of L of finite order. Then T is a subloop of L isomorphic to the restricted direct product of the L_p 's, over all primes p .*

Proof. First, we note that Theorem 3.5 implies that elements of relatively prime order commute and associate freely, so the unassociated product of elements of pairwise relatively prime order is well-defined. Consequently, by the Chinese Remainder Theorem, for every $\gamma \in L$ of order n , we have

$$(3.27) \quad \gamma = \prod_{p|n} \gamma_p,$$

where each γ_p is a power of γ , and the order of γ_p is a power of p .

It is therefore enough to show that if the orders of γ_i and δ_j are relatively prime for $i, j = 1, 2$, then $(\gamma_1 \delta_1)(\gamma_2 \delta_2) = (\gamma_1 \gamma_2)(\delta_1 \delta_2)$. However, using Theorem 3.5 repeatedly, we see that

$$(3.28) \quad \begin{aligned} (\gamma_1 \delta_1)(\gamma_2 \delta_2) &= \gamma_1(\delta_1(\gamma_2 \delta_2)) = \gamma_1((\delta_1 \gamma_2)\delta_2) = \gamma_1((\gamma_2 \delta_1)\delta_2) \\ &= \gamma_1(\gamma_2(\delta_1 \delta_2)) = (\gamma_1 \gamma_2)(\delta_1 \delta_2), \end{aligned}$$

and the theorem follows. \square

We next obtain Theorem A.

Proof of Theorem A. Since L^* is an abelian group generated by the set of all $\alpha(c, d, e)$ ($c, d, e \in C$), it is enough to show that $\alpha(c, d, e)^6 = 1$ for all $c, d, e \in C$. However, since (3.9) implies

$$(3.29) \quad \chi(c, e)\chi(d, e)\alpha(c, d, e)^3 = \chi(cd, e) = \chi(dc, e) = \chi(d, e)\chi(c, e)\alpha(d, c, e)^3,$$

using skew-symmetry, we have $\alpha(c, d, e)^3 = \alpha(d, c, e)^3 = \alpha(c, d, e)^{-3}$, and the theorem follows. \square

We then have the following analogue of Thm. 11.2 of Bruck [6, Ch. VIII].

Theorem 3.8. *If L is finitely generated, then L^* is finite. More precisely, L is a central (loop) extension of L/L^* (a finitely generated group of class ≤ 2) by a finite group of exponent 6.*

Proof. Since (3.13) implies that L^* is an abelian group generated by $\alpha(c, d, e)$, where γ, δ , and ϵ run over all *generators* of L , the theorem follows from Theorem A. \square

Finally, we note that Moufang loops of class 2 satisfy the following stronger version of the Moufang identity.

Theorem 3.9. *If n is the exponent of L^* , then L satisfies*

$$(3.30) \quad \gamma^k(\delta(\gamma\epsilon)) = ((\gamma^k\delta)\gamma)\epsilon$$

for all $\gamma, \delta, \epsilon \in L$, and precisely those integers k such that $k \equiv 1 \pmod{n}$.

The identity (3.30) is called the M_k -law. Note that the M_1 -law is just (2.7).

Proof. From the definition of α , we have

$$(3.31) \quad \begin{aligned} ((\gamma^k\delta)\gamma)\epsilon &= (\gamma^k\delta)(\gamma\epsilon)\alpha(c^k d, c, e) \\ &= \gamma^k(\delta(\gamma\epsilon))\alpha(c^k d, c, e)\alpha(c^k, d, ce). \end{aligned}$$

However, using (3.10)–(3.13), we obtain

$$(3.32) \quad \begin{aligned} \alpha(c^k d, c, e)\alpha(c^k, d, ce) &= \alpha(c^k, c, e)\alpha(d, c, e)\alpha(c^k, d, c)\alpha(c^k, d, e) \\ &= \alpha(c, d, e)^{k-1}, \end{aligned}$$

which means that the M_k -law is satisfied if and only if the order of any $\alpha(c, d, e)$ divides $k - 1$. The theorem follows. \square

We then have the following corollary. (This result on Moufang loops of class 2 can also be obtained more directly from Cor. IV.4.8 of Pflugfelder [24].)

Corollary 3.10. *If $L_3 \cap L^* = 1$, then L is a G -loop.*

Proof. If $L_3 \cap L^* = 1$, then L satisfies an M_k -law for all odd k , and so the corollary follows from Thm. IV.4.11 of Pflugfelder [24]. \square

4. SMALL FRATTINI MOUFANG LOOPS AND SYMPLECTIC CUBIC SPACES

In the rest of this paper, we assume all loops are finite; in fact, we will mostly consider loops of prime power order. To motivate our main definition (Definition 4.3), we begin by imitating the theory of extraspecial groups (see Aschbacher [1]).

Definition 4.1. Let p be a prime. We say that a Moufang p -loop L is *special* if $\Phi(L) = Z(L) = L'$, and we say that a special Moufang loop L is *extraspecial* if $Z(L)$ is cyclic.

For instance, every extraspecial group is an extraspecial Moufang loop.

Note that every nontrivial special Moufang loop is centrally nilpotent of class 2. Theorem 2.8 therefore implies that if L is a special Moufang loop, then $L/\Phi(L)$ is an elementary abelian group. Furthermore, copying the proof of (23.7) in Aschbacher [1] word for word, it also follows that $Z(L)$ is an elementary abelian group. We conclude that L is an extraspecial Moufang loop if and only if $\Phi(L) = Z(L) = L'$ has order p .

Remark 4.2. As the reader may have noticed, Theorem A implies that Definition 4.1 is new only when $p = 2$ or 3 ; otherwise, we are talking about (extra)special groups. However, since it requires little extra effort, we will continue to discuss the case of arbitrary p .

We generalize our situation slightly with the following definition.

Definition 4.3. A p -loop L is said to be *small Frattini* if $\Phi(L)$ has order dividing p . A small Frattini loop L is said to be *central small Frattini* if $\Phi(L) \leq Z(L)$.

For instance, every extraspecial Moufang loop is central small Frattini, as is any elementary abelian group. More generally:

Theorem 4.4. *Every small Frattini Moufang loop is central small Frattini.*

Recall that $C(L)$ denotes the Moufang center of a Moufang loop L (Definition 2.10).

Proof. Let L be a small Frattini Moufang loop. The theorem is clear for groups, so since $L^* \leq L' \leq \Phi(L)$, we may assume that $L^* = \Phi(L)$ has order p . In that case, for some $\gamma, \delta, \epsilon \in L$, $A = [\gamma, \delta, \epsilon] \neq 1$ and $L^* = \langle A \rangle$. Now, for all $y \in L$, $\langle A \rangle$ is a normal subgroup of order p in the group $\langle A, y \rangle$. Therefore, since y is of p -power order, $[A, y] = 1$, or in other words, $L^* = \langle A \rangle \leq C(L)$. (In particular, we now know that L satisfies the hypotheses of Proposition 3.1.)

It is therefore enough to show that $A \in N(L)$, or in other words, that $[A, \delta, \epsilon] = 1$ for all $\delta, \epsilon \in L$. Suppose $a = [A, \delta, \epsilon] \neq 1$ for some $\delta, \epsilon \in L$. Then $\langle a \rangle = L^*$, which means that $\langle a \rangle = \langle A \rangle$. However, Proposition 3.1 implies that a is central in $\langle A, \delta, \epsilon \rangle$, which means that A must also be central in $\langle A, \delta, \epsilon \rangle$, and so $[A, \delta, \epsilon] = 1$; contradiction. The theorem follows. \square

Notation. In the rest of this paper, we abbreviate the term “small Frattini Moufang” as SFM, and we abbreviate “small Frattini Moufang loop” as SFML. Also, for the rest of this section, let p be a prime, let L be an SFML of order p^{1+k} , let Z be a fixed central subgroup of L , and let $C \cong L/Z$ be an elementary abelian p -group of rank k (vector space of dimension k over \mathbf{F}_p). We also retain the convention of the previous section that $\gamma, \delta, \epsilon, \varphi \in L$ reduce to $c, d, e, f \in C$ in the quotient.

Applying Theorem 3.3, we see that χ and α are again well-defined functions which satisfy the formulas (3.6)–(3.13). We also need one more function.

Definition 4.5. We define the function $\sigma : C \rightarrow Z$ by $\sigma(c) = \gamma^p$. Note that σ is well-defined because Z is central and has exponent p and L/Z has exponent p .

The following is the analogue of Theorem 3.3 for σ .

Theorem 4.6. *For all $c, d \in C$, we have:*

$$(4.1) \quad \sigma(c^n) = \sigma(c)^n$$

$$(4.2) \quad \sigma(cd) = \begin{cases} \sigma(c)\sigma(d)\chi(c, d) & \text{for } p = 2, \\ \sigma(c)\sigma(d) & \text{for } p > 2. \end{cases}$$

Proof. (4.1) is clear. As for (4.2), if $r = p(p-1)/2$, then

$$(4.3) \quad (\gamma\delta)^p = \gamma^p\delta^p\chi(d, c)^r = \sigma(c)\sigma(d)\chi(d, c)^r.$$

The theorem follows from the fact that for $p > 2$, p divides r , and for $p = 2$, $r = 1$ and $\chi(c, d) = \chi(d, c)$. \square

We are led to the following definition.

Definition 4.7. Let Z be the group of order p , and let C be a finite-dimensional vector space over \mathbf{F}_p . A *symplectic cubic form* on C is defined to be a 3-tuple (σ, χ, α) , where $\sigma : C \rightarrow Z$, $\chi : C \times C \rightarrow Z$, and $\alpha : C \times C \times C \rightarrow Z$ satisfy (4.1)–(4.2), (3.6)–(3.9), and (3.10)–(3.13), for all $c, d, e, f \in C$ and all $n \in \mathbf{Z}$. A *symplectic cubic space* is defined to be a 4-tuple $(C, \sigma, \chi, \alpha)$. By abuse of notation, we often refer to such a space simply by C .

It is worth noting the different forms that (4.2) and (3.9) take for different p . That is, for $p = 2$, we have

$$(4.4) \quad \sigma(cd) = \sigma(c)\sigma(d)\chi(c, d),$$

$$(4.5) \quad \chi(cd, e) = \chi(c, e)\chi(d, e)\alpha(c, d, e),$$

and for $p > 2$, we have

$$(4.6) \quad \sigma(cd) = \sigma(c)\sigma(d),$$

$$(4.7) \quad \chi(cd, e) = \chi(c, e)\chi(d, e).$$

In other words, for $p = 2$, σ , χ , and α are related by polarization, and for $p > 2$, σ and χ are multilinear. As for α , for $p = 2$ or 3 , α is multilinear, and for $p > 3$, α is identically equal to 1.

We also note that (4.1), (3.8), and (3.12) imply

$$(4.8) \quad \sigma(1) = \chi(c, 1) = \alpha(c, d, 1) = 1$$

for all $c, d \in C$.

Note that choosing a different generator for Z has the effect of acting on σ , χ , and α by an element of $\text{Aut}(Z)$; in additive terms, this means that C is really only defined up to scalar multiple. The natural definition of isomorphism for symplectic cubic spaces is therefore the following one.

Definition 4.8. Let $(C_i, \sigma_i, \chi_i, \alpha_i)$ be a symplectic cubic space for $i = 1, 2$. We say that C_1 and C_2 are *isomorphic up to scalar multiple* if there is a vector space isomorphism $\varphi : C_1 \rightarrow C_2$ and some fixed $a \in \text{Aut}(Z)$ such that

$$(4.9) \quad \begin{aligned} \sigma_2(\varphi(c)) &= \sigma_1(c)^a, \\ \chi_2(\varphi(c), \varphi(d)) &= \chi_1(c, d)^a, \\ \alpha_2(\varphi(c), \varphi(d), \varphi(e)) &= \alpha_1(c, d, e)^a. \end{aligned}$$

If $a = 1$, then we say that C_1 and C_2 are *isomorphic*.

Finally, to describe the relationship between SFML's and symplectic cubic spaces, we introduce one more definition, in which we define γ^n inductively by $\gamma^0 = 1$ and $\gamma^{n+1} = \gamma\gamma^n$.

Definition 4.9. Let p be a prime, and let $(C, \sigma, \chi, \alpha)$ be a symplectic cubic space over \mathbf{F}_p . We say that a loop L is a *Frattini extension* of C if L satisfies the following conditions.

1. L has a central subgroup Z of order p such that $L/Z \cong C$.
2. Let $\gamma, \delta, \epsilon \in L$ denote arbitrary preimages of $c, d, e \in C$, respectively. Then:

$$(4.10) \quad \gamma^p = \sigma(c),$$

$$(4.11) \quad [\gamma, \delta] = \chi(c, d),$$

$$(4.12) \quad [\gamma, \delta, \epsilon] = \alpha(c, d, e),$$

where the values of σ , χ , and α are taken to be in the central subgroup Z .

Theorem 4.10. *Every SFML is a Frattini extension of a symplectic cubic space, and every Frattini extension of a symplectic cubic space is an SFML.*

Proof. If L is a Moufang loop with a central subgroup Z of order p such that $C \cong L/Z$ is an elementary abelian p -group, Theorems 3.3 and 4.6 imply that L is a Frattini extension of the symplectic cubic space $(C, \sigma, \chi, \alpha)$, where σ , χ , and α are from Definitions 3.2 and 4.5. Conversely, let L be a Frattini extension of a symplectic cubic space $(C, \sigma, \chi, \alpha)$. Because α satisfies (3.10)–(3.13), the proof of Theorem 3.9 in the case $k = 1$ shows that L is Moufang. (Note that for $k = 1$, the proof of Theorem 3.9 does not use power-associativity.) Therefore, since L/Z is an elementary abelian p -group, L is an SFML. \square

Remark 4.11. To conclude this section, we ask: Given a vector space C over \mathbf{F}_p , which functions σ , χ , and α give a symplectic cubic form? Now, for $p > 2$, (4.6) and (4.7) show that σ , χ , and α are multilinear and can be chosen independently, which makes this question easy. On the other hand, for $p = 2$, σ , χ , and α are related by polarization, so it is less clear *a priori* which symplectic cubic forms exist over \mathbf{F}_2 .

However, let C be a doubly even binary code, write Z (the group of order 2) as $\{\pm 1\}$ and define

$$(4.13) \quad \sigma(c) = (-1)^{|c|/4}$$

$$(4.14) \quad \chi(c, d) = (-1)^{|c \cap d|/2}$$

$$(4.15) \quad \alpha(c, d, e) = (-1)^{|c \cap d \cap e|},$$

where $|c|$ (resp. $|c \cap d|$, $|c \cap d \cap e|$) is defined (in additive notation) to be the number of non-0 coordinates in the vector c (resp. common to the vectors c and d , common to the vectors c , d , and e). It is not hard to show that (σ, χ, α) is a symplectic cubic form over \mathbf{F}_2 . The solution to the problem at hand then comes from the fact that Chein and Goodaire [8, Cor. 4] have shown (in the course of proving that every SFM 2-loop is a code loop) that for any positive integer m and any $\sigma_i \in \mathbf{F}_2$ ($1 \leq i \leq m$), $\chi_{ij} \in \mathbf{F}_2$ ($1 \leq i < j \leq m$), and $\alpha_{ijk} \in \mathbf{F}_2$ ($1 \leq i < j < k \leq m$), there exists a code C with basis $\{c_1, c_2, \dots, c_m\}$ such that $\sigma(c_i) = \sigma_i$, $\chi(c_i, c_j) = \chi_{ij}$, and $\alpha(c_i, c_j, c_k) = \alpha_{ijk}$. In other words, just as with $p > 2$, we may choose the values of σ , χ , and α freely on tuples of ordered distinct basis elements.

See also Theorem 7.11.

5. EXISTENCE AND UNIQUENESS OF FRATTINI EXTENSIONS

Because of Theorem 4.10, to obtain Theorem B, it remains mostly to show that every symplectic cubic space has a unique Frattini extension, which we do in this section (Theorems 5.1 and 5.6). Now, for code loops ($p = 2$), this is Thm. 10 of Griess [16], and for $p > 3$, we are in the associative case, in which case this result is essentially known. In fact, the difficult part (Theorem 5.6) of the general case follows from more general results of Johnson [21] (see Remark 5.8). Nevertheless, we continue with our version of these results, not only to remain self-contained, but also to emphasize the role of the *centrally twisted product* (Definition 5.2), a construction of independent interest (see Remark 5.7).

Notation. In this section, we use script letters $\mathcal{C}, \mathcal{D}, \mathcal{E}, \dots$ to denote Frattini extensions of the symplectic cubic spaces C, D, E, \dots , possibly with subscripts.

We first address uniqueness. Our proof follows §2 of Conway [10].

Theorem 5.1. *For $n = 1, 2$, let C_n be a symplectic cubic space of dimension k over \mathbf{F}_p , and let \mathcal{C}_n be a Frattini extension of C_n . If C_1 and C_2 are isomorphic up to scalar multiple, then \mathcal{C}_1 is isomorphic to \mathcal{C}_2 .*

Proof. First, by choosing a different generator for the distinguished central subgroup of \mathcal{C}_2 , we may assume that C_1 and C_2 are isomorphic. So let $\{c_i\}$ be a basis for $(C, \sigma, \chi, \alpha) = C_1$, and let \mathcal{C} be the loop given by the loop presentation

$$\begin{aligned} (5.1) \quad & \langle z, \gamma_i \mid \gamma_i^p = \sigma(c_i), \\ (5.2) \quad & [\gamma, \delta] = \chi(c, d), \\ (5.3) \quad & [\gamma, \delta, \epsilon] = \alpha(c, d, e), \\ (5.4) \quad & z^p = 1 \rangle, \end{aligned}$$

where i runs between 1 and k ; γ, δ, ϵ run over all loop words in the generators; c, d, e are the images in C of γ, δ, ϵ , respectively, under the map sending γ_i to c_i and z to 1; the values of σ, χ , and α are taken to be in $Z = \langle z \rangle$, which is a central subgroup of \mathcal{C} because of (5.2)–(5.4) and (4.8); and the expression γ_i^p is defined inductively by $\gamma_i^0 = 1$ and $\gamma_i^{n+1} = \gamma_i \gamma_i^n$.

Now, since isomorphisms take bases to bases, the above presentation is purely a function of the isomorphism class of C . Therefore, it is enough to show that any Frattini extension of C is isomorphic to \mathcal{C} . Furthermore, since the universal property of loop presentations (see Evans [13, I.2]) implies that *any* loop extension of C is a homomorphic image of \mathcal{C} , it is enough to show that \mathcal{C} has order at most p^{1+k} . However, since (5.2)–(5.4) imply that Z is a central subgroup of \mathcal{C} of order dividing p , and (5.1)–(5.3) implies that \mathcal{C}/Z is an elementary abelian p -group of rank k , the theorem follows. \square

Notation. We resume the convention that if γ, δ, ϵ (possibly with subscripts) are elements of a Frattini extension, then c, d, e (possibly with subscripts) are the corresponding elements of the quotient symplectic cubic space.

We turn to existence. Now, if \mathcal{D} and \mathcal{E} are subloops of the same Frattini extension, then for $\delta_i \in \mathcal{D}$, $\epsilon_i \in \mathcal{E}$, $(\delta_1 \epsilon_1)(\delta_2 \epsilon_2) = (z_0 \delta_1 \delta_2)(\epsilon_1 \epsilon_2)$, where $z_0 \in Z$ is expressible in terms of $\chi, \alpha, d_1, e_1, d_2$ and e_2 . This observation motivates the following definition.

Definition 5.2. Let p be a prime and let $Z = \mathbf{F}_p$ be the group of order p . Let D and E be linearly independent subspaces of a symplectic cubic space $(C, \sigma, \chi, \alpha)$; note that D and E are symplectic cubic spaces by restriction. Let \mathcal{D} (resp. \mathcal{E}) be a loop extension of D (resp. E). It is easily verified that we may define a loop Γ containing the central subgroup $Z \times Z$ by taking the set $\mathcal{D} \times \mathcal{E}$ and the binary operation given by

$$(5.5) \quad (\delta_1, \epsilon_1)(\delta_2, \epsilon_2) = (z\delta_1\delta_2, \epsilon_1\epsilon_2),$$

where

$$(5.6) \quad z = \chi(e_1, d_2)\alpha(d_1, e_1 d_2^{-1}, e_2)\alpha(d_1, e_1, d_2)^2\alpha(e_1, d_2, e_2)^{-2}.$$

We define the *centrally twisted product* of \mathcal{D} and \mathcal{E} to be the quotient of Γ by its central subgroup $\langle (z, z^{-1}) \rangle$, where z runs over all elements of Z .

Remark 5.3. Note that the main induction step in the proof of the main theorem of Johnson [21] is based on what is essentially the centrally twisted product; see Remark 5.8. Compare also Kitazume [22], whose Thm. 2 uses a particular example of the $p = 2$ case of the centrally twisted product.

Note that for $p = 2$, (5.6) becomes

$$(5.7) \quad z_0 = \chi(e_1, d_2)\alpha(d_1, e_1d_2, e_2),$$

for $p = 3$, (5.6) becomes

$$(5.8) \quad z_0 = \chi(e_1, d_2)\alpha(d_1, e_1d_2^{-1}, e_2)\alpha(d_1, e_1, d_2)^{-1}\alpha(e_1, d_2, e_2),$$

and for $p > 3$,

$$(5.9) \quad z_0 = \chi(e_1, d_2).$$

Notation. Imitating the ATLAS [11] notation $\mathcal{D} \circ \mathcal{E}$ for the central product of two groups \mathcal{D} and \mathcal{E} , we use $\mathcal{D} \oplus \mathcal{E}$ to denote the centrally twisted product of two code loops \mathcal{D} and \mathcal{E} . Note that if the χ and α factors on the right-hand side of (5.5) are always trivial, then $\mathcal{D} \oplus \mathcal{E}$ just becomes the central product. In that case, we write $\mathcal{D} \circ \mathcal{E}$, just as in the group case.

Theorem 5.4. *Let D and E be linearly independent symplectic cubic subspaces of $(C, \sigma, \chi, \alpha)$, let \mathcal{D} (resp. \mathcal{E}) be a Frattini extension of D (resp. E), and let $\mathcal{C} = \mathcal{D} \oplus \mathcal{E}$. Then \mathcal{C} is a Frattini extension of $D \oplus E$.*

Throughout the following proof, by convention, $\gamma = (\delta, \epsilon)$, possibly with subscripts. (Note that by our usual convention, we then have $c = de$.) We also freely identify Z with $Z \times 1$. Finally, the skew-symmetric, symplectic, and multilinear properties of χ and α (3.6)–(3.13) will be applied freely.

Proof. First, taking the quotient of $Z \times Z$ in \mathcal{C} as our distinguished central subgroup, it is easy to see that condition 1 of Definition 4.9 holds in \mathcal{C} . Furthermore, by collecting “signs” (elements of Z), it is easy to see that (4.10)–(4.12) hold “up to sign,” so it remains to check the signs.

We first verify (4.10), recalling our convention that γ^n is defined inductively by $\gamma^0 = 1$ and $\gamma^{n+1} = \gamma\gamma^n$. First, we claim that for all $n \geq 0$,

$$(5.10) \quad \gamma^n = (\chi(e, d)^r \delta^n, \epsilon^n),$$

where $r = n(n-1)/2$. In fact, if (5.10) holds for a given n , then

$$(5.11) \quad \begin{aligned} \gamma^{n+1} &= \gamma\gamma^n \\ &= (\delta, \epsilon)(\chi(e, d)^r \delta^n, \epsilon^n) \\ &= (\chi(e, d)^r \chi(e, d^n) \delta^{n+1}, \epsilon^{n+1}) \\ &= (\chi(e, d)^{r+n} \delta^{n+1}, \epsilon^{n+1}), \end{aligned}$$

and since $r + n = n(n+1)/2$, (5.10) follows by induction. In particular, if $n = p$, $r = p(p-1)/2$, which means that $\chi(e, d)^r = \chi(d, e)$ for $p = 2$ and $\chi(e, d)^r = 1$ for

$p > 2$. Therefore, collecting signs, we get

$$\begin{aligned}
(5.12) \quad \gamma^p &= (\chi(e, d)^r \sigma(d), \sigma(e)) \\
&= \begin{cases} \sigma(d)\sigma(e)\chi(d, e) & \text{for } p = 2 \\ \sigma(d)\sigma(e) & \text{for } p > 2 \end{cases} \\
&= \sigma(de) \\
&= \sigma(c).
\end{aligned}$$

Next, turning to (4.11), by collecting signs, we see that

$$(5.13) \quad \gamma_1 \gamma_2 = (z_+ \delta_1 \delta_2, \epsilon_1 \epsilon_2),$$

where

$$(5.14) \quad z_+ = \chi(e_1, d_2) \alpha(d_1, e_1 d_2^{-1}, e_2) \alpha(d_1, e_1, d_2)^2 \alpha(e_1, d_2, e_2)^{-2};$$

and

$$(5.15) \quad \gamma_2 \gamma_1 = (z_- \delta_1 \delta_2, \epsilon_1 \epsilon_2),$$

where

$$\begin{aligned}
(5.16) \quad z_- &= \chi(e_2, d_1) \chi(d_2, d_1) \chi(e_2, e_1) \\
&\quad \alpha(d_2, e_2 d_1^{-1}, e_1) \alpha(d_2, e_2, d_1)^2 \alpha(e_2, d_1, e_1)^{-2}.
\end{aligned}$$

To verify (4.11), we need to show that $z = z_+ z_-^{-1} = \chi(d_1 e_1, d_2 e_2)$. However, gathering the χ terms of z , we have

$$\begin{aligned}
(5.17) \quad &\chi(e_1, d_2) \chi(e_2, d_1)^{-1} \chi(d_2, d_1)^{-1} \chi(e_2, e_1)^{-1} \\
&= \chi(e_1, d_2) \chi(d_1, e_2) \chi(d_1, d_2) \chi(e_1, e_2) \\
&= \chi(d_1, d_2 e_2) \chi(e_1, d_2 e_2) \alpha(d_1, d_2, e_2)^3 \alpha(e_1, d_2, e_2)^3 \\
&= \chi(d_1 e_1, d_2 e_2) \alpha(d_1, e_1, d_2 e_2)^3 \alpha(d_1 e_1, d_2, e_2)^3,
\end{aligned}$$

and gathering the α terms of z , we have

$$\begin{aligned}
(5.18) \quad &\alpha(d_1, e_1 d_2^{-1}, e_2) \alpha(d_1, e_1, d_2)^2 \alpha(e_1, d_2, e_2)^{-2} \\
&\cdot \alpha(d_2, e_2 d_1^{-1}, e_1)^{-1} \alpha(d_2, e_2, d_1)^{-2} \alpha(e_2, d_1, e_1)^2 \\
&= \alpha(d_1, e_1, d_2)^3 \alpha(d_1, e_1, e_2)^3 \alpha(d_1, d_2, e_2)^3 \alpha(e_1, d_2, e_2)^3.
\end{aligned}$$

(4.11) follows because $\alpha^6 = 1$ identically.

Finally, using the same strategy to verify (4.12), we see that $(\gamma_1 \gamma_2) \gamma_3 = z \cdot \gamma_1 (\gamma_2 \gamma_3)$, where

$$\begin{aligned}
z &= \chi(e_1, d_2) \alpha(d_1, e_1 d_2^{-1}, e_2) \alpha(d_1, e_1, d_2)^2 \alpha(e_1, d_2, e_2)^{-2} \\
&\cdot \chi(e_1 e_2, d_3) \alpha(d_1 d_2, e_1 e_2 d_3^{-1}, e_3) \alpha(d_1 d_2, e_1 e_2, d_3)^2 \alpha(e_1 e_2, d_3, e_3)^{-2} \\
&\cdot \chi(e_2, d_3)^{-1} \alpha(d_2, e_2 d_3^{-1}, e_3)^{-1} \alpha(d_2, e_2, d_3)^{-2} \alpha(e_2, d_3, e_3)^2 \\
&\cdot \chi(e_1, d_2 d_3)^{-1} \alpha(d_1, e_1 d_2^{-1} d_3^{-1}, e_2 e_3)^{-1} \alpha(d_1, e_1, d_2 d_3)^{-2} \alpha(e_1, d_2 d_3, e_2 e_3)^2 \\
&\cdot \alpha(d_1, d_2, d_3) \alpha(e_1, e_2, e_3).
\end{aligned}$$

Collecting the χ terms of z , we have

$$\begin{aligned}
& \chi(e_1, d_2)\chi(e_1e_2, d_3)\chi(e_2, d_3)^{-1}\chi(e_1, d_2d_3)^{-1} \\
& = \chi(e_1, d_2)\chi(e_1, d_3)\chi(e_2, d_3)\alpha(e_1, e_2, d_3)^3 \\
(5.19) \quad & \chi(e_2, d_3)^{-1}\chi(e_1, d_2)^{-1}\chi(e_1, d_3)^{-1}\alpha(e_1, d_2, d_3)^3 \\
& = \alpha(e_1, e_2, d_3)^3\alpha(e_1, d_2, d_3)^3.
\end{aligned}$$

Completely expanding all α terms of z and collecting all terms which repeat subscripts, we have

$$\begin{aligned}
& \alpha(d_1, e_1, e_2)\alpha(d_1, d_2^{-1}, e_2)\alpha(d_1, e_1, d_2)^2\alpha(e_1, d_2, e_2)^{-2} \\
& \cdot \alpha(d_1, d_3^{-1}, e_3)\alpha(d_2, d_3^{-1}, e_3)\alpha(d_1, e_1, e_3)\alpha(d_2, e_2, e_3) \\
(5.20) \quad & \cdot \alpha(d_1, e_1, d_3)^2\alpha(d_2, e_2, d_3)^2\alpha(e_1, d_3, e_3)^{-2}\alpha(e_2, d_3, e_3)^{-2} \\
& \cdot \alpha(d_2, e_2, e_3)^{-1}\alpha(d_2, d_3^{-1}, e_3)^{-1}\alpha(d_2, e_2, d_3)^{-2}\alpha(e_2, d_3, e_3)^2 \\
& \cdot \alpha(d_1, e_1, e_2)^{-1}\alpha(d_1, e_1, e_3)^{-1}\alpha(d_1, d_2^{-1}, e_2)^{-1}\alpha(d_1, d_3^{-1}, e_3)^{-1} \\
& \cdot \alpha(d_1, e_1, d_2)^{-2}\alpha(d_1, e_1, d_3)^{-2}\alpha(e_1, d_2, e_2)^2\alpha(e_1, d_3, e_3)^2 = 1,
\end{aligned}$$

since (thankfully) every term in the first three lines of (5.20) is cancelled by some term in the next three lines.

The remaining α terms of z are then, after expansion,

$$\begin{aligned}
& \alpha(d_1, e_2, e_3)\alpha(d_2, e_1, e_3)\alpha(d_1, e_2, d_3)^2\alpha(d_2, e_1, d_3)^2 \\
& \cdot \alpha(d_1, d_2^{-1}, e_3)^{-1}\alpha(d_1, d_3^{-1}, e_2)^{-1}\alpha(e_1, d_2, e_3)^2\alpha(e_1, d_3, e_2)^2 \\
& \cdot \alpha(d_1, d_2, d_3)\alpha(e_1, e_2, e_3) \\
(5.21) \quad & = \alpha(d_1, e_2, e_3)\alpha(e_1, d_2, e_3)^{-1}\alpha(d_1, e_2, d_3)^2\alpha(e_1, d_2, d_3)^{-2} \\
& \cdot \alpha(d_1, d_2, e_3)\alpha(d_1, e_2, d_3)^{-1}\alpha(e_1, d_2, e_3)^2\alpha(e_1, e_2, d_3)^{-2} \\
& \cdot \alpha(d_1, d_2, d_3)\alpha(e_1, e_2, e_3) \\
& = \alpha(d_1, e_2, e_3)\alpha(d_1, e_2, d_3)\alpha(e_1, d_2, d_3)^{-2} \\
& \cdot \alpha(d_1, d_2, e_3)\alpha(e_1, d_2, e_3)\alpha(e_1, e_2, d_3)^{-2} \\
& \cdot \alpha(d_1, d_2, d_3)\alpha(e_1, e_2, e_3).
\end{aligned}$$

Multiplying (5.19)–(5.21), we see that $z = \alpha(d_1e_1, d_2e_2, d_3e_3)$, so (4.12), and the theorem, follow. \square

With Theorem 5.4, to obtain the existence of Frattini extensions, we just need the following example.

Example 5.5. Let $(C, \sigma, 1, 1)$ be a symplectic cubic space of dimension 1, and let c be a nonzero vector in C . If $\sigma(c) = 1$, then $Z \times C$ is a Frattini extension of C ; otherwise, the cyclic group of order p^2 is an Frattini extension of C .

Theorem 5.6. *If C is a symplectic cubic space, there exists a (unique) Frattini extension of C .*

Proof. Proceeding by induction on $k = \dim C$, let $C = D + E$, where $\dim D = k - 1$ and $\dim E = 1$, let \mathcal{D} be the Frattini extension of D (by induction), and let \mathcal{E} be the Frattini extension of E (from Example 5.5). Then from Theorem 5.4, $\mathcal{D} \oplus \mathcal{E}$ is a Frattini extension of C . \square

Remark 5.7. Consider again the loop \mathcal{C} given by the presentation in the proof of Theorem 5.1. Now, there is an easy “solution” to the loop word problem for \mathcal{C} . Namely, given a loop word w in the generators $\{\gamma_i\}$, w can be arranged into the normal form $z\gamma_1^r(\gamma_2^s(\gamma_3^t(\dots)))$ by simply powering, commuting, and associating elements, while keeping track of “error terms” with σ , χ , and α . Theorem 5.6 can then be interpreted as saying precisely that this solution is actually consistent, i.e., that we are never forced to kill Z .

In fact, this normal form procedure provides a method for doing calculations in any SFML. Furthermore, while building an SFML from 1-dimensional pieces becomes unwieldy for large dimension, by using larger associative (or at least familiar) pieces as building blocks, and gluing them together with the centrally twisted product, it is not hard to do hand calculations in, say, the Parker loop. See [20].

Finally, we prove Theorem B.

Proof of Theorem B. Because of Theorems 5.1 and 5.6, it remains only to show that if L and M are SFML’s, with distinguished central subgroups Z_L and Z_M , and associated symplectic cubic spaces C_L and C_M , and there is an isomorphism $\varphi : L \rightarrow M$ such that $\varphi(Z_L) = Z_M$, then C_L and C_M are isomorphic up to scalar multiple. However, since σ , χ , and α are only determined by the isomorphism type of an SFML, by choosing corresponding generators of Z_L and Z_M (i.e., by applying a scalar multiple), we can make C_L and C_M isomorphic. The theorem follows. \square

Remark 5.8. For the convenience of the reader, we now provide a short summary of the main result of Johnson [21]. Let L be a loop (not necessarily finite, Moufang, or IP) with a central subgroup Z such that $C \cong L/Z$ is an abelian group. Then, as in our case, there are well-defined commutator and associator functions $\chi : C \times C \rightarrow Z$ and $\alpha : C \times C \times C \rightarrow Z$ which satisfy the properties

$$(5.22) \quad \alpha(x, 1, y) = 1$$

$$(5.23) \quad \chi(x, x) = 1$$

$$(5.24) \quad \chi(y, x) = \chi(x, y)^{-1}$$

$$(5.25) \quad \alpha(wx, y, z)\alpha(w, x, yz) = \alpha(w, x, y)\alpha(w, xy, z)\alpha(x, y, z)$$

$$(5.26) \quad \chi(x, yz)\chi(x, y)^{-1}\chi(x, z)^{-1} = \alpha(y, x, z)\alpha(x, y, z)^{-1}\alpha(y, z, x)^{-1}$$

for all $w, x, y, z \in C$. (Note that the last two properties are precisely the pentagonal and hexagonal identities of MacLane [23, Ch. VII]; also, compare our formulas (3.9) and (3.17).) Conversely, Johnson shows, using what is essentially the centrally twisted product as the key induction step, that any χ and α which satisfy these properties can be realized by such a loop L , and that furthermore, we may freely choose the “power maps” (analogous to σ , or compare Definition 7.1) of the inverse images of a basis of C . Theorem 5.6 then follows easily from this result.

From this viewpoint, our work here stems from the observation that given χ and α which arise from a loop L in this manner, L is Moufang if and only if α is symplectic and skew-symmetric, which in turn holds if and only if α is symplectic multilinear. We note, however, that these properties of α (especially multilinearity) are crucial to the usefulness of our results. See, for instance, Section 6, especially Examples 6.8 and 6.9.

6. ISOTOPY IN SMALL FRATTINI MOUFANG 3-LOOPS

In this section, as a fairly straightforward application of Theorem B, we characterize isotopy in SFML's. Now, because of Corollary 3.10, any SFM p -loop is a G -loop, unless $p = 3$. Therefore, even though much of this section applies for all p , throughout this section, we assume that L is a finite SFM 3-loop, that Z is a fixed central subgroup of L , and that $C \cong L/Z$ is an elementary abelian 3-group. In other words, we assume that L is a Frattini extension of a symplectic cubic space $(C, \sigma, \chi, \alpha)$ over \mathbf{F}_3 . We also resume the convention that $\gamma, \delta, \epsilon, \kappa \in L$ reduce to $c, d, e, k \in C$.

Definition 6.1. Let L be a Moufang loop. For $\gamma, \delta, \kappa \in L$, we define

$$(6.1) \quad \gamma \circ_{\kappa} \delta = (\gamma\kappa)(\kappa^{-1}\delta).$$

It is easily verified that the set L and the operation \circ_{κ} form a loop (L, \circ_{κ}) , with identity 1. Because (U, V, ι) is an isotopism from L to (L, \circ_{κ}) , where $U(x) = x\kappa^{-1}$, $V(x) = \kappa x$, and $\iota(x) = x$, (L, \circ_{κ}) is called the κ -isotope of L .

When multiplication in both L and (L, \circ_{κ}) appear in the same formula, we denote the former by $\gamma \cdot \delta$ and the latter by $\gamma \circ_{\kappa} \delta$.

Remark 6.2. Note that di-associativity of L implies that for $\gamma \in L$, $\gamma^{-1} \circ_{\kappa} \gamma = (\gamma^{-1}\kappa)(\kappa^{-1}\gamma) = 1$. In other words, the inverse of an element in L is also its inverse in (L, \circ_{κ}) .

We now recall the following fundamental result on isotopy in Moufang loops (see Pflugfelder [24, Thm. IV.4.1]).

Theorem 6.3. *If L is a Moufang loop, then any loop-isotope of L is isomorphic to a κ -isotope of L .* \square

The following formula therefore reduces isotopy in SFML's to a matter of multilinear algebra.

Theorem 6.4. *We have*

$$(6.2) \quad \gamma \circ_{\kappa} \delta = \gamma\delta \cdot \alpha(c, k, d).$$

In particular, for $z \in Z(L)$, $(z\gamma) \circ \delta = (\gamma \circ \delta) \cdot z = \gamma \circ (z\delta)$, which means that $z \in Z(L, \circ_{\kappa})$.

Proof. Applying the multilinear and symplectic properties of α , we have:

$$(6.3) \quad \begin{aligned} \gamma \circ_{\kappa} \delta &= (\gamma\kappa)(\kappa^{-1}\delta) \\ &= \gamma(\kappa(\kappa^{-1}\delta)) \cdot \alpha(c, k, \kappa^{-1}d) \\ &= \gamma\delta \cdot \alpha(c, k, d). \quad \square \end{aligned}$$

We now only need the following definitions to proceed.

Definition 6.5. The *radical* of α (resp. χ), denoted by $\text{rad}(\alpha)$ (resp. $\text{rad}(\chi)$), is the set of all $c \in C$ such that $\alpha(c, d, e) = 1$ (resp. $\chi(c, d) = 1$) for all $d, e \in C$ (resp. $d \in C$). Note that $\text{rad}(\alpha) = N(L)/Z$ and $\text{rad}(\chi) = C(L)/Z$.

Definition 6.6. Let $(C, \sigma(c), \chi(c, d), \alpha(c, d, e))$ be a symplectic cubic space. For $k \in C$, the *adjoint translate* $\text{ad}_k(C)$ is defined to be the symplectic cubic space $(C, \sigma(c), \chi(c, d)\alpha(c, k, d), \alpha(c, d, e))$. The operation ad_k is called an *adjoint translation*.

In the following, we write $\gamma \circ_{\kappa} \delta$ as $\gamma \circ \delta$. Also, for $\gamma, \delta, \epsilon \in L$, we define $\gamma^{\circ n}$ inductively by $\gamma^{\circ 0} = 1$ and $\gamma^{\circ(n+1)} = \gamma \circ \gamma^{\circ n}$; we define $[\gamma, \delta]_{\circ}$ to be $(\delta \circ \gamma)^{-1} \circ (\gamma \circ \delta)$; and we define $[\gamma, \delta, \epsilon]_{\circ}$ to be $(\gamma \circ (\delta \circ \epsilon))^{-1} \circ ((\gamma \circ \delta) \circ \epsilon)$. (See Remark 6.2.) Theorem C then comes from the following result.

Theorem 6.7. *We have the formulas*

$$(6.4) \quad \gamma^{\circ n} = \gamma^n,$$

$$(6.5) \quad [\gamma, \delta]_{\circ} = \chi(c, d)\alpha(c, k, d)^{-1},$$

$$(6.6) \quad [\gamma, \delta, \epsilon]_{\circ} = \alpha(c, d, e).$$

In particular, $\gamma^{\circ 3} = \sigma(\gamma)$.

Proof. We first verify (6.4) by induction. If (6.4) holds for a given value of n , then by the di-associativity of L , we have

$$(6.7) \quad \gamma^{\circ(n+1)} = \gamma \circ \gamma^n = (\gamma\kappa)(\kappa^{-1}\gamma^n) = \gamma^{n+1}.$$

(6.4) follows by induction.

Next, from (6.2) and

$$(6.8) \quad \delta \circ \gamma = \delta\gamma \cdot \alpha(d, k, c) = \gamma\delta \cdot \chi(c, d)^{-1}\alpha(d, k, c),$$

it follows that

$$(6.9) \quad \begin{aligned} [\gamma, \delta]_{\circ} &= (\delta \circ \gamma)^{-1} \circ (\gamma \circ \delta) \\ &= ((\gamma\delta)^{-1} \cdot \chi(c, d)\alpha(d, k, c)^{-1}) \circ ((\gamma\delta) \cdot \alpha(c, k, d)) \\ &= \chi(c, d)\alpha(c, k, d)\alpha(c, k, d), \\ &= \chi(c, d)\alpha(c, k, d)^{-1}, \end{aligned}$$

with the last equality following because Z has exponent 3. (6.5) follows.

Finally, since

$$(6.10) \quad (\gamma \circ \delta) \circ \epsilon = (\gamma\delta)\epsilon \cdot \alpha(c, k, d)\alpha(cd, k, e)$$

$$(6.11) \quad \begin{aligned} \gamma \circ (\delta \circ \epsilon) &= \gamma(\delta\epsilon) \cdot \alpha(d, k, e)\alpha(c, k, de) \\ &= (\gamma\delta)\epsilon \cdot \alpha(c, d, e)^{-1}\alpha(d, k, e)\alpha(c, k, de), \end{aligned}$$

we have that

$$(6.12) \quad \begin{aligned} [\gamma, \delta, \epsilon]_{\circ} &= (\gamma \circ (\delta \circ \epsilon))^{-1} \circ ((\gamma \circ \delta) \circ \epsilon) \\ &= (((\gamma\delta)\epsilon)^{-1} \cdot \alpha(c, d, e)\alpha(d, k, e)^{-1}\alpha(c, k, de)^{-1}) \\ &\quad \circ ((\gamma\delta)\epsilon \cdot \alpha(c, k, d)\alpha(cd, k, e)) \\ &= \alpha(c, d, e)\alpha(d, k, e)^{-1}\alpha(c, k, d)^{-1}\alpha(c, k, e)^{-1} \\ &\quad \cdot \alpha(c, k, d)\alpha(c, k, e)\alpha(d, k, e) \\ &= \alpha(c, d, e). \end{aligned}$$

The theorem follows. \square

Proof of Theorem C. From (6.4)–(6.6), it follows that (L, \circ_{κ}) is precisely the Frattini extension of $\text{adt}_{k^{-1}}(C)$, since condition 1 of Definition 4.9 follows from (6.5) and (6.6), and the formulas (4.10)–(4.12) of condition 2 of Definition 4.9 follow from the formulas (6.4)–(6.6), respectively. Therefore, any κ -isotope of L is a Frattini extension of an adjoint translate of C , and vice versa. The theorem follows. \square

We now illustrate Theorems B and C by enumerating the isomorphism and isotopy classes of the nonassociative Frattini extensions of the symplectic cubic spaces of dimension 3 and 4 over \mathbf{F}_3 . For simplicity, we only discuss the exponent 3 ($\sigma = 1$) cases. In the following, let $(C, 1, \chi, \alpha)$ be the symplectic cubic space under discussion, let L be its Frattini extension, and let $Z = \langle \omega \rangle$, where $\omega^3 = 1$.

Example 6.8. In the dimension 3 case, either $\chi = 1$ (i.e., L is commutative), or there exists a basis $\{k, c, d\}$ of C such that $\text{rad}(\chi) = \langle k \rangle$ and $\chi(c, d) = \omega$. After possibly inverting k , we may assume that $\alpha(c, k, d) = \omega$, so there are two possibilities for L , up to isomorphism. However, in the case where $\chi \neq 1$, $\text{ad}_k(C)$ has $\chi = 1$ as its bilinear form, so the two isomorphism classes are isotopic.

Example 6.9. In dimension 4, since we assume α is nontrivial, there is some $c \in C$ such that $c \notin \text{rad}(\alpha)$. Therefore, since $\alpha(c, -, -)$ is a nontrivial bilinear symplectic form on C whose radical contains c , we may choose a basis $\{c, d, e, f\}$ for C such that $\alpha(c, d, -) = 1$ and $\alpha(c, e, f) = \alpha(d, e, f)^{-1}$. It may then be easily verified on the basis $\{c, d, e, f\}$ that $cd \in \text{rad}(\alpha)$. Therefore, $\text{rad}(\alpha)$ is 1-dimensional. It follows easily that α is unique up to isomorphism, and that we have four possible isomorphism classes for C (and therefore, for L):

1. χ trivial;
2. χ nondegenerate;
3. $\text{rad}(\chi)$ 2-dimensional, containing $\text{rad}(\alpha)$; and
4. $\text{rad}(\chi)$ 2-dimensional, not containing $\text{rad}(\alpha)$.

So now let $\text{rad}(\alpha) = \langle c \rangle$. First, for $d \in C$, $\chi(c, d)$ is invariant under adjoint translation, so isomorphism classes 1 and 2 cannot be adjoint translates. Conversely, if χ is nondegenerate, without loss of generality, we may choose a basis $\{c, k, d, e\}$ for C such that $\langle c, k \rangle$ and $\langle d, e \rangle$ are orthogonal with respect to χ and $\chi(d, e) = \alpha(d, k, e)$, in which case $\text{ad}_k(C)$ is in isomorphism class 4. On the other hand, if $\text{rad}(\alpha) = \langle c \rangle$ and $\text{rad}(\chi) = \langle c, k \rangle$, then by inverting k if necessary, we may choose a basis $\{c, k, d, e\}$ for C such that $\chi(d, e) = \alpha(d, k, e)$, in which case $\text{ad}_k(C)$ is in isomorphism class 1. Therefore, we have precisely two isotopy classes: isomorphism classes 1 and 3, and isomorphism classes 2 and 4.

Compare Bénéteau [3, IV.3] and Ray-Chaudhuri and Roth [25].

7. FINITE MOUFANG LOOPS OF CLASS 2 IN GENERAL

In this section, we extend our previous results to all finite Moufang p -loops of class 2, which also means that we can apply our results to *any* finite Moufang loop of class 2 (see Theorem 3.7). Essentially, we imitate Sections 4–6, using modules instead of vector spaces, and we find that the only problems arise with power maps.

Notation. We resume our $\gamma, \delta, \epsilon, \dots$ and c, d, e, \dots convention.

As before, let L be a finite Moufang loop with a central subgroup Z such that $C \cong L/Z$ is an abelian group. We would like to say that L gives C the structure of a “symplectic cubic module,” in some appropriate sense. Now, from Theorem 3.3, we know that χ and α work exactly as they do for SFML’s. However, if r is the exponent of Z , for a q th power function from C to Z to be well-defined, r must divide q . Therefore, if $r > p$, we can no longer use power functions like σ to capture all of the information we need. We fix this problem with the following definitions.

Definition 7.1. We define a *symplectic cubic p -module* to be a 6-tuple

$$(C, Z, \{c_i\}, \{z_i\}, \chi, \alpha),$$

where C and Z are finite abelian p -groups; $\{c_i\}$ is a basis (set of independent generators) for C ; $\{z_i\}$ is a set of elements of Z ; and $\chi : C \times C \rightarrow Z$ and $\alpha : C \times C \times C \rightarrow Z$ satisfy (3.6)–(3.9) and (3.10)–(3.13) for all $c, d, e, f \in C$ and all $n \in \mathbf{Z}$.

Definition 7.2. Let $(C_n, Z, \{c_{ni}\}, \{z_{ni}\}, \chi_n, \alpha_n)$ be a symplectic cubic p -module for $n = 1, 2$. We say that C_1 and C_2 are *isomorphic up to scalar multiple* if there is an isomorphism $\varphi : C_1 \rightarrow C_2$ and some fixed $a \in \text{Aut}(Z)$ such that

$$(7.1) \quad \begin{aligned} \varphi(c_{1i}) &= c_{2i}, \\ z_{2i} &= z_{1i}^a, \\ \chi_2(\varphi(c), \varphi(d)) &= \chi_1(c, d)^a, \\ \alpha_2(\varphi(c), \varphi(d), \varphi(e)) &= \alpha_1(c, d, e)^a. \end{aligned}$$

If $a = 1$, then we say that C_1 and C_2 are *isomorphic*.

Definition 7.3. Let $(C, Z, \{c_i\}, \{z_i\}, \chi, \alpha)$ be a symplectic cubic module over \mathbf{F}_p . We say that a loop L with a choice of distinguished elements $\gamma_i \in L$ is a *Frattini extension* of C if:

1. Z is a central subgroup of L , and $L/Z \cong C$.
2. If $\gamma, \delta, \epsilon \in L$ are preimages of $c, d, e \in C$, then

$$(7.2) \quad [\gamma, \delta] = \chi(c, d),$$

$$(7.3) \quad [\gamma, \delta, \epsilon] = \alpha(c, d, e).$$

3. For each i , γ_i is a preimage of c_i , and if q_i is the order of c_i , then

$$(7.4) \quad \gamma_i^{q_i} = z_i.$$

Following Theorem 4.10, we then see that:

Theorem 7.4. *Every Moufang p -loop of class 2 is a Frattini extension of a symplectic cubic p -module, and every Frattini extension of a symplectic cubic p -module is a Moufang p -loop of class 2.*

Proof. Let L be a Moufang p -loop of class 2, let $C \cong L/Z$ be an abelian group for some central subgroup Z of L , and choose a basis $\{c_i\}$ for C and corresponding preimages $\gamma_i \in L$. If we let $z_i = \gamma_i^{q_i}$, where q_i is the order of c_i , and we define χ and α as usual, Theorems 3.3 and 4.6 imply that L is a Frattini extension of $(C, Z, \{c_i\}, \{z_i\}, \chi, \alpha)$. Conversely, let L be a Frattini extension of a symplectic cubic p -module $(C, Z, \{c_i\}, \{z_i\}, \chi, \alpha)$. As before, the proof of Theorem 3.9 in the case $k = 1$ shows that L is Moufang. Since L/Z is abelian, the theorem follows. \square

Next, we turn to Section 5, starting with the uniqueness of Frattini extensions.

Theorem 7.5. *For $n = 1, 2$, let C_n be a symplectic cubic p -module, and let \mathcal{C}_n be a Frattini extension of C_n . If C_1 and C_2 are isomorphic up to scalar multiple, then \mathcal{C}_1 is isomorphic to \mathcal{C}_2 .*

Proof. The proof is the same as the proof of Theorem 5.1, except that we replace the single generator z with the elements of Z , (5.1) with (7.4), and (5.4) with the multiplication table of Z . \square

The definition of the centrally twisted product (Definition 5.2) carries over directly, as does Theorem 5.4:

Theorem 7.6. *Let D and E be symplectic cubic p -submodules of the symplectic cubic p -module C such that the chosen basis $\{c_i\}$ for C is the concatenation of bases for D and E ; let \mathcal{D} (resp. \mathcal{E}) be a Frattini extension of D (resp. E); and let $\mathcal{C} = \mathcal{D} \oplus \mathcal{E}$. Then \mathcal{C} is a Frattini extension of $D \oplus E$.*

Proof. The proof is the same as the proof of Theorem 5.4, except that we replace the verification of (4.10) by our hypothesis that concatenation of the bases of D and E produces a basis for C . \square

Finally, Frattini extensions of 1-dimensional symplectic cubic modules are easy to construct using central products of groups, so Theorem 5.6 becomes:

Theorem 7.7. *Every symplectic cubic module has a Frattini extension.* \square

Again, as noted in Remark 5.8, Theorem 7.7 also follows from the main result of Johnson [21].

The only result not carried over from Section 5 is the “isomorphic SFML’s implies isomorphic symplectic cubic spaces” statement of Theorem B, since the structure of a symplectic cubic module is highly basis-dependent in general. The one exception is that if Z is elementary abelian, we can actually define symplectic cubic modules in the following basis-independent manner.

Definition 7.8. Let Z be an elementary abelian p -group, let C be an abelian p -group, and let C_p be the subgroup of C of all elements of order dividing p . By a slight abuse of terminology, we define a *symplectic cubic p -module* to be a 5-tuple $(C, Z, \sigma, \chi, \alpha)$, where $\sigma : C_p \rightarrow Z$ is defined by $\sigma(c) = \gamma^p$; and $\chi : C \times C \rightarrow Z$ and $\alpha : C \times C \times C \rightarrow Z$ satisfy (3.6)–(3.9) and (3.10)–(3.13) for all $c, d, e, f \in C$ and all $n \in \mathbf{Z}$.

Note that σ actually determines all p^n th power maps, for if the order of c is p^{n+1} , then $\gamma^{p^{n+1}} = (\gamma^{p^n})^p = \sigma(c^{p^n})$. We may therefore obtain the z_i ’s of Definition 7.1 from $(C, Z, \sigma, \chi, \alpha)$ and a choice of basis c_i . Note also that the definition of isomorphism up to scalar multiple from Definition 4.8 now makes sense in this context. We may therefore recover the rest of Theorem B.

Theorem 7.9. *Let L and M be Moufang p -loops of class 2 with distinguished elementary abelian central subgroups Z_L and Z_M , and associated symplectic cubic modules C_L and C_M . Then there is an isomorphism $\varphi : L \rightarrow M$ such that $\varphi(Z_L) = Z_M$ if and only if C_L and C_M are isomorphic up to scalar multiple.*

Proof. The proof is the same as the proof of Theorem B at the end of Section 5, the main point being that σ , χ , and α are all determined by the isomorphism type of a Moufang p -loop of class 2 with distinguished elementary abelian central subgroup. \square

We can also generalize Theorem C to the case where Z is an elementary abelian 3-group and C is a symplectic cubic module with values in Z . (For example, this extension applies when L has exponent 3 and class 2.)

Theorem 7.10. *Let L be a Frattini extension of a symplectic cubic 3-module $(C, Z, \sigma, \chi, \alpha)$.*

Then every loop-isotope of L is isomorphic to the Frattini extension of an adjoint translate of C . In particular, σ and α are isotopy invariants of L ; that is, if M is a loop-isotope of L , then there is some isotopy from L to M which preserves both σ and α .

Proof. Since Section 6 (see Theorem 6.7) only uses the exponent of Z , and not its order, all of its definitions and proofs apply verbatim. \square

It remains only to address the question analogous to the one posed in Remark 4.11: Which χ , α , etc., can be chosen for a symplectic cubic module? Now, the z_i of Definition 7.1 are easy, since Theorem 7.6 and the 1-dimensional case shows that the z_i may be chosen freely on a basis for C . When Z has exponent p , this means precisely that σ may be chosen freely on a basis for C_p . As for the functions χ and α , they are multilinear for $p > 2$, so the problem is easy in that case, keeping in mind that $\alpha^6 = 1$. We therefore need only consider χ and α for the case $p = 2$ (Theorem 7.11).

Notation. We revert to additive notation for abelian groups. All summations, indices, etc., are from 1 to n in the manner indicated. (For instance, $i < j$ means for all $1 \leq i < j \leq n$.) We also let $\alpha_{ijk} = \alpha(x_i, x_j, x_k)$.

Theorem 7.11. *Let C and Z be finite abelian 2-groups, and let $\{x_i\}$ be a basis for C . Choose some symplectic multilinear function $\alpha : C \times C \times C \rightarrow Z$ such that $2\alpha = 0$ identically, and for all i, j , choose $\chi_{ij} \in Z$ such that:*

1. $\chi_{ii} = 0$;
2. $\chi_{ij} = -\chi_{ji}$; and
3. The (additive) order of χ_{ij} divides the order of x_i .

Let $c = \sum_i c_i x_i$ and $d = \sum_j d_j x_j$. The function $\chi : C \times C \rightarrow Z$ defined by

$$(7.5) \quad \chi(c, d) = \sum_{i \neq j} c_i d_j \chi_{ij} + \sum_{i < j} \sum_k c_i c_j d_k \alpha_{ijk} + \sum_i \sum_{j < k} c_i d_j d_k \alpha_{ijk},$$

along with any choice of elements $z_i \in Z$, gives C the structure of a symplectic cubic module. Furthermore, any symplectic cubic module of 2-power order may be constructed in this way.

Note that the first term of the right-hand side of (7.5) makes sense only when condition 3 is satisfied, since the c_i in $c = \sum_i c_i x_i$ is only well-defined as an integer mod the order of x_i . Also, the last two terms of (7.5) are invariant under a reordering of the basis only because α_{ijk} is symmetric in all three indices.

Proof. Given a symplectic cubic module, if $\chi_{ij} = \chi(x_i, x_j)$, then conditions 1, 2, and 3 follow from (3.6), (3.7), and Theorem 3.5, respectively. Furthermore, (7.5) follows from repeated application of (3.9) and (3.13), and $2\alpha = 0$ follows from Theorem A. Our last assertion follows easily.

As for the first assertion, it suffices to check (3.6)–(3.9); in fact, because of (3.14), it suffices to check (3.6), (3.7), and (3.9). In the following, let $c = \sum_i c_i x_i$, $d = \sum_i d_i x_i$, and $e = \sum_i e_i x_i$.

To check (3.6), we compute

$$\begin{aligned}
\chi(c, c) &= \sum_{i \neq j} c_i c_j \chi_{ij} + \sum_{i < j} \sum_k c_i c_j c_k \alpha_{ijk} + \sum_i \sum_{j < k} c_i c_j c_k \alpha_{ijk} \\
(7.6) \quad &= \sum_{i < j} (c_i c_j \chi_{ij} + c_j c_i \chi_{ji}) + \sum_{i < j} \sum_k c_i c_j c_k \alpha_{ijk} + \sum_{j < k} \sum_i c_j c_k c_i \alpha_{jki} \\
&= 0,
\end{aligned}$$

since $\chi_{ij} + \chi_{ji} = 0$, $\alpha_{jki} = \alpha_{ijk}$, and $2\alpha = 0$.

To check (3.7), we compute

$$\begin{aligned}
\chi(c, d) &= \sum_{i \neq j} c_i d_j \chi_{ij} + \sum_{i < j} \sum_k c_i c_j d_k \alpha_{ijk} + \sum_i \sum_{j < k} c_i d_j d_k \alpha_{ijk} \\
(7.7) \quad &= -\sum_{j \neq i} d_j c_i \chi_{ji} + \sum_{j < k} \sum_i d_j d_k c_i \alpha_{jki} + \sum_k \sum_{i < j} d_k c_i c_j \alpha_{kij} \\
&= -\chi(d, c),
\end{aligned}$$

since $\chi_{ij} = -\chi_{ji}$, $\alpha_{jki} = \alpha_{kij} = \alpha_{ijk}$, and $\alpha = -\alpha$.

Finally, to check (3.9), we compute

$$\begin{aligned}
\chi(c + d, e) &= \sum_{i \neq j} (c_i + d_i) e_j \chi_{ij} + \sum_{i < j} \sum_k (c_i + d_i) (c_j + d_j) e_k \alpha_{ijk} \\
&\quad + \sum_i \sum_{j < k} (c_i + d_i) e_j e_k \alpha_{ijk} \\
&= \sum_{i \neq j} c_i e_j \chi_{ij} + \sum_{i \neq j} d_i e_j \chi_{ij} \\
(7.8) \quad &\quad + \sum_{i < j} \sum_k c_i c_j e_k \alpha_{ijk} + \sum_{i < j} \sum_k d_i d_j e_k \alpha_{ijk} \\
&\quad + \sum_i \sum_{j < k} c_i e_j e_k \alpha_{ijk} + \sum_i \sum_{j < k} d_i e_j e_k \alpha_{ijk} \\
&\quad + \sum_{i < j} \sum_k c_i d_j e_k \alpha_{ijk} + \sum_{i < j} \sum_k d_i c_j e_k \alpha_{ijk} \\
&= \chi(c, e) + \chi(d, e) + \alpha(c, d, e),
\end{aligned}$$

since

$$\begin{aligned}
&\sum_{i < j} \sum_k c_i d_j e_k \alpha_{ijk} + \sum_{i < j} \sum_k d_i c_j e_k \alpha_{ijk} \\
(7.9) \quad &= \sum_{i < j} \sum_k c_i d_j e_k \alpha_{ijk} + \sum_{i > j} \sum_k c_i d_j e_k \alpha_{ijk} \\
&= \alpha(c, d, e),
\end{aligned}$$

using $\alpha_{ijk} = \alpha_{jik}$ and $\alpha_{kjk} = \alpha_{ikk} = 0$. The theorem follows. \square

Remark 7.12. Note that when the central subgroup Z is not elementary abelian, the results in this section say little about the isomorphism problem for Moufang loops of class 2. In fact, in that case, the result in group theory which is probably most analogous to the results of this section is the fact that every finite nilpotent group has a consistent polycyclic presentation. For more about polycyclic presentations, see Sims [27, 9.4].

8. ACKNOWLEDGEMENTS

The author was partly supported by a University of Michigan Rackham Summer Faculty Fellowship, and by the generosity of MSRI and its staff. (Research at MSRI is supported in part by NSF grant DMS-9022140.) The author would also like to thank J. H. Conway, G. Glauberman, and L. Schneps for their helpful remarks. Extraspecial thanks goes to R. L. Griess for making many helpful comments on an early draft of this paper, and for considerable help in formulating Definition 4.3 and proving Theorem 4.4.

REFERENCES

1. M. Aschbacher, *Finite group theory*, Cambridge Univ. Press, 1986.
2. ———, *Some multilinear forms with large isometry groups*, *Geom. Dedicata* **25** (1988), 417–465.
3. L. Bénéteau, *Commutative Moufang loops and related groupoids*, In Chein et al. [9], pp. 115–142.
4. R. H. Bruck, *Contributions to the theory of loops*, *Trans. AMS* **60** (1946), 245–354.
5. ———, *Some theorems on Moufang loops*, *Math. Z.* **73** (1960), 59–78.
6. ———, *A survey of binary systems*, *Ergebnisse der Mathematik und ihrer Grenzgebiete*, vol. 20, Springer-Verlag, New York, 1971.
7. O. Chein, *Examples and methods of construction*, In Chein et al. [9], pp. 27–93.
8. O. Chein and E. Goodaire, *Moufang loops with a unique nonidentity commutator (associator, square)*, *J. Alg.* **130** (1990), 369–384.
9. O. Chein, H. O. Pflugfelder, and J. D. H. Smith (eds.), *Quasigroups and loops: Theory and applications*, Sigma Series in Pure Mathematics, vol. 8, Berlin, Heldermann Verlag, 1990.
10. J. H. Conway, *A simple construction for the Fischer-Griess monster group*, *Invent. Math.* **79** (1985), 513–540.
11. J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *ATLAS of finite groups*, Oxford Univ. Press, 1985.
12. S. Eilenberg and S. MacLane, *Algebraic cohomology groups and loops*, *Duke J. Math.* **14** (1947), 435–463.
13. T. Evans, *Varieties of loops and quasigroups*, In Chein et al. [9], pp. 1–26.
14. G. Glauberman, *On loops of odd order II*, *J. Alg.* **8** (1968), 393–414.
15. G. Glauberman and C. R. B. Wright, *Nilpotence of finite Moufang 2-loops*, *J. Alg.* **8** (1968), 415–417.
16. R. L. Griess, *Code loops*, *J. Alg.* **100** (1986), 224–234.
17. ———, *Sporadic groups, code loops, and nonvanishing cohomology*, *J. Pure Appl. Alg.* **44** (1987), 191–214.
18. ———, *Code loops and a large finite group containing triality for D_4* , *Rend. Circ. Mat. Palermo* (2) Suppl. (1988), no. 19, 79–98.
19. ———, *A Moufang loop, the exceptional Jordan algebra, and a cubic form in 27 variables*, *J. Alg.* **131** (1990), 281–293.
20. T. Hsu, *Explicit constructions of code loops as centrally twisted products*, submitted.
21. P. M. Johnson, *Loops of nilpotence class two*, to appear in *J. Alg.*
22. M. Kitazume, *Code loops and even codes over F_4* , *J. Alg.* **118** (1988), 140–149.
23. S. MacLane, *Categories for the working mathematician*, Springer-Verlag, New York, 1971.
24. H. O. Pflugfelder, *Quasigroups and loops: Introduction*, Sigma Series in Pure Mathematics, vol. 7, Heldermann Verlag, Berlin, 1990.
25. D. K. Ray-Chaudhuri and R. Roth, *Hall triple systems and commutative Moufang exponent 3 loops: The case of nilpotence class 2*, *J. Comb. Thy. (A)* **36** (1984), 129–162.
26. T. M. Richardson, *Local subgroups of the Monster and odd code loops*, *Trans. AMS* **347** (1995), no. 5, 1453–1531.
27. C. C. Sims, *Computation with finitely presented groups*, Cambridge Univ. Press, 1994.
28. J. D. H. Smith, *A second grammar of associators*, *Math. Proc. Cam. Phil. Soc.* **84** (1978), 405–415.

29. ———, *Combinatorial characters of quasigroups*, Coding Theory and Design Theory (D. Ray-Chaudhuri, ed.), IMA Vols. in Math. and its Appls., vol. 20, Springer-Verlag, New York, 1990, pp. 163–187.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MICHIGAN, ANN ARBOR, MI 48109
E-mail address: `timhsu@math.lsa.umich.edu`