Journal of Geometry
Vol.30 (1987)

0047-2468/87/010001-11$1.50+0.20/0

SYLOW-LIKE THEOREMS IN GEOMETRY AND ALGEBRA

Thomas Q. Sibley

The notion of congruence provides a means to extend the Sylow theorems from group theory to a class of geometric structures called congruence spaces and to their corresponding loops. The extension of these results depends on the existence of a group acting transitively on the congruence space and preserving congruence. A partial ordering on the congruence spaces suggests a means to form all of these spaces from groups.

In $(R,+)$ we call segments $\overline{ab}$ and $\overline{cd}$ congruent, written $ab \equiv cd$, iff $|a-b| = |c-d|$ or, more explicitly, $|a+(-b)| = |c+(-d)|$. This geometrical notion can apply to groups and other algebraic structures given a suitable generalization of absolute value.

The work of Wolff [5] considers elementary properties of congruence for commutative groups and so is a special case of the present article. Further, this article differs significantly from the work of Kustaanheimo [3] on congruence, since this article does not depend on the pre-existing structure of an affine plane over a finite field. The congruence relation of Kustaanheimo can be obtained from the congruence relations presented here by suitable "lumping together" of absolute value classes. Such "lumping" is avoided here to ensure the generalization of the Sylow Theorems. However, the generalization of LaGrange's Theorem holds even then. The work of Chen and Teh [1] also sets extra conditions on the structures.

DEFINITION. A <u>congruence loop</u> $(L,*,1,^{-1},||)$, or just $(L,*)$, is a set L with a binary operation $*$, an identity and two unary

operations $^{-1}$ and $|\,|$ satisfying

a) $1*x = x = x*1$, $x*x^{-1} = 1 = x^{-1}*x$, $|(x*y)^{-1}| = |y^{-1}*x^{-1}|$.

b) $(L,*)$ forms a Latin square, i.e. every element appears exactly once in every row and column of the Cayley table of $*$.

c) $|x| = |x^{-1}| \in \{x,x^{-1}\}$.

DEFINITION. A <u>congruence space</u> is a set L with a relation $\equiv$ on $L\times L$ satisfying

a) $\equiv$ is an equivalence relation on $L\times L$, $ab\equiv ba$ and $(aa\equiv bc$ iff $b = c)$.

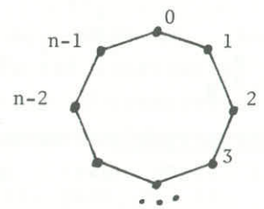
b) $(L,\equiv)$ is <u>regular</u>, i.e. every element $a\in L$ has the same number of incident edges ab in a given equivalence class of $\equiv$ as any other element of L has.

c) For all $a, b\in L$, $\{c: ab\equiv ac\}$ has at most two elements in it.

A congruence loop $(L,*)$ becomes a congruence space by defining $ab\equiv cd$ iff $|a*b^{-1}| = |c*d^{-1}|$. Sibley [4] proved that every congruence space can be obtained from one or more congruence loops using this definition of $\equiv$. The operation $|\,|$ serves here only to define the congruence on which the arguments are based. Hence, it will not matter whether $|x|$ is x or x^{-1}. Property c) in both definitions plays a central role in generalizing the Sylow theorems. This property guarantees that given a point and an equivalence class or "distance", there are at most two points at that "distance" from the given point. Further, the regularity of $(L,\equiv)$ means that in analyzing the geometric structure, we need only consider the structure around one element, which for us will be the identity. Then each "distance" corresponds to a value of $|\,|$. Congruence suggests the concept of an isometry, a mapping preserving $\equiv$ and so "distance".

DEFINITION. On $(L,\equiv)$, $\sigma: L\longrightarrow L$ is an <u>isometry</u> iff for all $x, y\in L$, $xy\equiv\sigma(x)\sigma(y)$. $I(L)$, or just I, is the group of isometries of $(L,\equiv)$. $(L,\equiv)$ is <u>isogonal</u> iff $I(L)$ is transitive on L. By extension, $(L,*)$ is also called isogonal in this case.

FACT. Every group is isogonal.
Indeed, the isometries $\sigma_a(x) = x*a$ form a regular subgroup of I which is isomorphic to the original group. The group $(Z/n,+)$ of the integers (mod n) appears in Lemma 6 below. Its congruence space looks like the vertices of a regular n-gon, as in the illustration at the right. To see this, note that $i+0 = i = (i+j)+(-j)$ and so $io\equiv(i+j)j$, even before applying $|\,|$. We will use this congruence space to describe certain orbits in congruence spaces.



EXAMPLE. For the sixteen units of the Cayley numbers, the usual multiplication gives a congruence loop, once we define $|e_a| = |-e_a| = e_a$, where e_a is any of the positive units except 1. This example generalizes to the 2^{n+1} units of the hyperCayley numbers, the 2^n-dimensional algebras over the reals. Although the multiplications for these structures are neither associative nor commutative, their congruence spaces are isogonal. Even more, the congruence spaces are isodigonal, as defined below. Proposition 2 shows this from the equality $|x*y| = |y*x|$ which says these spaces are "almost commutative". They are also "almost associative" in that $|x*(y*z)| = |(x*y)*z)|$ holds for all hyperCayley numbers.

DEFINITION. $(L,\equiv)$ is <u>isotoxal</u> iff for all $a, b, c, d\in L$, if $ab\equiv cd$, then there is $\sigma\in I(L):\sigma(\{a,b\}) = \{c,d\}$. (The isometry σ might switch the orientation of the "segments".) $(L,\equiv)$ is <u>isodigonal</u> iff for all $a, b, c, d\in L$, if $ab\equiv cd$, then there is $\sigma\in I(L):\sigma(a) = c$ and $\sigma(b) = d$. By extension, $(L,*)$ is isotoxal or isodigonal whenever $(L,\equiv)$ is.

REMARK. The properties of isotoxal and isodigonal require isometries which match any "segments" of the same "length". Isodigonal implies isotoxal, which in turn implies isogonal when we take $a = b$ and $c = d$.

<u>PROPOSITION 1</u>. If $(L,*)$ is a congruence loop and for all $a, x, y\in L$, $|(x*a)*(y*a)^{-1}| = |x*y^{-1}|$, then $(L,*)$ is isotoxal.

Thus every group is isotoxal.

PROOF. The condition in the proposition guarantees that $\sigma_a(x)=x*a$ is an isometry. Hence $(L,*)$ is isogonal. Let $ab\equiv cd$ and $\sigma_{a^{-1}}(b) = p$. One can readily check that either $\sigma_c\circ\sigma_{a^{-1}}$ or $\sigma_c\circ\sigma_{p^{-1}}\circ\sigma_{a^{-1}}$ is an isometry which carries $\{a,b\}$ to $\{c,d\}$. ∎

PROPOSITION 2. An isogonal loop $(L,*)$ is isodigonal iff for all $a,b\in L$, $|a*b| = |b*a|$.

PROOF. We have $|a*b| = |b*a|$ iff $|a*b^{-1}| = |b^{-1}*a|$ iff $ab\equiv b^{-1}a^{-1}$ iff $\mu(x) = x^{-1}$ is an isometry. One can readily check that this together with the isogonality of $(L,*)$ is equivalent to isodigonality. ∎

A subloop $(H,*)$ of $(L,*)$ is a subset closed under the operations $*$, $^{-1}$ and $|\ |$. There is a corresponding closure under $\equiv$ for the congruence space.

DEFINITION. $(H,\equiv)$ is a subspace of $(L,\equiv)$ iff for all a, b, $c\in H$ and $d\in L$, if $ab\equiv cd$, then $d\in H$.

LEMMA 3. A subspace with 1 in it is a subloop. Conversely, a finite subloop is a subspace.

The proof of this elaborates on the definitions of congruence loops and spaces. The congruence relation does not single out the special element 1. The subspaces without 1 are like cosets of the corresponding subloops.

THEOREM 4 (Extended LaGrange). Let $(L,\equiv)$ be a finite isogonal space and $(H,\equiv)$ be a subspace. Then $|H|$ divides $|L|$. Similarly, if $(H,*)$ is a subloop of a finite isogonal loop $(L,*)$, then $|H|$ divides $|L|$.

SKETCH OF PROOF. The isometries of $(L,\equiv)$ must take a subspace to a congruent set which is therefore another subspace by closure. Again because of closure, a subspace and its image

under an isometry are either disjoint or identical. Thus these congruent subspaces partition the whole space into equally sized pieces, extending LaGrange's Theorem to these spaces. Lemma 3 immediately extends this to the loops. ∎

Suppose $x\in H\subset L$ and $\sigma\in G$, a subgroup of $I = I(L)$. Then as usual, xG is the orbit of x under G, I_x is the subgroup of isometries leaving x fixed, I_H is the subgroup of isometries taking H onto H and $\langle\sigma\rangle$ is the subgroup generated by σ.

LEMMA 5. If $\sigma\in I(L)$ and σ has a fixed point, then σ^2 is the identity. Hence for all $a\in L$, I_a is a Boolean group.

PROOF. By the definition of a congruence space, $(L,\equiv)$ is regular. Hence any point can be used as the identity, so we can pick the fixed point of σ to be 1. For all $x\in L$, $x1\equiv\sigma(x)1$. Hence $\sigma(x) = x$ or $\sigma(x) = x^{-1}$ by property c) in the definition of a congruence loop. Either way, σ^2 is the identity. Since this holds in general, every element of I_a is of order 2. ∎

LEMMA 6. Let $\sigma\in I(L)$ be an isometry of odd order n. Then $(1\langle\sigma\rangle,\equiv)$ is a subspace isomorphic to $(Z/n,\equiv)$.

PROOF. The orbit $1\langle\sigma\rangle = \{\sigma^k(1) : 0\leq k<n\}$. By Lemma 5, $1\langle\sigma\rangle$ has n points. Since σ^k is an isometry, $\sigma^i(1)1\equiv\sigma^{i+k}(1)\sigma^k(1)$. This corresponds to $il\equiv i+kk$ in $(Z/n,\equiv)$ under the bijection taking $\sigma^k(1)$ to k. The odd order of $1\langle\sigma\rangle$ means that every "distance" inside of it appears twice coming from every point. Since that is the most part c) of the definition of a congruence space allows, $1\langle\sigma\rangle$ must be closed. ∎

It is well known that if I is transitive on L, then all the I_x are conjugate and $|I_x|\ |L| = |I(L)|$. Theorem 7 below uses isogonality to extend the Sylow theorems for $p\neq 2$ to congruence spaces. The case $p=2$ requires the stronger property of isotoxal, as shown in Theorem 8. Theorem 9 simply transfers these results to the corresponding loops.

THEOREM 7 (Extended Sylow, p≠2). Suppose $(L,\equiv)$ is a finite isogonal space with $p^k m$ elements, p an odd prime not dividing m. Then there is a subspace having p^j elements for $0\leq j\leq k$. Further, the number of subspaces of order p^k which contain a given element divides the order of L and is congruent to 1 (mod p).

PROOF. If $|L| = p^k m$, then Lemma 5 shows $|I(L)| = 2^i p^k m$, for some $i\leq 0$. By the Sylow Theorems for groups, there is a subgroup G of I(L) with $|G| = p^k$. By Lemma 5, the only isometry in G with a fixed point is the identity, because p is odd. Hence for all $x\in L$, xG must have p^k elements. We may assume that $(L,\equiv)$ comes from a finite isogonal loop. We will first show 1G is a subspace with p^k elements.

Let a, b, $c\in 1G$ and $ab\equiv cd$. G is clearly transitive on 1G so there are $\sigma,\tau\in G$ such that $\sigma(a) = 1 = \tau(c)$. Call $\sigma(b) = x$; then $x\in 1G$. Thus there is $\rho\in G$ such that $\rho(x) = 1$. Because ρ is of odd order, $\rho(1)\neq x$. By part c) of the definition of a congruence loop, $\rho(1) = x^{-1}$, ensuring $x^{-1}\in 1G$. Since $\tau(d)$ is either x or x^{-1}, $d = \tau^{-1}(\tau(d))\in 1G$, showing closure.

The above argument holds for any subgroup of odd order. Thus, the subgroups of I(L) with order p^j, $0\leq j\leq k$, give subspaces of those orders which contain 1. Since I is transitive, this holds for every point.

It remains to consider the number of subspaces with p^k elements. By the Sylow Theorems for groups, the number of Sylow p-subgroups of I divides $|I|$ and is congruent to 1 (mod p). We will next show that each of these subgroups give a different subspace containing 1.

Suppose G and H are two Sylow p-subgroups of I and that $\Upsilon = 1G = 1H$. We need to show G = H. G, H and I_1 are subgroups of I_Υ. Every element of I_Υ can be written as $\tau\circ\sigma$ where $\tau\in I_1$ and $\sigma\in G$. To show G = H, it suffices to show that

if neither τ nor σ is the identity, then $\tau\circ\sigma$ is of even order. Lemma 6 shows $1\langle\sigma\rangle$ is a subspace isomorphic to $(Z/n,\equiv)$, where n is the order of σ. Clearly, $\tau,\sigma\in I_{1\langle\sigma\rangle}$ and on $1\langle\sigma\rangle$, $I_{1\langle\sigma\rangle}$ acts like the dihedral group D_n. Now $\tau(1) = 1 \neq\sigma(1)$. There are two cases to consider, depending on whether $\tau(\sigma(1))$ is $\sigma(1)$ or $\sigma(1)^{-1}$.

CASE 1. $\tau(\sigma(1)) = \sigma(1)$. Then τ leaves $1\langle\sigma\rangle$ pointwise fixed. Since τ is not the identity, there is some $z\notin 1\langle\sigma\rangle$ which τ moves. Then $z\langle\tau,\sigma\rangle$, has 2n elements in it. Further, $\tau\circ\sigma$ must be of even order.

CASE 2. $\tau(\sigma(1)) = \sigma(1)^{-1} = \sigma^{-1}(1)$. Then τ and σ generate the dihedral group for $1\langle\sigma\rangle$. Thus, $\tau\circ\sigma$ is of even order.

In either case, $\tau\circ\sigma$ is of even order. Hence the only elements of odd order are already in G. Thus $H\subset G$. Since $|G| = |H|$, G = H. This shows that different Sylow p-subgroups give different subspaces containing 1. Further, every subspace S containing 1 among its p^k elements has $|I(S)| = 2^i p^k$. Hence every such subspace comes from some Sylow p-subgroup. This means the number of subspaces with p^k elements, including 1, equals the number of Sylow p-subgroups of I(L). Since this number divides $|I| = 2^i p^k m$ and is congruent to 1 (mod p), we need only show this number also divides $|L| = p^k m$. But each Sylow p-subgroup G is embedded in a distinct subgroup I_{1G} with $2^i p^k$ elements. The total number of these subgroups divides the index of each I_{1G}, i.e. m, and so divides $|L|$. ∎

THEOREM 8 (Extended Sylow, all prime p). Let $(L,\equiv)$ be an isotoxal space with $|L| = p^k m$, p any prime not dividing m. Then there is a subspace having p^j elements for $0\leq j\leq k$. Further, the number of subspaces of order p^k which contain a given element divides the order of L and is congruent to 1 (mod p).

PROOF. We need only consider the case p = 2, since isotoxal implies isogonal. So suppose $|L| = 2^k m$ and $|I_1| = 2^i$. Then

$|I(L)| = 2^{i+k}m$, m odd. By the Sylow Theorems for groups, there is a group G with $|G| = 2^{i+k}$. For all $x \in L$, $|I_x \cap G|$ is a power of 2 and $|I_x \cap G| \leq 2^i$. Further, $|I_x \cap G|\,|xG| = |G| = 2^{i+k}$. This means that for each x, $|xG|$ is a multiple of 2^k. The xG partition L, which has $2^k m$ elements. Since m is odd, at least one xG has exactly 2^k elements and for this x, $|I_x \cap G| = 2^i$. We may assume that $1G$ has exactly 2^k elements, since otherwise we could use an appropriate subspace conjugate to G. Claim: $1G$ is a subspace.

To show closure, let $a, b, c \in 1G$ and $ab \equiv cd$. As in Theorem 7, there are $\sigma, \tau \in G$ such that $\sigma(a) = 1 = \tau(c)$. Now $ab \equiv cd \equiv 1\sigma(b) \equiv 1\tau(d)$. Thus $\tau(d)$ is either $\sigma(b)$ or $\sigma(b)^{-1}$. As in Theorem 7, we have $\sigma(b) \in 1G$ and we need to show $\sigma(b)^{-1} \in 1G$ in order to use the previous argument that $d = \tau^{-1}(\tau(d)) \in 1G$. But $1\sigma(b) \equiv 1\sigma(b)^{-1}$ and L is isotoxal, so there is an isometry taking either 1 or $\sigma(b)$ to $\sigma(b)^{-1}$. Further, that isometry is in G because the other element, $\sigma(b)$ or 1, goes to 1. Hence $\sigma(b)^{-1} \in 1G$, which shows the claim that $1G$ is a subspace.

In a similar manner, we can show there are subspaces of orders 2^j for $0 \leq j \leq k$.

It remains to consider the total number of subspaces H with 2^k elements, including 1. Note that $|I_H| = 2^{i+k}$ since $|I_H| = |I_1|\,|H|$. Thus every such subspace H comes from some Sylow p-subgroup G as $H = 1G$. Unfortunately, some Sylow 2-subgroups could produce the same subspace and some could give no subspace containing 1 at all in this way.

The reasoning of the paragraphs showing closure entails that every Sylow 2-subgroup produces one subspace S with 2^k elements, even though this subspace might not contain 1. Since the images of S under $I(L)$ partition L into congruent subspaces, there is a subspace, say S_G, which contains 1. Then $S_G \subset 1G$ and $|S_G| = 2^k$. Then there must be some Sylow 2-subgroup G^* such that $S_G = 1G^*$. All of the Sylow 2-subgroups are conjugate, so the number of such subgroups G which have same

subspace $1G^* = S_G$ is the same for all these subspaces containing 1. Further, as in Theorem 7, every subspace with 2^k elements, including 1, comes from a Sylow 2-subgroup. Hence the number of such subspaces divides the number of Sylow 2-subgroups, which divides $2^{i+k}m$ and is congruent to $1 \pmod 2$. Since this number is odd, it must divide m and so $|L|$. Finally, $I(L)$ is transitive, so all of this holds for all points, not just 1. ∎

THEOREM 9 (Extended Sylow for Loops). If $(L,*)$ is an isogonal loop with $p^k m$ elements, p an odd prime not dividing m, then there is a subloop having p^j elements for $0 \leq j \leq k$ and the number of subloops of order p^k divides the order of L and is congruent to $1 \pmod p$. The above holds for $p = 2$ provided $(L,*)$ is isotoxal.

The proof of Theorem 9 simply applies Lemma 3 to Theorems 7 and 8. ∎

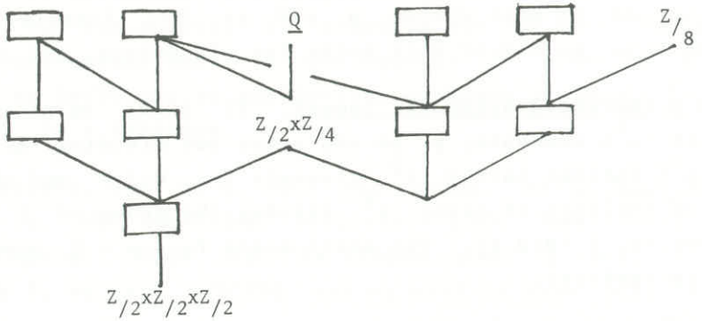
Unfortunately, just because a loop has only one "Sylow p-subloop" does not imply that that subloop will be "normal", i.e. the kernel of a homomorphism. There are also counter-examples which show that the case $p = 2$ for the extended Sylow Theorems need not hold if the loop (or space) is only isogonal. Further, it is not clear how to extend the class equation to these loops. Without associativity, $\{(x*y)*x^{-1} : x \in L\}$ need not equal $\{x*(y*x^{-1}) : x \in L\}$.

How much more general are isogonal loops than groups? I conjecture that all isogonal spaces (and so loops) are related to groups using a partial ordering on spaces of the same order.

DEFINITION. $(L,\equiv) \leqq (L,\equiv')$ iff $ab \equiv cd$ implies $ab \equiv' cd$. By extension, $(L,*) \leqq (L,*')$ iff this relation holds for $\equiv$ and $\equiv'$.

The diagram below shows the partial ordering for the isogonal spaces of order 8 which I have found. In addition to those formed from the five groups, I have found nine others formed from loops and represented by the boxes in the diagram. The symbol $\underline{Q}$ represents the group of quaternions. The different layers in the

diagram correspond to the number of elements of order 2 in the loop. In going from one loop or space up to one above it, two elements of order 2 turn into inverses of one another. This corresponds in the spaces to having the two different equivalence classes of edges become identified.



PROPOSITION 10. If $(L,\equiv) \leqq (L,\equiv')$, then $I(L,\equiv)$ is a subgroup of $I(L,\equiv')$. Hence, if $(L,*)$ is isogonal, then $(L,*')$ is also isogonal.

CONJECTURE All isogonal loops dominate some group under $\leqq$. Equivalently, if $I(L)$ is transitive, then it has a regular subgroup.

I have shown this conjecture holds if the order of the loop is an odd number or twice a prime number. This conjecture would allow the description of all isogonal loops from groups by turning various pairs of elements of order 2 into inverses of one another. The next conjecture would generalize the Fundamental Theorem of Finitely Generated Abelian Groups since the property $|a*b| = |b*a|$ for isodigonal loops generalizes the commutative property for groups.

CONJECTURE. $(L,\equiv)$ is isodigonal iff $(L,\equiv)$ is isomorphic to the congruence space of a commutative group or of $(Z_2)^k \times H$ for some k, where H is the loop of units of the hyperCayley numbers of some dimension.

Isogonal spaces and loops clearly have internal structures quite similar to groups. The geometric structure of congruence provides the key to generalizing groups.

REFERENCES

[1] CHEN, C. C. and H. H. Teh, "Construction of point-colour-symmetric graphs", J. Combin. Th. (B) 27 (1979),160-167.

[2] HOLTON, D. A. and SHEEHAN, J. "On Sylow graphs", J. Austral. Math. Soc. (A) 28 (1979), 27-38.

[3] KUSTAANHEIMO, P., "On the relation of congruence in finite geometries", Math. Scand. 5 (1957), 197-201.

[4] SIBLEY, T. Q., "Equidistance relations - a new bridge between geometric and algebraic structures", Cuttington Research Journal, Monrovia, Liberia, 1 (1982), 19-25.

[5] WOLFF, " 'Kreisel' ", Elemente der Mathermatik, 31 (1976) #6, 141-145.

Department of Mathematics
Science Center
St. John's University
Collegeville, MN 56321

(Eingegangen am 24. Juli 1984)

(Revidierte Form am 22. Juli 1986)