Non-Desarguesian planes and weak associativity

R. P. BURN

During the 19th century various criticisms of Euclid's geometry emerged and alternative axiom systems were constructed. That of David Hilbert ([1], 1899) paid particular attention to the independence of the axioms, and it is his insights which have shaped many of the further developments during the 20th century.

We can, from his insights, define an *affine plane* as a set of *points*, with distinguished subsets called lines such that

Axiom 1: Given two distinct points, there is a unique line containing them both.

Axiom 2: Given a line L and a point, p, not contained in L, there is a unique line containing p which does not intersect L.

Axiom 3: There exist at least three points, not belonging to the same line.

From axiom 1 we see that two distinct lines have at most one point in common.

From these axioms we can define an equivalence relation // (parallelism) on the lines of a plane by $L // M$ when $L = M$ or when L does not intersect M, and we call an equivalence class under this relation a *direction*. We can prove that every line contains the same number of points (at least 2), but there are no numbers which automatically follow, we just have points. So we use the points of one line (one of the lines of axiom 3) and the three directions, to label all the points of the plane and to build up operations of + and . . From axiom 3 there is a line with at least two points on it, which we label 0 and 1, whose only properties initially are that $0 \neq 1$, and we use x and y as labels for arbitrary points on that line. We can construct a binary operation (+) on the points of this line using the three directions of axiom 3 as in Figure 1. Both operations are defined on the points of this line.

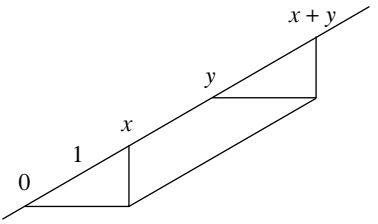


FIGURE 1

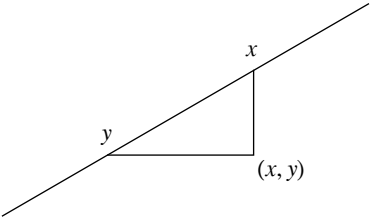


FIGURE 2

https://doi.org/10.1017/mag.2017.127 Published online by Cambridge University Press

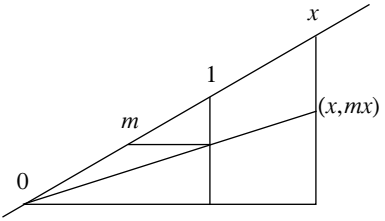


FIGURE 3

Notice $x + 0 = 0 + x = x$, and in the equation $x + y = z$, any two of the variables determines the third uniquely. In Figure 2 we show how the points of one line may be used to label all the points of the plane with ordered pairs. With coordinatisation, the point x becomes (x, x). Then we use this coordinatisation to construct another binary operation (.), as shown in Figure 3. Notice $0.x = x.0 = 0$, and $1.x = x.1 = x$ and in the equation y = m.x, any two of the variables determines the third uniquely.

If we denote the line whose points provide the coordinates by L, $(L, +)$ has a two-sided identity 0, and two elements determine the third in $x + y = z$. Likewise $(L\backslash\{0\}, .)$ has a two-sided identity 1, and two elements determine the third in $x.y = z$. The similar algebra of these two structures is given the name 'loop', intentionally reminiscent of 'group', but without any mention of associativity.

A long chapter in Hilbert (see [1]) is devoted to Desargues' theorem. Hilbert showed that if Desargues' theorem is added to the axioms 1, 2 and 3 above, then $(L, +, .)$ is a (not necessarily commutative) field. And if the existence of *planes* of incidence are adjoined to the axioms above, then Desargues' theorem is guaranteed. He established the independence of the 'Desargues' theorem' axiom in the plane by constructing an affine plane in which this theorem fails, with an elliptic bubble in the middle of the real plane. Hilbert also showed that if both Desargues' theorem and Pappus' theorem are adjoined to the axioms for an affine plane, then $(L, +, .)$ must be a commutative field. Actually Pappus' theorem implies Desargues' theorem in an affine plane as shown by Hessenberg in 1905; and also in 1905 Wedderburn proved that a finite Desarguesian plane is Pappian.

In a finite plane, each line contains the same number of points (the order of the plane) and the whole plane contains the square of this number of points. The only planes of order 2, 3, 4, 5, 7 and 8 are Pappian. There is no plane of order 6, and there are at least four different planes of order 9. All known finite planes have order the power of a prime number.

During the 1930s Ruth Moufang explored the consequences of assuming restricted forms of Desargues' theorem in an affine plane, by requiring that a particular point of the Desargues configuration lie on a particular line of that configuration, and found that $(L, +)$ must be an abelian group, that $(L, +, .)$ has both distributive laws, but $(L, .)$ is not associative or commutative. Multiplication satisfied some restricted forms of

https://doi.org/10.1017/mag.2017.127 Published online by Cambridge University Press

associativity, notably $a(ab) = a^2b$, $a(ba) = (ab)a$ and $(ab)b = ab^2$, which became known as 'alternative' laws; multiplicative inverses were two-sided, and the right and left inverse properties $a^{-1}(ab) = b$, $(ab)b^{-1} = a$, were valid. A weak form of associativity $a[b(cb)] = [(ab)c]b$, now known as a Moufang law, holds in these planes and implies all these other laws. The algebra here is known as an alternative field, of which the Octonians and Cayley-Dickson algebras are examples. For details of Moufang's work see [2]. It was also proved in the 1930s that a finite alternative field was a commutative field (see [3, p. 376, Theorem 20.6.2]).

Although these weakened forms of associativity arose in infinite loops, their identification has led to their investigation in general, and extensive studies of loops with these properties have been made (see [4, 5]). A finite loop can be exhibited using a latin square, with the loop identity in the first row and column, and the loop operation exhibited by presuming that the element in row i and column j is the 'product' of the ith element in column 1 and the jth element in row 1. It is convenient to make the first row the mirror image of the first column in the leading diagonal.

1			b	
a			ab	

Here is a Table which has been used as a problem in the early stages of a course on groups.

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

TABLE 1

It is easy enough to recognise the latin square property, and to see that there is a two-sided identity. Moreover because that identity appears down the main diagonal we can be sure that inverses, if there are any, are two-sided. But each element would have to have order 2, and that is impossible in a group of order 5 by Lagrange's theorem.

Which of the group axioms must fail here? Closure, a two-sided identity, and two-sided inverses are easy to check, so the only axiom remaining is the associative law, and behold $2(2.3) = 2.4 = 5$, while

https://doi.org/10.1017/mag.2017.127 Published online by Cambridge University Press

$(2.2)3 = 1.3 = 3$. So not just associativity, but even the left alternative law fails.

The device we will use to analyse properties of loops will be that which Cayley used to show that an abstract group is isomorphic to a permutation group, namely that of right (or left) multiplications, mappings of the loop to itself of the form $R_a : x \to x.a$ (or $L_a : x \to a.x$).

group table				
1	2	3	4	$R_1 = (1)(2)(3)(4)$
2	4	1	3	$R_2 = (1243)$
3	1	4	2	$R_3 = (1342)$
4	3	2	1	$R_4 = (14)(23)$

For a group, $xR_{ab} = x(ab) = (xa)b = xR_aR_b$, so that associativity is equivalent to $R_{ab} = R_aR_b$. Associativity in a loop is equivalent to the closure of right multiplications. (Note that $1R_aR_b = ab$, whether the loop is associative or not.) For the right multiplications of any loop, only R_1 can fix an element.

To see the power of this method, consider Table 2. Here the Table bears a remarkable resemblance to the group table of the non-commutative group of order 6. But look at the right multiplications $R_4R_4 = (23)(56)$, which is not a right multiplication. So the loop of Table 2 is not associative and $2(4.4) = 2$, while $(2.4)4 = 3$.

1	2	3	4	5	6	$R_1 = (1)(2)(3)(4)(5)(6)$
2	3	1	5	6	4	$R_2 = (123)(465)$
3	1	2	6	4	5	$R_3 = (132)(465)$
4	6	5	1	2	3	$R_4 = (14)(2536)$
5	4	6	3	1	2	$R_5 = (15)(2634)$
6	5	4	2	3	1	$R_6 = (16)(2435)$

TABLE 2

1	2	3	4	5	6	$R_1 = (1)(2)(3)(4)(5)(6)$
2	3	1	5	6	4	$R_2 = (123)(465)$
3	1	2	6	4	5	$R_3 = (132)(465)$
4	6	5	1	2	3	$R_4 = (142536)$
5	4	6	3	1	2	$R_5 = (152634)$
6	5	4	2	3	1	$R_6 = (162435)$

TABLE 3

https://doi.org/10.1017/mag.2017.127 Published online by Cambridge University Press

In Table 3, the square of each right multiplication is again a right multiplication. In fact $R_aR_a = R_{aa}$. This implies that in this loop $(ba)a = b(aa)$, the *right alternative law* holds, however $R_4R_5 = (465)$, which is not a right multiplication, so this loop is not associative.

1	2	3	4	5	6	$R_1 = (1)(2)(3)(4)(5)(6)$
2	1	6	5	4	3	$R_2 = (12)(34)(56)$
3	4	1	6	2	5	$R_3 = (13)(26)(45)$
4	3	5	1	6	2	$R_4 = (14)(25)(36)$
5	6	4	2	3	1	$R_5 = (153246)$
6	5	2	3	1	4	$R_6 = (164235)$

TABLE 4

In Table 4, each right multiplication has an inverse which is again a right multiplication. That is to say, $R_a^{-1} = R_{a'}$, so $R_aR_{a'} = R_1$. This gives $(ba)a' = b$, the *right inverse property*. Note that $(a'a)a' = a'$, so inverses are two-sided. Notice also that $R_5R_5 = (134)(265)$ which is not a right multiplication, so the right alternative law fails here, making the loop non-associative.

1	2	3	4	5	6	$R_1 = (1)(2)(3)(4)(5)(6)$	$L_1 = (1)(2)(3)(4)(5)(6)$
2	1	5	6	4	3	$R_2 = (12)(34)(56)$	$L_2 = (12)(3456)$
3	4	1	5	6	2	$R_3 = (13)(25)(46)$	$L_3 = (13)(2456)$
4	3	6	1	2	5	$R_4 = (14)(26)(35)$	$L_4 = (14)(2365)$
5	6	2	3	1	4	$R_5 = (15)(24)(36)$	$L_5 = (15)(2643)$
6	5	4	2	3	1	$R_6 = (16)(23)(45)$	$L_6 = (16)(2534)$

TABLE 5

In Table 5, since all the right multiplications are of order 2, each is its own inverse and so the right inverse property holds. Moreover the square of each right multiplication is the identity, so again the right alternative law holds. However, $R_2R_3 = (154)(236)$ which is not a right multiplication, so the loop is not associative. In general, if the table of a loop is transposed about its main diagonal, properties of right multiplications in the original loop give analogous properties of left multiplications in the transposed loop. In this particular loop each right multiplication commutes with its corresponding left multiplication, so we have $R_aL_a = L_aR_a$, or in the loop $a(ba) = (ab)a$, the *medial alternative law*.

Shortly after Moufang found the identity $a[b(cb)] = [(ab)c]b$, G. Bol (see [6]) identified the weaker identity $a[(bc)b] = [(ab)c]b$ now known as the *right Bol law*, and its *left* counterpart $[b(cb)]a = b[c(ba)]$. By putting $c = 1$ in the right Bol law we obtain the right alternative law,

https://doi.org/10.1017/mag.2017.127 Published online by Cambridge University Press

and by choosing c so that $bc = 1$, the right Bol law gives $ab = [(ab)c]b$, and so $a = (ab)c$, the right inverse property. Similarly the left Bol law implies the left alternative law and the left inverse property. The right Bol law may be expressed as $aR_{bc.b} = aR_bR_cR_b$ and so the right Bol law is equivalent to the condition that $R_bR_cR_b$ is a right multiplication (note that $1R_bR_cR_b = (bc)b$). Similarly the left Bol law is equivalent to the condition that $L_bL_cL_b$ is a left multiplication. The smallest non-associative loop satisfying either Bol law has 8 elements (see [7]).

Both right and left Bol laws together imply the Moufang law. We can show this since the left Bol law implies the left inverse property, so L_a^{-1} is a left multiplication. Now $xL_aR_aL_a^{-1} = a^{-1}[(ax)a]$ and with the right Bol law is equal to $[(a^{-1}a)x]a = xa = xR_a$. So $L_aR_aL_a^{-1} = R_a$ and $L_aR_a = R_aL_a$, establishing the medial alternative law. The medial alternative law applied to the right Bol law gives the Moufang law.

Conversely the Moufang law $a[b(cb)] = [(ab)c]b$ implies both the Bol laws. Putting $a = 1$, we get the medial alternative law, and when that is applied to the left-hand side of the identity we get the right Bol law. This implies the right inverse property and hence inverses are two-sided. Putting $a = b^{-1}$ in the Moufang law gives $b^{-1}[b(cb)] = cb$, which is the left inverse property.

The left inverse property gives $a^{-1}(ab) = b$, and so $[a^{-1}(ab)](ab)^{-1} = b(ab)^{-1}$.

Now using the right inverse property $a^{-1} = b(ab)^{-1}$, and so, using the left inverse property again, $b^{-1}a^{-1} = (ab)^{-1}$. Using this identity to invert the terms of the right Bol law gives the left Bol law so the Moufang law is in fact equivalent to both the Bol laws together. The smallest non-associative loop satisfying the Moufang law has 12 elements (see [8]).

We may relate properties of $(L, +, .)$ to geometrical properties of the plane as follows, assuming that lines have the form $x = a$ or $y = mx + c$, denoted by $[a]$ and $[m, c]$ respectively.

If $(L, +)$ is a group then the plane admits translations: $(x, y) \to (x, y + b), [m, c] \to [m, c + b]$.

If, in addition, $(L, +, .)$ has a left distributive law, the plane admits translations: $(x, y) \to (x + a, y), [m, c] \to [m, ma + c]$, and with both these sets of translations the plane admits translations taking any point to any other point. These two groups of translations are enough to show that the group which they generate together is abelian, (see [9, chapter 3]).

If in addition, $(L\backslash\{0\}, .)$ has the left inverse property, the plane admits the reflection: $(x, y) \to (y, x), [m, c] \to [m^{-1}, -(m^{-1}c)], [0] \leftrightarrow [0, 0]$.

If further $(L\backslash\{0\}, .)$ satisfies the left Bol law, every choice of the line L leads to the left inverse property so that the plane admits reflections in every axis $y = mx$, (see [10]).

If $(L, +)$ is an abelian group and $(L, +, .)$ has a right distributive law, then the plane admits shears of the form $(x, y) \to (x, y + ax + b)$, $[m, c] \to [m + a, c + b]$.

https://doi.org/10.1017/mag.2017.127 Published online by Cambridge University Press

There is a geometrical relation between left and right properties of multiplication. This can be described if an additional line ('at infinity') is added to our original affine plane on which each point is common to all the lines of one affine direction, to make a projective plane. Axiom 1 is retained, but Axiom 2 must then change to 'any two distinct lines intersect at a unique point'. The close parallel between Axiom 1 and our new Axiom 2, allows us to construct a new projective plane by taking each point of the new plane as a line of the original, each line of the new plan as a point of the original and reversing inclusion. Axiom 3 needs to posit a quadrilateral with no three points collinear in this context. This new plane is the dual of the original projective plane. Properties of left multiplication in one projective plane may often be recognised as properties of right multiplication in the dual plane, and vice versa. We found a reflection $(x, y) \to (y, x)$ when $(L, +)$ is an abelian group, $(L, +, .)$ has the left distributive law and $(L\backslash\{0\}, .)$ the left inverse property. In the dual plane, we have $(L, +)$ an abelian group, the right distributive law and the right inverse property, and the following (oblique) reflection: $(x, y) \to (x^{-1}, yx^{-1})$, $[m, c] \to [c, m]$ and $[0] \leftrightarrow [\infty]$, which fixes all points on the line [1].

References

1. D. Hilbert, *Grundlagen der Geometrie*; English translation by G. J. Townsend, *The foundations of geometry*, Open Court, Chicago (1902).
2. G. Pickert, *Projective Ebenen*, Springer (1955).
3. M. Hall, *The theory of groups*, Macmillan (1959).
4. R. H. Bruck, *A survey of binary systems*, Springer (1966).
5. H. O. Pflugfelder, *Quasi-groups and loops*, Heldermann (1990).
6. G. Bol, Gewebe und Gruppen, *Math.Ann.* **114** (1937) pp. 414-431.
7. R. P. Burn, Finite Bol loops, *Math. Proc. Camb. Phil. Soc*, **84** (1978) pp. 377-385.
8. O. Chein and H. O. Pflugfelder, The smallest Moufang loop, *Arch. Math.* **22** (1971) pp. 573-576.
9. R. P. Burn, *Deductive transformation geometry*, Cambridge (1975).
10. R. P. Burn, Bol quasi-fields and Pappus' theorem, *Math. Zeitschrift*, **105** (1968) pp. 351-364.

10.1017/mag.2017.127

R. P. BURN
Sunnyside, Barrack Road, Exeter EX2 6AB
e-mail: *rpburn@exeter.ac.uk*

Views on the *Gazette*

The Editorial team would welcome feedback on the *Gazette*. Perhaps we should set up a 'Panel' and seek comment on a regular basis? If you have views on this suggestion or would like to be involved please e-mail:

Bill Richardson *Editor-in-Chief@m-a.org.uk*

https://doi.org/10.1017/mag.2017.127 Published online by Cambridge University Press