THE DISTRIBUTIVE LAWS FOR HOMOGENEOUS LINEAR SYSTEMS

BY A. A. BENNETT

The terminology of addition and of multiplication may be readily extended to apply to homogeneous linear systems or to their geometrical interpretations, linear projective spaces. The product ab of two linear spaces a and b, denotes the intersection or greatest linear space common to the two given spaces. It is thus the logical product of the spaces. The sum $a+b$ denotes the join or least linear space containing the given spaces as subspaces. It is analogous to the logical sum but is distinguished from it by the fact that $a+b$ will in general contain also points which are in neither a nor b. Addition is commutative as is also multiplication. One has $a+a=a$, and $aa=a$, etc. Many of the formulas established for the algebra of logic hold here also.*

An essential feature of the algebra of logic is the following pair of relations, the first of which is applicable to ordinary algebra:

$$\text{I} \qquad a(b+c) = ab + ac,$$

$$\text{II} \qquad a + bc = (a+b)(a+c).$$

If I holds a is said to be distributive with respect to b and c in the first sense, if II holds, in the second sense. The proofs of these when based upon other postulates are not trivial.† For the case of even a one-dimensional projective space, these distributive relations fail to hold. Indeed if a, b, and c denote three distinct points of a line, and 0 denotes the null space, we have $b+c=$entire line, $a(b+c)=a$, but $ab=0$, $ac=0$, $ab+ac=0$. Hence $a(b+c)\neq ab+ac$. Similarly $a+bc=a$, but $(a+b)\ (a+c)$ $=$entire line.

While from two elements a and b, one can generate by addition and multiplication only the closed set ab, a, b, $a+b$, yet

* See A. A. Bennett, *Semi-serial order*, American Mathematical Monthly, vol. 37 (1930), pp. 418–423.

† See E. V. Huntington, *Postulates for the algebra of logic*, Transactions of this Society, vol. 5 (1904), pp. 288–309, particularly Peirce's proof, pp. 300–302.

from three elements, addition and multiplication yield in general an unlimited system. A special "distributive" system of 17 elements closed under addition and multiplication due to restrictions imposed upon a, b, c, is the following:

$$abc,\ ab,\ ac,\ bc,\ a(b+c),\ b(a+c),\ c(a+b),\ a,\ b,\ c,$$
$$a+bc,\ b+ac,\ c+ab,\ a+b,\ a+c,\ b+c,\ a+b+c,$$

where each of the three elements a, b, and c is distributive with respect to the other two in both senses, which as will be seen amounts to but one condition in ordinary spaces. The fact that it is actually closed under both operations may be verified by routine computation. The system is capable of realization by linear spaces in an unlimited number of ways. The following inequalities are readily proved from first principles:

$$\text{I}' \qquad a(b+c) \geqq ab+ac,$$
$$\text{II}' \qquad a+bc \leqq (a+b)(a+c),$$

but such inequalities do not tell the whole story.

In the formal algebra of logic there is no need of assuming the existence of prime non-zero quantities of such a sort that if p is a prime element (hence, $\neq 0$) and if $x<p$, then necessarily $x=0$. The existence of such prime elements, which serve as points in the geometrical interpretation, makes possible in the theory of spaces of at most a countable number of dimensions, a method of proof by mathematical induction, quite foreign in nature to the purely formal relations in the algebra of logic. In practice the theory of linear spaces of more than two dimensions is usually built up by use of mathematical induction from the theorems concerning collinear and coplanar points by use of transversality properties.

The following two theorems might appear to have a formal character independent of the existence of points. They are found to hold true for subspaces of any space of a countable number of dimensions, but no direct formal proof without the intervention of postulates comparable to that of the existence of points seems to be available.

THEOREM 1. *If three linear spaces a, b, and c are such that a is distributive with respect to b and c in one sense, it is distributive in both senses.*

THEOREM 2. *If three linear spaces a, b, and c are such that a is distributive with respect to b and c, then b is distributive with respect to a and c.*

These theorems will be proved only for spaces which contain points, although without the use of mathematical induction. The following property of points will be used.

PROPERTY. *If a, b, and c are non-empty spaces and x is a point of a that is in neither b nor c, but is in $b+c$, then there is a point y of b, and a point z of c, such that x is in $y+z$.*

Duality will not be available for if the total space be of infinitely many dimensions, it is not necessary to assume that the dual of a point has a meaning, although this is usually the case.

Two cases of the relations among a, b, c, will be considered.

CASE A. There exist three points x, y, z, such that simultaneously

$$(1)\quad ax = x, \quad (2)\quad x(ab + ac) = 0, \quad (3)\quad by = y,$$

$$(4)\quad y(ab + bc) = 0, \quad (5)\quad cz = z, \quad (6)\quad z(ac + bc) = 0$$

$$(7)\quad xy = xz = yz = 0, \quad (8)\quad x + y = x + z = y + z.$$

CASE B. No set of points x, y, and z exists, such that simultaneously all eight conditions are satisfied.

In Case A, consider the relation between $a(b+c)$ and $ab+ac$. Since $ax=x$, $by=y$, $cz=z$, and $y+z=x+y$, it follows that x is in a, and in $b+c$, but from $x(ab+ac)=0$ it follows that x is not in $ab+ac$. Hence $a(b+c)>ab+ac$.

On the other hand, if $a(b+c)=ab+ac$, there cannot exist so much as a single point x in both a and $b+c$, but not in $ab+ac$. It remains to show that if $a(b+c)\neq ab+ac$, then necessarily all the conditions of Case A are satisfied. Since $a(b+c)\geqq ab+ac$, the hypothesis implies that $a(b+c)>ab+ac$, and there exists at least a point x in both a and $b+c$, while not also in $ab+ac$. Since x is in a but not in $ab+ac$, it is not in ab, and hence not in b. Similarly x is not in c. Hence there is in b a point y, and in c a point z such that x is in $y+z$. Hence we see that $ax=x$, $x(ab+ac)=0$, $by=y$, $cz=z$. It remains to prove the other relations required for Case A. For (7), we must show that x, y, z are distinct points. If $x=y$, then this common point is in both

a and b; hence in ab and hence in $ab+ac$, contrary to hypothesis. Similarly $x \neq z$. If $y=z$, then $y+z=y$. Since x is in $y+z$, x would coincide with y contrary to the previous conclusion. Hence (7) is established. Since x, y, z are distinct points, and x is in $y+z$, condition (8) follows. We must show that (4) and (6) are satisfied. We may first show that y is not in ab. For if it were, then the line $y+z$ which is the line $x+y$ would join two distinct points x, y, both in a, and hence lie in a, so that z would be in a, and hence in ac. Then $y+z$ would lie in $ab+ac$, and $x(ab+ac)$ would be x contrary to hypothesis. Similarly z is not in ac. If now y were in $ab+bc$ then y would be a fortiori in $ab+c$, as would also z, so that x would be in $ab+c$. But z is not in ab, since it is not in $ab+ac$, and x, which is in a, is not also in c since it is not in ac. Hence there would exist points y' in ab and z' in c, such that x is in $y'+z'$. But now as by the previous argument the line $y'+z'$ is the line $x+y'$ which must lie in a, so that z' is in ac, and x is then in $ab+ac$ contrary to hypothesis. Hence, $y(ab+ac)=0$. Similarly $z(ac+bc)=0$.

Hence Case B is a necessary and sufficient condition that a be distributive with b and c in the first sense.

Consider next distribution in the second sense. If a fails to be distributive with respect to b and c in the second sense, there is a point t in both $a+b$ and $a+c$, which is not in $a+bc$. This point cannot then be in a or in bc. It is therefore not in both b and c. If it is not in b, then we may choose a point x in a and a point y in b, such that t is in $x+y$, while t, x, y are distinct. If it is also not in c, then using the same x we can take x in c such that t is in $x+z$. If t is in c, we may take t as z. In any case we have three distinct collinear points x, y, z, in a, b, c, respectively. Hence (1), (3), (5), (7), (8) of Case A are satisfied. The line $x+y=x+z$ is not in $a+bc$, hence neither y nor z is in bc. Since t is not in both b and c, we may so assign the notation that it is not in b. Then x is not in ab, since otherwise $x+y$ would be in b, and t would also be in b, contrary to hypothesis. If now x were in ac, $x+z$ would be in c, so that y which is in this line would be in c, and hence in bc. Then $x+y$ would be in $a+bc$ contrary to hypothesis. Hence x is in neither ab nor ac. If x were yet in $ab+ac$, then the line $x+y=x+z$ would be in $ab+ac+b=ac+b$, and in $ab+c$. But the line could not lie wholly in ab nor ac nor b nor c, since x is in neither b nor c. The line must then join a

point of ac with a point of b and join a point of ab with a point of c. Let x_1 in ab, x_2 in ac, be the points where this line meets these spaces. The line then contains x, x_1, x_2 all in a, where although x_1 and x_2 might coincide, neither could be x. But then the line would lie wholly in a, contrary to hypothesis. Hence $x(ab+ac)=0$, and (2) is established. Likewise y cannot be in $ab+bc$. For if it were then $x+y$ would be in $a+ab+bc=a+bc$, contrary to hypothesis. Thus (4) is established, and (6) follows similarly. Hence for a to fail to be distributive in the second sense implies Case A. Conversely given Case A, then a fails to be distributive with respect to b and c in the second sense. Indeed y will then be in $a+b$ and also in $x+y$ which is in $a+c$. But y will not be in $a+bc$. For y is in b, but not in $ab+bc$, hence not in ab nor bc, hence not in a nor bc. If y were yet in $a+bc$, there would be a point u in a, and a point v in bc such that y would be in $u+v$. But y and v are then distinct and are both in b. Hence $u+v$ is in b, and u is in b. Hence u is in ab. Hence y would be in $ab+bc$ contrary to hypothesis. Hence Case A is a necessary and sufficient condition that a fail to be distributive with respect to b and c in the second sense.

Since Case B is necessary and sufficient for a to be distributive with respect to b and c in the first sense and again also in the second sense, Theorem 1 is proved. Since this Case B is symmetric in a, b, and c, Theorem 2 is proved.

BROWN UNIVERSITY

ON FACTORING LARGE NUMBERS*

BY D. H. LEHMER† AND R. E. POWERS

1. *Introduction.* Various non-tentative methods of factoring a given odd number N, based on the expansion of $N^{1/2}$ in a regular continued fraction, have been described.‡ The success of most of these methods depends on the appearance of a perfect square among the denominators of the complete quotients. In practice, however, such an event occurs all too infrequently. More often

* Presented to the Society, April 11, 1931.

† National Research Fellow.

‡ Dickson, *History of the Theory of Numbers*, vol. 1, Chapter 14; and D. N. Lehmer, this Bulletin, vol. 13, p. 501, and vol. 33, pp. 35–36.