DESCRIPTIVE GEOMETRIES AS MULTIGROUPS

BY
WALTER PRENOWITZ

1. **Introduction.** Descriptive geometry is essentially the linear geometry of a convex region. Its historical importance lies in the fact that Euclidean, hyperbolic and other classic geometries are examples of descriptive geometry. In developing these subjects as mathematical disciplines it was found necessary to begin with nonmetrical properties, for example, betweenness, separability, interiority, and so on, and desciptive geometry arose as the abstract science of the "descriptive" (that is, nonmetrical) portions of classic geometry. The subject is characterized by postulates involving the notion *point* and a notion of intermediacy(1) indicated by one of the terms *order*, *between* or *segment*. Successive investigations by Pasch, Peano, Hilbert, E. H. Moore and Russell culminated in the definitive treatment of Veblen [1, 2] which we now describe(2).

Veblen adopts as primitive the notion *point* and a 3-term relation among points denoted *order*. The assertion that the relation *order* subsists for points a, b, c is indicated (abc), which may be read *points a, b, c are in the order abc* or *b lies between a and c*. The essential postulates of Veblen [2, pp. 5–6] as formulated by Forder [1, pp. 44–48] are:

O1. *If a, b, c are points and* (abc) *then a, b, c are distinct.*

O2. *If a, b, c are points and* (abc) *then* (bca) *is false.*

Definition. If a, b $(a \neq b)$ are points, the set consisting of a, b and all points x for which (xab) or (axb) or (abx) is called *line ab*. The set of points x for which (axb) is called *segment ab*. The set of points x satisfying (xab) is called a *ray* and it is said to *emanate* from a.

O3. *If* c, d $(c \neq d)$ *are points of line ab then a is a point of line cd.*

O4. *If* a, b $(a \neq b)$ *are points there is at least one point c such that* (abc).

O5. *There exist three points not in the same line.*

O6. (Transversal Postulate). *If a, b, c are distinct points and a is not in line bc and if d, e are points such that* (bcd) *and* (cea) *then there is a point f in line de such that* (afb)(3).

Presented to the Society, October 25, 1941; received by the editors July 28, 1945.

(1) This term is due to H. S. M. Coxeter (*Non-Euclidean geometry*, Toronto, 1942, p. 159).

(2) For further references on descriptive geometry see Veblen [1] and A. N. Whitehead, *The axioms of descriptive geometry*, Cambridge, 1907. Forder [1, chaps. 2, 3, 10] contains an unusually detailed and rigorous treatment of the subject. Numbers in brackets refer to the references cited at the end of the paper.

(3) Any system satisfying O1, · · · , O6 is termed a *descriptive geometry*. Observe that we do not assume a continuity postulate or any dimensional restriction other than O5.

Although the subject as developed from these postulates is a consummate example of logical precision and is quite elegant in comparison with earlier treatments, it has the disadvantages of synthetic methods as usually employed in geometry. In the first place many of the propositions (for example O6) are long and wordy and are kept in mind chiefly by geometric intuition. Thus the proofs usually are pictorially motivated and remembered. This often makes their verification burdensome since the intuitive geometric motivation must be disregarded in testing their validity. Further there is a scarcity of general ideas and methods. Special or degenerate cases frequently occur, requiring a sometimes annoying particularity in proofs. For example in order to discuss triangle *abc* or plane *abc* we must know that a, b, c are distinct and noncollinear. Also the number of variables, so to speak, is artificially limited—segments and triangles are studied but not simplexes or sets of n points in general. These disadvantages seem to be due to the early crystallization of geometry into a rigid structure on a naïve geometric basis. Later improvements in rigor did not materially alter this basis.

Modern algebra on the other hand is characterized by great generality of concept and method. The postulates, in the main, are simple unrestricted formal rules which lend themselves to abstract formal manipulation. They are easily extended to apply to an arbitrary (finite) number of variables. Defined notions when introduced are free of unnecessary specialization.

This contrast with modern algebra seems inevitable if we formulate descriptive geometry in the usual manner. But it has become evident in recent years that the nature and structure of a mathematical discipline may be altered radically by changing its axiomatization. Thus Stone has converted Boolean algebra into a branch of ring theory and Garrett Birkhoff has characterized projective geometries as lattices of a certain special type(4). In these cases the new formulation of the subject leads to a new conception of its nature and so to a new method of development. For example in Stone's theory ring concepts are used throughout, Boolean operations appearing as certain combinations of the basic ring operations.

We propose to axiomatize descriptive geometry so as to bring to the fore the general concepts of the subject and to characterize them by unrestricted properties which shall lend themselves so far as possible to algebraic development(5).

With this in mind, let us examine the broad outlines of the subject. The

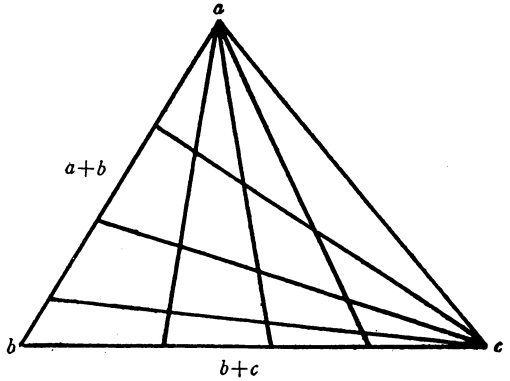
(4) See M. H. Stone, *The theory of representations for Boolean algebras*, Trans. Amer. Math. Soc. vol. 40 (1936) pp. 37–111; Garrett Birkhoff, *Combinatorial relations in projective geometries*, Ann. of Math. vol. 36 (1935) pp. 743–748. Menger was the first to study projective geometries as lattices, see K. Menger, *Bemerkungen zu Grundlagenfragen*, IV, Jber. Deutschen Math. Verein. vol. 37 (1928) pp. 309–325; also, *New foundations of projective and affine geometry*, Ann. of Math. vol. 37 (1936) pp. 456–482.

(5) The writer recently showed (Prenowitz [1]) how projective geometries could be characterized as a type of group-like system with many-valued composition. This originally motivated the present investigation.

basic operations of elementary geometry are (1) to *join* points to form segments and (2) to *extend* or prolong segments to form rays. The familiar objects studied (line, triangular region, half-plane, and so on) are easily constructed from points by repeated use of these operations. Let us characterize *join* and *extend* as 2-term operations in the domain of points, analogous to algebraic operations.

We define the *join* of distinct points a, b to be the segment ab. In order that the operation may be applicable without restriction, we must define the join of a and a—this we take to be a itself([6]). Further in order to iterate the operation we must define join of *sets*. Thus we define the *join* of the non-empty *point sets* A, B to be the point set formed by joining each point of A to each point of B and aggregating all "joins" formed in this way. We can easily characterize *extend* in terms of join. We define the *extension of a from b* as the set of points x whose join to b contains a. If a and b are distinct, this is the ray emanating from a which is directed away from point b, while if $a=b$ it consists solely of a.

The following properties of *join* and *extension* are familiar implicates of Veblen's postulates and are easily verified pictorially. We consider them basic.



(1) (Closure). *The join of a and b is a non-empty set of points.*

(2) (Commutativity). *The join of a and b is identical with the join of b and a.*

(3) (Associativity). *The join of a with the join of b and c is identical to the join with c of the join of a and b.*

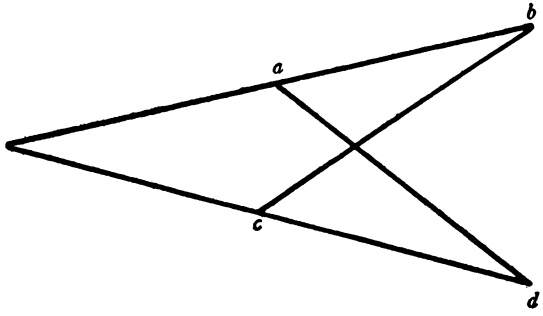
([6]) We could alternatively axiomatize the subject in terms of join as *closed* interval, but it is not so convenient. Our use of the term join is not quite the same as that in topology and lattice theory, since the join of a, b does not contain a and b when $a \neq b$. However our definition is very natural if we think of the join of a, b as the interior of the simplex with vertices a, b. The agreement that the join of a and a is a is essential for the unrestricted validity of the associative law for join (see property (3) below). Incidentally if in the familiar formula of elementary analytic geometry for the point which divides segment ab in a given positive ratio we set $a=b$, we get point a itself.

(4) (Idempotency). *The join of a and a is a*([7]).

(5) (Closure). *The extension of a from b is a non-empty set of points.*

(6) (Idempotency). *The extension of a from a is a.*

(7) (Transposition). *Let the extension of a from b meet the extension of c from d. Then the join of a and d meets the join of b and c.*



We observe that properties (1), · · · , (7) are perfectly general—they hold without restriction on the elements involved. Examining them individually, we note that (3) is essentially an algebraic restatement of the triangle postulate O6. However it has greater deductive power, since no restriction on a, b, c is assumed. Property (5) is essentially a restatement of O4 that "every segment can be extended." Property (6) signifies that a segment does not contain its end points and is essentially a form of O1. Property (7) is in essence a formulation in our language of a triangle postulate employed by Peano which may be stated in conventional form: *Segments which join two vertices of a triangle to respective points of their opposite sides intersect.* Postulate O3 which is a weakened form of "two points belong to a unique line" has not been included among the basic properties since it is neither simple nor natural in the present context.

We now formulate an abstract algebraic system suggested by our analysis of the fundamental properties of the operations join and extension. Consider a set G and a many-valued 2-term operation $+$, which associates to each ordered pair a, b of elements of G a set $a+b$ called the *sum* or *join* of a and b. We assume the following postulates.

J1. *If* $a, b \subset G$([8]), $a+b$ *is a uniquely determined, non-empty, subset of* G.

J2. *If* $a, b \subset G$, $a+b=b+a$.

([7]) We agree to identify element a and set (a) whose only member is a. Hence there is no inconsistency between properties (1) and (4).

([8]) In view of the agreement in footnote 7 we may use the inclusion signs $\supset$, $\subset$ for *elements* as well as sets. Furthermore our definitions and theorems involving non-empty subsets of G will hold for individual elements of G.

In the algebraic study of an operation defined for elements, it is desirable to extend the operation to sets. This is immediately necessary here in order to iterate the operation $+$. Thus we introduce the following definition.

Definition 1. Let A, B be non-empty subsets of G. Then $A+B$, the *sum* or *join* of A and B, is the set union $\sum_{a\subset A, b\subset B}(a+b)$([9]). For an arbitrary subset A of G we define $A+O=O+A=A$([10]).

J3. *If* $a, b, c\subset G$, $(a+b)+c=a+(b+c)$.

J4. *If* $a\subset G$, $a+a=a$([11]).

J5. *If* $a, b\subset G$ *the relation* $b+x\supset a$ *has a solution* x *in* G.

This suggests the notion *inverse operation*. Thus we adopt the following definition.

Definition 2. Suppose $a, b\subset G$. Then $a-b$, the *difference* of a and b, is the set of x in G for which $b+x\supset a$([12]).

J6. *If* $a\subset G$, $a-a=a$.

In order to state J7 we introduce another definition.

Definition 3. Let A, B be subsets of G. Then $A\approx B$, read A *meets* or *intersects* B, means that A and B have a common element, that is, the set product $A\cdot B\neq O$([13]).

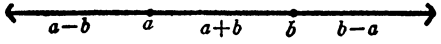
J7. *Suppose* $a, b, c, d\subset G$. *Then*

$$a - b \approx c - d$$

implies

$$a + d \approx b + c.$$

A descriptive geometry is an interpretation of the postulate system J1, $\cdots$, J7. For, let G be the set of points in a descriptive space and let $a+b$ be the *geometric* join of points a, b as defined earlier. Then $A+B$ in Definition 1 is the *geometric* join of sets A, B. By Definition 2, $a-b$ is the set of points whose join to b contains a, that is, the extension of a from b. Hence J1, $\cdots$, J7



reduce to properties (1), $\cdots$, (7) of join and extension and are verified. Observe that in this formulation of a descriptive geometry line ab takes on the interesting form

$$(a + b) \cup (a - b) \cup (b - a) \cup a \cup b([14]).$$

([9]) This is consistent with the notation $a+b$ adopted for the sum of *elements* of G, since if $A=a$, $B=b$ then $A+B$ reduces to $a+b$.

([10]) O denotes the empty set.

([11]) This is not inconsistent with J1, see footnote 7.

([12]) This seems to be the first study in which the inverse of a many-valued operation is consistently exploited.

([13]) Observe that if A is an element a, the assertion $A\approx B$ is equivalent to $a\subset B$.

([14]) We use the symbol $\cup$ to denote set theoretic addition.

The system $(G; +)$ although abstracted from a familiar geometrical situation is interesting in itself as a type of algebraic system. It is a form of generalized group with many-valued composition called a *multigroup* or *hypergroup*([15]). J1, J5 are closure laws for the many-valued operations $+$, $-$ respectively. The idempotent law, J3, is very familiar in modern algebra and played an important role in the author's characterization of projective geometries as multigroups (Prenowitz [1]). J6, the idempotent law for the inverse operation, seems less familiar but may be considered analogous to the principle $A-A=A$, where A is a subgroup of an additively expressed abelian group. The relation $\approx$ is analogous to a weak form of equality in classical algebra([16]). In view of this, J7 is a sort of transposition principle, since it permits us to transpose terms in the "equality" and change appropriate signs. J7 actually is a generalization of a familiar transposition principle of school algebra to which it reduces if the members $a-b$, $c-d$ are single-valued.

Postulates J1, $\cdots$, J7 strongly suggest a group theoretic treatment of descriptive geometry. It is our thesis that the proper exploitation of group theoretic concepts yields a treatment of descriptive geometry which attains the elegance and generality of modern algebra without loss of the intuitive geometric naturalness of the older theories. In the sequel we attempt to justify this thesis for the basic ideas of descriptive geometry, including among others *convex set, linear space, half-space, angle, separation of linear spaces, dimension.* These are related to or even subsumed under the group theoretic notions: *closure, subgroup, coset, factor group, homomorphism, congruence relation, linear independence.*

Postulate system J1, $\cdots$, J7 is weaker than Veblen's system (see below §3, Theorem 7)([17]). Nevertheless we shall not strengthen it now for two reasons. In the first place, our theory in §§1–8 is valid in more general systems than descriptive geometries, and the verification is no more difficult([18]). Secondly, and perhaps this is more important, we obtain a new type of characterization of descriptive geometry. For, the additional postulates can be framed so as to characterize descriptive geometry in a sense as the simplest and most natural type of system $(G; +)$ which satisfies J1, $\cdots$, J7. This yields an insight into the nature of descriptive geometry as a type of abstract mathematical system not afforded by the usual axiomatization which is so strongly conditioned by the historical origin of geometry in a rude form of surveying.

([15]) More precisely a multigroup is a system closed under an associative many-valued operation o, which contains elements x, y satisfying the relations $a \circ x \supset b, y \circ a \supset b$ when a, b are in the system. See Dresher and Ore [1, pp. 706, 707]. A list of references on the subject is found in J. E. Eaton, *Associative multiplicative systems*, Amer. J. Math. vol. 62 (1940) pp. 222–232.

([16]) Observe that if A, B consist of single elements $A \approx B$ is equivalent to $A = B$.

([17]) Our system lacks O3, O5. We introduce their equivalent as J8, J9, J10 (§§9, 10).

([18]) Such systems include direct sums of descriptive geometries (see §3, Definition 2 and the corollary to Theorem 6) and "partially ordered" geometries in which for three "collinear" points no order relation need subsist (see §10, the discussion following the statement of J9).

The multigroups characterized by J1, · · ·, J7 are not covered by the current theories of multigroups. Hence we shall develop our theory directly from the postulates and the paper will be essentially self-contained.

In §2 we develop the formal algebraic principles constantly employed in the paper. Section 3 treats the theory of order in a system satisfying J1, · · ·, J7, and sheds light on the divergence of our theory from that of Veblen. In §§4, 5 convex sets and linear spaces are studied respectively as additively closed sets and subgroups in a system $(G; +)$. In §6 the notion linear independence is treated and is used to characterize the geometric idea simplex. §7 contains a new theory of cosets and factor groups which subsumes the geometric theories of half-spaces, separation by linear spaces, angles and spherical geometry. This naturally leads to the study of homomorphisms and congruence relations in §8, which contains analogues of familiar theorems in classical group theory. Thus far only J1, · · ·, J7 have been postulated. In §§9, 10 the postulate system is strengthened in a natural way by the addition of three postulates, to yield the theory of dimensionality and of separation of linear spaces by linear spaces. The principal results of §11 are the general theorem on the decomposition of a linear space by a simplex and the characterization of descriptive geometries as systems $(G; +)$.

2. **Formal properties.** We consider an abstract system $(G; +)$ satisfying J1, · · ·, J7. For convenience we call $(G; +)$ or simply G a *group*; and refer to the more familiar type of group with single-valued composition as a *classical* group. We use $a, b, c, \cdots$ to denote elements of G and $A, B, C, \cdots$ subsets of G. G usually is not mentioned in the theorems unless some special property of G is assumed. Theorems and definitions are numbered serially in each section and in referring to them the numeral is prefixed by the number of the section, thus Theorem 5 of §3 is referred to as Theorem 3.5.

In this section we derive certain algebraic formulas and formal properties constantly used in succeeding sections. The results are suggested by the familiar manipulatory algebra of operations $+$, $-$ and practically all of them reduce to familiar principles of classical abelian group theory if the composition is *single*-valued.

First in order to extend the inverse operation to sets we adopt the following definition.

Definition 1. If $A, B \neq O$, $A-B$ denotes the set union $\sum_{a\subset A, b\subset B}(a-b)$. For arbitrary A, we define $A-O=A$, $O-A=O$[19].

Now we can define the general type of algebraic expression which we shall study.

Definition 2. A *polynomial* $f(A_1, \cdots, A_n)$, where the A's are variable subsets of G, is a function which can be expressed by applying the operations $+$, $-$ a finite number of times to $A_1, \cdots, A_n$, for example, $A_1-(A_2+A_3)$

(19) No other meaning for $O-A$ will validate the general transposition principle in Theorem 4 of §2.

or $(A_1-A_2)+(A_1-A_3)$ or even A_1. If the A's are given specific determinations in $f(A_1, \cdots, A_n)$ the resulting expression is called a *polynomial expression*[20].

We shall derive a very simple and useful "monotonic" law. First we show that the functions $A \pm B$ are monotonic.

THEOREM 1. *Suppose* $O \neq A' \subset A$ *and* $O \neq B' \subset B$. *Then* $A' \pm B' \subset A \pm B$.

Proof. By Definitions 1.1, 2.1

$$A' \pm B' = \sum_{a \subset A', b \subset B'} (a \pm b) \subset \sum_{a \subset A, b \subset B} (a \pm b) = A \pm B.$$

By induction this is easily generalized to establish the monotonicity of polynomials.

COROLLARY 1. *Suppose* $O \neq A_i' \subset A_i$, $1 \leqq i \leqq n$. *Then* $f(A_1', \cdots, A_n') \subset f(A_1, \cdots, A_n)$, *where* f *is any polynomial function*[21].

Taking A_i' as an element a_i we have the following corollary.

COROLLARY 2. *Suppose* $a_i \subset A_i$, $1 \leqq i \leqq n$. *Then* $f(a_1, \cdots, a_n) \subset f(A_1, \cdots, A_n)$, *where* f *is any polynomial function.*

By Definitions 1.1, 2.1 if $x \subset A \pm B$ and $A, B \neq O$ then $x \subset a \pm b$, where $a \subset A$, $b \subset B$. We generalize this principle in the following theorem.

THEOREM 2. *Let* $f(X_1, \cdots, X_n)$ *be a polynomial function in which no letter is repeated; let* $A_i \neq O$, $1 \leqq i \leqq n$. *Then* $x \subset f(A_1, \cdots, A_n)$ *implies* $x \subset f(a_1, \cdots, a_n)$, *where* $a_i \subset A_i$[22].

Proof. If $n=1$ the theorem is trivial. We have already noted its truth for $n=2$. The general result is easily proved by induction.

Now we derive an important principle which enables us to extend "identical" relations involving variable *elements* to variable *sets*.

COROLLARY. *Let* f *be a polynomial function in which no letter is repeated. Let* $f(a_1, \cdots, a_n) \subset g(a_1, \cdots, a_n)$ *for arbitrary* a_i, $1 \leqq i \leqq n$. *Then* $f(A_1, \cdots, A_n) \subset g(A_1, \cdots, A_n)$ *for arbitrary* $A_i \neq O$[23].

Proof. Suppose $x \subset f(A_1, \cdots, A_n)$, $A_i \neq O$. By Theorem 2.2, the hypothesis, and Corollary 2 of Theorem 2.1, we have $x \subset f(a_1, \cdots, a_n) \subset g(a_1, \cdots, a_n) \subset g(A_1, \cdots, A_n)$, where $a_i \subset A_i$.

---

[20] This is a notion of general or "universal" algebra, see Birkhoff [1, pp. 2–4] where the term "function" is used.

[21] Compare Birkhoff [1, p. 21, Theorem 2.7].

[22] The restriction that f contain no repeated letter is essential. For let A consist of a_1, a_2 ($a_1 \neq a_2$) and suppose $x \subset a_1 + a_2$. Then $x \subset A + A$ but $x \not\subset a + a$ for $a \subset A$.

[23] This principle is extended easily to cover identical *equations* $f(a_1, \cdots, a_n) = g(a_1, \cdots, a_n)$, provided both f and g are polynomial functions in which no letter is repeated.

This principle is used constantly and enables us automatically to generalize almost all identical relations derived for elements to arbitrary non-empty sets. As an illustration of its utility consider J2, J3 and the relations $a \subset a \pm a$ which follow from J4, J6. Applying the principle we have the following theorem.

THEOREM 3. (a) $A+B=B+A$; (b) $(A+B)+C=A+(B+C)$; (c) $A \subset A \pm A$ [24].

We continue to extend our formal principles to sets. The formal significance of Definition 1.2 is: $a-b \supset c$ *if and only if* $a \subset b+c$. This can be rewritten: $a-b \approx c$ *if and only if* $a \approx b+c$. We generalize this in the next theorem.

THEOREM 4. $A-B \approx C$ *implies* $A \approx B+C$. *Conversely* $A \approx B+C$ *implies* $A-B \approx C$, *provided* $C \neq O$.

Proof. Suppose $A-B \approx C$. If $B \doteq O$, certainly $A \approx B+C$. Suppose $B \neq O$. Let $c \subset A-B$, C. Then $A \neq O$ and, by Theorem 2.2, $c \subset a-b$, where $a \subset A$, $b \subset B$. Hence by Definition 1.2 and Corollary 2 of Theorem 2.1, $a \subset b+c \subset B+C$, so that $A \approx B+C$. Conversely suppose $A \approx B+C$ and $C \neq O$. If $B=O$, $A-B \approx C$ is trivial. Suppose $B \neq O$. Let $a \subset A$, $B+C$. Then $a \subset b+c$, where $b \subset B$, $c \subset C$. Hence $c \subset a-b \subset A-B$ so that $A-B \approx C$, and the theorem is proved.

Now we can easily derive a generalized form of J7.

THEOREM 5. $A-B \approx C-D$ *implies* $A+D \approx B+C$.

Proof. If $B=D=O$, the theorem is trivial. Suppose only one of B, $D=O$, say B. Then by hypothesis $A \approx C-D$, so that by the last theorem $A+D \approx C=B+C$ and the theorem holds. Now suppose B, $D \neq O$. Suppose $x \subset A-B$, $C-D$. Certainly A, $C \neq O$. Hence by Theorem 2.2, $x \subset a-b$, $c-d$ where a, b, c, $d \subset A$, B, C, D respectively. Thus by definition $a-b \approx c-d$ and, by J7, $a+d \approx b+c$. The conclusion is immediate since $A+D \supset a+d$ and $B+C \supset b+c$ by Corollary 2 of Theorem 2.1.

Now we derive several "associative" laws for expressions involving $+$ and $-$.

THEOREM 6. $a-(b+c)=(a-b)-c$.

Proof. Supposing $x \approx a-(b+c)$, we have

$$x + (b + c) \approx a \qquad \text{(Theorem 2.4)},$$

$$(x + c) + b \approx a \qquad \text{(J2, J3)},$$

$$x + c \approx a - b \qquad \text{(Theorem 2.4)},$$

$$x \approx (a - b) - c \qquad \text{(Theorem 2.4)}.$$

[24] At this point our theory differs from classical abelian group theory in which (c) does not hold. This is a consequence of our assumption of the idempotent law J4.

We complete the proof by retracing our steps.

Applying the corollary of Theorem 2.2 we have the following corollary.

COROLLARY. $A-(B+C)=(A-B)-C=(A-C)-B$.

THEOREM 7. $a-(b-c)\subset(a+c)-b$.

Proof. Suppose $x\approx a-(b-c)$. Transposing $(b-c)$ and x successively (Theorem 2.4) we have

$$x+(b-c)\approx a, \qquad b-c\approx a-x.$$

Applying J7,

$$b+x\approx a+c,$$

and solving for x, we have

$$x\approx(a+c)-b.$$

COROLLARY. $A-(B-C)\subset(A+C)-B$ *provided* $B\neq O$.

THEOREM 8. $a+(b-c)\subset(a+b)-c$.

Proof. Suppose $x\approx a+(b-c)$. Using the method of the last theorem, we have

$$x-a\approx b-c \qquad \text{(Theorem 2.4)},$$

$$x+c\approx a+b \qquad \text{(J7)},$$

$$x\approx(a+b)-c \qquad \text{(Theorem 2.4)}.$$

COROLLARY. $A+(B-C)\subset(A+B)-C$ *provided* $B\neq O$.

Now we derive several formulas of a more specialized nature which are used later in the theory of half-spaces.

THEOREM 9. $a-(a-b)\supset b$[25].

Proof. We have $a-b\approx a-b$. Transposing, successively, b to the right member and $a-b$ to the left member (Theorem 2.4), we get $a-(a-b)\approx b$.

COROLLARY 1. $A-(A-B)\supset B$ *provided* $A\neq O$.

COROLLARY 2. $a-(a-b)\supset a+b$.

Proof. Adding a to both members in Theorem 2.9 we have by Theorem 2.1, the corollary of Theorem 2.8 and J4

$$a+b\subset a+(a-(a-b))\subset(a+a)-(a-b)=a-(a-b).$$

COROLLARY 3. $A-(A-B)\supset A+B$ *provided* $A\neq O$.

It is interesting to compare this with the situation in classical abelian group theory, where $A-(A-B)=(A-A)+B$. Suppose $A-A\supset A$ (Theo-

[25] Observe that in ordinary (single-valued) algebra this is valid in the form $a-(a-b)=b$.

rem 2.3 (c)), which holds if A contains the identity element. Then $(A-A)+B \supset A+B$ and the present principle would be valid.

We conclude this section with several "distributive laws" which follow directly from Definitions 1.1, 2.1.

THEOREM 10. *Suppose* $A, B \neq O$. *Then* $(A \cup B) \pm C = (A \pm C) \cup (B \pm C)$ and $C-(A \cup B) = (C-A) \cup (C-B)$.

3. **Theory of order.** We introduce the notion *order* in a group G because of its intrinsic interest and also to compare our postulate system with that of Veblen([26]). We reduce the theory of order for "collinear points" to the solution of simultaneous linear equations and show that the greater part of the familiar theory of order on a descriptive line is valid in our system. As a corollary we get that $a+b$ is an infinite set if $a \neq b$. In contrasting our system with that of Veblen, we show that *the direct sum of two groups is a group*, an interesting algebraic property of our system.

We introduce the idea *order* in a group G by inverting the definition of $+$ (join) in a descriptive geometry (§1).

Definition 1. (abc) means $a \neq c$ and $b \subset a+c$.

We proceed to derive the properties of this relation. First we have

THEOREM 1. (abc) *implies that* $a+b \approx b+c$ *is false.*

Proof. Suppose (abc) and

$$a + b \approx b + c. \tag{1}$$

Then by definition we have

$$b \approx a + c. \tag{2}$$

Solving (1), (2) for a, we get

$$(b + c) - b \supset a, \qquad b - c \supset a. \tag{3}$$

Thus we can eliminate a, getting $(b+c)-b \approx b-c$. Transposing and "collecting" terms we get $b=c$. Substituting in the second part of (3) we get $a=c$, contrary to hypothesis. Thus (1) is false and the theorem is proved.

In showing that $b=c$ implies $a=c$, contrary to (abc), we have justified the following corollary.

COROLLARY. (abc) *implies that* a, b, c *are distinct.*

Additional order properties of three elements are included in the discussion of Veblen's postulates (Theorem 3.5). There is little else of interest in this topic. Thus we continue with the properties of four elements between

([26]) It is not necessary to introduce the notion order in the formal study of systems G. Most of the order properties derived are special cases of formal principles or algorithmic methods of §2 and need not be extracted from the general principles to further the development of our theory.

which subsist two order relations([27]). For example consider (abc), (bcd). By definition we have

$$(1) \qquad b \approx a + c, \quad . \quad c \approx b + d.$$

Eliminating a common letter, say c, in (1) as in the last theorem, we get $b-a \approx b+d$ so that $b \approx a+b+d$ and $b \approx a+d$. We can assert $a \neq d$, since otherwise, by J4, $b=d$, contrary to the supposition (bcd). Hence by definition (abd). Similarly, eliminating b in (1) we get (acd). Thus we may assert (Forder [1, p. 51, Theorem 8.1]) the following theorem.

THEOREM 2. (abc), (bcd) *imply* (abd), (acd).

In a similar way elimination of a common letter between the relations $b \approx a+c$ and $c \approx a+d$ yields (Forder [1, p. 52, Theorems 8.5, 8.6]) the following theorem.

THEOREM 3. (abc), (acd) *imply* (abd), (bcd).

The familiar argument of the foundations of geometry which shows that a segment is an infinite set([28]) can now be used to justify the following corollary.

COROLLARY. *If* $a \neq b$, $a+b$ *is an infinite set.*

Using the above method of elimination in linear relations we derive the following theorem.

THEOREM 4. (abx), (aby) *imply the falsity of* (xay), (xby). *Similarly* (axb), (ayb) *imply the falsity of* (xay), (xby)([29]).

Theorems 3.2–3.4 in essence cover the theory of order for collinear points. This topic is quite important in the classical treatment since it is needed to derive the separation theorem for a line (Forder [1, p. 51, Theorem 8]). It plays no such role here since we develop the separation theory for linear spaces (§10) by general methods, independent of dimension.

The remainder of this section deals with the comparison of the postulate systems O1, · · · , O6 and J1, · · · , J7. First we have the following theorem.

THEOREM 5. *The relation order in G satisfies postulates* O1, O2, O4, O6.

Proof. O1 is the corollary of Theorem 3.1.

([27]) In a descriptive geometry this is the case of four collinear points, compare Forder [1, pp. 51, 52, Theorems 8.1–8.6].

([28]) See for example Forder [1, p. 53, the demonstration of Theorem 10]. To formalize this, of course, an inductive argument or the equivalent must be employed.

([29]) Compare Forder [1, pp. 51, 52, Theorems 8.2–8.4]. In a descriptive geometry the falsity of (xay) is equivalent to the truth of (axy) or (ayx) provided a, x, y are distinct. This is not true in general for groups G.

By Theorem 3.2, (abc) and (bca) imply (aba), contrary to O1. Thus O2 is verified.

O4 is valid since it is essentially a restatement of J5.

To verify O6, suppose a, b, c distinct, a not in line bc, and (bcd), (cea). Then $c \approx b+d$, $e \approx c+a$. Eliminating c between these relations and solving for $a+b$, we get $a+b \approx e-d$. Let $f \subset a+b$, $e-d$. Then (afb). Clearly f is in line de provided the line exists, that is, if $d \neq e$. Suppose $d=e$. Then by Theorem 3.2 (bcd), (cea) imply (bca), so that a is in line bc contrary to hypothesis. Thus $d \neq e$ and the proof is complete.

Consider now postulates O3, O5. Obviously O5 is independent of J1, $\cdots$, J7 since we have included no postulate of dimension and G may be a line, point or even O. To show the independence of O3 we introduce the important abstract algebraic idea, *direct sum*.

Definition 2. Let G_1, G_2 be arbitrary groups. If $A_1 \subset G_1$, $A_2 \subset G_2$ we use the symbol (A_1, A_2) to denote the set of ordered pairs (a_1, a_2) where $a_1 \subset A_1$, $a_2 \subset A_2$. We define a composition in (G_1, G_2) as follows: $(a_1, a_2)+(b_1, b_2) = (a_1+b_1, a_2+b_2)$([30]). We call (G_1, G_2) with addition so defined the *direct sum* of groups G_1, G_2.

Now we can prove the following theorem.

THEOREM 6. *The direct sum of two groups is a group*([31]).

Proof. The definition of $+$ in (G_1, G_2) is easily extended to yield similar principles for addition of sets and for subtraction of elements, namely,

$$(A_1, A_2) + (B_1, B_2) = (A_1 + B_1, A_2 + B_2)$$

and

$$(a_1, a_2) - (b_1, b_2) = (a_1 - b_1, a_2 - b_2).$$

Hence the operations $+$, $-$ which occur in J1, $\cdots$, J7 may be performed component by component and J1, $\cdots$, J7 are easily seen to be verified in (G_1, G_2).

Since a descriptive geometry can be formulated as a system satisfying J1, $\cdots$, J7, that is, a group, it is significant to speak of the *direct sum* of two descriptive geometries. Thus we may assert the following corollary.

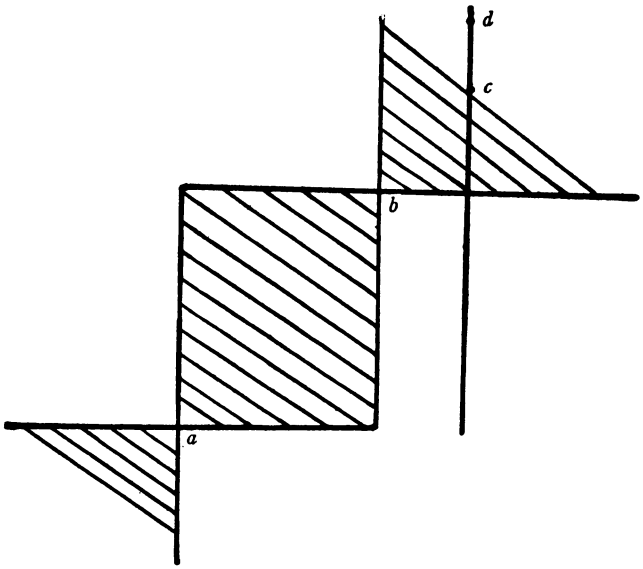
COROLLARY. *The direct sum of two descriptive geometries is a group.*

Using the last theorem we can easily establish the independence of O3. We convert the set of real numbers into a group G_1 by defining $a+b$, if $a \neq b$, to be the set of numbers between a and b, and $a+a$ to be a. Let $G_2 = G_1$ and form $G = (G_1, G_2)$. Then G is the cartesian plane as the domain of an operation $+$ (join) defined in a rather unusual way. Let element (x_1, x_2) of G be denoted

([30]) For convenience we use the same symbol $+$ for the addition operations in G_1 and G_2.

([31]) That is, the direct sum satisfies J1, $\cdots$, J7. It need not satisfy J8, J9, J10 which are introduced later in §§9, 10.

x. Choose elements a, b, c, d in G such that $a_i<b_i<c_i$, $c_1=d_1$, $c_2<d_2$. Then, plotting points in the usual way, line ab (indicated in the diagram by shading)



is composed of a, b, all points which are above and to the right of b, all points which are below and to the left of a and all points which are simultaneously above and to the right of a and below and to the left of b. Line cd is the ordinary Euclidean vertical "line" cd. Line $ab \supset c$, d where $c \neq d$, but line $cd \not\supset a$. Thus O3 is not verified in G. Hence in view of the last theorem we may assert the following theorem.

THEOREM 7. *Postulate* O3 *is independent of* J1, $\cdots$, J7.

4. **Convex sets—closure under addition.** Having developed the necessary formal properties in §2, in this and succeeding sections we study *structural* properties so familiar in modern algebra. Sometimes such notions are suggested directly by the familiar geometric concept under consideration. For example, convex sets, the fundamental object of study in descriptive geometry, are usually characterized by the property of containing, with any two points, the segment joining them. This suggests the following definition.

Definition 1. Let set S have the property: $S \supset a$, b implies $S \supset a+b$. Then we say S is *additively closed* or *closed under addition*, or in geometrical language S is *convex*[32]. (Observe that G, O and individual elements of G are additively closed.)

---

[32] In projective geometry we can take $a+b$ to be the (linear) join of points a, b and this becomes the definition of linear space, see Prenowitz [1, p. 240, Definition 4].

We give a more compact and convenient formulation of this property in the following theorem.

THEOREM 1. *A is additively closed (convex) if and only if* (a) $A \supset A+A$ *or* (b) $A = A+A$.

Proof. (a) is essentially a restatement of Definition 4.1, and (b) is a combination of (a) and Theorem 2.3 (c).

COROLLARY (Absorption). *Let $A \supset B$ where A is additively closed (convex). Then $A \supset A+B$.*

Proof. Add A to both members of $A \supset B$.

We consider operations applied to convex sets in the following theorem.

THEOREM 2. *Let A, B be additively closed (convex). Then $A \cdot B, A+B, A-B$ are also additively closed (convex).*

Proof. It is obvious that $A \cdot B$ is closed under addition, just as in classical group theory. To show $A+B$ additively closed, we observe by Theorem 4.1 that $A+A=A$, $B+B=B$. Hence $(A+B)+(A+B)=(A+A)+(B+B)$ $=A+B$ and $A+B$ is additively closed by Theorem 4.1. To complete the proof we have

$$
\begin{aligned}
(A-B)+(A-B) &\subset ((A-B)+A)-B && \text{(Theorem 2.8, corollary)}\\
&= (A+(A-B))-B\\
&\subset ((A+A)-B)-B && \text{(Theorem 2.8, corollary; Theorem 2.1)}\\
&= (A-B)-B\\
&= A-(B+B) && \text{(Theorem 2.6, corollary)}\\
&= A-B
\end{aligned}
$$

and the conclusion follows by Theorem 4.1.

By an easy induction we have the following corollary.

COROLLARY 1. *Let $A_1, \cdots, A_n$ be additively closed. Then any polynomial expression $f(A_1, \cdots, A_n)$ is additively closed.*

Taking the A's to be elements $a_1, \cdots, a_n$ and restricting f suitably we have another corollary.

COROLLARY 2. *$a_1+\cdots+a_n$ is additively closed (convex)*[33].

The familiar notion "convex envelope of point set S" (the least convex set containing S) suggests the following definition.

[33] If in a descriptive geometry a simplex has vertices $a_1, \cdots, a_n$ then $a_1+\cdots+a_n$ may be considered its interior. Thus this corollary includes the result that the interior of a simplex is convex. For case $n=3$ compare Forder [1, p. 237, Theorem 2, part (i) of proof].

Definition 2. Suppose $S \subset G$. By the *additively closed (convex) set determined* or *generated* by S, denoted $[S]$, we mean the least additively closed subset of G which contains S[34]. If $[S]=A$ we say S is a set of *additive generators* of A. If the elements of S are $s_1, \cdots, s_n$ (where the s_i are not necessarily distinct) we write $[S]=[s_1, \cdots, s_n]$. (An illustration of this in descriptive geometry is the closed convex polyhedral region (convex polyhedron plus its interior) whose vertices are $s_1, \cdots, s_n$.)

The existence and uniqueness of $[S]$ is proved in the familiar way by considering the intersection of all additively closed subsets of G which contain S.

Following a very familiar path in modern algebra (cf. subgroup or subring generated by a set of elements) we get the following theorem.

THEOREM 3. *$[S]$ is the set union of all polynomial expressions of the form $a_1+\cdots+a_n$, where the a's are in S.*

If S is *finite* we get a simple explicit formula for $[S]$ by enumerating all nonidentical expressions of the given form. Thus we have the following corollary.

COROLLARY. $[a_1, \cdots, a_n]=a_1+\cdots+a_n \cup a_2+\cdots+a_n \cup a_1+a_3+\cdots+a_n \cup \cdots \cup a_1 \cup \cdots \cup a_n$[35][36].

In general this formula contains no redundant terms since the addends may be disjoint. Conditions for disjointness are formulated in §6.

Let A be an additively closed set. It is natural to enquire whether there exists a *minimal* set of additive generators of A. That is, a set of additive generators of A, no proper subset of which is a set of additive generators of A. In a sense this constitutes the simplest type of set of additive generators of A. Such a minimal set need not exist for a given A, for example let $A=a+b$ $(a \neq b)$ in a descriptive geometry. Covering the case in which it does exist we have the following theorem.

THEOREM 4. *Let A be an additively closed (convex) set which has a minimal set of additive generators. Then A has a unique minimal set of additive generators.*

Proof. Let S be a minimal set of additive generators of A, let T be *any* set of additive generators of A. It suffices to show $S \subset T$. Suppose $x \subset S$. Then $x \subset A = [T]$, so that by Theorem 4.3 we have

$$x \subset t_1+\cdots+t_n, \qquad t_i \subset T, \qquad (1 \leqq i \leqq n). \tag{1}$$

(34) Compare Alexandroff-Hopf [1, p. 602, *Konvexe Hülle*]. $[S]$ may be read briefly the *additive closure* of S. It corresponds in a projective geometry to the linear space determined by S, see Prenowitz [1, p. 241, Definition 5].

(35) For simplicity of notation in expressions involving $+$, $-$, $\cup$ we adopt the convention that expressions separated by $\cup$ signs are to be considered enclosed in parentheses.

(36) Compare the decomposition of a closed triangular (or tetrahedral) region effected by its vertices.

Similarly since $t_i \subset [S]$ we have

$$t_i \subset s_{i,1} + \cdots + s_{i,m_i}, \qquad s_{i,j} \subset S \qquad (1 \leqq i \leqq n). \tag{2}$$

By Corollary 2 of Theorem 2.1 (monotonicity) we have from (1), (2)

$$x \subset s_{1,1} + \cdots + s_{1,m_1} + \cdots + s_{n,1} + \cdots + s_{n,m_n}. \tag{3}$$

Suppose x is not present in the right member of (3). Then x is "dependent" on other elements of S so that it can be deleted from S and the resulting set is still a set of additive generators of A. This contradicts the *minimal* property of S. Hence at least one of the $s_{i,j}$ is identical with x. Moreover if any of the $s_{i,j}$ is distinct from x, we can transpose x in (3) to the left member and get the same contradiction. Hence each $s_{i,j}$ is identical with x. Hence, by (2), $t_i = x$ so that $x \subset T$. Thus $S \subset T$ and the result follows.

If A happens to have a *finite* set of additive generators, S', we can delete redundant elements in S', one by one, eventually yielding a minimal set of additive generators of A. Thus we may assert the following corollary.

COROLLARY. *An additively closed set with a finite set of additive generators has a unique minimal set of additive generators.*

Imposing restrictions on the terms in the corollary of Theorem 2.7 we are able to derive a stronger result.

THEOREM 5. *Let $A \neq O$ be additively closed (convex). Then $A-(A-B) = (A+B)-A$.*

Proof. By the corollary of Theorem 2.7, $A-(A-B) \subset (A+B)-A$. To establish the converse inclusion we have, subtracting A (Theorem 2.1) from both members in Corollary 3 of Theorem 2.9,

$$(A + B) - A \subset (A - (A - B)) - A. \tag{1}$$

By the corollaries of Theorems 2.6, 2.8, and Theorems 2.1, 4.1

$$\begin{aligned}(A - (A - B)) - A &= A - (A + (A - B)) \subset A - ((A + A) - B) \\ &= A - (A - B).\end{aligned}$$

This with (1) implies $(A+B)-A \subset A-(A-B)$ which completes the proof.

5. **Linear spaces—subgroups.** In this section we investigate the geometrical notion *linear space* identifying it with the algebraic idea *subgroup*. We derive several interesting formulas for determination of linear spaces, which are analogous to familiar results on the generation of subgroups in classical group theory. The most important result in this section is Theorem 5.6, a restricted form of Dedekind's modular principle so familiar in lattice theory.

Having given an algebraic formulation of the notion *convex set* we proceed to study its important specialization, *linear manifold* or *linear space*. Linear spaces are usually characterized by the property of *linearity* or *flat-*

ness: a linear space S contains the line joining each pair of its points. Since line ab in a descriptive geometry is expressible in the form $a+b \cup a-b \cup b-a \cup a \cup b$, this is equivalent to: *S is a linear space if* $S \supset a, b$ *implies* $S \supset a \pm b$. This suggests the classical notion *subgroup*. Thus we adopt the following definition.

Definition 1. Let set S have the property: $S \supset a, b$ implies $S \supset a \pm b$. Then we say S is a *subgroup* of G or, in geometrical language, S is a *linear subspace* of G or simply a *linear space*[37].

We are using the term subgroup (or submultigroup) in a strong sense. It is used also in a weaker sense to denote a subset S which is a multigroup with respect to the composition in the given multigroup (see Dresher and Ore [1, p. 714]). In the present context this is equivalent to: $S \supset a, b$ implies $S \supset a+b$ and $S \approx a-b$. It is worthy of note that if G is a descriptive geometry of finite dimension its subgroups in the weaker sense are precisely its open convex subsets.

We weaken the closure requirement of Definition 5.1 in the following theorem.

THEOREM 1. *A is a subgroup (linear subspace) of G if and only if* (a) *A is closed under $-$, or* (b) $A \supset A-A$, *or* (c) $A = A-A$.

Proof. (a), (b) are obviously equivalent and (b) is equivalent to (c) in view of Theorem 2.3 (c). Thus we consider only (c). Its necessity is trivial. To prove its sufficiency, suppose $A = A-A$. We need show merely that A is closed under $+$. By Corollary 3 of Theorem 2.9

$$A + A \subset A - (A - A) = A - A = A$$

and the result follows by Theorem 4.1.

One of the most familiar geometrical ideas is that of *linear space determined by a set of elements*, for example, line determined by two points or plane determined by three noncollinear points. We can take this to characterize the simplest or least linear space which contains the given set of elements. In the present context, this is merely the least subgroup of G which contains the given set of elements. This suggests the following definition.

Definition 2. Suppose $S \subset G$. By the *subgroup of G generated by S* or the *linear subspace of G determined by S*, denoted $\{S\}$, we mean the least subgroup of G which contains S[38]. If $\{S\} = A$ we say S is a set of *generators* of group A. Similarly if $S_1, \cdots, S_n \subset G$ we define the *subgroup of G generated by* $S_1, \cdots, S_n$ to be the least subgroup of G which contains $S_1, \cdots, S_n$ and

[37] Observe that O, G and individual elements of G are subgroups of G. If A, B are subgroups of G so is $A \cdot B$ but not necessarily $A+B$. If $A \cdot B \neq O$, $A-B$ is a subgroup of G (Theorem 5.5).

[38] $\{S\}$ may be read briefly the *linear closure* or simply the *closure* of S. Compare Definition 4.2; $[S]$, $\{S\}$ are analogous respectively to *ring, field* generated by a set of elements in a field.

we denote it $\{S_1, \cdots, S_n\}$. (An illustration is the plane determined by two intersecting lines or the space determined by two skew lines.)

Observe that in a descriptive geometry line ab may be expressed as $\{a, b\}$, where $a \neq b$. In other words a line may be characterized as a linear space determined by two points. By contrast the ad hoc character of the standard definition, based on the property that a line is separated into three parts by any two of its points, is very marked. The two characterizations of line are equivalent when our postulate system is strengthened (see Theorem 11.2). It seems more in the spirit of modern mathematics to characterize basic notions by general properties and to deduce their special algebraic representations from the appropriate postulates, rather than to insinuate them into the base by the process of definition.

Obviously $\{S\}$, $\{S_1, \cdots, S_n\}$ exist and are uniquely determined. Note that $\{a\} = a$ and $\{O\} = O$. We proceed to derive formulas for $\{S\}$. First we have an easily proved analogue of a familiar result in classical group theory.

THEOREM 2. *$\{S\}$ is the set union of all polynomial expressions involving elements of S.*

COROLLARY. *$x \subset \{S\}$ if and only if $x \subset \{a_1, \cdots, a_n\}$ where $a_i \subset S$, $1 \leqq i \leqq n$.*

Now we deduce a simple formula for $\{S\}$.

THEOREM 3. $\{S\} = [S] - [S]$.

Proof. Any subgroup of G which contains S certainly contains $[S] - [S]$. Moreover by Theorem 2.3 (c), $[S] - [S] \supset [S] \supset S$. Thus we have to show merely that $[S] - [S]$ is a subgroup of G. Letting $A = [S]$ we have

$$
\begin{aligned}
(A-A)-(A-A) &= (A-(A-A))-A && \text{(Theorem 2.6, corollary)} \\
&\subset ((A+A)-A)-A && \text{(Theorem 2.7, corollary; Theorem 2.1)} \\
&= (A+A)-(A+A) && \text{(Theorem 2.6, corollary)} \\
&= A-A && \text{(Theorem 4.1)}
\end{aligned}
$$

and the result follows by Theorem 5.1.

Applying Theorem 4.3, we easily get a sharper result than Theorem 5.2.

COROLLARY 1. *$\{S\}$ is the set union of all polynomial expressions of the form $(a_1 + \cdots + a_n) - (b_1 + \cdots + b_m)$, involving elements of S.*

If S is additively closed $[S] = S$ and we have the following corollary.

COROLLARY 2. *$\{S\} = S - S$, if S is additively closed.*

We next consider the subgroup generated by a pair of sets.

THEOREM 4. $\{S, T\} = \{S+T\}$ [39].

[39] We can also show $\{S, T\} = \{S-T\}$ provided $S \neq O$.

Proof. If S or $T=O$ the theorem is trivial. Suppose S, $T\neq O$. Clearly $\{S, T\}\supset S+T$, so that $\{S, T\}\supset\{S+T\}$. Thus we need prove merely $\{S+T\}\supset S, T$. We have

$$\begin{aligned}\{S+T\} &\supset (S+T)-(S+T)\\ &= ((S+T)-S)-T && \text{(Theorem 2.6, corollary)}\\ &\supset (S-(S-T))-T && \text{(Theorem 2.7, corollary; Theorem 2.1)}\\ &\supset T-T && \text{(Theorem 2.9, corollary; Theorem 2.1)}\\ &\supset T && \text{(Theorem 2.3 (c)).}\end{aligned}$$

By symmetry $\{S+T\}\supset S$ and the proof is complete.

By induction we have the following corollary.

COROLLARY 1. $\{S_1, \cdots, S_n\}=\{S_1+\cdots+S_n\}$.

Taking the S's to be additively closed and applying Corollary 1 of Theorem 4.2 and Corollary 2 of Theorem 5.3 we get the following corollary.

COROLLARY 2. *Let $S_1, \cdots, S_n$ be additively closed. Then* $\{S_1, \cdots, S_n\}=(S_1+\cdots+S_n)-(S_1+\cdots+S_n)$.

Substituting for the S's individual elements, $a_1, \cdots, a_n$, we have the following corollary.

COROLLARY 3. $\{a_1, \cdots, a_n\}=(a_1+\cdots+a_n)-(a_1+\cdots+a_n)$[40].

This is, for *finite* sets S, a better result than Corollary 1 of Theorem 5.3. In view of the corollary of Theorem 5.2 we have for arbitrary S the following corollary.

COROLLARY 4. $\{S\}$ *is the set union of all polynomial expressions of the form* $(a_1+\cdots+a_n)-(a_1+\cdots+a_n)$, *involving elements of* S.

By Corollary 2 above, $\{A, B\}=(A+B)-(A+B)$, if A, B are additively closed. From this we derive the following important result.

THEOREM 5. *Let A, B be subgroups (linear subspaces) of G; $A\cdot B\neq O$. Then* $\{A, B\}=A-B$[41].

[40] As a geometrical illustration let $a_1, \cdots, a_n$ be the vertices of a convex polyhedron. Then $\{a_1, \cdots, a_n\}$ is the space which it determines and $a_1+\cdots+a_n$ is its interior.

[41] Compare Dresher and Ore [1, p. 725, Theorem 3], also Eaton and Ore [1, p. 67, Theorem 2]. This result is very important. Like its analogue in classical abelian group theory, $\{A, B\}=A+B$ (see van der Waerden [1, p. 134, Example 2 and Remark]), it gives the structure of $\{A, B\}$, the lattice join of A and B, directly in terms of an algebraic operation on these subgroups. Without it we could not obtain analogues of many important principles in classical group theory including modularity, semi-modularity (Theorems 5.6, 5.7) and the basic Isomorphism Theorem for factor groups (Theorem 7.3). The condition $A\cdot B\neq O$ is redundant in the classical case but is essential in our theory. As a counter-example take $A=a$, $B=b$, $a\neq b$, in a descriptive geometry.

Proof. First we show $A-B \supset B$. We have by Theorem 5.1 and Corollary 1 of Theorem 2.9([42])

$$A - B \supset A \cdot B - (A \cdot B - B) \supset B.$$

To complete the proof we have

$$\begin{aligned}
\{A, B\} &= (A + B) - (A + B) && \text{(Theorem 5.4, corollary 2)}\\
&= ((A + B) - A) - B && \text{(Theorem 2.6, corollary)}\\
&= (A - (A - B)) - B && \text{(Theorem 4.5)}\\
&= (A - B) - (A - B) && \text{(Theorem 2.6, corollary)}\\
&\subset ((A - B) + B) - A && \text{(Theorem 2.7, corollary)}\\
&\subset (A - B) - A && \text{(Theorem 4.1, corollary)}\\
&= (A - A) - B && \text{(Theorem 2.6, corollary)}\\
&= A - B && \text{(Theorem 5.1)}\\
&\subset \{A, B\}.
\end{aligned}$$

COROLLARY 1. $\{S, T\} = \{S\} - \{T\}$, *provided* $\{S\} \cdot \{T\} \neq O$.

COROLLARY 2. *Let* A, B *be subgroups of* G; $A \cdot B \neq O$. *Then* $A - B = B - A$.

COROLLARY 3. *Let* A, B *be subgroups of* G; $A \cdot B \neq O$. *Then* $A - (A - B) = A - B$.

Proof. $A - B = \{A, B\} \supset A - (A - B) = A - \{A, B\} \supset A - B$.

We can now deduce a restricted form of Dedekind's famous modular law which is important in the lattice theory of certain algebraic systems and of projective geometry.

THEOREM 6. *Let* A, B, C *be subgroups of* G; $A \cdot B \neq O$. *Then* $A \subset C$ *implies* $\{A, B\} \cdot C = \{A, B \cdot C\}$([43]).

Proof. First we show

$$(A - B) \cdot C = A - B \cdot C. \tag{1}$$

It is easily shown that $A, B \cdot C \neq O$, so that

$$A - B \cdot C \subset A - B \tag{2}$$

([42]) Henceforth we shall use the monotonic principles (Theorem 2.1 and its corollaries) without reference.

([43]) See Birkhoff [1, p. 34, Postulate L5, p. 35, Theorem 3.2]. Compare Dresher and Ore [1, p. 736, Theorem 5]. This is a kind of distributive law since $A = A \cdot C$. The condition $A \cdot B \neq O$ is essential, for a counter-example let A be a point and B, C parallel lines in a descriptive geometry. In lattice theoretic terminology this result is equivalent to: *The lattice of all subgroups of* G *which contain a given non-empty subgroup of* G *is modular.* This implies: *The lattice of all linear subspaces of a descriptive geometry which contain a given point is modular.*

follows by the monotonic principle. Further, since C is a subgroup of G, the relations $A, B \cdot C \subset C$ imply

$$A - B \cdot C \subset C. \tag{3}$$

From (2), (3) we have $A - B \cdot C \subset (A - B) \cdot C$.

To establish the converse inclusion let $x \subset (A - B) \cdot C$. Then we have by Theorem 2.2

$$x \subset a - b \tag{4}$$

where $a \subset A$, $b \subset B$; in addition $x \subset C$. Solving (4) for b we have $b \subset a - x$. Since $A \subset C$ and C is a subgroup of G, this implies $b \subset C$ and hence $b \subset B \cdot C$. Thus (4) implies $x \subset A - B \cdot C$. Hence $(A - B) \cdot C \subset A - B \cdot C$ and (1) is justified.

Since $A \cdot B = A \cdot (B \cdot C) \neq O$ we may apply Theorem 5.5 to (1) getting $\{A, B\} \cdot C = \{A, B \cdot C\}$.

A slight modification of the derivation of (1) above yields the following corollary.

COROLLARY. *Let A, B, C be subgroups of G; $A \cdot C \neq O$. Then $B \subset C$ implies* $(A - B) \cdot C = A \cdot C - B$.

We now introduce a familiar notion of classical group theory which has been studied abstractly in lattice theory.

Definition 3. Let A, B be subgroups of G such that B is a maximal *proper* subset of A. Then we say A *covers* B.

Following well known lattice theoretic developments we derive from the last theorem a restricted form of semi-modularity.

THEOREM 7. *Let A, B, C be subgroups of G such that A and B cover $C \neq O$ and $A \neq B$. Then $\{A, B\}$ covers A, B*(44).

Proof. We show $\{A, B\}$ covers A. $\{A, B\} \supset A$. Suppose $\{A, B\} = A$. Then $A \supset B \supset C$ which implies, since A covers C, that $B = A$ or C, contrary to hypothesis. Hence $\{A, B\} \neq A$. Let X be a subgroup of G satisfying

$$\{A, B\} \supset X \supset A. \tag{1}$$

It suffices to show $X = \{A, B\}$ or $X = A$. Multiplying (1) by B, we get

$$B \supset B \cdot X \supset A \cdot B \supset C.$$

Hence $B \cdot X = B$ or $B \cdot X = C$, since B covers C. Suppose $B \cdot X = B$. Then $X \supset B$ and (1) implies $X = \{A, B\}$. Consider the other possibility, $B \cdot X = C$. $C \neq O$ implies $A \cdot B \neq O$. Hence (1), Theorem 5.6 imply

$$X = \{A, B\} \cdot X = \{A, B \cdot X\} = \{A, C\} = A$$

and the proof is complete.

(44) Compare Birkhoff [1, p. 34, Corollary 3]. We are following a proof due to Birkhoff, *On the combination of subalgebras*, Proc. Cambridge Philos. Soc. vol. 29 (1933) pp. 441–464.

6. **Linear independence.** In this section we introduce the notion *linear independence* and use it to characterize the geometric idea *simplex*.

In forming a set of generators of a group (linear space) it is desirable for many purposes to omit redundant elements. This suggests the following definition.

Definition 1. Suppose $S \subset G$. Suppose[45] $\{S \dot{-} x\} \not\supset x$ for each $x \subset S$. Then we say S is *linearly independent* or simply *independent*[46].

In §4 we might have framed a similar definition for *additive* independence merely by replacing { } by [ ] in Definition 6.1. It would then follow that S is additively independent if and only if S is a minimal set of generators of $[S]$.

The following properties of independent sets are easily derived: (1) *Any subset of an independent set is also independent.* (2) *A set is independent provided each of its finite subsets is independent.* (3) *Let S be a set of generators of group G. Then S is independent if and only if S is a minimal set of generators of G.*

We characterize linear independence solely in terms of the operation $+$ in the following theorem.

THEOREM 1. *S is independent if and only if the sets $a_1 + \cdots + a_n$, where the a's are in S and $a_i \neq a_j$ for $i \neq j$, are disjoint*[47].

Proof. Suppose S independent. Let $a_1 + \cdots + a_n$, $a_1' + \cdots + a_m'$ be sets of the type described, satisfying

$$a_1 + \cdots + a_n \approx a_1' + \cdots + a_m'. \tag{1}$$

If a letter appears in only one member of (1) we can solve (1) for this letter, which is therefore "dependent" on the other letters in (1). This contradicts our supposition. Hence the members of (1) are identical except possibly for the order of the letters, and the necessity of the condition is established.

To prove its sufficiency, suppose S satisfies the given condition. Assume S not independent. Then $a \subset \{S \dot{-} a\}$ for some $a \subset S$. By the corollary of Theorem 5.2 and Corollary 3 of Theorem 5.4

$$a \subset \{a_1, \cdots, a_n\} = (a_1 + \cdots + a_n) - (a_1 + \cdots + a_n)$$

where $a_i \subset S \dot{-} a$. Hence

$$a + a_1 + \cdots + a_n \approx a_1 + \cdots + a_n$$

contrary to our supposition. Thus S is independent and the proof is complete.

This is immediately applicable to the expansions of $[S]$ given in §4.

---

(45) We use the symbol $\dot{-}$ to denote *set theoretic* subtraction.

(46) Compare Alexandroff-Hopf [1, p. 595, Definition].

(47) That is if $a_1 + \cdots + a_n$, $a_1' + \cdots + a_m'$ are such sets having a common element, then $m = n$ and the a''s form a permutation of the a's.

COROLLARY 1. *The expansion of* $[S]$ (*Theorem* 4.3) *as the set union of all expressions* $a_1+\cdots+a_n$, *where the a's are in S, is a decomposition* (*that is, an expansion into disjoint sets*) *if and only if S is an independent set.*

COROLLARY 2. *The expansion of* $[a_1, \cdots, a_n]$ (*Theorem* 4.3, *corollary*) *in terms of sums of the a's is a decomposition if and only if* $a_1, \cdots, a_n$ *are distinct and form an independent set.*

These corollaries suggest the study of those additively closed (convex) sets A which have *independent* sets of additive generators, S. Such a set S is easily seen to be a *minimal* set of additive generators of A. Thus in view of Theorem 4.4 we may assert the following theorem.

THEOREM 2. *Let the additively closed* (*convex*) *set A have an independent set of additive generators S. Then S is a minimal set of additive generators of A and is uniquely determined*[48].

In a sense the simplest and fundamental type of additively closed (convex) set is that having a set of additive generators which is *finite* and *independent*. This suggests the following definition.

Definition 2. Suppose $a_1, \cdots, a_n$ are distinct and form an independent set. Then $[a_1, \cdots, a_n]$ is called an *n-simplex* or *simplex of rank* n[49].

One easily derives the following theorem.

THEOREM 3. *An n-simplex A has a uniquely determined rank. Any set of additive generators of A contains at least n elements. A set of additive generators of A containing exactly n elements is independent and is uniquely determined.*

7. **Half-spaces—cosets.** This section is devoted to the study of *half-spaces* (rays, half-planes, and so on) which bear a striking analogy to *cosets* in classical abelian group theory. Many related geometric notions, for example, *angle, spherical geometry, separation of linear spaces*, appear embedded in a nexus of algebraic ideas associated with the notion *factor group*.

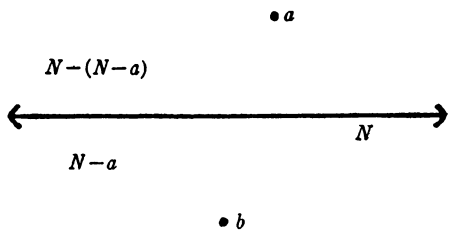
Half-spaces may be considered to arise as "separation sets" in the decomposition of a linear space N effected by a linear subspace of dimension one less than that of N. This approach is not convenient in the present context since we should have to establish elaborate separation theorems before discussing half-spaces[50]. Our viewpoint is best explained by an example. In a descriptive space let N be a line and suppose point $a \not\subset N$. We usually say point b is on the *opposite side* of N from a, if $a+b \approx N$. Since this condition is equivalent to $b \subset N-a$, the set of points on the opposite side of N from a may be

[48] Compare Alexandroff-Hopf [1, p. 604, Theorem 6].

[49] This is usually called an $(n-1)$-simplex or simplex of dimension $n-1$. In the present context our definition is more natural.

[50] As a matter of fact it is impossible to deduce the familiar descriptive separation theory on the basis J1, $\cdots$, J7 (see §10).

represented by $N-a$. This suggests taking $N-(N-a)$ to be the set of points on the *same side* of N as a, or the half-plane with edge N determined by a. Thus we adopt the following definition.



Definition 1. Let $N \neq O$ be a subgroup of G. Then $N-(N-a)$, denoted $(a)_N$, is called the *half-space*[51] *with edge N determined by a*. To indicate its role in the algebraic development we also call it the *coset of N determined by a*. We adopt the notation $(A)_N$ to represent the set of cosets of the form $(a)_N$ where $a \subset A$[52].

We proceed to develop the algebraic properties of cosets. In the main they are analogous to the classical ones.

THEOREM 1. *Let $N \neq O$ be a subgroup of G. Then the cosets of N are additively closed*[53], *disjoint, and exhaust G.*

Proof. By Theorem 4.2, $(a)_N$ is additively closed. By Corollary 1 of Theorem 2.9, $a \subset (a)_N$. It remains to show the cosets disjoint. Supposing

$$a \subset (b)_N = N - (N - b) \tag{1}$$

it suffices to show $(a)_N = (b)_N$. From (1) by the formal principles of §2 and the relations $N+N=N-N=N$ we get

$$\begin{aligned} N - a &\subset N - (N - (N - b)) \subset (N + (N - b)) - N \\ &\subset (N - b) - N = N - b. \end{aligned}$$

Solving (1) for b, we have $b \subset N-(N-a)=(a)_N$, so that $N-b \subset N-a$ by the above argument. Thus $N-a=N-b$ so that $(a)_N=(b)_N$ and the proof is complete.

---

(51) This is to some extent a misnomer since in a descriptive geometry $N-(N-a)$ is a half-space in the familiar *geometric* sense only if $a \not\subset N$. If $a \subset N$ then $N-(N-a)=N$ (Theorem 7.3, corollary). However this exception causes no difficulty since the familiar properties of geometric half-spaces are subsumed in the coset theory which follows.

(52) Observe that in classical abelian group theory $N-(N-a)=N+a$, the familiar expression for a coset. In adopting the notation $(A)_N$ we consider $(\ )_N$ a functional operator which is applied to each $a \subset A$; compare $f(S)$ in topology where S is a point set and f a point mapping.

(53) This property holds in virtue of J4; it fails in classical group theory.

COROLLARY 1. $(a)_N \supset a$; $b \subset (a)_N$ *implies* $(a)_N = (b)_N$.

COROLLARY 2. *Let* $N \neq O$ *be a subgroup of* G. *Then* $(a)_N = (b)_N$ *if and only if* $N-a = N-b$.

We now introduce the notion *congruence modulo* N and deduce its basic properties.

Definition 2. If $(a)_N = (b)_N$ we write $a \equiv b \pmod N$. In general, if for each $a \subset A$ there is a $b \subset B$ such that $a \equiv b \pmod N$ and vice versa, we write $A \equiv B \pmod N$. Clearly this is equivalent to $(A)_N = (B)_N$.

The algebraic motivation of the relation $a \equiv b \pmod N$ should not be allowed to obscure its important geometric content. It is obviously equivalent to: a and b are in the same coset of N. Thus it signifies in a descriptive geometry that a, b are in N or are on the *same side* of N.

THEOREM 2. *The relation congruence modulo* N *has the following properties*: (a) $a \equiv a \pmod N$; (b) $a \equiv b \pmod N$ *implies* $b \equiv a \pmod N$; (c) $a \equiv b \pmod N$, $b \equiv c \pmod N$ *imply* $a \equiv c \pmod N$; (d) $a \equiv a' \pmod N$, $b \equiv b' \pmod N$ *imply* $a+b \equiv a'+b' \pmod N$; (e) $a+n \equiv a \pmod N$ *for* $n \subset N$[54].

Proof. (a), (b), (c) are immediate. To establish (d), (e) we first prove that

$$N - (N - A) = N - (N - B) \tag{1}$$

implies $A \equiv B \pmod N$[55]. Suppose (1). Suppose $a \subset A$. Then $a \subset N-(N-A)$ by Corollary 1 of Theorem 2.9 and (1) implies $a \subset N-(N-b) = (b)_N$ for some $b \subset B$. Thus by Corollary 1 of Theorem 7.1, $(a)_N = (b)_N$ and $a \equiv b \pmod N$. Similarly for each $b \subset B$ there exists an $a \subset A$ such that $b \equiv a \pmod N$. Thus $A \equiv B \pmod N$ and our assertion is proved.

Now to prove (d) suppose $a \equiv a' \pmod N$ and $b \equiv b' \pmod N$. Hence by Corollary 2 of Theorem 7.1, $N-a = N-a'$ and $N-b = N-b'$. Thus using the corollary of Theorem 2.6

$$\begin{aligned} N - (N - (a + b)) &= N - ((N - a) - b) = N - ((N - a') - b) \\ &= N - ((N - b) - a') = N - ((N - b') - a') \\ &= N - (N - (a' + b')) \end{aligned}$$

and $a+b \equiv a'+b' \pmod N$ by the assertion proved in the first paragraph.

To prove (e) suppose $n \subset N$. Then by Theorem 5.5, $N-n = \{N, n\} = N$. Hence

$$N - (N - (a + n)) = N - ((N - n) - a) = N - (N - a)$$

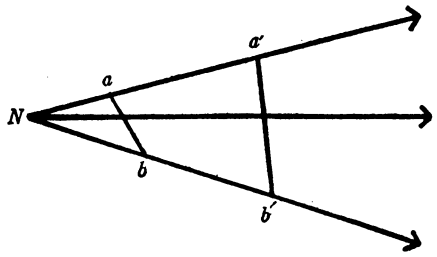
and $a+n \equiv a \pmod N$ follows.

---

(54) Thus n is an identity element of $+$ with respect to the equivalence relation "congruence modulo N."

(55) The converse also is true.

The reader should find it interesting to interpret the theorem geometrically. The diagram illustrates (d), which involves a basic property of angles of arbitrary dimension (see Forder [1, p. 70, Theorem 7]).



As in classical group theory we adopt the following definition.

Definition 3. Let G/N denote the set of all cosets of N determined by elements of G. We define addition in G/N thus: $(a)_N+(b)_N=(a+b)_N$[56]. We call G/N with addition so defined the *factor group of G with respect to N*. The *order* of the factor group G/N is the cardinal number of the set G/N.

G/N, similar to G, is a group-like system with many-valued composition—in fact it is a multigroup, although not in general of the type of G. Hence we carry over to G/N various notations and definitions adopted in G—in particular the use of the inclusion signs $\supset$, $\subset$ to cover sets *and* elements and the definitions of addition and subtraction (Definitions 1.1, 1.2, 2.1). Capital letters A, B, C, $\cdots$ are used to represent elements of G/N. These agreements sometimes entail ambiguity, for example $(a)_N+(b)_N$ may mean a sum of sets in G or a sum of elements (cosets) in G/N. To resolve this and similar ambiguities the context will always indicate the universe of discourse whether G or G/N.

To determine the geometric significance of the factor group let G be a descriptive space of finite dimension and let $N\neq O$, G be a linear subspace of G. Then the elements of G/N are half-spaces with edge N. Let $(a)_N$, $(b)_N$ be half-spaces which form an angle aNb[57]. Their sum, as elements of G/N, is the set of half-spaces *in*[58] the angle aNb. Thus the notion of angle of arbitrary dimension and its rather peculiar and specialized properties (see, for example, Forder [1, pp. 69–72]), which in the classical treatment seem to be motivated solely by geometrical intuition, are contained in the theory of factor groups.

---

(56) The apparent ambiguity in the determination of the sum is resolved in the succeeding corollary.

(57) This is equivalent to the restriction $a, b \not\subset N$ and $(a)_N, (b)_N$ are distinct and not opposite half-spaces. See Forder [1, p. 69, Definition 3, p. 85, Definition 25.2] for plane, dihedral angles respectively.

(58) See Forder [1, p. 69, Definition 5, p. 85, Definition 25.4].

Now let us restrict G to be a *Euclidean* space and N a *point*. Then G/N is essentially the set of rays issuing from point N. Projecting the rays of G/N onto a hypersphere centered at N, we see that G/N is essentially a *spherical space*, geometrized by defining the minor arc of a great circle joining two points as their "sum" or "join"([59]). It is an indication of the integrating power of our group theoretic methods in classic geometry that the age-old relation between Euclidean and spherical geometries should turn out to be that one is a factor group, and in the light of the next section, a homomorph of the other. This intimate connection may be advantageously used to study both subjects.

We proceed to study factor groups. As we observed in Definition 7.2, $A \equiv B \pmod{N}$ is equivalent to $(A)_N = (B)_N$. Thus a "congruence modulo N" in G becomes an equality in G/N. As an application of this, suppose $(a)_N = (a')_N$, $(b)_N = (b')_N$. Then $a \equiv a' \pmod{N}$, $b \equiv b' \pmod{N}$ so that $a+b \equiv a'+b' \pmod{N}$ by the last theorem. Thus $(a)_N+(b)_N = (a+b)_N = (a'+b')_N = (a')_N+(b')_N$ and we may assert the following corollary.

COROLLARY. *Addition of cosets in G/N is independent of the elements of G which determine the cosets.*

It is easily seen that $+$ in G/N, as in G, is associative, commutative, idempotent. In regard to subtraction, G/N is exactly analogous to a classical abelian group and is conveniently studied in the familiar manner. Thus we introduce the following definition.

Definition 4. Let I be an element of G/N such that $A+I = I+A = A$ for each A in G/N. Then we say I is an *identity element* of G/N([60]).

As in classical group theory we have the following theorem.

THEOREM 3. *G/N has a unique identity element, namely, N.*

Proof. Suppose $n \subset N$. By (e) of the last theorem, $a+n \equiv a \pmod{N}$. Hence $(a+n)_N = (a)_N+(n)_N = (a)_N$. By Theorem 5.5, $(n)_N = N-(N-n) = N$ so that N is an identity element of G/N. Obviously it is the only identity element.

COROLLARY. *If $n \subset N$ then $(n)_N = N$.*

The existence of an identity element in G/N naturally suggests the notion of inverse element as characterized in the following theorem.

THEOREM 4. *In G/N, for each element A there exists a unique element X satisfying $A+X \supset N$*([61]).

Proof. Suppose

([59]) This is true even if N is not a point (see Theorem 10.1).

([60]) Weaker notions of identity element or unit have been introduced in multigroup theory, see Dresher and Ore [1, p. 707].

([61]) That is, coset N is an element in the set of cosets $A+X$—there is no ambiguity since G/N is indicated as the universe of discourse. It is of interest that the relation $A+X = N$ is impossible unless $A = N$.

$$A + X \supset N \tag{1}$$

where $A=(a)_N$, $X=(x)_N$. Then $(a)_N+(x)_N=(a+x)_N\supset N$ so that $a+x\supset n$ where $(n)_N=N$ and $n\subset N$. Thus we have

$$a + x \approx N. \tag{2}$$

This implies $N-x\supset a$ so that $X=N-(N-x)\supset N-a$. Thus (1) has at most one solution X, by Theorem 7.1. To show (1) has a solution we choose $x\subset N-a$; then (2) is satisfied, and we retrace our steps to (1).

This theorem suggests a formal definition of *inverse* in G/N.

Definition 5. In G/N, the unique solution of the relation $A+X\supset N$ is called the *inverse* of A or the half-space *opposite* to A, and is denoted by $-A$. Similarly if α is a subset of G/N (that is, a set of cosets of N) $-\alpha$ denotes the set of inverses of the elements in α.

We can now conveniently express some results which are implicit in the last theorem.

COROLLARY 1. *In* G/N, $-(-A)=A$.

COROLLARY 2. $-(a)_N=(a')_N$ *if and only if* (1) $a+a'\approx N$ *or* (2) $a'\subset N-a$.

In proving the last theorem we showed, in view of the unique determination of X, that $X=-A\supset N-a\supset X$. Thus we may assert the following corollary.

COROLLARY 3. $-(a)_N=N-a$.

This principle is useful since it gives us a simple formula in G for the inverse of a coset. We now obtain from it an important simplification in the formal expression for a coset. Suppose $a+a'\approx N$. Taking inverses of the members in Corollary 2, and applying Corollaries 1, 3 we have $(a)_N=-(a')_N=N-a'$. Thus we may assert the following corollary.

COROLLARY 4. *Let* N *be a subgroup of* G. *Suppose* $a+a'\approx N$ *or equivalently* $a'\subset N-a$. *Then* $(a)_N=N-(N-a)=N-a'$.

We now establish the familiar formula for the inverse of a sum.

THEOREM 5. *In* G/N, $-(A+B)=(-A)+(-B)$[62].

Proof. Let S be the set union of the cosets contained in the left member of this equation. Let T have the same relation to the right member. In view of Theorem 7.1 this equation in G/N is equivalent to $S=T$ in G. Thus we have only to identify S and T as sets in G.

Suppose $A=(a)_N$, $B=(b)_N$. By preceding definitions and Corollary 3 of the last theorem we have, denoting set summation in G by Σ,

[62] In geometrical language: *the set of half-spaces opposite those in a given angle is identical with the set of half-spaces in its vertical angle.*

$$S = \sum_{X \subset -(A+B)} X = \sum_{X \subset -(a+b)_N} X = \sum_{x \subset a+b} -(x)_N = \sum_{x \subset a+b} (N - x)$$
$$= N - (a + b).$$

Similarly if $a+a' \approx N$ and $b+b' \approx N$ we have by Corollary 2 of the last theorem

$$T = \sum_{X \subset (-A)+(-B)} X = \sum_{X \subset (a'+b')_N} X = \sum_{x \subset a'+b'} (x)_N = N - (N - (a' + b')).$$

We proceed to show $N-(a+b)=N-(N-(a'+b'))$. We have, using formal principles of §2 and the last corollary,

$$N - (a + b) = (N - a) - b = (N - (N - a')) - b = (N - b) - (N - a')$$
$$= (N - (N - b')) - (N - a') = N - ((N - a') + (N - b'))$$
$$\subset N - (((N - a') + N) - b') \subset N - (((N + N) - a') - b')$$
$$= N - (N - (a' + b')).$$

The converse inclusion is derived similarly. Thus $S=T$ and the theorem is established.

COROLLARY 1. $N-(a+b)=\sum_{X \subset -(a+b)_N} X$.

COROLLARY 2. *Let N be a subgroup of G. Suppose $a+a' \approx N$, $b+b' \approx N$. Then $N-(a+b)=N-(N-(a'+b'))$.*

We complete the present line of development by deducing the familiar relationship between subtraction and addition. Interpreted geometrically, it becomes a property of supplementary adjacent angles (cf. Forder [1, p. 71, Theorem 9.4]).

THEOREM 6. *In G/N, $A-B=A+(-B)$.*

Proof. We use the method of the last theorem. Suppose $S=\sum_{X \subset A-B} X$ and $T=\sum_{X \subset A+(-B)} X$. Suppose $X=(x)_N$, $A=(a)_N$, $B=(b)_N$. We transform the relation $X \subset A-B$ into a more convenient form in G. It is equivalent to $B+X \supset A$ and so to $(b+x)_N \supset (a)_N$. This is seen to be equivalent to $b+x \approx (a)_N$ and so by Corollary 4 of Theorem 7.4 to $x \subset (a)_N - b = N-(a'+b)$, where $a+a' \approx N$. Hence

$$S = \sum_{x \subset N-(a'+b)} (x)_N = \sum_{x \subset N-(a'+b)} (N - (N - x))$$
$$= N - (N - (N - (a' + b))).$$

Similarly we can show $T=N-(N-(a+b'))$, where $b+b' \approx N$. Hence by the last corollary $S=T$ and the result follows.

Thus far in the present section we have studied analogues of general results in classical group theory. Now we consider a simple special property which suggests an important geometric concept.

THEOREM 7. *Let $N \neq O$ be a proper subgroup of G. Then the order of G/N is greater than or equal to 3.*

Proof. Suppose $a \subset G$, $a \not\subset N$. Then G/N contains N, $(a)_N$, and its inverse $(b)_N$. These cosets are easily seen to be distinct. For example if we suppose $(a)_N = (b)_N$ we have by Corollary 2 of Theorem 7.4, $a+a \approx N$, that is $a \subset N$. Thus the order of G/N is at least 3.

The case in which the order of a factor group G/N is exactly 3 is especially interesting, since here the coset decomposition of G (Theorem 7.1) is as simple as possible, without being trivial. This suggests the following definition.

Definition 6. Let A, B be subgroups (linear subspaces) of G such that the order of A/B is 3. Then we say B *separates* A.

Suppose B separates A. Then A/B consists of three elements. These must be B and two other cosets S, S' which are inverses of each other. Thus B, S, S' form a coset decomposition of A and we may assert the following theorem.

THEOREM 8. *Let B separate A. Then A is decomposed into B, S, S' where S, S' are mutually inverse cosets of B.*

Now suppose $a \subset A$, $a \not\subset B$, $a+a' \approx B$. Then cosets B, $(a)_B$, $(a')_B$ are distinct and must constitute the coset decomposition of A. Further $(a)_B = B-a'$ and $(a')_B = B-a$ by Corollary 4 of Theorem 7.4. Thus we may assert the following corollary.

COROLLARY. *Let B separate A. Suppose $a \subset A$, $a \not\subset B$, $a+a' \approx B$. Then $A = B \cup B-a \cup B-a'$, where the addends are disjoint.*

Now we relate Definition 6 to the more familiar idea of separation in the foundations of geometry. Suppose B separates A. Then A is decomposed into B, S, S' where S, S' are mutually inverse cosets of B. Hence the following properties hold: (1) $A = B \cup S \cup S'$ and B, S, S' are disjoint; (2) S, $S' \neq O$ are convex sets (Theorem 7.1); (3) the join of any element of S to any element of S' meets B (Theorem 7.4, Corollary 2). Properties (1), (2), (3) are essentially the criteria of the foundations of geometry for the separation of a linear space A by a linear subspace B[63].

Conversely suppose that A, B are linear spaces for which sets S, S' exist satisfying (1), (2), (3) above. Suppose $a \subset S$. Then by (3), $x \subset S'$ implies $x+a \approx B$ and $x \subset B-a$. Thus $S' \subset B-a$ Similarly $S \subset B-a'$, where $a' \subset S'$. By (3), $a+a' \approx B$ and we can apply Corollary 4 of Theorem 7.4, getting $B-a' = (a)_B$, $B-a = (a')_B$. Hence in view of (1), $A = B \cup (a)_B \cup (a')_B$. The cosets B, $(a)_B$, $(a')_B$ are distinct since B, S, S' are disjoint and $(a)_B$, $(a')_B$ are mutually inverse by Corollary 2 of Theorem 7.4. Hence A/B has order 3

---

[63] See Veblen [2, p. 21, corollary].

and B separates A in the sense of Definition 7.6. Thus our definition is equivalent to the familiar *geometric* notion of separation of linear spaces. For our purposes it is preferable because it facilitates algebraic discussion and enables us to derive, by a *general* argument, a separation theorem for linear spaces of arbitrary dimension (Theorem 10.6).

8. **Congruence relations and homomorphisms.** In this section we study the intimately related notions of *congruence relation* and *homomorphism*. We obtain analogues of familiar homomorphism and isomorphism theorems of classical group theory and our discussion of congruence relations with an identity leads to a deeper, group theoretic characterization of the notion *coset*.

The notion *congruence relation* arises by abstraction from the basic properties of the relation "congruence modulo N" in Theorem 7.2. We define it in a general type of mathematical system not necessarily a group.

Definition 1. Let $(S; \circ)$ be a mathematical system involving elements $a, b, c, \cdots$ and an arbitrary 2-term operation $\circ$ (not necessarily single-valued). Let $\equiv$ be a relation defined in S which satisfies: (a) $a \equiv a$; (b) $a \equiv b$ implies $b \equiv a$; (c) $a \equiv b$, $b \equiv c$ imply $a \equiv c$; (d) $a \equiv a'$, $b \equiv b'$ imply $a \circ b \equiv a' \circ b'$([64]). Then we call $\equiv$ a *congruence relation*([65]) in $(S; \circ)$ or simply in S. If element i has the property $x \circ i \equiv i \circ x \equiv x$ for each x in S, we say i is an *identity element for* $\circ$ *with respect to* $\equiv$ or simply an *identity element* of $\equiv$.

By (a), (b), (c), $\equiv$ is an equivalence relation and so effects a decomposition of S into a set, denoted $S(\equiv)$, of maximal classes of congruent elements called the *residue classes* of $\equiv$. We convert $S(\equiv)$ into a "factor" or "quotient" system by defining in $S(\equiv)$ a composition $\circ$ as follows:

$$R(x) \circ R(y) = R\left(\sum_{u \subset R(x),\, v \subset R(y)} u \circ v \right)$$

where $R(x)$ denotes the residue class containing x and $R(X)$, for X a subset of S, denotes the set of $R(x)$ for $x \subset X$. In virtue of (d), $R(x) \circ R(y) = R(x \circ y)$. This of course suggests the concept homomorphism and so we introduce the following definition.

Definition 2. Let $(S; \circ)$, $(S'; \circ)$ be two systems such that there exists a single-valued mapping f of S on S' satisfying $f(x \circ y) = f(x) \circ f(y)$. Then we call f a *homomorphism* of S and say that $(S; \circ)$ is *homomorphic* to $(S'; \circ)$ or simply that S is *homomorphic* to S'([66]). If f is (1-1) we say S is *isomorphic* to S' and we write $S \cong S'$.

Hence we may assert: S *is homomorphic to* $S(\equiv)$. Thus we have associated a homomorphism of S to any given congruence relation in S. Conversely let f

([64]) We interpret statements of the form $A \equiv B$ where A, B are sets to mean: *every element of each set has the relation* $\equiv$ *to some element of the other set.*

([65]) Compare the notion *conjugation* of H. Campaigne, *Partition hypergroups*, Amer. J. Math. vol. 62 (1940) pp. 599–612.

([66]) Compare Dresher and Ore [1, p. 720]; also see Eaton and Ore [1, pp. 68, 69].

be a homomorphism of S into S'. Let $x \equiv y$ mean $f(x) = f(y)$. Then $\equiv$ is a congruence relation in S and in addition: *S' is isomorphic to $S(\equiv)$*. Thus the notions homomorphism and congruence relation are essentially equivalent and it is immaterial in theory which we choose to study([67]).

The most important instance of the idea congruence relation for our present purposes is of course the relation *congruence modulo N* in a group G. In this case the residue classes are the cosets of N and $G(\equiv)$ is G/N. Thus we may assert the following theorem.

THEOREM 1. *G is homomorphic to G/N.*

We shall not consider general congruence relations (or homomorphisms) in G. But we do wish to characterize the relations *congruence modulo N* in the class of all congruence relations in G. In view of Theorem 7.2 this is settled by the following theorem.

THEOREM 2. *Any congruence relation in G which has an identity element is the relation congruence modulo N, where N is the set of identity elements of the given congruence relation.*

Proof. Let $\equiv$ be a congruence relation in G whose set of identity elements $N \neq O$. First we show N is a subgroup of G. Suppose $n \subset n_1 - n_2$ where $n_1, n_2 \subset N$. Then $n \equiv n + n_2 \supset n_1$, so that $n \equiv n_1$. Hence for arbitrary x in G, $x + n \equiv x + n_1 \equiv x$ so that n is an identity element of $\equiv$, and $n \subset N$. Thus N is a subgroup of G by Theorem 5.1. Observe that in proving this we have shown that $n \equiv n_1$ where $n_1 \subset N$ implies $n \subset N$.

Now suppose $a \equiv b$. Let $b' \subset N - b$. Then $a + b' \equiv b + b' \approx N$. Hence $a + b' \supset t$ where $t \equiv n_3$ and $n_3 \subset N$. Thus $t \subset N$ so that $a + b' \approx N$ and $a \subset N - b' \subset N - (N - b)$. Hence $(a)_N = (b)_N$ and $a \equiv b \pmod{N}$. Conversely suppose $a \equiv b \pmod{N}$. Then $a \subset N - (N - b)$ so that by repeated transposition $N - a \approx N - b$ which implies $N + a \approx N + b$. Since $a \equiv N + a$, $b \equiv N + b$ we have $a \equiv b$ and the proof is complete.

Let us see what this result signifies for the characterization of the idea *coset*. In classical abelian group theory cosets are defined as expressions in the form $a + N$, where N is a subgroup of the given group. It is then easy to show that these expressions are characterized by the property of being residue classes of congruence relations, which of necessity in *classical* group theory have identity elements. In our groups G the expressions $a + N$ do not enjoy this property—in fact they do not even constitute a decomposition of G. Geometric intuition suggested studying half-spaces as expressions in the form $N - (N - a)$, which *did* have properties analogous to those of cosets in the classical abelian theory. Nevertheless the question arises whether it is appropriate to *identify* this algebraic form with the idea coset. The answer, I

([67]) Compare Birkhoff [1, p. 3] for single-valued operations.

think, is indicated in the last theorem and is given explicitly by the following corollary.

COROLLARY 1. *The residue classes of any congruence relation in G which has an identity element are of the form $N-(N-a)$, where $N\neq O$ is a fixed subgroup of G.*

Thus we have a purely group theoretic motivation for the study of half-spaces in descriptive geometry!

We continue by paraphrasing the last theorem in terms of homomorphism. In the abstract theory sketched above, a congruence relation in S which has an identity element corresponds to a *homomorphism* of S into S' such that S' has an *identity element* in the sense of Definition 7.4, that is, an element i such that $x \circ i = i \circ x = x$ for each x in S'. Thus we may assert the following corollary.

COROLLARY 2. *Let group G be homomorphic to a system G' having an identity element i. Then G' is isomorphic to G/N, where N is the set of elements of G mapped on i*([68]).

We conclude this section with a well known isomorphism theorem of classical group theory. First it is necessary to establish the following lemma.

LEMMA. *Let A, B be subgroups of G; $A \cdot B \neq O$. Then $\{A, B\} = \sum_{b \subset B} (b)_A$.*

Proof. By Corollary 3 of Theorem 5.5

$$\{A, B\} = A - (A - B) = \sum_{b \subset B} (A - (A - b)) = \sum_{b \subset B} (b)_A.$$

As an illustration let A, B be distinct intersecting lines in a descriptive space. Then $\{A, B\}$ is the plane "determined by" A, B and the lemma asserts essentially that a point is in this plane if and only if it lies on the same side of A as a point of B.

Now we can prove the following theorem.

THEOREM 3 (ISOMORPHISM THEOREM). *Let A, B be subgroups of G; $A \cdot B \neq O$. Then $\{A, B\}/A$ is isomorphic to $B/A \cdot B$*([69]).

Proof. In view of the lemma, any coset in $\{A, B\}/A$ is expressible in the form $(b)_A$ where $b \subset B$. Let T denote the correspondence $(b)_A \rightarrow (b)_{A \cdot B}$, where $b \subset B$. T maps $\{A, B\}/A$ into $B/A \cdot B$. We show T is a (1-1) correspondence. Suppose $(b_1)_A = (b_2)_A$ where $b_1, b_2 \subset B$. We have by Corollary 2 of Theorem 7.1

$$A - b_1 = A - b_2.$$

([68]) Compare Eaton and Ore [1, p. 68, Theorem 3].

([69]) Compare Dresher and Ore [1, p. 726, Theorem 6]; also see Eaton and Ore [1, p. 68]. For classical groups see Albert [1, p. 134, Theorem 15]; van der Waerden [1, p. 136, the first Isomorphism Theorem].

Thus

$$(A - b_1)\cdot B = (A - b_2)\cdot B$$

and by the corollary of Theorem 5.6

$$A\cdot B - b_1 = A\cdot B - b_2$$

so that by Corollary 2 of Theorem 7.1, $(b_1)_{A\cdot B} = (b_2)_{A\cdot B}$. Thus the image of $(b)_A$ under T is unique. Now we show that the pre-image of $(b)_{A\cdot B}$ is unique. Suppose $(b_1)_{A\cdot B} = (b_2)_{A\cdot B}$ where $b_1, b_2 \subset B$. Then

$$(b_1)_A = A - (A - b_1) \supset A\cdot B - (A\cdot B - b_1) = (b_1)_{A\cdot B} \supset b_2,$$

so that $(b_1)_A = (b_2)_A$. Hence T is (1-1). Now let b_1, b_2 be arbitrary elements of B. Then

$$(b_1)_A + (b_2)_A = (b_1 + b_2)_A \rightarrow (b_1 + b_2)_{A\cdot B} = (b_1)_{A\cdot B} + (b_2)_{A\cdot B}.$$

Thus T is an isomorphic mapping of $\{A, B\}/A$ on $B/A\cdot B$ and the theorem is proved.

This principle has interesting geometric content.

9. **Theory of dimension.** In this section we study the theory of *rank* or *dimension* for groups (linear spaces) based on the idea *linear independence.* It is necessary to introduce an additional postulate, J8, to get the familiar theory of dimension in a descriptive geometry. We generalize J8 in Theorem 1 (Steinitz-MacLane exchange principle) which enables us to apply the theory of dimension for exchange lattices.

In Theorem 5.7 we derived the important lattice theoretic property of *upper semi-modularity—if* $A \neq B$ *and* A, B *cover* C, *then* $\{A, B\}$ *covers* A, B— with the proviso $C \neq O$([70]). Evidently the simplest systems G satisfying J1, · · · , J7 are those for which this principle holds without exception. If $C = O$ the hypothesis reduces to: A, B are distinct *elements* of G. Thus we introduce postulate

J8. If $a, b \subset G$ and $a \neq b$ then $\{a, b\}$ covers a.

This is a consequence of the postulate, *two points belong to a unique line,* and hence is necessary for the validation of the familiar dimension theory of linear spaces in a descriptive geometry. As we shall see it is also sufficient, in the face of J1, · · · , J7. J8 does not have the simple formal algebraic character of J1, · · · , J7 but is introduced as a *structural* judgment to ensure that a system G satisfying J1, · · · , J7 have a natural simplicity of structure. It is equivalent in view of Theorem 5.7 to *the lattice of subgroups of* G *is upper semi-modular.*

J8 *is independent of* J1, · · · , J7. Consider the independence example G, and the associated diagram, used in establishing Theorem 3.7. Clearly $\{c, b\} = G$ and $\{c, d\}$ is represented by the vertical "line" cd in the diagram.

([70]) See Birkhoff [1, §73]. We are not assuming finite dimensionality when we use the term semi-modularity.

Thus $\{c, b\} \supset \{c, d\} \supset c$ and $\{c, d\} \neq \{c, b\}, c$ so that J8 is false in G. Since J1, $\cdots$, J7 are valid in G as shown in Theorem 3.6 the independence of J8 is settled.

Henceforth we assume that G satisfies J1, $\cdots$, J8. We generalize J8 in the following theorem.

THEOREM 1. *If A is a subgroup of G and $A \not\supset b$ then $\{A, b\}$ covers A.*

Proof. The case $A = O$ is trivial. Assume $A \neq O$. Suppose $\{A, b\} \supset X \supset A$, where X is a subgroup of G. Assuming $X \neq A$, it suffices to show $X = \{A, b\}$. Suppose $x \subset X$, $x \not\subset A$, $a \subset A$. Then we have, using Theorem 5.5,

$$x \subset \{A, b\} = \{A, \{a, b\}\} = A - \{a, b\},$$

and we have

$$x \subset A - y \tag{1}$$

where $y \subset \{a, b\}$, and

$$y \subset A - x \subset X. \tag{2}$$

$\{a, y\} \neq a$, for otherwise $y \subset A$ and by (1) $x \subset A$. Hence by J8, $\{a, b\} \supset \{a, y\} \supset a$ implies

$$\{a, b\} = \{a, y\}. \tag{3}$$

Thus by (3), (2)

$$b \subset \{a, y\} \subset X$$

so that $X = \{A, b\}$ and the proof is complete.

This may be considered a weakened form of the well known exchange principle of Steinitz in the theory of algebraic dependence([71]). We can now employ the methods of Steinitz to develop a theory of dimension for subgroups of a group. However, since MacLane [1] has given the Steinitz theory a very simple abstract lattice theoretic basis, we shall express the significance of Theorem 9.1 in terms of lattice theory and then merely outline the conclusions for dimension theory in groups.

Theorem 9.1 is an alternate statement of the *exchange property* E_2 (MacLane [1, p. 459]) as applied to the lattice of subgroups of G under the relation set inclusion. The other conditions in the definition of an exchange lattice (MacLane [1, p. 456])([72]) are almost trivial for the type of algebraic system under consideration. Thus we may assert the following corollary.

COROLLARY 1. *The subgroups of G form an exchange lattice.*

Further, since any descriptive geometry may be formulated as a group, we have the following corollary.

([71]) See van der Waerden [1, p. 96, Theorem 4].

([72]) See also Birkhoff [1, §§76, 77].

COROLLARY 2. *The linear subspaces of any descriptive space form an exchange lattice.*

We now outline the theory of dimension([73]). Any subgroup A of G has an independent set of generators called a *basis* of A. Any two bases of A have the same cardinal number called the *dimension* or *rank* of A, denoted functionally $d(A)$([74]). If B also is a subgroup of G, $A \supset B$ implies $d(A) \geqq d(B)$. For subgroups A, B of *finite* dimension we have more specific information: First we have the *dimensional inequality*

$$d(\{A, B\}) + d(A \cdot B) \leqq d(A) + d(B).$$

If $A \cdot B \neq O$, this can be strengthened to the corresponding *equality*([75]), which includes in essence the whole theory of intersection of linear subspaces in a finite-dimensional descriptive space([76]). Further the relation A covers B is equivalent to the dimensional condition, $d(A) = d(B) + 1$. For finite n, a set of n independent elements is contained in a unique subgroup of G of dimension n. Finally, if $d(A) = n$ is finite, any independent set of n elements of A is a basis of A. These results subsume the familiar theory of alignment and intersection in descriptive geometry.

10. **Factor groups and separation.** We now study factor groups more deeply, using results of the last section. We introduce the notion *simplicity* as in classical group theory and show that all simple factor groups are isomorphic, provided $d(G) > 2$. This motivates the adoption of postulate J9 from which the general separation principle for linear spaces (Theorem 10.6) easily follows.

We reduce a factor group to a normal form in the following theorem.

THEOREM 1. *Any factor group A/B is isomorphic to a factor group of the form A'/b.*

Proof. Suppose $b \subset B$. Then $A \supset B \supset b$. By the property of *relative complementation* valid in any exchange lattice (MacLane [1, p. 458, Theorem 7]) there exists A', a subgroup of G such that $\{A', B\} = A$ and $A' \cdot B = b$. Hence by Theorem 8.3

$$A/B = \{A', B\}/B \cong A'/A' \cdot B = A'/b$$

and the proof is complete.

([73]) See MacLane [1, §§3, 4]. The treatment in Prenowitz [1, §§7, 8] for projective geometries can be modified slightly to yield the results stated here.

([74]) As defined, the dimension of a linear space in a descriptive geometry exceeds by unity the familiar geometrical dimension. This is very natural in the present context.

([75]) This follows from Theorem 5.6 by a well known lattice theoretic argument, see for example Birkhoff [1, p. 40, lemma].

([76]) As an illustration let A, B $(A \neq B)$ be intersecting planes in a space C, that is, $d(A) = d(B) = 3$, $d(C) = 4$. We can easily show $d(\{A, B\}) = 4$ so that by the dimensional equality $d(A \cdot B) = 2$, or $A \cdot B$ is a line.

We are especially interested in *simple* factor groups as characterized in the following definition.

Definition 1. A *subgroup* of a factor group is a *non-empty*([77]) subsystem closed under $+$ and $-$. It easily follows as in classical group theory that the identity element constitutes a subgroup of every factor group. If the only proper subgroup of a factor group is the identity group, we say it is *simple*.

The following criterion for simplicity is easily derived.

THEOREM 2. *A/B is simple if and only if A covers B and $B \neq O$*([78]).

Now in Theorem 10.1, suppose A/B simple. Then A'/b is simple and, by the last theorem, A' covers b or $d(A')=2$. Suppose $a \subset A'$, $a \neq b$. Then a, b form a basis of A' so that $A' = \{a, b\}$. Thus we may assert the following corollary.

COROLLARY. *Let A/B be simple. Then $A/B \cong \{a, b\}/b$ where $a \neq b$.*

We shall use this elementary normal form in the proof of Theorem 10.4 on the abstract identity of all simple factor groups. As a lemma we need the following principle which in itself is interesting.

THEOREM 3. *Suppose $B \neq O$ is a subgroup of A and $x \not\subset A$. Then $\{A, x\}/\{B, x\} \cong A/B$.*

Proof. First we show

$$A \cdot \{B, x\} = B. \tag{1}$$

Suppose this false. Then, since the left member contains B, there exists $p \subset A$, $\{B, x\}$ such that $p \not\subset B$. By Theorem 9.1, $\{B, x\}$ covers B, so that $\{B, x\} = \{B, p\}$. Hence $x \subset \{B, p\} \subset A$, contrary to hypothesis, and (1) is justified. By Theorem 8.3 and (1)

$$\{A, x\}/\{B, x\} = \{A, \{B, x\}\}/\{B, x\} \cong A/A \cdot \{B, x\} = A/B.$$

Now we can establish the following important theorem.

THEOREM 4. *Let $d(G) > 2$. Then all simple groups A/B are isomorphic.*

Proof. By the corollary of Theorem 10.2 we need show merely

$$\{a, b\}/b \cong \{a', b'\}/b', \tag{1}$$

where $a \neq b$ and $a' \neq b'$. We can find elements a_1, a_1', p such that $\{a, b\} = \{a_1, b\}$; $\{a', b'\} = \{a_1', b'\}$; $\{a_1, p\} = \{a_1', p\}$; $p \not\subset \{a_1, b\}, \{a_1', b'\}$. The existence of p requires the assumption $d(G) > 2$ and that if $u \neq v$, $\{u, v\}$ contains elements other than u, v, which is trivial by the corollary of Theorem

([77]) This restriction entails no essential loss of generality. It is imposed so that each subgroup may contain the identity element of the factor group.

([78]) Compare Albert [1, p. 134, Theorem 14].

3.3. It easily follows that $b \not\subset \{a_1, p\}$ and $b' \not\subset \{a_1', p\}$. Using Theorem 10.3 several times we have

$$\{a, b\}/b \cong \{\{a_1, b\}, p\}/\{b, p\} = \{\{a_1, p\}, b\}/\{p, b\} \cong \{a_1, p\}/p.$$

Similarly we show

$$\{a', b'\}/b' \cong \{a_1', p\}/p$$

Since $\{a_1, p\} = \{a_1', p\}$ we have verified (1) and the theorem is established.

An immediate consequence is the following corollary.

COROLLARY. *Suppose $d(G) > 2$. Then all simple factor groups A/B have the same order.*

This result suggests the imposition of a further restriction on our groups G. For, by Theorem 7.7, the common order of all simple factor groups in the last corollary is at least 3. Clearly the simplest type of system satisfying J1, $\cdots$, J8 is one in which this common order is precisely 3. However, we can weaken this condition considerably. For, by the last corollary, if $d(G) > 2$ it is enough to assume that one particular simple group A/B has order 3. Further, it is easily shown (see Theorem 10.5 below) that any group A/B with order 3 is simple. Thus we adopt postulate

J9. There exists a group A/B of order 3([79]).

We have motivated J9 algebraically; let us now consider its geometric significance. By Definition 7.6 we may restate it: *G contains subgroups (linear spaces) A, B such that B separates A.* Thus J9 is obviously verified in a descriptive geometry since we can take A as any line and B as one of its points. It is thus a very weak form of *separation* postulate. The role of J9 may be described differently. Let us say in a group G that the elements of a set are *collinear* if they are contained in a linear space of dimension 2, that is, $\{p, q\}$ where $p \neq q$. Then if $d(G) > 2$, J9 implies that if a, b, c are distinct and collinear one of the order relations (abc), (bca), (cab) of §3 obtains([80]). Borrowing a term from the theory of dyadic order relations we may say J9 ensures that a set of collinear elements is *fully* or *simply* ordered([81]).

It seems very desirable to give an independence proof for J9, since in the classic treatment of the subject separation principles are derived, not postulated. The independence proof is rather laborious, requiring the construction of a "partially" ordered space and will be published separately([82]).

We continue with the consequences of J9. In order to avoid introducing the hypothesis $d(G) > 2$ in most of the succeeding theorems we adopt postulate

J10. $d(G) > 2$.

([79]) J9 is similar to J8 in being a structural rather than an algorithmic requirement.

([80]) This is a consequence of Theorem 11.2.

([81]) Compare Birkhoff [1, p. 9, Definition 1.3].

([82]) See *Partially ordered fields and geometries* by the writer, to appear in Amer. Math. Monthly.

In the remainder of the paper we assume J1, $\cdots$, J10.

We establish another criterion for simplicity in the following theorem.

THEOREM 5. *A/B is simple if and only if it has order 3.*

Proof. Suppose A/B has order 3. Any subgroup of A/B distinct from the identity group must contain the identity element I, an element $X \neq I$ and $-X$, the inverse of X. Since these are distinct, the subgroup is identical with A/B and A/B is simple. The converse is easily proved. For by J9 there exists a factor group of order 3. As we have just seen such a factor group is simple. Hence in view of J10 we may apply the last corollary and conclude that *all* simple factor groups have order 3.

The criteria for simplicity in Theorems 10.2, 10.5 are equivalent. Hence applying Definition 7.6 we have the *general separation theorem for linear spaces of arbitrary dimension*:

THEOREM 6. *B separates A if and only if A covers B and $B \neq O$.*

If $d(A)$ is finite this is the familiar result: *An $n+1$-space is separated by any of its contained n-spaces.*

Applying the corollary of Theorem 7.8 we have the following corollary.

COROLLARY 1. *In G let A cover B. Suppose $a \subset A$, $a \not\subset B$, $a + a' \approx B$. Then $A = B \cup B - a \cup B - a'$, and the addends are disjoint.*

This easily leads to another corollary.

COROLLARY 2. *Let B be a subgroup of G. Suppose $a + a' \approx B$. Then*

$$\{a, B\} = B \cup B - a \cup B - a' = B \cup B - a \cup B - (B - a).$$

Moreover the addends are disjoint provided $a \not\subset B$.

Proof. If $a \subset B$ the result is trivial. Suppose $a \not\subset B$. Then $\{a, B\}$ covers B by Theorem 9.1, and the result follows by the last corollary and Corollary 4 of Theorem 7.4.

11. **Decomposition theorems.** The principal purpose of this final section is to establish Theorems 11.3, 11.5, 11.6 which give the essential relations in the decomposition and separation of a linear space of dimension n by an n-simplex. The key principle in the discussion is the decomposition theorem for $n = 2$ (Theorem 11.2). In addition this theorem identifies $\{a, b\}$ as line ab, when $a \neq b$, and leads easily to the characterization of descriptive geometries in the final theorem.

THEOREM 1. *Let N be a subgroup of G. Suppose $a + a' \approx N$, $b + b' \approx N$. Then*

$$\{a, b, N\} = N - (a + b) \cup N - (a + b') \cup N - (a' + b) \cup N - (a' + b') \cup N - a \cup N - b \cup N - a' \cup N - b' \cup N(83).$$

(83) Compare the expression for $\{a, b, N\}$ in classical abelian group theory which can be formulated as the set union of the terms $N - (ma + nb)$ where m, n are integers.

Proof.

$$\begin{aligned}\{a, b, N\} &= \{\{a, N\}, \{b, N\}\} \\ &= \{a, N\} - \{b, N\} && \text{(Theorem 5.5)} \\ &= (N \cup N - a \cup N - a') - (N \cup N - b \cup N - b') \\ & && \text{(Theorem 10.6, corollary 2)} \\ &= N - N \cup N - (N - b) \cup N - (N - b') \cup (N - a) - N \\ &\quad \cup (N - a) - (N - b) \cup (N - a) - (N - b') \cup (N - a') - N \\ &\quad \cup (N - a') - (N - b) \cup (N - a') - (N - b') && \text{(Theorem 2.10).}\end{aligned}$$

Consider a term in this set union of the form $(N-a)-(N-b)$. Applying the corollary of Theorem 2.6 and Corollary 4 of Theorem 7.4, we see that this equals $(N-(N-b))-a=(N-b')-a=N-(a+b')$. Using similar, or even simpler, transformations on the other terms and noting that $N-N=N$ we get the desired result.

Each term in this formula for $\{a, b, N\}$ is a set of cosets of N. This suggests an analogous formula for $\{a, b, N\}/N$, which we now derive.

COROLLARY. *Let $N \neq O$ be a subgroup of G. Then*

$$\begin{aligned}\{a, b, N\}/N = (a)_N + (b)_N \cup (a)_N - (b)_N \cup (b)_N - (a)_N \cup - ((a)_N + (b)_N) \\ \cup (a)_N \cup (b)_N \cup - (a)_N \cup - (b)_N \cup N\text{(84)}.\end{aligned}$$

Proof. Using the notation of the theorem, we have

$$\begin{aligned}\{a, b, N\}/N = (N - (a + b))_N \cup (N - (a + b'))_N \cup (N - (a' + b))_N \\ \cup (N - (a' + b'))_N \cup (N - a)_N \cup (N - b)_N \\ \cup (N - a')_N \cup (N - b')_N \cup N.\end{aligned} \tag{1}$$

We express these addends in terms of operations on cosets, that is, operations in G/N. To illustrate the method consider $(N-(a+b'))_N$. By Corollary 1 of Theorem 7.5 we have

$$N - (a + b') = \sum_{X \subset -(a+b')_N} X. \tag{2}$$

By Theorem 7.5, Corollary 2 of Theorem 7.4 and Theorem 7.6

$$-(a + b')_N = -(a)_N + (b)_N = (b)_N - (a)_N.$$

Hence by (2)

$$N - (a + b') = \sum_{X \subset (b)_N - (a)_N} X$$

and

$$(N - (a + b'))_N = (b)_N - (a)_N.$$

(84) Although in the theorem N is a subset of G, here it is a coset, that is, an element of G/N.

Applying similar methods to the first four terms in the right member of (1) and using Corollary 4 of Theorem 7.4 to identify other terms as cosets we get the desired result.

Now we are able to obtain an important expansion for $\{a, b\}$.

THEOREM 2. $\{a, b\} = a+b \cup a-b \cup b-a \cup a \cup b$([85]).

Proof. If $a=b$ the theorem is trivial. Suppose $a \neq b$. By J10 there exists an element n such that a, b, n are distinct and form an independent set. We expand $\{a, b, n\}/n$ by the last corollary. Hence if $x \subset \{a, b\}$ there are at most nine classes into which $(x)_n$ can fall. We proceed to explore these possibilities.

First suppose $(x)_n \subset (a)_n + (b)_n$([86]). Then $(x)_n \subset (a+b)_n$, so that $(x)_n = (x')_n$ where $x' \subset a+b$. We show $x=x'$. We have $x' \subset \{n, x\}$ so that $x, x' \subset \{a, b\} \cdot \{n, x\}$. By the dimensional equality of §9, $d(\{a, b\} \cdot \{n, x\}) = d(\{a, b\}) + d(\{n, x\}) - d(\{\{a, b\}, \{n, x\}\}) = 2+2-3=1$, since $\{\{a, b\}, \{n, x\}\} = \{a, b, n\}$. Thus $\{a, b\} \cdot \{n, x\}$ consists of a single element, so that $x=x'$ and $x \subset a+b$.

Next consider the possibility $(x)_n \subset (a)_n - (b)_n$. By definition, $(b)_n + (x)_n \supset (a)_n$ so that $(b+x)_n \supset (a)_n$ and $(a)_n = (a')_n$ where $a' \subset b+x$. The supposition $x=b$ implies $a'=b$ and $(a)_n = (b)_n$, contrary to the independence of a, b, n. Thus $x \neq b$. Hence applying J8 to the relation $\{a, b\} \supset \{b, x\} \supset b$ we get $\{b, x\} = \{a, b\}$. Thus $a \subset \{a, n\} \cdot \{b, x\}$. Evidently $a' \subset \{a, n\} \cdot \{b, x\}$. Applying the dimensional equality as in the last paragraph we show $a=a'$. Thus $a \subset b+x$ and $x \subset a-b$.

Similarly $(x)_n \subset (b)_n - (a)_n$ implies $x \subset b-a$. If $(x)_n = (a)_n$ we easily get $x=a$. Likewise $(x)_n = (b)_n$ implies $x=b$. Thus five terms in the expansion of $\{a, b, n\}/n$ correspond to terms in the expansion of $\{a, b\}$. We show these are the only terms in the expansion of $\{a, b\}$.

Suppose $(x)_n \subset -((a)_n + (b)_n) = -(a+b)_n$. Then $(x)_n = -(x')_n$ where $x' \subset a+b$. By Corollary 2 of Theorem 7.4, $x+x' \approx n$. Since $\{a, b\} \supset x, x'$ we have $\{a, b\} \supset x+x' \supset n$. This is impossible, since a, b, n are distinct and form an independent set. Similarly we can show the other three possibilities for $(x)_n$ vacuous. Thus $x \subset a+b \cup a-b \cup b-a \cup a \cup b$ and $\{a, b\} = a+b \cup a-b \cup b-a \cup a \cup b$.

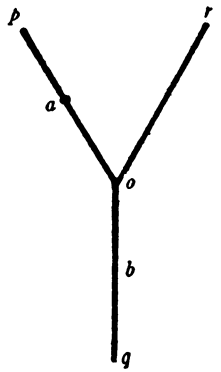
Postulate J10 is essential for the validity of this theorem. To show this we construct the following system. In the adjoined diagram let $G = op \cup oq \cup or$ where the addends denote segments (open intervals). We define $+$ in G as follows: (1) $x+x=x$; (2) if x, $y (x \neq y)$ are in the same segment op, oq, or let

---

([85]) Compare the corresponding expression in classical abelian group theory, namely the set of all elements $ma+nb$ where m, n are integers.

([86]) There is no essential ambiguity here—since the right member is a set of cosets, the left member is considered as a single coset.

$x+y$ be segment xy; (3) if x, y are in distinct segments $x+y=xo\cup oy$ where the addends denote segments. It is not difficult although somewhat laborious



to verify J1, $\cdots$, J9 in system $(G; +)$. Let $a, b \subset op, oq$ respectively as in the diagram. Then J10 is invalid since $\{a, b\} = G$ and $d(G) = 2$. The theorem fails, since $a+b\cup a-b\cup b-a\cup a\cup b = op\cup oq \neq \{a, b\}$. This example also shows that J10 is essential for several succeeding propositions of this section.

The expansion of $\{a, b\}$ obtained in the last theorem readily leads to the following corollary.

COROLLARY 1. $a-(a-b)=b+a\cup b-a\cup b$([87]).

Proof. If $a=b$ this is trivial. Suppose $a\neq b$. By Corollary 2 of Theorem 10.6

$$\{a, b\} = a - (a - b) \cup a - b \cup a$$

where the addends are disjoint. By the last theorem

$$\{a, b\} = b + a \cup b - a \cup b \cup a - b \cup a.$$

The addends here also are disjoint, since the contrary supposition implies $a=b$. For example $a-b\approx b+a$ implies $a\approx a+b$, $a-a\approx b$ and $a\approx b$, that is $a=b$. Hence after equating the expressions for $\{a, b\}$ we may "cancel" $a-b\cup a$ from both members, getting the desired equation.

Corollary 1 is easily generalized to yield another corollary.

COROLLARY 2. $a-(a-B)=B+a\cup B-a\cup B$.

In order to generalize Theorem 11.2 we prove the following lemma.

LEMMA. $(a+B)-(a+C)=(a+B)-C\cup B-(a+C)\cup B-C$.

([87]) This is a familiar expression for ray ab, see Forder [1, p. 53, Definition 10.3].

Proof. Using the corollary to Theorem 2.6, Theorem 4.5, the last corollary and Theorem 2.10 we have

$$\begin{aligned}(a + B) - (a + C) &= ((a + B) - a) - C = (a - (a - B)) - C \\ &= (B + a \cup B - a \cup B) - C \\ &= (a + B) - C \cup B - (a + C) \cup B - C.\end{aligned}$$

Now we generalize Theorem 11.2 and obtain a much sharper formula for $\{a_1, \cdots, a_n\}$ than that in Corollary 3 of Theorem 5.4.

THEOREM 3. *$\{a_1, \cdots, a_n\}$ is the set union of all polynomial expressions of the form $(a_{i_1} + \cdots + a_{i_r}) - (a_{i_{r+1}} + \cdots + a_{i_s})$([88]), where $1 \leqq i_j \leqq n$, and $i_j \neq i_k$ if $j \neq k$. Furthermore if $a_1, \cdots, a_n$ are distinct and form an independent set the addends are disjoint*([89]).

Proof. By Corollary 3 of Theorem 5.4

$$\{a_1, \cdots, a_n\} = (a_1 + \cdots + a_n) - (a_1 + \cdots + a_n).$$

We apply the lemma to the right member in order to eliminate repetition of the letter a_1, getting

$$\begin{aligned}\{a_1, \cdots, a_n\} = (a_1 + \cdots + a_n) - (a_2 + \cdots + a_n) \\ \cup (a_2 + \cdots + a_n) - (a_1 + \cdots + a_n) \\ \cup (a_2 + \cdots + a_n) - (a_2 + \cdots + a_n).\end{aligned}$$

Similarly we eliminate repetitions of the letter a_2 in each addend of this set union, for example we reduce

$$(a_1 + \cdots + a_n) - (a_2 + \cdots + a_n)$$

to

$$\begin{aligned}(a_1 + \cdots + a_n) - (a_3 + \cdots + a_n) \\ \cup (a_1 + a_3 + \cdots + a_n) - (a_2 + \cdots + a_n) \\ \cup (a_1 + a_3 + \cdots + a_n) - (a_3 + \cdots + a_n).\end{aligned}$$

Continuing to eliminate repeated letters in this way we eventually get an expression for $\{a_1, \cdots, a_n\}$ in which all addends have the desired form. Hence, since $\{a_1, \cdots, a_n\}$ contains every expression of this form, it is the set union of all such expressions.

([88]) In summing elements of G we adopt the convention that if the initial value of a summation index exceeds its final value the sum shall be 0. Hence the given form includes sums of the a's, since we may choose $r+1>s$.

([89]) Compare the corresponding result in classical abelian group theory, that $\{a_1, \cdots, a_n\}$ is the set of all elements of the form $m_1a_1 + \cdots + m_na_n$, where the m's are integers. Further that if $a_1, \cdots, a_n$ are independent, each element is uniquely expressible in this form. Similarly the second part of the conclusion of our theorm is equivalent to the assertion that each element of $\{a_1, \cdots, a_n\}$ is uniquely contained in an expression of the given form.

Now let $a_1, \cdots, a_n$ be distinct and form an independent set. Suppose

$$(1)\qquad (a_{i_1}+\cdots+a_{i_r})-(a_{i_{r+1}}+\cdots+a_{i_s}) \approx (a_{j_1}+\cdots+a_{j_t})-(a_{j_{t+1}}+\cdots+a_{j_u})$$

holds, where the i's are distinct and the j's are distinct. We show the members of (1) identical. By Theorem 2.5, (1) implies

$$(2)\qquad a_{i_1}+\cdots+a_{i_r}+a_{j_{t+1}}+\cdots+a_{j_u} \approx a_{j_1}+\cdots+a_{j_t}+a_{i_{r+1}}+\cdots+a_{i_s}.$$

By Theorem 6.1, relation (2) is an equality and the same letters are present in both members of (2). Hence each a_{i_p}, $1\leqq p\leqq r$, is an a_{j_q}, $1\leqq q\leqq t$, and vice versa. Thus $a_{i_1}+\cdots+a_{i_r}=a_{j_1}+\cdots+a_{j_t}$. Similarly $a_{i_{r+1}}+\cdots+a_{i_s}=a_{j_{t+1}}+\cdots+a_{j_u}$, so that (1) becomes an equality. Hence the addends in the expansion of $\{a_1, \cdots, a_r\}$ are disjoint, and the theorem is established.

The reduction process here used to eliminate repetitions of letters in $(a_1+\cdots+a_n)-(a_1+\cdots+a_n)$ could be applied equally well to any expression $A-B$ where A, B are sums of letters $a_1, \cdots, a_n$. Thus we may assert the following corollary.

COROLLARY. *Let A, B be sums of letters chosen from $a_1, \cdots, a_n$. Then $A-B$ is expressible as a set union of addends $A'-B'$, where A', B' are sums of letters appearing in A, B respectively, involving no common letter.*

The simplest and most important case of the last theorem occurs when $a_1, \cdots, a_n$ are distinct and form an independent set, that is, when they form a set of additive generators of an n-simplex. In this case the terms in the decomposition of $\{a_1, \cdots, a_n\}$ fall into three classes which play different roles in the structure of $\{a_1, \cdots, a_n\}$. This suggests the following definition.

Definition 1. Let $a_1, \cdots, a_n$ be distinct and form an independent set. Then $a_1+\cdots+a_n$ is called the *interior* of simplex $[a_1, \cdots, a_n]$. The *frontier* of $[a_1, \cdots, a_n]$ is the set union of all sums of the a's involving fewer than n terms. The *exterior* of $[a_1, \cdots, a_n]$ is the set union of all expressions $(a_{i_1}+\cdots+a_{i_r})-(a_{i_{r+1}}+\cdots+a_{i_s})$ where $1\leqq i_j\leqq n$, $1\leqq r<s$ and the i's are distinct(90). Observe that $I+I=I+F=I$ if I, F are respectively the interior, frontier of a given simplex.

Using this definition we may restate the sufficiency portion of Theorem 6.1, Corollary 2, as the following theorem.

THEOREM 4. *Let S be an n-simplex; let I, F be its respective interior, frontier. Then $S=I\cup F$, where the addends are disjoint.*

---

(90) These are precisely the terms of the decomposition in the last theorem which effectively involve subtraction.

Further we may express the most important part of Theorem 11.3 as the following theorem.

THEOREM 5. *Let S be an n-simplex; let I, F, E be its respective interior, frontier, exterior. Then the linear space $\{S\} = I \cup F \cup E$, where the addends are disjoint.*

We complete the discussion of these properties by showing that the frontier of a simplex "separates" its interior and exterior.

THEOREM 6. *Let I, E, F be the interior, exterior, frontier respectively of simplex S. Suppose $p \subset I$. Then $E = F - p$.*

Proof. Suppose $x \subset E$. We shall prove

$$x \subset F - p. \tag{1}$$

Let $S = [a_1, \cdots, a_n]$ where $a_1, \cdots, a_n$ are distinct and form an independent set. Then by Definition 11.1 we have

$$x \subset A - B \tag{2}$$

where A, $B \neq O$ are sums of a's involving no common letter. Let $B = a_{i_1} + \cdots + a_{i_r}$, $r \geqq 1$. Then using the corollary of Theorem 2.6 we have

$$x \subset (A - B_1) - a_{i_1} \tag{3}$$

where $B_1 = a_{i_2} + \cdots + a_{i_r}$. In addition we have from the hypothesis, by Definition 11.1,

$$p \subset A_1 + a_{i_1} \tag{4}$$

where A_1 is the sum of the a's other than a_{i_1}. Since a_{i_1} appears in B, it can not appear in A. Hence each letter of A is a letter of A_1 so that $A_1 + A = A_1$. Solving (3), (4) for a_{i_1} we see that

$$(A - B_1) - x \approx p - A_1.$$

Hence by Theorem 2.5 and the corollary of Theorem 2.8 we have

$$p + x \approx A_1 + (A - B_1) \subset (A_1 + A) - B_1 = A_1 - B_1. \tag{5}$$

We apply the corollary of Theorem 11.3 to $A_1 - B_1$ in (5) getting

$$p + x \approx A_1' - B_1' \tag{6}$$

where A_1', B_1' are sums of letters in A_1, B_1 respectively, involving no common letter. Thus A_1', B_1' respectively involve at most $n-1$, $r-1$ of the a's. The effect of our argument thus far is to eliminate at least one letter, namely a_{i_1}, from B in (2), replacing (2) by (6). We proceed to eliminate letters from B_1', one at a time. Let $B_1' = B_2 + a_{i_2}$, where B_2 is the sum of the a's, other than a_{i_2}, in B_1'. From (6) we have

$$p + x \approx (A_1' - B_2) - a_{i_1}. \tag{7}$$

The hypothesis implies

$$p \subset A_2 + a_{i_1} \tag{8}$$

where A_2 is the sum of the a's other than a_{i_1}. Eliminating a_{i_1} between (7), (8) by the method used to derive (5), (6) from (3) and (4) we get

$$p + x \approx A_2 - B_2$$

and finally,

$$p + x \approx A_2' - B_2'$$

where A_2', B_2' respectively are sums of at most $n-1$, $r-2$ a's involving no common letter. Continuing to eliminate a's in this way we get after at most r steps

$$p + x \approx A_i' - B_i'$$

where A_i' is a sum of at most $n-1$ a's and $B_i' = O$, so that (1) follows.

Conversely we show

$$F - p \subset E. \tag{9}$$

By Theorem 11.5 we have

$$F - p \subset I \cup F \cup E. \tag{10}$$

Suppose $F-p \approx I \cup F$. Then

$$F \approx (I \cup F) + p \subset (I \cup F) + I = (I + I) \cup (F + I) = I \cup I = I$$

contrary to Theorem 11.4. Hence $(F-p)\cdot(I \cup F) = O$ and (9) follows in view of (10). This completes the proof.

We conclude with a characterization of descriptive geometries.

THEOREM 7. *Descriptive geometries may be characterized as groups G satisfying* J1, · · · , J10.

Proof. We must prove the postulate systems O1, · · · , O6 and J1, · · · , J10 equivalent. We defined + in terms of order (§1) and we have seen as we introduced J1, · · · , J10, that they are valid in a descriptive geometry, that is they are implied by O1, · · · , O6. Conversely in §3, we defined order([91]) in terms of + and showed that J1, · · · , J7 imply O1, O2, O4, O6. Thus we have merely to show that the postulation of J8, J9, J10 yields O3, O5.

In order to do this we must identify the term *line* in a group G. In view of Definition 3.1, line ab as defined in §1 is the set $a+b \cup a-b \cup b-a \cup a \cup b$. Hence by Theorem 11.2 line ab is $\{a, b\}$, where $a \neq b$. We show: *If* $a \neq b$ *and*

([91]) In defining order in a group G in terms of + we lose part of the content of the converse definition of + in terms of order, namely $a+a=a$. This causes no difficulty, since $a+a=a$ is postulated in G.

$\{a, b\} \supset c$, $d(c \neq d)$ *then* $\{c, d\} = \{a, b\}$ ([92]). Assuming $a \neq b$ the dimension of $\{a, b\}$ is 2. Hence c, d form a basis of $\{a, b\}$ and $\{c, d\} = \{a, b\}$. This obviously implies O5. To show that O3 is verified, observe that by J10 there exist elements a, b, c which are distinct and form an independent set. Suppose a, b, c are contained in a line, say line $\{p, q\}$. By the principle just established $\{a, b\} = \{p, q\} \supset c$, contrary to the independence property of a, b, c. Thus a, b, c are not in the same line and O5 is verified.

References

A. A. Albert

1. *Modern higher algebra*, Chicago, 1937.

P. Alexandroff and H. Hopf

1. *Topologie*, vol. 1, Berlin, 1935.

G. Birkhoff

1. *Lattice theory*, Amer. Math. Soc. Colloquium Publications, vol. 25, New York, 1940.

M. Dresher and O. Ore

1. *Theory of multigroups*, Amer. J. Math. vol. 60 (1938) pp. 705–733.

J. E. Eaton and O. Ore

1. *Remarks on multigroups*, Amer. J. Math. vol. 62 (1940) pp. 67–71.

H. G. Forder

1. *The foundations of Euclidean geometry*, Cambridge, 1927.

S. MacLane

1. *A lattice formulation for transcendence degrees and p-bases*, Duke Math. J. vol. 4 (1938) pp. 455–468.

W. Prenowitz

1. *Projective geometries as multigroups*, Amer. J. Math. vol. 65 (1943) pp. 235–256.

O. Veblen

1. *A system of axioms for geometry*, Trans. Amer. Math. Soc. vol. 5 (1904) pp. 343–384.
2. *The foundations of geometry*, in *Monographs on topics of modern mathematics*, edited by J. W. A. Young, New York, 1915.

B. L. van der Waerden

1. *Moderne Algebra*, vol. 1, 1st ed., Berlin, 1930.

([92]) This is easily shown directly from J8 without using the dimensional principles of §9. For $c \neq a$ or b. Suppose $c \neq a$. Then $\{a, b\} \supset \{a, c\} \supset a$ implies by J8 $\{a, b\} = \{a, c\}$. Thus $\{a, c\} \supset d$. Since $d \neq c$ we can show similarly $\{a, c\} = \{c, d\}$, so that $\{a, b\} = \{c, d\}$.

Brooklyn College,
Brooklyn, N. Y.