THE TERNARY OPERATION $(abc)=ab^{-1}c$ OF A GROUP

JEREMIAH CERTAINE

1. Introduction. This note is the result of some investigations into the ternary operation $ab^{-1}c$ in a group. We shall assume familiarity on the part of the reader with the notions of a group, a one-one transformation (we shall use the shorter term permutation) of an arbitrary set of elements, an automorphism, and a coset.[1] We shall use the multiplicative notation for a group G with elements $a, b, c, \cdots$. We shall also use the following convention for multiplication of permutations. Given two permutations T_i: $x \to xT_i$ $(i=1, 2)$, then T_1T_2 is $x \to (xT_1)T_2$. Finally, we denote automorphisms by small Greek letters.

In §2 we shall review certain properties of the ternary operation in a given group, determining all subsets closed with respect to this operation and the group of permutations of G which preserve this operation. These results had been previously obtained by Reinhold Baer.[2]

In §§3 and 4 we give postulates for this operation with proofs of their independence and consistency. Thus, if a ternary operation satisfies these postulates in an arbitrary set of elements, then the set may be made into a group (unique within isomorphism) in which $(abc)=ab^{-1}c$. The first set of postulates appears as a weakened form of a set given by Baer in his paper,[3] in which he mentions the group property. This and an equivalent set completely determine the ternary function as $ab^{-1}c$. However, by further weakening one of these postulates, it is possible to get a system which no longer has this last property. That is, the group property still holds but the ternary operation is not determined by the group operation.

In the remaining sections we get a geometric interpretation of the ternary operation and derive therefrom simple conditions on pairs of elements (vectors) under which they form a group. In the case where an abelian group is desired, the conditions are even simpler, reducing essentially to a single law.

I wish to express my gratitude to Garrett Birkhoff for his kind

---

Received by the editors February 10, 1943, and, in revised form, May 5, 1943.

[1] Cf. H. Zassenhaus, *Lehrbuch der Gruppentheorie*, Leipzig and Berlin, 1937, pp. 1, 5, 41 and 10.

[2] *Zur Einführung des Scharbegriffs*, J. Reine Angew. Math. vol. 160 (1929) pp. 199–206.

[3] Cf. Baer, op. cit. p. 202, footnote.

assistance and encouragement, without which this note would probably not have been written.

2. **The ternary operation in a group.**

THEOREM 1. *$S \subset G$ is closed under (abc) if and only if S is a coset of some subgroup of G; indeed a right- (left-) coset of $S^{-1}S$ (SS^{-1}).*

PROOF. For the first part see Baer's paper.[4] As for the second observe that if $S=sT$ ($s \in S$), then $T=s^{-1}S$ ($s \in S$) and hence $T=S^{-1}S$. Similarly, $S=Ts$ ($s \in S$) implies $T=SS^{-1}$.

DEFINITION 1. *The set of all permutations of G of the form αT_a: $x \to (x\alpha)a$, where α is an automorphism of G, is called the holomorph of G, or simply the holomorph.*[5]

THEOREM 2. *The group of all permutations which preserve the ternary operation is the holomorph.*[6]

Explanation. A permutation T preserves the ternary operation, by definition, if and only if $(abc)T=(aT\ bT\ cT)$. The group property follows from the general theorem that the set of all automorphisms of any algebra form a group, and the set in question is exactly that of the automorphisms with respect to the ternary operation.[7]

3. **Postulates for the ternary operation.** The reader will observe, as stated in the introduction, that we may consider the postulates given below as postulates for a group under the ternary operation. The first set is interesting, considered as postulates for a group, because it does not (explicitly) require the existence of either the identity or the inverse.[8] The other sets require only the existence of an identity. An analogous situation is that of generalized groups defined by the use of an n-ary function.[9] However, the postulates given below seem to be the simplest for the general case.

[4] Cf. Baer, op. cit. Satz 3 (part 3). As may be seen, Baer's "schar" is simply a coset studied under the operation $ab^{-1}c$. By Theorem 1, and also by the fact that $sT=sTs^{-1}s$, where sTs^{-1} is a subgroup if and only if T is (and indeed equals T if and only if T is normalized by s), we see that the property of being a coset is intrinsic.

[5] Cf. Zassenhaus, op. cit. p. 46.

[6] Cf. Baer, op. cit. Satz 11 (part 3). An alternative proof would be to consider T as given and define $d=eT$, e the identity of G, and α: $x \to (xT)d^{-1}$. Using $ab=(aeb)$, it is easy to verify that $(ab)\alpha=(a\alpha)(b\alpha)$, and that $T=\alpha T_d$. The converse is straightforward.

[7] Cf. Garrett Birkhoff, Proc. Cambridge Philos. Soc. vol. 31 (1935) p. 434.

[8] Cf. Rainich, *Note on group postulates*, Bull. Amer. Math. Soc. vol. 43 (1937) pp. 81–84.

[9] Cf. E. L. Post, Trans. Amer. Math. Soc. vol. 48 (1940) pp. 208–350.

We shall assume, unless otherwise stated, that the systems defined below are closed with respect to (abc) and that they contain all elements under discussion.

DEFINITION 2. *Let G be a set of elements on which there is defined a ternary operation (abc) satisfying the following postulates:*

$$(3.1) \qquad A_1\colon ((abc)de) = (ab(cde)), \quad A_2\colon (abb) = a, \quad A_3\colon (bba) = a.$$

We shall call G an abstract coset.

We shall not use these postulates directly but use a weakened yet equivalent set given below. The equivalence is a corollary to Theorem 3 proved below.

$$(3.2) \qquad \begin{aligned} &A_1\colon ((abc)de) = (ab(cde)).\\ &B\colon \text{ There exists } u \text{ in the set satisfying (a) } (auu) = a, \text{ (b) } (aau) = u. \end{aligned}$$

THEOREM 3. *If G is a set satisfying* (3.2) *and we define $ab = (aub)$, then G becomes a group and $(abc) = ab^{-1}c$.*

PROOF. Closure is obvious.

In A_1 take $b = d = u$, and we get the associative law $(ac)e = a(ce)$.

By definition and B(a), it follows that u is a right identity.

If a is given, choose $x = (uau)$. Then $ax = (au(uau)) = ((auu)au) = (aau) = u$. It follows that G is a group under the binary operation and hence u is a left identity also, that is, $(uua) = ua = a$ for all a.

Finally, $(abc) = ((auu)bc) = (au(ubc)) = a(ubc) = a(ub(uuc)) = a((ubu)uc) = ab^{-1}c$.

COROLLARY 1. (3.1) *and* (3.2) *are equivalent.*

PROOF. The proof is obvious.

Thus we see that if G satisfies (3.1), we may choose any element u in G and define a group G_u with u as its identity, and $ab = (aub)$ as its law of composition. However, the following corollary shows that we get essentially the same group no matter which element we choose for the identity.

COROLLARY 2. *The groups G_u are isomorphic for all u in G, an abstract coset. Moreover, $(abc) = ab^{-1}c$.*

PROOF. Consider G_u and G_v. Define $T\colon x \to (xuv)$. T is in the holomorph of G_u with α the identity permutation. By Theorem 2 it follows that $(aub)T = (aT\ uT\ bT)$. But $uT = v$, which completes the proof.

Remark. G may thus be considered either as a group or as an abstract coset. We could define the holomorph of an abstract coset as the group of all permutations preserving the ternary operation (abc). This evidently coincides with the holomorph of G (considered as a group) given by Definition 1.

Now we shall examine the system we get from (3.2) by weakening postulate A_1.

DEFINITION 3. *Let G be a set of elements on which there is defined a ternary operation satisfying, for some u in G,*

$$(3.3)\qquad \begin{aligned} &\text{A: } ((auc)de) = (au(cde)),\\ &\text{B: (a) } (auu) = a, \quad \text{(b) } (aau) = u. \end{aligned}$$

THEOREM 4. *If G is a set satisfying Definition 3, and we define $ab = (aub)$, then G becomes a group and the following properties are equivalent:*

$$\text{T: } (abc) = ab^{-1}c, \qquad A_1\text{: } ((abc)de) = (ab(cde)), \qquad A_3\text{: } (bba) = a.$$

PROOF. The fact that G is a group follows from the proof of Theorem 3. It is obvious that T implies A_1 and A_3. But A_1 implies T by Theorem 3. It suffices to prove that A_3 implies T. But, by the proof of Theorem 3 again, $(abc) = a(ubc)$. Now $b(ubc) = (bbc) = c$ or $(ubc) = b^{-1}c$, so the result follows.

The following example shows that T does not hold for all sets satisfying (3.3).

Example. Let G be the set of two elements u and a combined according to the following rules:

$$(uuu) = (aau) = (aaa) = (aua) = u,$$
$$(auu) = (uau) = (uua) = (uaa) = a.$$

Obviously B is satisfied. The reader may check A, noting that it is unnecessary to check A for the first element equal to u since $(uux) = x$ for all x in G. But, since $(aaa) = u \neq a$, we see that (xyz) is not in general equal to $xy^{-1}z$. Also, since any group of order 2 (and there is only one) satisfies Definition 3 with $(abc) = ab^{-1}c$, we see that this set of postulates is insufficient to determine the ternary operation in terms of the group operation.

Remark. It is obvious that if we replace B(b) by A_3 in (3.3) we get a set equivalent to (3.1) and (3.2).

DEFINITION 4. *G is said to be commutative if $(abc) = (cba)$.*

THEOREM 5. *A necessary and sufficient condition that an abstract*

coset be commutative is that $(abc) = (cba)$ *where* b *is some fixed element and* a *and* c *are arbitrary.*

PROOF. Necessity is obvious. For the sufficiency, let b be given as in the hypothesis and b' be arbitrary. Consider G_b and $G_{b'}$. G_b is commutative by hypothesis. By Theorem 3, Corollary 2, it follows that $G_{b'}$ is also commutative, whence $(ab'c) = (cb'a)$.

Remark. An analogous theorem for sets satisfying Definition 3 does not hold. For if it did then $(ubc) = (cbu) = c(ubu) = cb^{-1}$, whence it would follow that $(abc) = ab^{-1}c$. Yet, in the above example, we have $(xuy) = (yux)$ for all x, y and $(xyz) \neq xy^{-1}z$ in general. As a corollary to this remark we have proved that every commutative system satisfying Definition 3 is a (commutative) abstract coset. We also have complete associativity, that is, $((abc)de) = (a(bcd)e) = (ab(cde))$.[10] Thus any system of this type is not only a Prüfer schar[11] but also a Dörnte 3-group.[12] In fact, the commutative law, A_1 and A_2 (A_3 is then also true) constitute exactly Prüfer's set of postulates. To sum up, we may assert that *in the commutative case the three sets of postulates are equivalent to those of Prüfer and Dörnte and to each other.*

4. **Consistency and independence of the sets of postulates.** The consistency of these postulates was really proved in the example given above. Actually, any group with $(abc) = ab^{-1}c$ (or $cb^{-1}a$) will satisfy these postulates, with the possible exception of the commutative law. The latter is obviously satisfied if G is commutative.

For the independence, we observe first that the commutative law is obviously independent of the others. To prove the other laws independent we find that a single set of systems will suffice for all three sets of postulates.

Consider the two element systems defined as follows:

$$(abb) = (aaa) = (aba) = (bba) = a, \quad (bbb) = (baa) = (aab) = (bab) = b. \quad (G_1).$$

$$(abb) = (aaa) = (aba) = (aab) = a, \quad (baa) = (bbb) = (bab) = (bba) = b. \quad (G_2).$$

Finally, let G_3 be derived from G_2 by defining $[a'b'c'] = (c'b'a')$.

THEOREM 6. (3.1) *is a set of independent postulates.*

PROOF. Note first that the closure postulate is independent. But G_1 satisfies A_2 and A_3 by inspection. Yet $(ab(bab)) = (abb) = a \neq b$

[10] Pointed out by the referee.

[11] Cf. H. Prüfer, *Theorie der Abelschen Gruppen*, Math. Zeit. vol. 20 (1924) pp. 166–187.

[12] Cf. W. Dörnte, *Untersuchungen über einen verallgemeinerten Gruppenbegriff*, Math. Zeit. vol. 29 (1928) pp. 1–19.

$=(aab)=((abb)ab)$ so that A_1 is independent of A_2 and A_3.

Now consider G_2 and observe that $(xyz)=x$ for all x, y, and z. This gives A_1 and A_2. However A_3 is not satisfied since $(aab)=a\neq b$.

We observe finally that the definition of G_3 from G_2 carries A_1 into itself and permutes A_2 and A_3. For instance $[[a'b'c']\ d'e']$ $=(e'd'(c'b'a'))=((e'd'c')b'a')=[a'b'[c'd'e']]$. This proves A_2 is independent of A_1 and A_3.

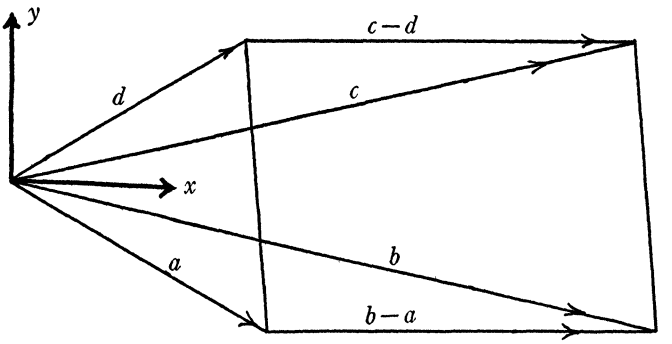
COROLLARY 1. (3.2) *is an independent set of postulates.*

PROOF. We observe first that the systems are symmetric in a and b. The corollary then follows immediately.

COROLLARY 2. (3.3) *is a set of independent postulates.*

PROOF. By symmetry, and proof of Theorem 6, G_1 gives the independence of A. The remainder of the proof follows from the above corollary.

5. **Axioms for free vectors.** By a system of free vectors is usually meant a set of vectors which may be translated without changing their value. For example, the system of forces in physical space constitute such a set. Let us investigate the (commutative) abstract coset derived from the group of all points in the plane under addition, or even a subset which is a coset. We shall then have $(abc)=a-b+c=d$.



By means of the accompanying diagram we see that d is simply the fourth vertex of a parallelogram whose vertices are described cyclicly as a, b, c, and d. For obviously $c-d=b-a$ or $d=a-b+c$. We may thus describe the closure of G as the property of containing with any three points the fourth vertex of the cyclicly ordered parallelogram

(a, b, c, d). This concept generalizes to any group by defining a parallelogram as the ordered quadruple $(a, b, c, ab^{-1}c)$. But we may also consider the difference $b-a$ as a vector (the vector from a to b, say) and interpret the equality $c-d=b-a$ as the statement that parallel vectors of the same length and direction are equal. This is the same as saying that these vectors are free. We shall now define this concept in the abstract.

DEFINITION 5. *By a set of free vectors we mean all pairs of elements (points) of an arbitrary set, the pairs* (a, b) *being connected by an equivalence relation (reflexive, symmetric and transitive relation) denoted by* $\sim$ *and satisfying*:

V_1: $(a, b)\sim(a', b')$ *implies* $(b, a)\sim(b', a')$.

V_2: $(a, c)\sim(a', c')$, $(b, c)\sim(b', c')$ *imply* $(a, b)\sim(a', b')$.

V_3: *Given* (a, b) *and* c, *there exists a unique* d *such that* $(a, b)\sim(d, c)$.

These postulates have a very simple interpretation in the light of the preceding paragraph. V_1 simply says that opposite sides of parallelograms are equal when their sense is taken into consideration. V_2 may be interpreted as a statement on congruent triangles and V_3 as a guarantee of the existence of a unique vector through a given point parallel to a given vector.

THEOREM 7. *Given any system of free vectors it is possible to define from them a group.*[13]

Explanation. We shall define as elements of the group the couples ab which are respectively the classes of all pairs equivalent to (a, b). We shall define $ab+cd=ah$, where $(d, c)\sim(h, b)$ and h is given by V_3.

PROOF. We shall divide the proof into several parts.

(a) Given (a, b) and c there exists a unique d such that $(a, b)\sim(c, d)$. By V_3, there exists a d(unique) such that $(b, a)\sim(d, c)$. Apply V_1.

(b) Addition is unique. To prove this we must show that if $(a, b)\sim(a', b')$ and $(c, d)\sim(c', d')$, then $ab+cd=a'b'+c'd'$. But consider h, h' where $(d, c)\sim(h, b)$, $(d', c')\sim(h', b')$. We get by V_1 and hypothesis $(h, b)\sim(h', b')$. V_2 and hypothesis give $(a, h)\sim(a', h')$.

(c) $ab+bc=ac$. By definition, this sum is ah where $(c, b)\sim(h, b)$. The reflexive law and V_3 imply $h=c$, the desired result.

(d) Now let u be fixed. Then uu is a right zero, for by V_3 an arbitrary vector $ab=cu$ for suitable c. Hence $ab+uu=cu+uu=cu=ab$. Again, by (a) $ab=ud$ for suitable d, whence by V_1, $ba=du$. Thus

[13] In connection with this result, which shows that Definition 5 may be considered as a definition of a group, cf. B. A. Bernstein, Trans. Amer. Math. Soc. vol. 43 (1938) pp. 1–6 and H. Boggs and G. Y. Rainich, Bull. Amer. Math. Soc. vol. 43 (1937) pp. 81–84.

$ab+ba=uu$, so ba is a right negative. Since the associative law obviously follows from (c) and (a), the proof is complete.

In the commutative case the postulates may be reduced to a very simple form. We shall prove the following theorem.

THEOREM 8. *Any set of pairs of elements for which there is defined an equivalence relation satisfying the following postulates constitutes a commutative group of free vectors (under the definitions of Theorem 7).*

V_0: $(a, b)\sim(a', b')$ *implies* $(a, a')\sim(b, b')$.

V_3: *Given* (a, b) *and* c *there exists a unique* d *such that* $(a, b)\sim(d, c)$.

PROOF. We first show that these form a system of free vectors. To prove V_1, let $(a, b)\sim(a', b')$. By V_0, we get $(a, a')\sim(b, b')$ or $(b, b')\sim(a, a')$. By V_0 again we have $(b, a)\sim(b', a')$. The hypotheses of V_2 give $(a, a')\sim(b, b')\sim(c, c')$, using V_0. Hence $(a, b)\sim(a', b')$. It remains only to prove that the group which we get is commutative. To this end consider ab and cd and choose e such that $(b, e)\sim(c, d)$ and f such that $(a, b)\sim(e, f)$. But $ab+cd=ae$ while $cd+ab=be+ef=bf$. Since $(a, e)\sim(b, f)$, the result follows.

The question which naturally arises is whether all systems of free vectors (as defined in Definition 5) are necessarily commutative, in which case we should surely use the conditions of Theorem 8. In fact *a necessary and sufficient condition that the group of free vectors be commutative is that* V_0 *hold.* Sufficiency being obvious, suppose $(a, b)\sim(a', b')$. Then $aa'=ab+ba'=ba'+ab=bb'$ since $(a, b)\sim(a', b')$. Hence we get $(a, a')\sim(b, b')$. To settle this question completely and to prove the consistency of these postulates, we now show how any group may be made into a system of free vectors.

THEOREM 9. *Any group* G *with elements* $a, b, \cdots$ *may be converted into a group of free vectors* V, *and conversely. Moreover,* G *and* V *are isomorphic.*

PROOF. *Necessity.* Let G be given and define $(a, b)\sim(c, d)$ if and only if $ab^{-1}=cd^{-1}$. This is obviously an equivalence relation. V_3 is also obvious. But $ab^{-1}=a'b'^{-1}$ implies $ba^{-1}=b'a'^{-1}$ (V_1); and $ac^{-1}=a'c'^{-1}$, $bc^{-1}=b'c'^{-1}$ imply $ab^{-1}=ac^{-1}(bc^{-1})^{-1}=a'c'^{-1}(b'c'^{-1})^{-1}=a'b'^{-1}$, which completes the proof.

Sufficiency. Let V be given and let u be any fixed element. Then the correspondence $a\rightleftarrows au$ is one-one between the elements of the proposed G and the elements of V. We define a binary operation in G by $ab\rightleftarrows au+bu$, thus making G into a group isomorphic to V. Now, by Theorem 7, $a^{-1}\rightleftarrows ua$, and $ab^{-1}\rightleftarrows au+ub=ab$. Thus $ab^{-1}=cd^{-1}$ if and only if $(a, b)\sim(c, d)$.

As for the isomorphism, we need only consider the case where V is defined from G. Obviously, the correspondence $ab^{-1} \rightleftarrows ab$ is one-one from G onto V. Moreover, the correspondent of $ab+cd$ is ah^{-1} where $dc^{-1}=hb^{-1}$ or $h^{-1}=b^{-1}cd^{-1}$. This establishes the isomorphism.

HARVARD UNIVERSITY

AN INVARIANT OF INTERSECTION OF TWO SURFACES

CHUAN-CHIH HSIUNG

1. **Introduction.** Projective invariants of several pairs of surfaces have been deduced and characterized geometrically by various authors.[1] In this paper we shall supplement their investigations by studying in ordinary space two surfaces intersecting at an ordinary point with distinct tangent planes.

In §2 we show by analysis the existence of a projective invariant determined by the neighborhood of the second order of the two surfaces at the point of intersection.

The final two sections are devoted to the presentation of projectively, as well as metrically, geometric characterizations of this invariant.

2. **Derivation.** Suppose that two surfaces S_1, S_2 in ordinary space intersect at an ordinary point O with distinct tangent planes τ_1, τ_2, and let the common tangent t be distinct from the asymptotic tangents. Let t_1, t_2 be the harmonic conjugate lines of t with respect to the asymptotic tangents of the surfaces S_1, S_2, respectively, at the point O. If we choose the point O to be the origin, the lines t, t_2, t_1 to be, respectively, the axes x, y, z of a general nonhomogeneous projective coordinate system, then the power series expansions of the surfaces S_1, S_2 in the neighborhood of the point O may be written in the form

$$S_1: \quad y = l_1x^2 + m_1z^2 + \cdots, \tag{1}$$

$$S_2: \quad z = l_2x^2 + m_2y^2 + \cdots. \tag{2}$$

Presented to the Society, September 13, 1943; received by the editors June 15, 1943.

[1] See the bibliography at the end of the paper.