1. Introduction. The background for this paper is provided by Klein's work presented in the Erlangerprogram [1], and more recent developments of these ideas as well as their application outside the field of geometry [2; 3; 4; 5; 6].

Klein deals with the Euclidean space $A$ as a fundamental structure. Its group of automorphisms $G_0(A)$ consists of the similitudes. Let $G(A)$ denote any group arrived at by adjoining to $G_0(A)$ new transformations of the set $A$. The basic problems then are of the following type: Given an extension $G(A)$ of $G_0(A)$, find invariants of $G(A)$ which characterize it.

Analogous problems can be formulated in the theory of abstract groups [2]. Now the fundamental structure itself is an abstract group $A$. Its automorphism-group $G_0(A)$ may be extended to a group $G(A)$, by adjoining new transformations of the set $A$. The group-multiplication of $A$, the characterizing invariant of $G_0(A)$, is not invariant under $G(A)$. The basic problems, stated above for geometry, take the same form in group theory, namely, what are characterizing invariants for $G(A)$.

A study of this type has already been made in the case $G(A)$ is taken to be the holomorph $H(A)$, i.e., the group of transformations obtained by adjoining to $G_0(A)$ the translations of $A$ [4]. The present paper deals with the case $G(A) = G_1(A)$, the group consisting of the automorphisms and anti-automorphisms of $A$. Characterizing invariants of $G_1(A)$ are investigated.

In a group $A$ on a set $A$ one can define two multiplications $p(x, y) = x \cdot y$ and $q(x, y) = y \cdot x$. The automorphism group $G_0(A)$ consists of the automorphisms of the operation $p$, while the anti-automorphisms are those transformations $T$ of the set $A$ which interchange $p$ and $q$. It follows that the set $\{p, q\}$ is invariant under all transformations belonging to the group $G_1(A)$ consisting of the automorphisms and anti-automorphisms of $A$. Furthermore, this invariant characterizes $G_1(A)$, i.e., every transformation $T$ of the set $A$ which keeps the set $\{p, q\}$ invariant belongs to $G_1(A)$. However, there are simpler characterizing invariants for $G_1(A)$, namely relations whose arguments

Received by the editors September 13, 1955, and, in revised form, December 11, 1955.

1134
range over the set $A$. For example $G_1(\overline{A})$ clearly is the group of automorphisms of the 6-term relation $\beta$ defined as follows:

$$\beta(x, y, z, u, v, w) : (xy = z \land uv = w) \lor (yx = z \land vu = w).$$

Theorem 1 shows that even a 3-term relation will serve to characterize $G_1(\overline{A})$.  

**Theorem 1.** The automorphisms and anti-automorphisms of a group $\overline{A}$ constitute the group of automorphisms of the relation

$$\alpha(x, y, z) : xy = z \lor yx = z$$

i.e., the relation $\alpha$ is a characterizing invariant for $G_1(\overline{A})$.

The significance of this theorem is that it shows how to replace the rather complex relation $\beta$ by a simpler relation $\alpha$ which is a characterizing invariant for the same group of transformations. It is natural to ask whether this result can be further improved. The relation $\alpha$ is a disjunction of two equations. The question is whether there is a relation expressible in the form of a single equation, which characterizes the group $G_1(\overline{A})$ of automorphisms and anti-automorphisms. The answer is negative, it is possible to prove.

**Theorem 2.** There is no finite or infinite set of relations expressible as equations between words, which would constitute a system of invariants characterizing the group $G_1(\overline{A})$ of automorphisms and anti-automorphisms. I.e., there is a group $\overline{A}_0$ and a transformation $T$ on $\overline{A}_0$ such that every equation between words which in every group $\overline{A}$ is invariant under $G_1(\overline{A})$ is also invariant in $\overline{A}_0$ under $T$, and such that $T$ is not a member of $G_1(\overline{A}_0)$.

In algebra one prefers to deal with operations rather than relations. An operation on the set $A$, which characterizes $G_1(\overline{A})$, is given in §3. However, such an operation is neither definable explicitly by a word, nor is it definable implicitly as a solution of an equation of group theory. This follows as a corollary to Theorem 2.

2. Proofs. Theorem 1 states: If $\overline{A}$ is a group and $T$ is a transformation of the set $A$ having the property that for all $x, y \in A$, $T(x \cdot y)$ is either equal to $Tx \cdot Ty$ or equal to $Ty \cdot Tx$, and $T^{-1}(x \cdot y)$ is either equal to $T^{-1}x \cdot T^{-1}y$ or equal to $T^{-1}y \cdot T^{-1}x$, then $T$ must be an automorphism or an anti-automorphism of $\overline{A}$. In this form the theorem was independently obtained by W. R. Scott [8]. As his proof appears in this journal, our proof of Theorem 1 will be omitted.

Let us define a semi-automorphism of a group $\overline{A}$ to be a mapping which preserves $e$ and the functions $Sx = x^{-1}$ and $s(x, y) = xyx$. Let
$G_1(\overline{A})$ and $G_2(\overline{A})$ denote respectively the group of automorphisms plus anti-automorphisms, and the group of semi-automorphisms. The proof of Theorem 2 now proceeds as follows: first a complete description of all equations invariant under $G_1$ in all groups $\overline{A}$ is given. It then can be seen easily that, in the abelian case, all these equations are invariant also under $G_2$. The proof is completed by displaying abelian groups $\overline{A}_0$ for which $G_2(\overline{A}_0)$ is not contained in $G_1(\overline{A}_0)$.

An equation of group theory will be called reduced if it is either the equation $e = e$ or then is of the type $a_1a_2 \cdots a_n = e$, whereby every $a_i$ is of the form $x$ or $x^{-1}$, $x$ being a variable, and none of the pairs $a_ia_{i+1}$ and $a_ia_n$ is of the form $xx^{-1}$ or $x^{-1}x$. Clearly, to every equation $f = g$ one can find a reduced equation $h = e$, such that $(f = g) \leftrightarrow (h = e)$ holds in all groups. It follows that every relation expressible by an equation $f = g$ can also be expressed by a reduced equation $h = e$. In describing the equational invariants of $G_1$ and $G_2$ it therefore is sufficient to deal with reduced equations only. This procedure will be followed in the sequel. Furthermore, the following notations will be used: Let $x$ be a variable, then $[x]$ stands for $x^{-1}$ and $[x^{-1}]$ stands for $x$. Let $w$ be a word of group theory, i.e., an expression $a_1a_2 \cdots a_n$, whereby every $a_i$ is of the form $x$ or $x^{-1}$. Then $w^*$ stands for the word $a_n \cdots a_2a_1$, and $[w]$ stands for the word $[a_1][a_2] \cdots [a_n]$. The symbol \"\sim\" is used to denote syntactic identity of words.

L1: If $g = e$ and $h = e$ are reduced equations such that $(g = e) \leftrightarrow (h = e)$ is true in all groups, then $h$ results by a cyclic permutation of the constituents of either $g$ or $[g^*]$.

To prove this one best uses Gödel's completeness theorem for first order predicate calculus. It says that in L1 one can replace \"true in all groups\" by \"provable in first-order group theory.\" Although the validity of the resulting meta-group-theoretic statement is fairly obvious on intuitive grounds, its proof is rather lengthy and therefore it is omitted.

Next we define a reduced equation $g = e$ to be regular in case $g^*$ results from $g$ by a cyclic permutation, and to be regular in case $[g] = e$. The next step is to investigate the invariants under $G_2$ of regular
equations. For this purpose the structure of regular equations has
to be described. This is done in L4.

L3: Let $g$ be a word of length $n$, and let $P$ be the cyclic permuta-
tion of $n$ objects through $m$ places. If $Pg \approx g$, then there is a word $w$, such that $g \approx w w \cdots w$ and $m$ is a multiple of the length $l$ of $w$.

**Proof.** Let $g$ be the word $a_1 \cdots a_n$. The equation

$$a_i \approx a_{i+n}, \quad \text{for all integers } i,$$

clearly defines a function $i \to a_i$ of the integers into the set $\{a_1, \cdots, a_n\}$, which is periodic with period $n$. Because $Pg \approx g$, it follows that the function $i \to a_i$ is also periodic with period $m$, i.e.,

$$a_i \approx a_{i+m}, \quad \text{for all integers } i.$$

Let $l$ be the largest common divisor of $n$ and $m$. Then, $l = pm + qm$ for some integers $p$ and $q$. Therefore, by (1) and (2), the function $i \to a_i$ is also periodic with period $l$, i.e.,

$$a_i \approx a_{i+l}, \quad \text{for all integers } i.$$

Let $w$ be the word $a_1 \cdots a_i$. Because $l$ divides $n$, $g$ is of the form $w w \cdots w$. Because $l$ divides $m$, $m$ is a multiple of the length $l$ of $w$.

Q.E.D.

L4: If the equation $g = e$ is regular, then the word $g$ must be of the
form $g_1 g_2$, whereby both $g_1$ and $g_2$ are symmetric words, i.e., $g_1 = g_1^*$ and $g_2 = g_2^*$.

If the equation $g = e$ is regular, then the word $g$ must be of the
form $v[v]v[v] \cdots v[v]$, whereby $v$ is some word.

**Proof.** Let $g = e$ be regular. Then there is a number $i$ such that a
cyclic permutation of $g$ through $i$ places yields $g^*$. It may be assumed
that $i$ is less or equal to half of the length of $g$, so that $g$ is of the
form $a_1 \cdots a_i b_1 \cdots b_i$ whereby $i \leq j$. The cyclic permutation of $g$ through $i$ places then yields $b_1 \cdots b_i a_1 \cdots a_i$, while $g^*$ is the word $b_i \cdots b_1 a_1 \cdots a_i$. Because these two words are identical it follows
that $b_1 \cdots b_i$ is identical with $b_i \cdots b_1$, and $a_1 \cdots a_i$ is identical
with $a_i \cdots a_i$. Therefore $g$ is of the form $g_1 g_2$, whereby both $g_1$ and $g_2$
are symmetric.

Next let $g = e$ be regular. Then there is a number $i$ such that the
cyclic permutation $P$ through $i$ places takes $g$ into $[g]$, i.e., $Pg \approx [g]$.
It follows that $PPg \approx P[g] \approx [Pg] \approx [[g]] \approx g$, i.e., $PPg \approx g$. By L3,
there is a word $w$ of length $l$, such that $g$ is of the form $w \cdots w$ and
$2i$ is a multiple of $l$, say $2i = s \cdot l$. Suppose first that $s$ is even. Then $i$
would be a multiple of $l$, and therefore, $Pg$ would be identical to $g$.

Because $Pg$ is identical with $[g]$, it would follow that $g$ and $[g]$ are
identical, which is impossible. Consequently $s$ must be odd, and therefore it follows from $2i = s \cdot l$, that $l$ is even, and $w$ is of the form $w_1w_2$, whereby both $w_1$ and $w_2$ are of length $l/2$. Thus, the situation is as follows:

$$g \approx aa,$$

whereby $a \approx w_1w_2w_1w_2 \cdots w_1w_2$,

$$Pg \approx bb,$$

whereby $b \approx w_2w_1w_2w_1 \cdots w_2w_1$,

$$[g] \approx cc,$$

whereby $c \approx [w_1][w_2][w_1][w_2] \cdots [w_1][w_2]$.

Because $Pg \approx [g]$ it follows that $w_2 \approx [w_1]$, and therefore

$$g \approx w_1[w_1]w_1[w_1] \cdots w_1[w_1].$$

Q.E.D.

L5: If the equation $g = e$ is regular, then in all groups $\overline{A}$ it is invariant under $G_2(\overline{A})$.

If the equation $g = e$ is regular, then in all abelian groups $\overline{A}$ it is invariant under $G_2(\overline{A})$.

Proof. Suppose $g = e$ is regular. Then by L4, $g = e$ must be of the form $g_1g_2 = e$, whereby $g_1$ and $g_2$ are both symmetric. It is easily seen that every symmetric word is provably equal to an expression composed from $s(x, y) = xyx$ and $Sx = x^{-1}$, furthermore, $g_1g_2 = e$ is provably equivalent to $g_1 = S(g_2)$. It follows that there are expressions $E_1$ and $E_2$ in $e$, $S$ and $s$, such that $(g = e) \iff (E_1 = E_2)$ holds in all groups. Because $E_1$ and $E_2$ are defined from $e$, $S$ and $s$, the equation $E_1 = E_2$ must be invariant under the automorphism group $G_2(\overline{A})$ of $e$, $S$ and $s$. It follows that $g = e$ is invariant under $G_2(\overline{A})$.

Suppose the equation $g = e$ is regular. Then by L3 it must be of the form $v[v]v[v] \cdots v[v] = e$. In every abelian group $\overline{A}$ this equation is identically satisfied, and therefore invariant under $G_2(\overline{A})$. Q.E.D.

L6: There are abelian groups $\overline{A}_0$ for which $G_2(\overline{A}_0)$ is not contained in $G_1(\overline{A}_0)$.

Proof. Let $\overline{A}_0$ be a Boolean group, i.e., a group which satisfies the equation $x^2 = e$ identically. In this group $Sx = x$ and $s(x, y) = y$. It follows that $G_2(\overline{A}_0)$ consists of all transformations of the set $A_0$ which keep $e$ fixed. On the other hand, because $\overline{A}_0$ is abelian, $G_1(\overline{A}_0)$ consist of all automorphisms of $\overline{A}_0$. Clearly $G_2(\overline{A}_0)$ is not contained in $G_1(\overline{A}_0)$, when $A_0$ has more than two elements. (For other examples see Dinkines [7].) Q.E.D.

By L2 and L5, it follows that, for abelian groups $\overline{A}$, if an equation is invariant under $G_1(\overline{A})$, then it is also invariant under $G_2(\overline{A})$. Because of L6, this yields that the equations invariant under $G_1(\overline{A})$ cannot characterize $G_1(\overline{A})$. This concludes the proof of Theorem 2.
3. Remarks. Since by Theorem 1, $\alpha$ and $\beta$ have the same group of automorphisms in any $A$, they may be said to be equivalent in Klein's sense [1]. This suggests that a stronger sort of equivalence may be established by finding a definition of $\beta$ in terms of $\alpha$. That this is possible will be shown elsewhere by use of the following stronger form of Theorem 1: If two groups $\langle A, \cdot \rangle$ and $\langle A, * \rangle$ have the same $\alpha$, then they must either be identical or anti-groups of each other. From this it also follows that the $\alpha$-theory is an abstraction ([4]; [5]) of group theory, and that every concept of group theory which is invariant under anti-automorphisms is definable in terms of $\alpha$.

The notion of an anti-automorphism applies to any algebraic system $\overline{A} = \langle A, \cdot \rangle$ consisting of a set $A$ and a binary operation $x \cdot y$. While the relation $\beta$ will still be a characterizing invariant for the group $G_1(\overline{A})$ consisting of all automorphisms and anti-automorphisms of $\overline{A}$, this will in general not be the case for $\alpha$. However, our proof for Theorem 1 as well as W. R. Scott's makes use of the associative-law and both cancellation-laws only. Therefore, if $\overline{A}$ is a cancellation-semi-group, then $\alpha$ is a characterizing invariant for $G_1(\overline{A})$. The following example shows that cancellation-semi-groups still do not exhaust all systems $\langle A, \cdot \rangle$ for which Theorem 1 holds: Let $A$ be any set and let $x \cdot y = x$. Then $\overline{A} = \langle A, \cdot \rangle$ violates one of the cancellation-laws, however, $G_1(\overline{A})$ and the group of automorphisms of $\alpha$ are identical, they both consist of all transformations of the set $A$.

In connection with Theorem 2 it should be noted that it is a statement about invariants which are "uniformally" defined for all groups (general invariants in the sense of Baer [2]). In particular groups it may well happen that the anti-automorphisms may be characterized by an equational relation. Thus, as it is shown by F. Dinkines [7], there are many groups in which the semi-automorphisms are exactly the automorphisms and anti-automorphisms. For these groups the equations $x = e$, $z = xyx$ clearly constitute a system of characterizing invariants for the group of automorphisms and anti-automorphisms.

As a corollary to Theorem 2 it follows that there is no word $w$ in grouptheory, such that in every group $\overline{A}$ the operation $w_\overline{A}$ defined by $w$ is a characterizing invariant for $G_1(\overline{A})$. However, there are other ways of uniformly defining operations by the use of expressions in grouptheory. For example consider the function $f_\overline{A}(a, b, c)$ which takes the value $c$ or $e$ according to whether $\alpha(a, b, c)$ holds or does not hold in $\overline{A}$. One can recover the relation $\alpha(a, b, c)$ from $f$, $Sx = x^{-1}$ and $e$, by defining: $\alpha(a, b, c)$, if and only if, $(c \neq e \land f(a, b, c) = c) \lor (c = e \land S\alpha = b)$. It follows that $(e, S, f)$ is a system of characterizing invariants for $G_1(\overline{A})$.

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
Theorem 2 belongs into meta-group theory, i.e., it is a statement about a first order functional calculus $F[e, \cdot, -^1]$ with extralogical primitives $e$, $\cdot$, and $-^1$, and extralogical axioms corresponding to conventional group-axioms. The statement may become false if a different formalization of group theory is used, for example the rather non-conventional formalization $F [e, \cdot, -^1, f]$ with an additional primitive $f$ and an additional axiom, $f(x, y, z) = n \leftrightarrow ((xy \equiv z \lor yx \equiv z) \land n = z) \lor (xy \not\equiv z \land yx \not\equiv z \land n = e)$.

Bibliography

1. F. Klein, Vergleichende Betrachtungen über neuere geometrische Forschungen, Erlangen (1872), Verlag von Andreas Deichert.

University of Illinois and
University of Michigan