ORDERED GROUPS

BY F. W. LEVI
(Calcutta)

Received July 28, 1942
(Communicated by Prof. B. S. Madhava Rao, D.Sc., F.A.Sc.)

The theory of ordered fields has a kind of counterpart in the theory of ordered groups. Every element $\neq 1$ of an ordered group is necessarily of infinite order. This condition being satisfied Abelian groups as well as every group* the commutator-group of which is situated in the centre, can be ordered. In general, the order is of a non-Archimedean type. Those elements which in Archimedean sense are either comparable with a particular element $a$ or infinitely small to $a$ form a group $A$; the latter class of elements form a normal subgroup $E$. The group $A/E$ will be proved to be an abelian group which is isomorphic to a module of real numbers every coset of $E$ in $A$ being characterised by a real number $\lambda = \log(b)$ which has the character of a logarithmus to the base $a$. As the groups considered in this paper are not necessarily abelian, the multiplicative language is used, and the unitelement is denoted by 1. With regard to the terms "positive" and "negative", the notation $O$ would have some advantage.

§1. Suppose a group $G$ is partitioned into two sets $S$ and $S'$ satisfying the following conditions.
1. $S \cup S' = G$, $S \cap S' = 1$.
2. $S$ is a semi group and normal invariant in $G$ ($gSg^{-1} = S$).
3. If $b$ belongs to $S$ (to $S'$) then $b^{-1}$ belongs to $S'$ (to $S$).

The order is established in $G$ by the following definition.

If $ab^{-1} \neq 1$ belongs to $S$, then $a > b$ (1)

Hence

either $a = b$, or $a > b$ or $a < b$ holds. (2)

* In a recent paper, the author has investigated groups of this kind from a different point of view. See "Groups in which the commutator-operation satisfies certain algebraic conditions," Jour. Ind. Math. Soc., 6, p. 87-97.
Ordered Groups

The notations $\geq$ and $\leq$ are used in the customary manner. An element $a$ belongs to $S$ or to $S'$ according as $a \geq 1$ or $a \leq 1$ holds. The elements $> 1$ are called positive, the elements $< 1$ negative elements. The absolute value $|a|$ of $a$ is defined by

$$|a| = a \quad \text{if} \quad a \geq 1$$

$$|a| = a^{-1} \quad \text{if} \quad a \leq 1.$$

(3)

If $a > b$, then $b < a$ and conversely;

moreover $b^{-1} > a^{-1}, a^c > b^c, ca > cb, b^{-1}a > 1$. (4)

$$a \geq b \quad \text{and} \quad b \geq c \quad \text{imply} \quad a \geq c$$

(5)

where the sign $\equiv$ holds in the third inequality if and only if it holds in both the suppositions.

$$a > a' \quad \text{and} \quad b > b' \quad \text{imply} \quad ab > a'b'.$$

(6)

Suppose on the other hand that relations $>$ and $<$ are defined in $G$ in such a way that (2), (4), (5) and (6) hold, then the system $S$ of the elements $\geq 1$, and the system $S'$ of the elements $\leq 1$ satisfy the conditions 1, 2 and 3. For the absolute values of a product, the following formulas can easily be shown for

$$|ab| = |a| \cdot |b| \quad \text{if} \quad a > 1, b > 1$$

$$= |b| \cdot |a| \quad \text{if} \quad a < 1, b < 1$$

$$= |a| \cdot |b|^{-1} \quad \text{or} \quad |b| \cdot |a|^{-1} \quad \text{if} \quad a > 1, b < 1$$

$$= |b|^{-1} \cdot |a| \quad \text{or} \quad |a|^{-1} \cdot |b| \quad \text{if} \quad a < 1, b > 1;$$

in the two last lines, the first or the second alternative holds true, according as $|a| > |b|$ or $|a| < |b|$. Moreover $|a|^n = |a^n|$. For $a \neq 1$, $1 < |a| < \ldots < |a|^n = |a^n|$ holds. Hence $a$ is of infinite order.

§2. Suppose that for two positive integral numbers $m$ and $n$, and for two elements $a$ and $b$ of $G$ the inequality

$$|a|^m < |b|^n$$

holds, then there are two possibilities. Either (7) holds for every pair of positive integrals $m$ and $n$, then $|b|$ is said to be infinitely small to $|a|$, and this statement is denoted by

$$|a| \gg |b| \quad \text{and} \quad |b| \ll |a|.$$  

(8)

Or there exists a pair of positive integrals $m', n'$ for which

$$|a|^{m'} < |b|^{n'}$$

(7')
holds, then \( a \) and \( b \) are said to be comparable. Comparability will be denoted by

\[ a \sim b. \quad (9) \]

Suppose that \( a \sim b, \ b \sim c \), then \(|b|^p > |c|^p\), \(|b|^{p'} < |c|^{p'}\) holds for suitable positive integers \( p, q, p' \) and \( q \). Hence \(|a|^{mp} > |c|^{mq}\) and \(|a|^{m'p'} < |c|^{m'q'}\); thus \( a \sim c \). Comparability is therefore a transitive property, and since it is also reflexive and symmetric, comparable elements of an ordered group form a class. For every \( a \neq 1 \)

\[ 1 \ll |a| \]

holds; hence \( 1 \) forms a class by itself. If all the other elements are comparable, the order of \( G \) is of an Archimedean character. Similarly one shows that

\[ |a_1| \geq |a| \gg |b| \gg |b_1| \implies |a_1| \gg |b_1| \]

and that

\[ a' \sim a, \ |a| \gg |b|, \ b \sim b' \implies |a'| \gg |b'|. \]

§3. Let \( A \) be an abelian group in which every element \( \neq 1 \) is of infinite order. It will be proved that \( A \) can be ordered. An element \( a \) is said to be dependent on the elements \( a_1, \ldots, a_m \) if for any \( n \neq 0 \), an equation

\[ a^n = a_{r_1}^{n_1} \ldots a_{r_s}^{n_s} \quad (10) \]

holds. The exponents in (10) can be multiplied with any integral number, and can be divided by any common factor. Hence if \( a \neq 1 \) is dependent on \( a_1, \ldots, a_m \), there exists a canonical form of the equation (10) where \( n > 0, n_1, \ldots, n_s \) are all \( \neq 0 \), their h.c.f. is equal to 1 and the indices are ordered in the ascending order. A well ordered system

\[ a_1, a_2, \ldots, a_s, \ldots \quad (11) \]

is said to be a basis of \( A \) if every element \( \neq 1 \) of \( A \) is dependent on a finite number of elements of (11) and if there exists only one canonical form of representation.

Given a basis (11) of \( A \), and let

\[ a^n = a_{r_1}^{n_1} \ldots a_{r_s}^{n_s} \]

be a canonical representation, then \( a \) is supposed to belong to \( S \) or to \( S' \) according as \( n_1 > 0 \) or \( n_1 < 0 \) holds; the element 1 is taken as a common element of \( S \) and \( S' \). The conditions 1, 2 and 3 of §1 are obviously satisfied, and therefore \( A \) is ordered.
Ordered Groups

It remains to prove\(^\dagger\) that \(A\) has a basis. As \(A\) is a group, it is also a set, and therefore it can be well ordered. Let

\[
\begin{align*}
   b_1, b_2, \ldots, b_\mu, \ldots.
\end{align*}
\]

be the elements \(\neq 1\) of \(A\) given as a well ordered set. Omit in (12) all those elements which are dependent on the preceding ones, the remaining set is non-empty (since it contains \(b_1\)) and well ordered; denote it by (11). There cannot be any relation \(a_1 a_2 \cdots a_\mu = 1\) with exponents \(\neq 0\), otherwise the \(a_1\) with the highest index is dependent on \(a_2\)'s with lower indices, contrary to the supposition that no element (11) depends on elements which precede it. On the other hand every element (12) can be shown to depend on the elements (11). If not so, there is amongst the elements not depending on (11) one with a lowest index, say \(b_\mu\). Since \(b_\mu\) is not an element (12), it depends on elements which precede it and which therefore are dependent on the elements (12). Hence \(b_\mu\) depends on the elements (12). Suppose now that any \(b\) admits two different canonical representations, say

\[
\begin{align*}
   b^n &= a_{\nu_1} m_1 \cdots a_{\nu_s} m_s, \quad \nu_1 < \ldots < \nu_s
   \\
   b^m &= a_{\mu_1} m_1 \cdots a_{\mu_t} m_t, \quad \mu_1 < \ldots < \mu_t, \text{ then}
   \\
   a_{\nu_1} m_1 \cdots a_{\nu_s} m_s a_{\mu_1}^{-m_1} \cdots a_{\mu_t}^{-m_t} &= 1.
\end{align*}
\]

Hence all the exponents are all zero, i.e., \(\nu_i = \mu_i\), \(m_i = n m_i\), for \(i = 1, \ldots, s = t\), and that is impossible when the two canonical representations are different. Hence (11) is a basis of \(A\).

§4. Let \(Y\) be a subset of an ordered group \(G\) with the property that if \(a\) belongs to \(Y\), then also \(a^{-1}\) and all the elements situated between \(a\) and \(a^{-1}\) belong to \(Y\); then \(Y\) will be called a symmetric section of \(G\).

Let \(Y\) be a symmetric section of \(G\) and be a subgroup of \(G\); if \(y\) belongs to \(Y\), whereas \(c\) is an element of \(G\) not belonging to \(Y\), then \(|y|^m < |c|^n\) for every pair of positive integers \(m\) and \(n\). Hence

\[
   |y| \ll |c|.
\]

On the other hand, let \(c\) be any particular element of \(G\), then the elements \(y\) satisfying (13) form a symmetric section \(Y\) of \(G\) which is also a subgroup of \(G\). If \(a\) does not belong to \(Y\), then either \(a\) is comparable with \(c\), or \(|c| \ll |a|\), hence (13) remains true if \(c\) is replaced by any element which does not belong to \(Y\). If in particular \(a \sim c\), then every element \(y\) satisfying \(|y| \ll |a|\), satisfies also (13).

\(^\dagger\) For the convenience of the reader the proof is given in full.
Given an element $a$; the elements which are comparable with $a$ and those of which the absolute value is infinitely small to $|a|$ form together a symmetric section $A$ which will be proved to be a subgroup of $G$. Let $a$ and $\beta$ be two elements of $A$, say $|a| \geq |\beta|$, then $|a^{-1} \beta^{-1}|$ and $|\beta^{-1} a^{-1}|$ are smaller than $|a|^2$, and therefore these elements belong to $A$; hence $A$ is a subgroup of $G$. The elements whose absolute values are infinitely small to $A$ form a group which is a subset and therefore a subgroup, say $E$ of $A$. It will be proved to be a normal subgroup of $A$. If an element $b$ of $A$ does not belong to $E$, then $b \sim a$, and therefore $|\epsilon|^n < |b|$ for every $n$ and every element $\epsilon$ of $E$. Now $b | \epsilon | b^{-1} > 1$. Hence $1 < \beta^n = b | \epsilon | b^{-1} < b | b^{-1} = |b|$. Thus $\beta \ll |b|$ belongs to $E$ and the same holds for $\beta^{-1} = b | \epsilon | b^{-1}$. Hence $E$ is a normal subgroup of $A$.

The elements of $G$ which by any homomorphism are mapped on $1$ form a normal subgroup of $G$. If in particular the homomorphism is order-invariant, then this subgroup is a symmetric section. It follows therefore that when by an order invariant homomorphism, $y$ is mapped on $1$ and $c$ is mapped on an element $\neq 1$, then $|y| \ll |c|$ holds. This statement admits two inverse propositions.

(1) Let $G$ be ordered, and let a normal subgroup $N$ of $G$ be a symmetric section of $G$, then the homomorphism which maps $N$ on $1$ is order-invariant.

If $a$ is an element of any coset of $N$ in $G$ and $\epsilon$ is an element of $N$, then $a \epsilon$ is positive or negative, according as $a$ is positive or negative. Thus every coset of $N$ contains either only positive or only negative elements of $G$. In the first case the coset is considered to be a positive element of $G/N$, in the second case as a negative one. By this definition the conditions 1, 2 and 3 of §1 are satisfied. The positive elements of $G$ are mapped on the positive elements and on the unitelement of $G/N$ and similarly for the negative elements. Hence the mapping is order-invariant.

(2) Let $G/N$ be ordered and also $N$ be ordered in such a way that by an inner automorphism of $G$ the positive (negative) elements of $N$ are transformed into positive (negative) elements of $N$, then the order in $N$ can be extended to an order in $G$, and this order is invariant for the mapping $G \rightarrow G/N$.

Consider the elements of the positive (negative) cosets of $G/N$ and the positive (negative) elements of $N$ as the positive (negative) elements of $G$. Then the conditions 1, 2 and 3 of §1 as well as the last proposition are satisfied.
Ordered Groups

261

If in particular the elements \( \neq 1 \) of a group \( A \) as well as those of its factor-group \( A/C(A) \) are of infinite order and the commutator-group \( C(A) \) lies in the centre of \( A \), then every element of \( C(A) \) remains invariant for the inner automorphisms of \( A \). Thus one has only to give an order to the two abelian groups \( C(A) \) and \( A/C(A) \) to obtain an order in the group \( A \).

\$\S 5\$. Suppose that \( m : n > p : q \), and \( a^p > b^q \), where \( m, n, p, q \) are positive integers and \( a, b \) is a pair of positive elements of an ordered group \( G \). Then \( a^{mp} > a^{pq} > b^{pq} \); hence \( a^m > b^q \). If therefore \( a \) and \( b \) are positive comparable elements of \( G \), they determine a Dedekind section say, \( \lg b \) of the rational positive numbers to the effect that

\[
\begin{align*}
a^p &> b^q & \text{if } p : q > \lg b \\
a^p &< b^q & \text{if } p : q < \lg b.
\end{align*}
\]

\( \lg b \) may be rational or irrational; if it is rational, say \( s : t \), then \( a^s \) might be greater or less than \( b^t \), or the elements might be equal. The definition (14) can be extended to non-positive elements \( b \) (the "basis" \( a \) is always considered to be a positive element) by

\[
\begin{align*}
\lg \epsilon &= 0, \text{ for } \epsilon \ll a \\
\lg (b^{-1}) &= -\lg b.
\end{align*}
\]

The following formulas are immediate consequences of the definition.

\[
\begin{align*}
\lg (a^m) &= m, \\
\lg (b^n) &= n, \\
\lg b^c &= c, \\
\lg b > \lg c &\implies b > c, \\
\text{and for } b > 1, \quad \lg b + \lg a &= 1, \quad \lg b + \lg c = \lg c.
\end{align*}
\]

(15)

In particular \( \lg b = 1 \) implies \( \lg a = 1 \), but from this relation it does not follow necessarily that \( a \) and \( b \) are equal.

This function \( \lg (b) \) will be used now to investigate the groups \( A, E \) and \( A/E \) introduced in \( \S 4 \). By

\[
a, b, c \ldots \ldots \quad \text{(with and without indices)}
\]

the positive elements of \( A \) will be denoted which do not belong to \( E \), whereas \( \epsilon \) (with or without an index) denotes elements of \( E \), and \( a, \beta \ldots \ldots \) denote arbitrary elements of \( A \). Hence the \( \lg \)-function exists for every basis (16) and every variable \( a \), and there is

\[
\lg (b) > 0, \quad \lg (b^{-1}) < 0, \quad \lg (\epsilon) = 0.
\]

Moreover \( a^p \leq a^m \leq a^q \) implies \( p : m \leq \lg a \leq q : m \) if \( m \) is positive.

When the group \( A \) is abelian, one can show easily that

\[
\lg a \beta = \lg a + \lg \beta.
\]

(17)

The general validity of (17) will be proved now.
Since $E$ is a normal subgroup of $A$, all the commutators $(a, e)$ belong to $E$. Hence
\[(eb)^n = e(b, e)eb^2(eb)^{n-2} = e_2b^2(eb)^{n-2} = e_2(b^2, e)b^3(eb)^{n-3} = \]
\[= e_2b^3(eb)^{n-2} = \ldots = e_nb^n.
\]
Now $|e_n| < b$, hence $b^{n-1} < e_nb^n = (eb)^n < b^{n+1}$ for every positive integer $n$. Hence $a\lg (eb) = 1$
\[a\lg (eb) = a\lg b
\]
and similarly $a\lg (be) = a\lg b$. (18)

From (18) it follows that if $a\lg a_1 \neq a\lg a_2$,
\[a_1 = a_2 a_2^{-1} \cdot a_2 \neq e_1 a_2
\]
\[= a_2 \cdot a_2^{-1} a_2 \neq a_2, e_2. \quad \text{Hence}
\]
a\lg (a_1 a_2^{-1}) \neq 0, a\lg (a_2^{-1} a_1) \neq 0. (19)

Let $b$ run over all the elements (16); then two cases are distinguished.

1. Among the positive numbers $a\lg b$ (where the basis $a$ is kept constant) there is a smallest one.

2. To every $a_n$, there exists an element $a_{n+1}$ such that $0 < a\lg a_{n+1} < a\lg a_n$ holds.

i. In the first case, one can interchange the elements (16) in such a manner that the minimum value of $a\lg b$ is obtained for $b = a$. Hence $a\lg b \geq 1$.

Suppose $a\lg b = 1$, then for every $a$ there is $a\lg a = a\lg a$.

Thus there is no loss of generality in supposing that $b < a$.

Since $a\lg b^2 = 2$, \quad $a < b^2$;

hence $1 < b^{-1}a < b$, and therefore $1 < a b^{-1} < (ab^{-1})^2 = a \cdot b^{-1}a \cdot b^{-1} < a$.

Therefore $0 \leq 2 a\lg (ab^{-1}) = a\lg (ab^{-1})^2 < a\lg a = 1$.

Hence $a\lg (ab^{-1}) = 0$, $ab^{-1} = e$, $a = eb = b \cdot b^{-1}eb = b e'$.

On the other hand, a left or right hand factor $e$ does not change the value of the $a\lg$ function. The elements $b$ of $A$ for which $a\lg b = 1$ form therefore a coset of $E$. To every element $a$ of $A$, there exists a (not necessarily positive) integral number $m$, such that
\[m \leq a\lg a < m + 1. \quad \text{Hence}
\]
a\lb_{m-1} < a < a\lb_{m+1}
\[a^{-1} < a a^{-m} < a \quad \text{and therefore} \quad -1 \leq a\lg (aa^{-m}) \leq 1.
\]
Ordered Groups

Hence \( \log(a^{-m}) \) can only have the values \( 1, 0, -1 \) and correspondingly it is of the form \( a \epsilon = \epsilon a \), or \( \epsilon \), or \( a^{-1} \epsilon = \epsilon a^{-1} \), and therefore

\[
a = \epsilon a^p,
\]
where \( p \) is any integral number, and from (18) it follows that \( \log a = p \). Let \( \beta \) be any other element of \( A \), then

\[
\beta = \epsilon a^r, \quad \log \beta = q.
\]
Hence \( a \beta = \epsilon a^p \epsilon a^r = \epsilon (a^p \epsilon) a^{p+q} = a^{p+q} \).

Thus \( \log(a \beta) = p + q = \log a + \log \beta \).

II. Suppose that to every element \( a_r \) of (16) there exists an element \( b \) such that \( 0 < \log b < \log a_r \) holds. If \( b^2 < a \), then put \( b = a_{r+1} \), but if \( b^2 > a_r \), then

\[
1 < a_r b^{-1} < b \quad \text{and} \quad 1 < b^{-1} a_r < b;
\]
hence

\[
a_r < a_r b^{-1} a_r < a_r b \quad \text{and} \quad 1 < a_r b^{-1} < (a_r b^{-1})^2 < a_r. \]

Put \( a_r b^{-1} = a_{r+1} \), then

(see 19) \( 0 < \log a_{r+1} \leq \frac{1}{2} \log a_r \). Hence one can construct a sequence of positive elements not belonging to \( E \) for which

\[
\log a = 1, \quad 0 < \log a_2 \leq \frac{1}{2}, \ldots, 0 < \log a_n \leq \frac{1}{2} \log a_{n-1} \leq 2^{-n}, \ldots \quad (20)
\]
holds. For every \( n \) there exists integral numbers \( r \) and \( s \) such that

\[
a_n^{r+1} < a \leq a_n^{r+1}, \quad a_n^r < a < a_n^{r+1}. \]

Hence

\[
a_n^{r+1} < a \beta a_n^r < a_n^{r+1} \quad \text{and} \quad a_n^{r+1} < (a, \beta) < a_n^{r+1}.
\]
Thus \( |(a, \beta)| < a^2 \) for \( n = 2, 3, \ldots \), hence \( \log |(a, \beta)| = 0 \)

i.e., \( (a, \beta) = \epsilon \). Now \( (a, \beta)^{m} = (a, \beta) (\beta, a^2) a^2 \beta \beta a^m \beta a + \epsilon a^{m+1} a \beta \beta a + \epsilon a^{m+1} \beta + \epsilon a^m \beta + \epsilon a \).

Moreover \( a^u \leq a^m < a^{n+1} \), \( \log a = \lim u : m \)

\[
a^u \leq \beta^m < a^{n+1}, \quad \log \beta = \lim v : m
\]

\[
a^u+1 \leq \epsilon a^m \beta = (a \beta)^{m} < a^{u+1} \quad \log (a \beta) = \lim (u + v) : m.
\]

Hence \( \log(a \beta) = \log a + \log \beta \).

Thus (17) holds in every case.

The mapping \( a \rightarrow \log a \) is therefore a homomorphism mapping \( A \) on the modul of the real numbers \( \log a \) and \( E \) on \( 0 \). Thus this homomorphism is an isomorphism of \( A/E \).