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 $\lambda = {}_a\mathrm{lg}(b)$ 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. $S \vee S' = G$, $S \wedge S' = 1$.
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)

" " S′, " $a < b$.

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.

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

$$\begin{aligned} |a| &= a \quad \text{if } a \geqq 1 \\ |a| &= a^{-1} \text{ if } a \leqq 1. \end{aligned} \tag{3}$$

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

$$\text{moreover } b^{-1} > a^{-1},\ ac > bc,\ ca > cb,\ b^{-1}a > 1. \tag{4}$$

$$a \geqq b \text{ and } b \geqq c \text{ imply } a \geqq c \tag{5}$$

where the sign $=$ holds in the third inequality if and only if it holds in *both* the suppositions.

$$a > a' \text{ and } b > b' \text{ imply } ab > a'b'. \tag{6}$$

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 $\geqq 1$, and the system S′ of the elements $\leqq 1$ satisfy the conditions 1, 2 and 3. For the absolute values of a product, the following formulas can easily be shown

$$\begin{aligned} |ab| &= |a|\ |b| \text{ if } a > 1,\ b > 1 \\ &= |b|\ |a| \text{ if } a < 1,\ b < 1 \\ &= |a|\ |b|^{-1} \text{or} = |b|\ |a|^{-1} \quad \text{if } a > 1,\ b < 1 \\ &= |b|^{-1}|a| \text{ or } = |a|^{-1}|b| \quad \text{if } a < 1,\ b > 1; \end{aligned}$$

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 $a \neq 1$, $1 < |a| < \dots < |a|^n = |a^n|$ 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

$$|a|^m < |b|^n \tag{7}$$

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

$$|a| \gg |b| \text{ and } |b| \ll |a|. \tag{8}$$

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

$$|a|^{m'} < |b|^{n'} \tag{7'}$$

holds, then a and b are said to be *comparable*. Comparability will be denoted by

$$a \sim b. \tag{9}$$

Suppose that $a \sim b$, $b \sim c$, then $|b|^p > |c|^q$, $|b|^{p'} < |c|^{q'}$ holds for suitable positive integers $\mathbf{p}$, $\mathbf{q}$, $\mathbf{p}'$ and $\mathbf{q}$. Hence $|a|^{mp} > |c|^{nq}$ and $|a|^{m'p'} < |c|^{n'q'}$; 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

$$|a_1| \geq |a| \gg |b| \geq |b_1| \text{ implies } |a_1| \gg |b_1|$$

and that

$$a' \sim a,\ |a| \gg |b|,\ b \sim b' \text{ implies } |a'| \gg |b'|.$$

§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 $\mathbf{n} \neq 0$, an equation

$$a^n = a_{\nu_1}^{n_1} \ldots a_{\nu_r}^{n_r} \tag{10}$$

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 $\mathbf{n} > 0$, $\mathbf{n}_1, \ldots, \mathbf{n}_\mu$ are all $\neq 0$, their *h.c.f.* is equal to $\mathbf{1}$ and the indices are ordered in the ascending order. A well ordered system

$$a_1, a_2, \ldots, a_\nu, \ldots\ldots \tag{11}$$

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

$$a^n = a_{\nu_1}^{n_1} \ldots a_{\nu_t}^{n_t}$$

be a canonical representation, then a is supposed to belong to S or to S′ according as $\mathbf{n}_1 > 0$ or $\mathbf{n}_1 < 0$ 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.

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

$$b_1, b_2, \ldots, b_\mu, \ldots\ldots \tag{12}$$

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 $a_r^\rho \ldots a_s^\sigma = 1$ with exponents $\neq 0$, otherwise the a with the highest index is dependent on a'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_μ. Since b_μ is not an element (12), it depends on elements which precede it and which therefore are dependent on the elements (12). Hence b_μ depends on the elements (12). Suppose now that any b admits two different canonical representations, say

$$b^n = a_{\nu_1}^{n_1} \ldots a_{\nu_s}^{n_s} \qquad \nu_1 < \ldots < \nu_s$$

$$b^m = a_{\mu_1}^{m_1} \ldots a_{\mu_t}^{m_t}, \qquad \mu_1 < \ldots < \mu_t, \text{ then}$$

$$a_{\nu_1}^{mn_1} \ldots a_{\nu_s}^{mn_s}\, a_{\mu_1}^{-nm_1} \ldots a_{\mu_t}^{-nm_t} = 1.$$

Hence all the exponents are all zero, *i.e.*, $\nu_i = \mu_i$, $mn_i = nm_i$, 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 $|y|^n < |c|^m$ for every pair of positive integers **m** and **n**. Hence

$$|y| \ll |c|. \tag{13}$$

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).

† 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 α and β be two elements of A, say $|\alpha| \geq |\beta|$, then $|\alpha^{\pm 1}\beta^{\pm 1}|$ and $|\beta^{\pm 1}\alpha^{\pm 1}|$ are smaller than $|\alpha|^2$, 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 ϵ of E. Now $b|\epsilon| > b$ and therefore $\beta = b|\epsilon|b^{-1} > 1$. Hence $1 < \beta^n = b|\epsilon|^n b^{-1} < b|b|b^{-1} = |b|$. Thus $\beta \ll |b|$ belongs to E and the same holds for $\beta^{-1} = b|\epsilon|^{-1}b^{-1}$. 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 ϵ 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 $G \to G/N$.

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.

If in particular the elements $\neq 1$ of a group A as well as those of its factorgroup $A/C(A)$ are of infinite order and the commutatorgroup $C(A)$ 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.

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

$$a^p > b^q \quad \text{if } \mathbf{p} : \mathbf{q} > {}_a\lg b \qquad (14)$$
$$a^p < b^q \quad \text{if } \mathbf{p} : \mathbf{q} < {}_a\lg b.$$

${}_a\lg b$ may be rational or irrational; if it is rational, say $\mathbf{s} : \mathbf{t}$, 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

$${}_a\lg \epsilon = 0, \text{ for } \epsilon \ll a \qquad (14')$$
$${}_a\lg (b^{-1}) = -{}_a\lg b.$$

The following formulas are immediate consequences of the definition. ${}_a\lg (a^m) = \mathbf{m}$, ${}_a\lg(b^m) = \mathbf{m}\,{}_a\lg b$, ${}_a\lg b > {}_a\lg c$ implies $b > c$,

$$\text{and for } b > 1, \; {}_a\lg b \; {}_b\lg a = \mathbf{1}, \; {}_a\lg b \; {}_b\lg c = {}_a\lg c \qquad (15)$$

In particular ${}_a\lg b = \mathbf{1}$ implies ${}_b\lg a = \mathbf{1}$, but from this relation it does not follow necessarily that a and b are equal.

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

$$a, b, c \ldots\ldots \quad \text{(with and without indices)} \qquad (16)$$

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

$${}_a\lg(b) > 0, \; {}_a\lg(b^{-1}) < 0, \; {}_a\lg(\epsilon) = 0.$$

Moreover $a^p \leq a^m \leq a^q$ implies $\mathbf{p} : \mathbf{m} \leq {}_a\lg \alpha \leq \mathbf{q} : \mathbf{m}$ if $\mathbf{m}$ is positive.

When the group A is *abelian*, one can show easily that

$${}_a\lg \alpha\beta = {}_a\lg \alpha + {}_a\lg \beta. \qquad (17)$$

The general validity of (17) will be proved now.

Since E is a normal subgroup of A, all the commutators (α, ϵ) belong to E. Hence

$$(\epsilon b)^n = \epsilon\,(b, \epsilon)\,\epsilon b^2\,(\epsilon b)^{n-2} = \epsilon_2 b^2\,(\epsilon b)^{n-2} = \epsilon_2\,(b^2, \epsilon)\,b^3\,(\epsilon b)^{n-3} =$$
$$= \epsilon_3 b^3\,(\epsilon b)^{n-3} = \ldots = \epsilon_n b^n.$$

Now $|\,\epsilon_n\,| < b$, hence $b^{n-1} < \epsilon_n b^n = (\epsilon b)^n < b^{n+1}$ for every positive integer $\mathbf{n}$. Hence ${}_{b}\mathrm{lg}\,(\epsilon b) = \mathbf{1}$

$${}_{a}\mathrm{lg}\,(\epsilon b) = {}_{a}\mathrm{lg}\,b$$
$$\text{and similarly} \quad {}_{a}\mathrm{lg}\,(b\epsilon) = {}_{a}\mathrm{lg}\,b. \tag{18}$$

From (18) it follows that if ${}_{a}\mathrm{lg}\,a_1 \neq {}_{a}\mathrm{lg}\,a_2$,

$$a_1 = a_1 a_2^{-1} \cdot a_2 \neq \epsilon_1 a_2$$
$$= a_2 \cdot a_2^{-1} a_1 \neq a_2\,\epsilon_2 \cdot \quad \text{Hence}$$
$${}_{a}\mathrm{lg}\,(a_1 a_2^{-1}) \neq 0, \; {}_{a}\mathrm{lg}\,(a_2^{-1}\,a_1) \neq 0. \tag{19}$$

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

1. Among the positive numbers ${}_{a}\mathrm{lg}\,b$ (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 $0 < {}_{a}\mathrm{lg}\,a_{n+1} < {}_{a}\mathrm{lg}\,a_n$ holds.

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

Suppose ${}_{a}\mathrm{lg}\,b = 1$, then for every α there is ${}_{a}\mathrm{lg}\,\alpha = {}_{b}\mathrm{lg}\,\alpha$.

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

Since ${}_{a}\mathrm{lg}\,b^2 = \mathbf{2}$, $\quad a < b^2$;

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 $0 \leq \mathbf{2}\,{}_{a}\mathrm{lg}\,(ab^{-1}) = {}_{a}\mathrm{lg}\,(ab^{-1})^2 < {}_{a}\mathrm{lg}\,a = \mathbf{1}$.

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

On the other hand, a left or right hand factor ϵ does not change the value of the ${}_{a}\mathrm{lg}$ function. The elements b of A for which ${}_{a}\mathrm{lg}\,b = \mathbf{1}$ form therefore a coset of E. To every element α of A, there exists a (not necessarily positive) integral number $\mathbf{m}$, such that

$\mathbf{m} \leq {}_{a}\mathrm{lg}\alpha < \mathbf{m} + 1$. Hence

$a^{m-1} < \alpha < a^{m+1}$

$a^{-1} < \alpha\,a^{-m} < a$ and therefore $-1 \leq {}_{a}\mathrm{lg}\,(\alpha a^{-m}) \leq \mathbf{1}$.

Hence ${}_a\lg\,(\alpha a^{-m})$ can only have the values **1, 0, − 1** and correspondingly it is of the form $a\epsilon = \epsilon' a$, or ϵ, or $a^{-1}\,\epsilon_1 = \epsilon_2 a^{-1}$, and therefore

$\alpha = \epsilon a^{p}$, where **p** is any integral number, and

from (18) it follows that ${}_a\lg\alpha = \mathbf{p}$. Let β be any other element of A, then $\beta = \epsilon' a^{q}$, ${}_a\lg\,\beta = \mathbf{q}$. Hence $\alpha\,\beta = \epsilon a^{p}\,\epsilon' a^{q} = \epsilon(a^{p}, \epsilon')\epsilon' a^{p+q} = \epsilon_1 a^{p+q}$.

Thus ${}_a\lg(\alpha\beta) = \mathbf{p} + \mathbf{q} = {}_a\lg\alpha + {}_a\lg\beta$.

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

$$1 < a_\nu\, b^{-1} < b \text{ and}$$

$$1 < b^{-1}\, a_\nu < b\text{; hence}$$

$$a_\nu < a_\nu\, b^{-1}\, a_\nu < a_\nu\, b \text{ and}$$

$$1 < a_\nu\, b^{-1} < (a_\nu\, b^{-1})^2 < a_\nu.$$ Put $a_\nu\ b^{-1} = a_{\nu+1}$, then (see 19) $0 < {}_a\lg\,a_{\nu+1} \leq \frac{1}{2}\,{}_a\lg\,a_\nu$. Hence one can construct a sequence of positive elements not belonging to E for which

$$ {}_a\lg a = 1,\ 0 < {}_a\lg a_2 \leq \tfrac{1}{2}, \ldots,\ 0 < {}_a\lg a_n \leq \tfrac{1}{2}\,{}_a\lg a_{n-1} \leq 2^{-n}, \ldots \qquad (20)$$

holds. For every **n** there exists integral numbers **r** and **s** such that

$$a_n^{\,r} \leq \alpha < a_n^{\,r+1},\ a_n^{\,s} \leq \beta < a_n^{\,s+1}. \text{ Hence}$$

$$a_n^{\,r+s} \leq \alpha\,\beta < a_n^{\,r+s+2}$$

$$a_n^{\,s-1} < \alpha\,\beta\,\alpha^{-1} < a_n^{\,s+2} \text{ and } a_n^{-2} < (\alpha, \beta) < a_n^{2}$$

Thus $|\,(\alpha, \beta)\,| < a_n^{2} \leq a_{n-1}$ for $\mathbf{n} = 2, 3, \ldots.$ Hence ${}_a\lg\,|\,(\alpha, \beta)\,| = 0$ *i.e.*, $(\alpha, \beta) = \epsilon$. Now $(\alpha, \beta)^m = (\alpha, \beta)\,(\beta, \alpha^2)\,\alpha^2\beta^2\,(\alpha\beta)^{m-2} = \epsilon_1\alpha^2\beta^2\,(\alpha\beta)^{m-2} = \ldots = \epsilon'\alpha^m\beta^m$ for any positive **m.**

Moreover $a^{u} \leq \alpha^{m} < a^{u+1}$, ${}_a\lg\,\alpha = \lim\limits_{m\to+\infty} \mathbf{u} : \mathbf{m}$

$$a^{v} \leq \beta^{m} < a^{v+1},\ {}_a\lg\,\beta = \lim_{m\to+\infty} \mathbf{v} : \mathbf{m}$$

$$a^{u+v-1} < \epsilon'\alpha^{m}\beta^{m} = (\alpha\beta)^{m} < a^{u+v-3}\ {}_a\lg\,(\alpha\beta) = \lim_{m\to+\infty} (\mathbf{u} + \mathbf{v}) : \mathbf{m}.$$

Hence ${}_a\lg(\alpha\beta) = {}_a\lg\,\alpha + {}_a\lg\,\beta$.

Thus (17) holds in every case.

The mapping $\alpha \to {}_a\lg\,\alpha$ is therefore a homomorphism mapping A on the modul of the real numbers ${}_a\lg\,\alpha$ and E on 0. Thus this homomorphism is an isomorphism of A/E.