

THE FIELD OF REAL NUMBERS WITH A SMALL SUBGROUP OF THE CIRCLE GROUP

1. ORIENTED ABELIAN GROUPS

In this section, we use additive notation for abelian groups, unless specified otherwise. Let G be an ordered abelian group with distinguished element $1 > 0$. We define an abelian group $G_{\text{mod}1}$ as follows: the underlying set of $G_{\text{mod}1}$ is the subset

$$[0, 1) := \{g \in G : 0 \leq g < 1\}$$

of G , and its addition operation $+_1$ is “addition modulo 1”, that is, for $g, h \in [0, 1)$,

$$g +_1 h = g + h \text{ if } g + h < 1, \quad g +_1 h = g + h - 1 \text{ otherwise.}$$

Let $G(1)$ be the convex hull of $\mathbb{Z} \cdot 1$ in G . For $x \in G(1)$ we define $x_{\text{mod}1} \in [0, 1)$ by $x - x_{\text{mod}1} \in \mathbb{Z} \cdot 1$, so we have a surjective group morphism

$$x \mapsto x_{\text{mod}1} : G(1) \rightarrow G_{\text{mod}1}$$

with kernel $\mathbb{Z} \cdot 1$. We equip $G_{\text{mod}1}$ with the ternary relation \mathcal{O} on its underlying set defined as follows: for $g, h, k \in [0, 1)$,

$$\mathcal{O}(g, h, k) :\iff g < h < k, \text{ or } h < k < g, \text{ or } k < g < h.$$

It is easy to check that for all $g, h, k \in [0, 1)$ we have

$$\begin{aligned} \mathcal{O}(g, h, k) &\iff \text{there are } x, y, z \in G(1) \text{ such that } x < y < z, \ z - x < 1, \\ &\quad x_{\text{mod}1} = g, \ y_{\text{mod}1} = h, \ z_{\text{mod}1} = k. \end{aligned}$$

The relation \mathcal{O} is an orientation on $G_{\text{mod}1}$ in the following sense: Let A be an abelian group. An *orientation* on A is a ternary relation \mathcal{O} on A such that for all $a, b, c, d \in A$:

- (1) $\{(x, y) \in A^2 : \mathcal{O}(0, x, y)\}$ is a strict linear order on the set $A \setminus \{0\}$,
- (2) $\mathcal{O}(a, b, c) \Rightarrow \mathcal{O}(b, c, a)$,
- (3) $\mathcal{O}(a, b, c) \Rightarrow \mathcal{O}(a + d, b + d, c + d)$,
- (4) $\mathcal{O}(0, a, b) \Rightarrow \mathcal{O}(0, -b, -a)$.

Here it is part of (1) that if $x, y \in A$ and $\mathcal{O}(0, x, y)$, then $x \neq 0$ and $y \neq 0$.

Example. Let $\mathbb{S} := \{(a, b) \in \mathbb{R}^2 : a^2 + b^2 = 1\}$ be the (multiplicative) circle group. It has identity $(1, 0)$ and multiplication given by

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2 - b_1 b_2, a_1 b_2 + a_2 b_1).$$

We have a group isomorphism

$$t \mapsto (\cos 2\pi t, \sin 2\pi t) : \mathbb{R}_{\text{mod}1} \rightarrow \mathbb{S},$$

and we give \mathbb{S} the orientation that makes this an isomorphism of oriented groups. It is tedious but not hard to construct a quantifier-free formula $\mathcal{O}(x_1, y_1, x_2, y_2, x_3, y_3)$ in the sublanguage $\{0, <\}$ of the language of ordered rings such that

$$\mathcal{O}((a_1, b_1), (a_2, b_2), (a_3, b_3)) \iff \mathbb{R} \models \mathcal{O}(a_1, b_1, a_2, b_2, a_3, b_3).$$

for all $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in \mathbb{S}$. Thus $\mathbb{R}_{\text{mod}1}$ and \mathbb{S} are definable groups in the field \mathbb{R} of real numbers, and are isomorphic as groups. Note that the isomorphism indicated above is not definable in the ordered field \mathbb{R} , but is definable in this ordered field expanded by the restriction of the sine function to $[0, 2\pi]$.

For each real closed field R we put

$$\mathbb{S}(R) := \{(a, b) \in R^2 : a^2 + b^2 = 1\}$$

and consider $\mathbb{S}(R)$ as a commutative group with identity $(1, 0)$ and multiplication given by the same identity used to define the multiplication of \mathbb{S} . We also give it the orientation defined by the equivalence above involving the formula $\mathcal{O}(x_1, y_1, x_2, y_2, x_3, y_3)$, but with R instead of \mathbb{R} , and $\mathbb{S}(R)$ instead of \mathbb{S} .

An *oriented abelian group* is an abelian group with an orientation on it. We are going to show that every oriented abelian group is isomorphic to $G_{\text{mod}1}$ for some ordered abelian group G with distinguished element $1 > 0$. In the rest of this section A is an oriented abelian group with orientation \mathcal{O} , and we let a, b, c, d range over A .

Observations.

- (i) Given any a , the set $\{(x, y) \in A^2 : \mathcal{O}(a, x, y)\}$ is a strict linear order on $A \setminus \{a\}$, to be denoted by $<_a$, so $b <_a c$ means $\mathcal{O}(a, b, c)$, and $b <_a c$ implies in particular that a, b, c are distinct.
- (ii) $\mathcal{O}(a, b, c) \Leftrightarrow \mathcal{O}(-c, -b, -a)$.
- (iii) $(\mathcal{O}(a, b, c) \ \& \ \mathcal{O}(0, a, c)) \Rightarrow \mathcal{O}(0, a, b)$.
- (iv) $(\mathcal{O}(a, b, d) \ \& \ \mathcal{O}(b, c, d)) \Rightarrow \mathcal{O}(a, b, c)$.
- (v) $a <_0 b \Rightarrow -b <_0 a - b$.

To see why (iii) holds, assume $\mathcal{O}(a, b, c)$ and $\mathcal{O}(0, a, c)$. Then $\mathcal{O}(a, c, 0)$, so $b <_a c$ and $c <_a 0$, hence $b <_a 0$, so $\mathcal{O}(a, b, 0)$, and thus $\mathcal{O}(0, a, b)$. To get (iv) we first state (iii) as the implication $(\mathcal{O}(b, c, d) \ \& \ \mathcal{O}(0, b, d)) \Rightarrow \mathcal{O}(0, b, c)$. By axiom (3) we can replace 0 here by any element of A , and this gives (iv).

Lemma 1.1. *We have the following equivalences:*

- (1) $(a <_0 -b \ \text{and} \ a + b <_0 -c) \Leftrightarrow (b <_0 -c \ \text{and} \ a <_0 -b - c)$,
- (2) $(-b <_0 a \ \text{and} \ -c <_0 a + b) \Leftrightarrow (-c <_0 b \ \text{and} \ -a <_0 b + c)$.

Proof. We only show (1), since (2) can be proved in a similar way. If the forward direction of (1) holds, then the other direction follows by switching a and c . So assume $a <_0 -b$ and $a + b <_0 -c$; we want to show $b <_0 -c$ and $a <_0 -b - c$. By observation (v) above we get $b <_0 a + b$, hence $b <_0 -c$.

From $\mathcal{O}(0, a + b, -c)$ we get $\mathcal{O}(-b, a, -b - c)$ by adding $-b$, so $\mathcal{O}(a, -b - c, -b)$. In combination with $\mathcal{O}(0, a, -b)$ this gives $a <_0 -b - c$ by observation (iii). \square

Consider an ordered abelian group B with distinguished element $1 > 0$, and let $a, b \in [0, 1] \subseteq B$. Then we have the following equivalences:

$$\begin{aligned} a + b < 1 &\Leftrightarrow a = 0 \ \text{or} \ b = 0 \ \text{or} \ a <_0 -b, \\ a + b = 1 &\Leftrightarrow a \neq 0 \ \text{and} \ b \neq 0 \ \text{and} \ a +_1 b = 0, \\ a + b > 1 &\Leftrightarrow a \neq 0 \ \text{and} \ b \neq 0 \ \text{and} \ -b <_0 a. \end{aligned}$$

Here the lefthand sides use addition in B and the righthand sides refer to the operations and relations on $B_{\text{mod}1}$, in particular, $-b$ as used on the righthand sides denotes the negative of b in $B_{\text{mod}1}$. This motivates the following case distinctions in the abstract setting of any oriented abelian group A :

$$\begin{aligned}(a, b) \prec 1 & :\Leftrightarrow a = 0 \text{ or } b = 0 \text{ or } a <_0 -b, \\ (a, b) \asymp 1 & :\Leftrightarrow a \neq 0 \text{ and } b \neq 0 \text{ and } a + b = 0, \\ (a, b) \succ 1 & :\Leftrightarrow a \neq 0 \text{ and } b \neq 0 \text{ and } -b <_0 a.\end{aligned}$$

Let a, b be given. Then exactly one of $(a, b) \prec 1$, $(a, b) \asymp 1$, $(a, b) \succ 1$ holds, and $(a, b) \prec 1$ iff $(b, a) \prec 1$, $(a, b) \asymp 1$ iff $(b, a) \asymp 1$, and $(a, b) \succ 1$ iff $(b, a) \succ 1$. We also define $(a, b) \preceq 1$ to mean that $(a, b) \prec 1$ or $(a, b) \asymp 1$, and define $(a, b) \succeq 1$ to mean that $(a, b) \succ 1$ or $(a, b) \asymp 1$.

To construct an ordered abelian group G with an element $1 > 0$ such that A and $G_{\text{mod}1}$ are isomorphic as oriented abelian groups, we set $A^* = \mathbb{Z} \times A$, and define the binary operation $+$ on A^* as follows:

$$(k, a) + (l, b) = \begin{cases} (k + l, a + b) & \text{if } (a, b) \prec 1, \\ (k + l + 1, a + b) & \text{otherwise,} \end{cases}$$

where $k, l \in \mathbb{Z}$. We shall prove that A^* is an abelian group with $+$ as its addition operation. It is clear that $(0, 0) + (k, a) = (k, a)$, $(k, a) + (-k, -a) = (0, 0)$ if $(a, -a) \prec 1$, and $(k, a) + (-k - 1, -a) = (0, 0)$ if $(a, -a) \not\prec 1$. It is also clear that the operation $+$ on A^* is commutative. Verifying its associativity requires many case distinctions. To help in this we define:

$$\begin{aligned}((a, b), c) \prec 1 & :\Leftrightarrow (a, b) \prec 1 \text{ and } (a + b, c) \prec 1 \\ 1 \preceq ((a, b), c) \prec 2 & :\Leftrightarrow ((a, b) \prec 1 \text{ and } (a + b, c) \succeq 1) \\ & \text{or } ((a, b) \succeq 1 \text{ and } (a + b, c) \prec 1) \\ 2 \preceq ((a, b), c) & :\Leftrightarrow (a, b) \succeq 1 \text{ and } (a + b, c) \succeq 1.\end{aligned}$$

Likewise, we define

$$\begin{aligned}(a, (b, c)) \prec 1 & :\Leftrightarrow (b, c) \prec 1 \text{ and } (a, b + c) \prec 1 \\ 1 \preceq (a, (b, c)) \prec 2 & :\Leftrightarrow ((b, c) \prec 1 \text{ and } (a, b + c) \succeq 1) \\ & \text{or } ((b, c) \succeq 1 \text{ and } (a, b + c) \prec 1) \\ 2 \preceq (a, (b, c)) & :\Leftrightarrow (b, c) \succeq 1 \text{ and } (a, b + c) \succeq 1.\end{aligned}$$

Given a, b, c , exactly one of the three statements $((a, b), c) \prec 1$, $1 \preceq ((a, b), c) \prec 2$, $2 \preceq ((a, b), c)$ holds, and also exactly one of the three statements $(a, (b, c)) \prec 1$, $1 \preceq (a, (b, c)) \prec 2$, $2 \preceq (a, (b, c))$ holds.

Let $j, k, l \in \mathbb{Z}$; using the above notation, we have

$$((j, a) + (k, b)) + (l, c) = \begin{cases} (j + k + l, a + b + c) & \text{if } ((a, b), c) \prec 1 \\ (j + k + l + 1, a + b + c) & \text{if } 1 \preceq ((a, b), c) \prec 2 \\ (j + k + l + 2, a + b + c) & \text{if } 2 \preceq ((a, b), c) \end{cases}$$

and likewise,

$$(j, a) + ((k, b)) + (l, c) = \begin{cases} (j + k + l, a + b + c) & \text{if } (a, (b, c)) \prec 1 \\ (j + k + l + 1, a + b + c) & \text{if } 1 \preceq (a, (b, c)) \prec 2 \\ (j + k + l + 2, a + b + c) & \text{if } 2 \preceq (a, (b, c)) \end{cases}$$

So checking associativity of $+$ reduces to verifying the equivalences

$$\begin{aligned} ((a, b), c) \prec 1 &\Leftrightarrow (a, (b, c)) \prec 1, & 1 \preceq ((a, b), c) \prec 2 &\Leftrightarrow 1 \preceq (a, (b, c)) \prec 2, \\ 2 \preceq ((a, b), c) &\Leftrightarrow 2 \preceq (a, (b, c)). \end{aligned}$$

The first equivalence follows by making the obvious case distinctions, with the main case handled by (1) of Lemma 1.1. The third equivalence follows likewise by (2) of Lemma 1.1, and the second equivalence follows from the first and third.

We define a strict linear order on the set A^* by

$$(k, a) < (l, b) \quad :\Leftrightarrow \quad k < l \text{ or } (k = l \text{ and } a <_0 b) \text{ or } (k = l \text{ and } a = 0 \text{ and } b \neq 0).$$

Let $j, k, l \in \mathbb{Z}$, and assume that $(j, a) < (k, b)$. We claim that then

$$(j, a) + (l, c) < (k, b) + (l, c).$$

If $j + 1 < k$, then $j + l + 1 < k + l$, and so our claim holds. Other cases split into various subcases that can be handled using the observations(i)–(v). We only indicate the main points to be verified.

Suppose $j + 1 = k$. Then a tedious checking of cases shows that the claim holds.

Suppose $j = k$ and $a <_0 b$. If $(b, c) \prec 1$, then $(a, c) \prec 1$, so $(j, a) + (l, c) = (j + l, a + c)$, $(k, b) + (l, c) = (k + l, b + c)$, and a tedious checking of cases gives $\mathcal{O}(0, a + c, b + c)$, and our claim holds. If $(a, c) \prec 1$ and $(b, c) \succeq 1$, then $(j, a) + (l, c) = (j + l, a + c)$, $(k, b) + (l, c) = (k + l + 1, b + c)$, so the claim holds. Finally, if $(a, c) \succeq 1$ and $(b, c) \succeq 1$, then $(j, a) + (l, c) = (j + l + 1, a + c)$, $(k, b) + (l, c) = (k + l + 1, b + c)$, and one can check that $a + c <_0 b + c$, so the claim holds.

It is also easy to show that the claim holds when $j = k$ and $a = 0$, $b \neq 0$. Thus A^* is an ordered abelian group with the ordering defined above.

Let $G = A^*$ and take $(1, 0) \in G$ as its distinguished element $1 > 0$. Then

$$\{x \in G : 0 \leq x < 1\} = \{(0, a) : a \in A\},$$

and we have an isomorphism $A \rightarrow G_{\text{mod } 1}$ of oriented abelian groups given by $a \mapsto (0, a)$. This makes results from the beginning of this section available. When convenient we identify A with the oriented abelian group $G_{\text{mod } 1}$ via the isomorphism above, and \mathbb{Z} with the ordered subgroup $\mathbb{Z} \cdot 1$ of G via $k \mapsto (k, 0) = k \cdot 1$.

Lemma 1.2. *For each $n > 0$ we have $|A^*/nA^*| = |\mathbb{Z}/\mathbb{Z} \cap nA^*| \cdot |A/nA|$.*

Proof. The surjective group morphism $A^* \rightarrow A$ taking (k, a) to a has kernel \mathbb{Z} . For $n > 0$, the induced map $A^*/nA^* \rightarrow A/nA$ has kernel isomorphic to $\mathbb{Z}/\mathbb{Z} \cap nA^*$. The lemma follows. \square

We express the index $|\mathbb{Z}/\mathbb{Z} \cap nA^*|$ in the lemma above in terms of A alone without mentioning A^* , when n is a prime power. So let p be a prime number and let e range over \mathbb{N} . We have

$$(*) \quad \mathbb{Z} \cap p^e A^* = \mathbb{Z} \text{ iff } 1 \in p^e A^* \text{ iff } |A[p^e]| = p^e.$$

Also $A[p^e] \subsetneq A[p^{e+1}]$ if and only if $|A[p^{e+1}]| = p^{e+1}$. So either $|A[p^e]| = p^e$ for all e , and then we set $e(A, p) := \infty$, or there is a largest e such that $|A[p^e]| = p^e$,

in which case we define $e(A, p)$ to be this largest e . So $e(A, p) \in \mathbb{N} \cup \{\infty\}$. Let $e > e(A, p)$. Then it is easy to see that $|A[p^e]| = p^{e(A, p)}$. Also $p^{e-e(A, p)}\mathbb{Z} \subseteq \mathbb{Z} \cap p^e A^*$ since there is $a^* \in A^*$ such that $p^{e(A, p)} a^* = 1$. Next we prove the other inclusion.

Lemma 1.3. *Let p be a prime number and $e > e(A, p)$. Then*

$$\mathbb{Z} \cap p^e A^* \subseteq p^{e-e(A, p)}\mathbb{Z}.$$

Proof. We proceed by induction on $e - e(A, p)$. If $e = e(A, p) + 1$, then $\mathbb{Z} \cap p^{e(A, p)+1} A^* \subseteq \mathbb{Z}$. Hence $\mathbb{Z} \cap p^e A^* \subseteq p\mathbb{Z}$. So let $e - e(A, p) > 1$, and let $p^e a^* \in \mathbb{Z}$ with $a^* \in A^*$. By induction hypothesis $\mathbb{Z} \cap p^{e-1} A^* \subseteq p^{e-1-e(A, p)}\mathbb{Z}$. Hence $p^e a^* \in p^{e-1-e(A, p)}\mathbb{Z}$. So $p^{e(A, p)+1} a^* \in \mathbb{Z}$, and by using the induction hypothesis once again, we get $p^{e(A, p)+1} a^* \in p\mathbb{Z}$. Thus

$$p^e a^* = p^{e-e(A, p)-1} p^{e(A, p)+1} a^* \in p^{e-e(A, p)}\mathbb{Z},$$

finishing the proof. \square

Using also Lemma 1.2 we have the following consequence.

Corollary 1.4. *Let p be a prime number, $e \in \mathbb{N}$. Then*

- (1) $\mathbb{Z} \cap p^e A^* = \mathbb{Z}$ and $|A^*/p^e A^*| = |A/p^e A|$ for $e \leq e(A, p)$.
- (2) $\mathbb{Z} \cap p^e A^* = p^{e-e(A, p)}\mathbb{Z}$ and $|A^*/p^e A^*| = p^{e-e(A, p)}|A/p^e A|$ for $e > e(A, p)$.

We want to define a notion of ‘regularly dense’ for oriented abelian groups, in analogy with the corresponding notion for ordered abelian groups. First we prove a general lemma on ordered abelian groups.

Lemma 1.5. *Let G be an ordered abelian group with a distinguished element $1 > 0$ such that $\mathbb{Z} \cdot 1$ is cofinal in G , and the interval $(0, 1) \subseteq G$ is a nonempty dense linearly ordered set without endpoints. Suppose S is a subgroup of G such that $S \cap (0, 1)$ is dense in $(0, 1)$. Then S is dense in G .*

Proof. Note: we do not assume that $1 \in S$. By induction on m , we show that for every $g, h \in G$ with $0 < g < h < 1$, the interval $(m + g, m + h)$ contains an element of S . The case $m = 0$ is just the assumption that $S \cap (0, 1)$ is dense in $(0, 1)$. Assume the statement holds for a certain m , and take $0 < g < h < 1$. We need to find $x \in S$ such that $m + 1 + g < x < m + 1 + h$. Using the induction hypothesis, take $s \in S \cap (m + h, m + 1)$. It suffices to find $y \in S$ such that $m + 1 + h < y + s < m + 1 + h$, that is, $m + 1 + g - s < y < m + 1 + h - 1$. There is such a y since $0 < m + 1 + g - s < m + 1 + h - s < 1$. \square

We can now prove the following lemma, which says that a certain condition on A is equivalent to A^* being regularly dense as an ordered abelian group.

Lemma 1.6. *The following conditions are equivalent:*

- (1) A^* is regularly dense as an ordered abelian group,
- (2) $|A| > 2$ and for each prime number p and all $a, b \in A$ with $a <_0 b$ there is $c \in A \setminus \{0\}$ such that $ic <_0 (i + 1)c$ for $i = 1, \dots, p - 1$ and $\mathcal{O}(a, pc, b)$.

Proof. Assume (1), let p be a prime number, and let $a, b \in A$ satisfy $a <_0 b$. Put $x = (0, a)$, $y = (0, b)$, so $0 < x < y < 1$ in A^* where $0 := (0, 0)$ and $1 := (1, 0)$. Take z in A^* with $x < pz < y$. Then $0 < z < 2z < \dots < pz < 1$, so $z = (0, c)$ with $c \in A \setminus \{0\}$. One checks easily that then $c <_0 2c <_0 \dots <_0 pc$ and $\mathcal{O}(a, pc, b)$.

Now assume (2). It is clear that $A \setminus \{0\}$ is a nonempty dense linearly ordered set without endpoints. Then $(0, 1) \subseteq A^*$ is a nonempty dense linear ordering without endpoints, and for each prime number p the set $(0, 1) \cap pA^*$ is dense in $(0, 1)$. Applying the previous lemma with $G = A^*$ and $S = pA^*$, we get that A^* is regularly dense. \square

Definition 1.7. We say that the oriented abelian group A is *regularly dense*, if condition (2) of Lemma 1.6 is satisfied.

Hence A is regularly dense if and only if A^* is regularly dense as an ordered abelian group. **checked so far**

Remark. Suppose for every prime p there is nonzero $a \in A$ such that $pa = 0$. Then A is regularly dense iff for every prime number p and all $a, b \in A$ with $a <_0 b$, there is $c \in A$ such that $\mathcal{O}(a, pc, b)$.

We say A is *dense* if it is nontrivial and $<_0$ is a dense linear order without endpoints on $A \setminus \{0\}$. It is easy to see that A is dense iff A^* is dense as an ordered abelian group.

Our main interest is in the dense subgroups of \mathbb{S} . Note that \mathbb{S}^* and \mathbb{R} are isomorphic as ordered abelian groups. Thus the dense subgroups of \mathbb{S} are exactly the regularly dense subgroups. Therefore from now on we restrict our attention to regularly dense oriented abelian groups.

Let \mathcal{L} be the language of abelian groups augmented by a ternary relation symbol. Also let \mathcal{L}_o be the language of ordered abelian groups, and $\mathcal{L}_o(1)$ the language extending \mathcal{L}_o by a constant symbol 1. When A is an oriented abelian group, we construe it as an \mathcal{L} -structure by interpreting the ternary relation symbol as \mathcal{O} , and construe A^* as an $\mathcal{L}_o(1)$ -structure by interpreting 1 as $(1, 0) \in A^*$. Note that then the identification $a \mapsto (0, a) : A \rightarrow A^*$ defines the structure A in the structure A^* .

Below elementary equivalences of oriented abelian groups are in the language \mathcal{L} , and those of ordered abelian groups are in the language $\mathcal{L}_o(1)$, unless stated otherwise.

Corollary 1.8. *Let A, B be regularly dense oriented abelian groups. Then $A \equiv B$ if and only if $A^* \equiv B^*$.*

Proof. The implication $A^* \equiv B^* \Rightarrow A \equiv B$ follows by defining A and B in A^* and B^* as above.

Now let $A \equiv B$. It is shown in [2] that $A^* \equiv B^*$ as \mathcal{L}_o -structures if and only if $|A^*/pA^*| = |B^*/pB^*|$ for every prime number p . Thus by Corollary 1.4, we get $A^* \equiv B^*$ as \mathcal{L}_o -structures. To show $A^* \equiv B^*$, it remains to prove that $(1, 0)$ has the same \mathcal{L}_o -type (over \emptyset) in A^* and B^* . By the quantifier elimination result, Lemma 7.7 from [1], for regularly dense ordered abelian group it is enough to show that

$$1 \in nA \iff 1 \in nB,$$

for every $n > 0$. This follows from the fact that $|A[n]| = |B[n]|$ for every $n > 0$. \square

From [2] we have a complete list of invariants for the elementary theory of a regularly dense ordered abelian group, and together with Corollary 1.4 and the proof of Corollary 1.8 this gives a complete double list of invariants for the elementary theory of a regularly dense oriented abelian group:

Corollary 1.9. *Let A and B be regularly dense oriented abelian groups. Then $A \equiv B$ if and only if for every prime number p we have $[p]A = [p]B$ and $e(A, p) = e(B, p)$.*

For every prime p , take two elements d_p, e_p of $\mathbb{N} \cup \{\infty\}$. We construct a regularly dense oriented abelian group A such that $[p]A = d_p$ and $e(A, p) = e_p$ for every p . Indeed for we construct a dense subgroup G of the additive group \mathbb{R} such that $[p]G = d_p$, $1 \in p^{e_p}G \setminus p^{e_p+1}G$ for $e_p \neq \infty$ and $1 \in p^eG$ for all e for $e_p = \infty$. Our desired A is then $G_{\text{mod}1}$.

Let $G' := \bigoplus_p \mathbb{Z}_{(p)}^{d_p}$, where $\mathbb{Z}_{(p)}$ is the additive group of localization of \mathbb{Z} at p . Then we can embed G' into \mathbb{R} in a way that the image of G' under this embedding contains $1 \in \mathbb{R}$ and not $1/p \in \mathbb{R}$ for every p . Let G'' denote the image of G' , and let $\mathbb{Z}(p)$ denote $\frac{1}{p^{e_p}}\mathbb{Z}$ if $e_p \neq \infty$, and $\bigcup_e \frac{1}{p^e}\mathbb{Z}$ if $e_p = \infty$. Then let $G := G'' + \bigoplus_p \mathbb{Z}(p)$. This G satisfies the desired properties.

Let A be an oriented abelian group with a subgroup A' such that $A_{\text{tor}} = A'_{\text{tor}}$, and let $a \in A$. Then we define

$$A'\langle a \rangle_A := \{b \in A : nb = a' + ka \text{ for some } n > 0, a' \in A' \text{ and } k \in \mathbb{Z}\}.$$

Note that $A'\langle a \rangle_A$ is the smallest pure subgroup of A containing both A' and a .

Next we obtain an extension procedure for regularly dense oriented abelian groups, using the analogous procedure in [2] for regularly dense ordered abelian groups.

Let A and B be regularly dense oriented abelian groups with $[p]A = [p]B$ for every prime p . Let $f : A' \rightarrow B'$ be an oriented abelian group isomorphism between pure subgroups A' and B' of A and B respectively such that $A'_{\text{tor}} = A_{\text{tor}}$ and $B'_{\text{tor}} = B_{\text{tor}}$. Suppose also that B is κ -saturated, where $\kappa > |B'|$ is an uncountable cardinal. This gives an ordered abelian group isomorphism $f^* : (A')^* \rightarrow (B')^*$ taking (l, a') to $(l, f(a'))$ for all $(l, a') \in (A')^*$.

Let $a \in A \setminus A'$. **Please explicitly state as a claim what it is that you are going to prove.** Take a κ -saturated elementary extension C^* of B^* , and consider $a^* := (0, a) \in A^*$. Then by the extension procedure mentioned in [2], there is $c^* \in C^*$ such that for all $a' \in (A')^*$, $k \in \mathbb{Z}$, $n > 0$:

- (1) $a' < na^* \iff f^*(a') < nc^*$;
- (2) $a' + ka^* \in nA^* \iff f^*(a') + kc^* \in nC^*$,

In particular c^* is of the form $(0, c)$, where c is contained in the oriented group extension $C := (C^*)_{\text{mod}1}$ of B . By κ -saturation of B , there is $b \in B$ such that $\text{tp}_C(b|B') = \text{tp}_C(c|B')$. Thus for all $a' \in (A')^*$, $k \in \mathbb{Z}$, $n > 0$:

- (1) $a' < na^* \iff f^*(a') < nb^*$;
- (2) $a' + ka^* \in nA^* \iff f^*(a') + kb^* \in nB^*$,

where $b^* := (0, b)$. For this b^* we can extend f^* to an ordered group isomorphism $(A')^*\langle a^* \rangle_{A^*} \rightarrow (B')^*\langle b^* \rangle_{B^*}$ sending a^* to b^* . This induces an oriented abelian group isomorphism $A'' \rightarrow B''$ extending f , where $A'' := ((A')^*\langle a^* \rangle_{A^*})_{\text{mod}1} \subseteq A$ and $B'' := ((B')^*\langle b^* \rangle_{B^*})_{\text{mod}1} \subseteq B$. It is easy to see that A'' is $A'\langle a \rangle_A$ and, and similarly B'' is $B'\langle b \rangle_B$.

2. THE FIELD OF REAL NUMBERS WITH A SUBGROUP OF THE CIRCLE GROUP

Fix a dense subgroup Γ of the oriented abelian group $\mathbb{S} \subseteq \mathbb{C}^\times$ with the Mann property. We identify \mathbb{C} with \mathbb{R}^2 in the usual way, via

$$z = a + bi \mapsto (a, b), \quad (a, b \in \mathbb{R}).$$

This makes Γ a subset of \mathbb{R}^2 . For an element $\alpha = (\alpha_1, \alpha_2)$ of \mathbb{C} , we let $\operatorname{Re}(\alpha) := \alpha_1$ and $\operatorname{Im}(\alpha) := \alpha_2$, so we have subsets $\operatorname{Re}(\Gamma)$ and $\operatorname{Im}(\Gamma)$ of \mathbb{R} .

The *orientation axioms* of Γ are the following: given $\gamma_1, \dots, \gamma_n \in \Gamma$ and a polynomial $Q(X_1, \dots, X_n) \in \mathbb{Z}[X_1, \dots, X_n]$, the orientation axiom for $\vec{\gamma}, Q$ is

$$Q(\operatorname{Re}(\gamma_1), \dots, \operatorname{Re}(\gamma_n)) > 0,$$

if this inequality holds in \mathbb{R} , and it is

$$Q(\operatorname{Re}(\gamma_1), \dots, \operatorname{Re}(\gamma_n)) \leq 0$$

otherwise.

Let $\mathcal{L}_{o,P}(\Gamma)$ be the language of ordered rings augmented by a binary relation symbol P and by a name γ for each $\gamma \in \Gamma$.

For every linear equation

$$a_1x_1 + \dots + a_nx_n = 1 \quad (n \geq 2, a_1, \dots, a_n \in \mathbb{Q}^\times)$$

take a finite list of its nondegenerate solutions in Γ ,

$$\gamma_1 = (\gamma_{11}, \dots, \gamma_{1n}), \dots, \gamma_k = (\gamma_{k1}, \dots, \gamma_{kn}),$$

and let the corresponding *Mann axiom* of Γ be the sentence

$$\forall y \forall z \left[\left(P(y, z) \wedge \sum_{i=1}^n a_i y_i = 1 \wedge \sum_{i=1}^n a_i z_i = 0 \wedge \bigwedge_I \left(\sum_{i \in I} a_i y_i \neq 0 \vee \sum_{i \in I} a_i z_i \neq 0 \right) \right) \longrightarrow \bigvee_{j=1}^k (y, z) = \gamma_j \right]$$

in the language $\mathcal{L}_o(P, \Gamma)$, where $y = (y_1, \dots, y_n)$ and $z = (z_1, \dots, z_n)$ are tuples of distinct variables, $P(y, z)$ abbreviates $P(y_1, z_1) \wedge \dots \wedge P(y_n, z_n)$, the conjunction \bigwedge_I is over all nonempty proper $I \subseteq \{1, \dots, n\}$, “ $\sum_{i=1}^n a_i y_i = 1$ ”, “ $\sum_{i=1}^n a_i z_i = 0$ ”, “ $\sum_{i \in I} a_i y_i \neq 0$ ”, and “ $\sum_{i \in I} a_i z_i \neq 0$ ” represent certain obvious formulas in the language of rings, and $(y, z) = \gamma_j$ abbreviates $y_1 = \operatorname{Re}(\gamma_{j1}) \wedge \dots \wedge y_n = \operatorname{Re}(\gamma_{jn}) \wedge z_1 = \operatorname{Im}(\gamma_{j1}) \wedge \dots \wedge z_n = \operatorname{Im}(\gamma_{jn})$.

Let $\operatorname{RCF}(\Gamma)$ be the $\mathcal{L}_o(P, \Gamma)$ -theory whose models are of the form $(K, G, (\gamma')_{\gamma \in \Gamma})$ such that

- (1) K is a real closed ordered field,
- (2) G is a dense subgroup of $\mathbb{S}(K) \subseteq K^2$,
- (3) $\gamma \mapsto \gamma' : \Gamma \rightarrow G$ is a group morphism,
- (4) $(K, (\gamma')_{\gamma \in \Gamma})$ satisfies the orientation axioms for Γ ,
- (5) $(K, G, (\gamma')_{\gamma \in \Gamma})$ satisfies the Mann axioms for Γ ,
- (6) $G_{\operatorname{tor}} = \Gamma_{\operatorname{tor}}$.

Whenever $(K, G, (\gamma')_{\gamma \in \Gamma})$ is a model of $\operatorname{RCF}(\Gamma)$, there is an isomorphic copy of the abelian group Γ in G . We identify this copy of Γ with itself, and hence a model of $\operatorname{RCF}(\Gamma)$ will be denoted as $(K, G, (\gamma)_{\gamma \in \Gamma})$ or simply $(K, G, (\gamma))$. Next is our main result characterizing the models of $\operatorname{RCF}(\Gamma)$ up to elementary equivalence.

Theorem 2.1. *Let $(K, G, (\gamma))$ and $(L, H, (\gamma))$ be two models of $\text{RCF}(\Gamma)$. Then $(K, G, (\gamma)) \equiv (L, H, (\gamma))$ if and only if $[p]G = [p]H$ for all p , and for all $\gamma \in \Gamma$, and $n > 0$,*

$$\gamma \text{ is an } n^{\text{th}} \text{ power in } G \Leftrightarrow \gamma \text{ is an } n^{\text{th}} \text{ power in } H.$$

Proof. We only prove the backward direction. So let $(K, G, (\gamma))$ and $(L, H, (\gamma))$ be such that $[p]G = [p]H$ for all p , and for all $\gamma \in \Gamma$, and $n > 0$,

$$\gamma \text{ is an } n^{\text{th}} \text{ power in } G \Leftrightarrow \gamma \text{ is an } n^{\text{th}} \text{ power in } H.$$

We need to prove that $(K, G, (\gamma)) \equiv (L, H, (\gamma))$. We do this by constructing a nonempty back-and-forth system between $(K, G, (\gamma))$ and $(L, H, (\gamma))$. We assume they are κ -saturated with κ an uncountable cardinal.

Let $\text{Sub}(K, G)$ be the collection of $\mathcal{L}_o(P)$ -structures (K', G') such that K' is a real closed ordered subfield of K of cardinality less than κ , G' is a pure subgroup of G containing Γ , and $K'(i)$ and $\mathbb{Q}(G)$ are free over $\mathbb{Q}(G')$ (as subfields of $K(i)$). Using Lemma 5.13 from [1], we get that if $(K', G') \in \text{Sub}(K, G)$, then (K', G') is a substructure of (K, G) , and $\mathbb{Q}(G)|\mathbb{Q}(G')$ is regular. Hence $K'(i)$ and $\mathbb{Q}(G)$ are linearly disjoint over $\mathbb{Q}(G')$. Define $\text{Sub}(L, H)$ likewise, and let \mathcal{I} be the collection of isomorphisms between members of $\text{Sub}(K, G)$ and $\text{Sub}(L, H)$ fixing Γ pointwise. We show that \mathcal{I} is a non-empty back-and-forth system. For non-emptiness, let

$$G' := \{g \in G : g^n \in \Gamma \text{ for some } n > 0\}, \quad K' := \mathbb{Q}(\text{Re}(\Gamma))^{\text{rc}} \subseteq K,$$

$$H' := \{h \in H : h^n \in \Gamma \text{ for some } n > 0\}, \quad L' := \mathbb{Q}(\text{Re}(\Gamma))^{\text{rc}} \subseteq L.$$

It is clear that $(K', G') \in \text{Sub}(K, G)$ and $(L', H') \in \text{Sub}(L, H)$ and by the orientation axioms there is an ordered field isomorphism $K' \rightarrow L'$ extending the identity map on Γ , which in turn is an isomorphism between (K', G') and (L', H') belonging to \mathcal{I} .

Now let $\iota : (K', G') \rightarrow (L', H')$ be in \mathcal{I} , and $\alpha \in K \setminus K'$.

Case 1. Let $\alpha \in \text{Re}(G)$. Let $\alpha' \in K$ such that $\alpha + i\alpha' \in G$. Then by using the previous remark on the regularly dense oriented abelian groups, there is an oriented abelian group isomorphism $G'\langle\alpha\rangle_G \rightarrow H'\langle\beta\rangle_H$ extending $\iota|_{G'}$. In particular, β realizes the cut over $\text{Re}(H')$ corresponding to the cut of α over $\text{Re}(G')$. Moreover we can arrange β to realize the cut over L' corresponding to the cut of α over K' . Hence $K'(\alpha)^{\text{rc}}$ and $L'(\beta)^{\text{rc}}$ are isomorphic as ordered fields through a map extending ι , sending α to β . This is an isomorphism of $\mathcal{L}_o(P)$ -structures $(K'(\alpha)^{\text{rc}}, G'')$ and $(L'(\beta)^{\text{rc}}, H'')$. We need to check that $K'(\alpha, i)^{\text{rc}}$ and $\mathbb{Q}(G)$ are free over $\mathbb{Q}(G'')$. It follows by usual arguments. **(This also covers the case $\alpha \in \text{Im}(G)$)**

Case 2. If $\alpha \in K'(\text{Re}(G) \cup \text{Im}(G))^{\text{rc}}$, then we apply the previous case several times.

Case 3. Now let $\alpha \notin K'(\text{Re}(G) \cup \text{Im}(G))^{\text{rc}}$. Then take $\beta \in L$ such that $\beta \notin L'(\text{Re}(H) \cup \text{Im}(H))^{\text{rc}}$ realizing the type over L' corresponding to the type of α over K' . So $K'(\alpha)^{\text{rc}}$ and $L'(\beta)^{\text{rc}}$ are isomorphic as ordered fields. In fact, it is an $\mathcal{L}_o(P)$ -isomorphism extending ι , finishing the proof. \square

REFERENCES

- [1] L. VAN DEN DRIES, A. GÜNAYDIN, The fields of real and complex numbers with a small multiplicative group, *Proceedings of London Mathematical Society*, **93**, (2006), pp. 43–81.
- [2] A. ROBINSON, E. ZAKON, Elementary properties of ordered abelian groups, *Trans. AMS* **96** (1960), 222–236.