On Decompositions of Infinite Groups

A. Horn, D. Simms, et al.

18th February 2020

A *decomposition* of a group G is a pair of groups A, B such that neither of A, B is trivial, and $G \cong A \times B$.

1 $(\mathbb{Z}, +)$

$\mathbb{Z}$ is not decomposable. Suppose we had $\mathbb{Z} \cong G \times H$ for nontrivial G, H. Then since the subgroups of $\mathbb{Z}$ are of the form $k\mathbb{Z}$, we have $G \cong n\mathbb{Z}$ and $H \cong m\mathbb{Z}$ for some n, m.

Since $k\mathbb{Z} \cong \mathbb{Z}$, this implies $\mathbb{Z} \cong G \times H \cong \mathbb{Z} \times \mathbb{Z}$. This is not possible since $\mathbb{Z}$ has $2\mathbb{Z}$ as its only subgroup of index two, but $\mathbb{Z} \times \mathbb{Z}$ has two subgroups of index two: $2\mathbb{Z} \times \mathbb{Z}$ and $\mathbb{Z} \times 2\mathbb{Z}$.

Hence $\mathbb{Z}$ is not decomposable.

2 $(\mathbb{Q}, +)$

Suppose we had $\mathbb{Q} \cong G \times H$ for some nontrivial groups G, H. Both G and H have a subgroup isomorphic to $\mathbb{Z}$, since each contains a nonzero element, and each element of $\mathbb{Q}$ has infinite order.

Hence $\mathbb{Q}$ has a subgroup isomorphic to $\mathbb{Z} \times \mathbb{Z}$. Suppose $a/b, c/d \in \mathbb{Q}$ generate the corresponding subgroups isomorphic to $\mathbb{Z} \times 0\mathbb{Z}$ and $0\mathbb{Z} \times \mathbb{Z}$ respectively, so $\mathbb{Z} \times \mathbb{Z} \cong \langle a/b \rangle \times \langle c/d \rangle$. Without loss of generality, both generators are positive.

Then, however, $bc(a/b) = ad(c/d)$. This implies that in the subgroup isomorphic to $\mathbb{Z} \times \mathbb{Z}$, we have $(bc, 0) = (0, ad)$, which is a contradiction as neither of these terms can be 0 if $a/b, c/d$ are to be generators.

So also $\mathbb{Q}$ is not decomposable.

3 $(\mathbb{R}, +)$

Let $\mathcal{H}$ be a Hamel basis for $\mathbb{R}$ as a vector space over $\mathbb{Q}$. Then any partition of $\mathcal{H}$ as a disjoint union $\mathcal{H} = \mathcal{H}_1 \cup \mathcal{H}_2$ gives rise to two subgroups $G_1 = \operatorname{span} \mathcal{H}_1, G_2 = \operatorname{span} \mathcal{H}_2 \leq \mathbb{R}$. These are subgroups since they are subspaces by definition.

Now we can apply the Direct Product Theorem, since

(i) By linear independence, if $x_1 \in G_1, x_2 \in G_2$ with $x_1 = x_2$, then $x_1 = x_2 = 0$, so $G_1 \cap G_2$ is precisely $\{0\}$.

(ii) $\mathbb{R}$ is abelian, so trivially, $x_1 + x_2 = x_2 + x_2 \,\forall\, x_1 \in G_1, x_2 \in G_2$.

(iii) Each $x \in \mathbb{R}$ can be written as a linear combination of elements of $\mathcal{H}$, by definition. Then simply splitting this linear combination into linear combinations of the elements in $\mathcal{H}_1$ and $\mathcal{H}_2$, we get $x_1 \in G_1, x_2 \in G_2$ with $x_1 + x_2 = x$.

So $\mathbb{R} \cong G_1 \times G_2$ for any such choice.

To be explicit, a possible choice here might be $\mathcal{H}_1 = \mathcal{H} \cap \mathbb{Q}$, $\mathcal{H}_2 = \mathcal{H} \setminus \mathbb{Q}$, or possibly replacing $\mathbb{Q}$ with some more imaginative subsets of $\mathbb{R}$. Here, we know $|\mathcal{H}_1| = 1$ precisely, as there must be a rational in $\mathcal{H}$, so neither of G_1, G_2 is trivial.

Note that really this implies that anything that is the additive group of a vector space over *some* field, of dimension at least two, is decomposable (with a generous sprinkling of the axiom of choice).

4 $(\mathbb{C}, +)$

$\mathbb{C}$ is quite straightforwardly isomorphic to $\mathbb{R} \times \mathbb{R}$ via $z \mapsto (\operatorname{Re} z, \operatorname{Im} z)$.

5 $(\mathbb{Q}^\times, \cdot)$

This is isomorphic to $C_2 \times (\mathbb{Q}^+, \cdot)$ via $x \mapsto (\operatorname{sgn} x, |x|)$ (where $\operatorname{sgn} x \coloneqq x/|x|$).

6 $(\mathbb{R}^\times, \cdot)$

This is isomorphic to $C_2 \times (\mathbb{R}^+, \cdot)$ via $x \mapsto (\operatorname{sgn} x, |x|)$.

7 $(\mathbb{C}^\times, \cdot)$

This is isomorphic to $S^1 \times (\mathbb{R}^+, \cdot)$ via $re^{i\theta} \mapsto (e^{i\theta}, r)$.

8 $(\mathbb{Q}^+, \cdot)$

Consider the following two subgroups:

$$G = \{2^n : n \in \mathbb{Z}\} \cong \mathbb{Z}$$
$$H = \left\{\frac{a}{b} : a, b \in \mathbb{Z}, 2 \nmid a, b\right\}$$

The fact that they are subgroups follows quite quickly from the efficient subgroup criterion.

Now we can apply the Direct Product Theorem to these, since

(i) Let 2^n be an element of G, and a/b be an element of H. Suppose 2^n is an integer.

If $a/b = 2^n$, then $a = 2^n b$, so $2^n \mid a$. Hence $2^n = 1$.

Suppose instead 2^n is fractional. Then, we get $2^{-n} a = b$, so $2^{-n} \mid b$, which is not possible.

So $G \cap H = 1$.

(ii) All elements of G and H commute trivially since $\mathbb{Q}^+$ is abelian.

(iii) If $p/q \in \mathbb{Q}$ is a general element with p, q in lowest terms, then either only p has a largest factor of 2^n for some n, so $p/q = 2^n \cdot (p/2^n)/q$, or q has a largest factor of 2^n for some n, so $p/q = 2^{-n} \cdot p/(q/2^n)$, or neither does, and $p/q = 1 \cdot p/q$.

In each case, we have written $p/q = gh$ for some $g \in G, h \in H$.

So $(\mathbb{Q}^+, \cdot) \cong G \times H \cong \mathbb{Z} \times H$ and $\mathbb{Q}$ is decomposable. This process can be repeated with the next prime number (3, probably) to decompose H as $\mathbb{Z} \times H'$, and so on.

9 $(\mathbb{R}^+, \cdot)$

This is isomorphic to $(\mathbb{R}, +)$ via $x \mapsto \log x$, so we can reuse the previous construction.

10 $S^1 \cong \mathbb{R}/\mathbb{Z}$

11 $\mathbb{Q}/\mathbb{Z}$

Let

$$G = \{a/2^n : a \in \mathbb{Z}, n \in \mathbb{Z}_{\geq 0}\}$$
$$H = \{a/m : a \in \mathbb{Z}, m \in \mathbb{Z}_{\geq 0}, 2 \nmid m\}$$

These are subgroups of $\mathbb{Q}$ containing $\mathbb{Z}$, so $G/\mathbb{Z}, H/\mathbb{Z} \leq \mathbb{Q}/\mathbb{Z}$.

We can apply the Direct Product Theorem, since

(i) $G \cap H$ is precisely the integers, since the only power of two with no factor of two is 1. But the quotient map $\mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$ precisely takes all the integers to the identity coset, so $G/\mathbb{Z} \cap H/\mathbb{Z}$ is trivial.

(ii) $\mathbb{Q}/\mathbb{Z}$ is abelian, so trivially, all elements of $G/\mathbb{Z}$ and $H/\mathbb{Z}$ commute.

(iii) In $\mathbb{Q}$, let $b/(2^n m)$ be a general element, with $2 \nmid m$. Now by Bézout's Theorem, the diophantine equation $mx + 2^n y = 1$ has a solution for $x, y \in \mathbb{Z}$, since $\gcd(2^n, m) = 1$. But this precisely means that $1/(2^n m) = x/2^n + y/m$, a sum of elements of G, H.

Then by well-definedness of the quotient map, we immediately get that any given coset $b/(2^n m) + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$ is just $(x/2^n + \mathbb{Z}) + (y/m + \mathbb{Z})$.

Hence $\mathbb{Q}/\mathbb{Z} \cong G/\mathbb{Z} \times H/\mathbb{Z}$, which is a nontrivial decomposition.

12 $\left(\{a/2^n : a \in \mathbb{Z}, n \in \mathbb{Z}_{\geq 0}\}, +\right) \cong \bigcup_{n \in \mathbb{N}} 2^{-n}\mathbb{Z}$

13 $\left(\{a/m : a \in \mathbb{Z}, n \in \mathbb{Z}_{\geq 0}, 2 \nmid m\}, +\right)$

14 $\left(\{a/2^n : a \in \mathbb{Z}, n \in \mathbb{Z}_{\geq 0}\}, +\right)/\mathbb{Z}$

Call this group G for convenience. Also we refer to elements of G as their unique coset representatives in $[0, 1)$. Any infinite subgroup $H \leq G$ must be G, since in order to be infinite, H must contain elements that have arbitrary large denominators written in lowest terms, since there are finitely many (2^n) elements that can be written with any denominator 2^n.

But if we have $x/2^n$ where $2 \nmid x$, then $xy \equiv 1 \pmod{2^n}$ is solvable since $x, 2^n$ are coprime. So $\langle x/2^n \rangle \leq H$ contains $1/2^n$ and hence also $a/2^n$ for all a, which gives all elements of denominator at most 2^n. Since the denominators found in H are arbitrarily large, H contains all elements, and $H = G$.

But if $G \cong A \times B$ nontrivially, then A, B are both isomorphic to proper subgroups of G (since there is a non-identity $b \in B$ implying $(e, b) \notin A \times \{e\}$ and vice versa), so A, B are both finite.

But then $A \times B$ is finite with order $|A||B|$, which contradicts the fact that G is infinite (eg since G contains $1/2^n$ for all $n \in \mathbb{Z}_{\geq 0}$).

So G is not decomposable.

This argument works for the family of similar groups given by fractions with denominators power of any prime, mod $\mathbb{Z}$.

15 $\mathbb{R}/\mathbb{Q}$

Tentatively, this is a quotient space of $\mathbb{R}$ over $\mathbb{Q}$, so by the same argument as for $\mathbb{R}$, is decomposable.

$\mathbb{Q}$ is a subspace of $\mathbb{R}$ over $\mathbb{Q}$ as it is just the span of any (nonzero) rational number (eg 1). Particularly, once $\mathbb{R}$ is equipped with a Hamel basis $\mathcal{H}$, $\mathbb{Q}$ is the kernel of the vectors space homomorphism $\mathbb{R} \to \mathbb{R}$ given by "ignore the rational term in the linear combination of basis vectors", which has image isomorphic to $\mathbb{R}/\mathbb{Q}$.