JÓNSSON ALGEBRAS

EXAMPLES AND SOME NEAT RESULTS

James Holland

Start Date: 2018-03-02
End Date: 2018-04-12
Revised: 2019-08-18

Contents

i. *Jónsson Algebras in Logic*

The recently deceased Bjarni Jónsson was an Icelandic algebraist and logician. As such, his work borders the two fields. Of the many concepts named after him, Jónsson algebras themselves are somewhat more general than what is presented here due to a broader use of the work "algebra" by logicians. In logic, an algebra is any class equipped with a countable number of operations. In this sense, groups, rings, etc. are all algebras. In the sense of the majority of algebra, however, these are not all algebras, and so the terminology used here reflects this restricted usage. Instead of "Jónsson algebra" as in the literature, "Jónsson structure" will be used to avoid confusion.

In logic, "Jónsson" is seen more as a property of cardinals than of structures. That is to say that what is important is whether an (infinite) cardinal admits a Jónsson structure rather than what structures are Jónsson. This combinatorial property poses interesting questions for infinitary combinatorics. In particular, the question whether $\aleph_\omega$ admits a Jónsson structure is still open, although the answer is "yes" for all cardinals below $\aleph_\omega$[2]. Really, however, the open question is whether it's independent that $\aleph_\omega$ admits a Jónsson structure. The answer to whether cardinals admit Jónsson structures can be tied to so called "large cardinal" axioms, which are independent of the standard basis of mathematics ZFC [2]. Logic, however, is more interested in the non-existence of Jónsson structures on cardinals. In fact, a cardinal is called Jónsson if there are no Jónsson structures on it [1]! One thing to be gleamed from this is that we can't prove there are no Jónsson structures on any given cardinal.

Now the usage of "Jónsson" used here will actually be slightly more general than in logic. In some sense, there is some cheating going on with the notion of "structure" as opposed to "algebra" that forbids taking trivial examples of Jónsson structures on $\aleph_\omega$ for example. In particular, structures like vector spaces aren't necessarily "algebras" in the logical sense. When we've fixed a field $\mathbb{F}$, we're adding unary operations corresponding to scalar multiplication: $v \mapsto f \cdot v$ for each $f \in \mathbb{F}$. If $\mathbb{F}$ is uncountable, then the structure won't be an "algebra" in the sense of logic, because the logic usage requires at most countably many operations.

This does not mean that Jónsson structures are worthless for the study of algebra. The concept of being Jónsson can be separated from the stricter sense used in logic. In some sense, the property of being Jónsson is a weakening of certain kinds of simplicity, like for modules. As such, the existence and construction of simple structures is even harder than that of Jónsson ones. But this weakening can still yield fruitful results, as the search for Jónsson structures actually motivated the discovery of a simple group on $\aleph_1$ [5]. And of course, as an algebraist himself, Bjarni thought them worthy enough of algebraic study.

Section 1. *Introduction and Examples*

Recall that a module is called "simple" iff it has no non-trivial submodules. The property of being Jónsson is related to this kind of simplicity. We allow substructures, but they must be smaller. Denote cardinality with $|\cdot|$ so that $|\mathbb{N}| = \aleph_0$. An overview of some basic cardinal arithmetic is given in Appendix A.

1 • 1. Definition

A structure W is called Jónsson iff every substructure $V < W$ satisfies $|V| < |W|$.

Note that this definition is really a definition scheme. For different notions of structure, there are different notions of being Jónsson. For example, a group is Jónsson iff every proper subgroup has smaller cardinality. A vector space or module is Jónsson iff every proper submodule is smaller. A field is Jónsson iff every proper subfield is smaller, and so on and so forth. One immediate result of this is that every finite structure is Jónsson. This is because any proper subset of a finite set is smaller in cardinality, demonstrating just how weird finite numbers are.

Now let's start off with some examples of *infinite* Jónsson structures. Our first example will be a Jónsson group. This group will be a countably infinite Jónsson group, meaning that it's an infinite group with no infinite proper subgroup. This example will come to be fairly important for the results about groups.

1 • 2. Example (1 • 2. Example 1)

Let $p \in \mathbb{N}$ be prime. Define $\mathbb{Z}(p^\infty) := \mathbb{Z}[1/p]/\mathbb{Z}$ under the operation of (modular) addition.

We will later see in Section 2 that these are the *only* infinite, abelian, Jónsson groups, meaning that all abelian, Jónsson groups are actually only countable. Note that the elements of $\mathbb{Z}(p^\infty)$ will be finite sums of the form

$$\sum_{i \le N} \frac{m_i}{p^{n_i}},$$

for $m_i \in \mathbb{Z}$ and $n_i \in \mathbb{N}$. But we can rewrite this as just one fraction m/p^N. Furthermore, because we've "modded out" by $\mathbb{Z}$, we can assume $|m| < p^N$, and $\gcd(m, p) = 1$. It's interesting to note that this $\mathbb{Z}(p^\infty)$ is isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$, the p-adic numbers modulo the p-adic integers. This group is commonly called the p-quasicyclic group, or the Prüfer p-group after Heinz Prüfer [2].

First note that $\mathbb{Z}(p^\infty)$ is always countably infinite.

1 • 3. Result

Let $p \in \mathbb{N}$ be prime. Thus $|\mathbb{Z}(p^\infty)| = \aleph_0$.

Proof .:.

$|\mathbb{Z}(p^\infty)| \ge \aleph_0$, since we have for each $n \in \mathbb{N}$, a $1/p^n \in \mathbb{Z}(p^\infty)$.

$|\mathbb{Z}(p^\infty)| \le \aleph_0$, since its elements are of the form m/p^n for $m, n \in \mathbb{Z}$, meaning $|\mathbb{Z}(p^\infty)| \le |\mathbb{Q}| = \aleph_0$. ⊣

Now we will show that all of the proper subgroups of $\mathbb{Z}(p^\infty)$ are finite. In doing so, we will actually show that all the subgroups are cyclic groups of order p^n for some $n \in \mathbb{N}$. This makes sense by noting that $\mathbb{Z}(p^\infty)$ can also be written in the form

$$\mathbb{Z}(p^\infty) = \bigcup_{n \in \mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$$

where we take appropriate isomorphisms on the $\mathbb{Z}/p^n\mathbb{Z}$s in order to make the group operation intelligible.

1 • 4. Result

For $p \in \mathbb{N}$ prime, $\mathbb{Z}(p^\infty)$ is an infinite, Jónsson group.

Proof .:.

Note that $\mathbb{Z}(p^\infty)$ is generated by the elements $1/p^n$ for $n \in \mathbb{Z}$. Hence if $\{0\} < H < \mathbb{Z}(p^\infty)$ is a proper subgroup, then there is a least $\eta > 1$ for which $1/p^{\eta+1} \notin H$. Note that if $1/p^n \in H$ for $n > \eta$, then $\langle 1/p^{\eta+1}\rangle \subseteq \langle 1/p^n\rangle \subseteq H$, because $p^{n-\eta}/p^n \in \langle 1/p^n\rangle$. So η is the maximal n for which $1/p^n \in H$.

We will show that in fact $H = \langle 1/p^\eta\rangle$. So let $m/p^n = h \in H$ in reduced form be arbitrary. This means that there are $a, b \in \mathbb{Z}$ where $am + bp^n = 1$. It then follows that

$$\frac{1}{p^n} = (am + bp^n)\frac{1}{p^n} = \frac{am}{p^n} + b = ah + b.$$

Since $\mathbb{Z}(p^\infty)$ is modulo $\mathbb{Z}$ and $b \in \mathbb{Z}$, $ah + b = ah \in H$. So $h \in \langle 1/p^n\rangle \subseteq \langle 1/p^\eta\rangle$. Hence $H \subseteq \langle 1/p^\eta\rangle$, and we have equality.

But note that the order of $1/p^\eta$ is just p^η. Hence by Result 1 • 3 $|H| = p^\eta < \aleph_0 = |\mathbb{Z}(p^\infty)|$. ⊣

So there are infinite, Jónsson groups. What about other kinds of structures? Well it's easy to show that 1-dimensional vector spaces are always Jónsson. In the case that the field is infinite, we have an infinite, Jónsson vector space. In particular, consider the following example.

1 • 5. Example

Consider the complex numbers $\mathbb{C}$ as a vector space over $\mathbb{C}$ as a field.

The choice of $\mathbb{C}$ isn't terribly important, as any field $\mathbb{F}$ also has the following result. But in an effort to be more concrete, I'll consider $\mathbb{C}$ as an example.

1 • 6. Result

$\mathbb{C}$ is a Jónsson vector space over $\mathbb{C}$.

Proof .:.

Suppose $M \subseteq \mathbb{C}$ is a subspace of $\mathbb{C}$. If $M = \{0\}$, then we're done: $|M| = 1 < |\mathbb{C}|$. Otherwise, take some non-0 element $m \in M$. As a subspace, M is closed under scalar multiplication. As a field, $1/m \in \mathbb{C}$. Hence for any $c \in \mathbb{C}$, $(c/m) \cdot m = c \in M$, meaning $M = \mathbb{C}$. Thus $M = \{0\}$ or $M = \mathbb{C}$. ⊣

This very simple proof alludes to the idea that begin Jónsson is, just like simplicity, contingent on what kind of structure a thing is regarded as. As a field, $\mathbb{C}$ is not Jónsson, since $|\mathbb{R}| = |\mathbb{C}| = 2^{\aleph_0}$.

Now we can actually provably say that all infinite Jónsson vector spaces are of this form: a line. Hence all Jónsson vector spaces are finite or else just a line. In proving this, we rely on a recalled result of the cardinality of vector spaces.

1 • 7. Result (Recalled 1)

For V a vector space over a field $\mathbb{F}$ of dimension $\dim V = d$.

$$|V| = \begin{cases} |\mathbb{F}|^d & \text{if } d < \aleph_0 \\ \max(|\mathbb{F}|, d) & \text{if } d \geq \aleph_0 \end{cases}.$$

The proof of this result isn't so difficult, but is overly long, and so is relegated to Appendix B. The reason why $|V|$ depends on whether the dimension is infinite is a result of the fact that the elements of V are only *finite* sums of basis elements. The following result tells us that only finite vector spaces, and vector spaces of dimension 1 are Jónsson vector spaces.

1 • 8. Result

A vector space V over a field $\mathbb{F}$ is Jónsson iff $\dim(V) = 1$, or $\dim(V) < \aleph_0$ and $|\mathbb{F}| < \aleph_0$.

Proof .:.

(only if) Suppose V is Jónsson. We consider two cases: if $\dim(V)$ is infinite, and if $\mathbb{F}$ is infinite.

First, suppose $\dim(V)$ is infinite with $B \subseteq V$ a basis, and $b \in B$. Consider the set $B \setminus \{b\}$ and the subspace generated by this: $Y = \operatorname{span}(B \setminus \{b\})$. This does not contain b since B is a linearly independent set. So $Y < V$. But V and Y have the same dimension, since $|B \setminus \{b\}| = |B|$. By Recalled 1 (1 • 7), V and Y have the same cardinality, so that Y witnesses that V isn't Jónsson.

Now suppose $\mathbb{F}$ is infinite. We may assume by the above that $\dim V = d$ is finite. But as an infinite set, $|\mathbb{F}| = |\mathbb{F}|^2$. Hence $|\mathbb{F}| = |\mathbb{F}|^n$ for all positive $n \in \mathbb{N}$. So by Recalled 1 (1 • 7), $|V| = |\mathbb{F}|$.

Let $B \subseteq V$ be a basis of V. If $d \neq 1$, then B has at least two elements, and so for $b \in B$, $B \setminus \{b\}$ is non-empty. The subspace generated by this, $Y = \operatorname{span}(B \setminus \{b\})$, has dimension $d - 1 > 0$. Hence we again have $Y < V$, but $|Y| = |\mathbb{F}|^{d-1} = |\mathbb{F}| = |V|$. So Y witness that V isn't Jónsson.

(if) If $\dim(V) = 1$, then V has no nontrivial, proper subspaces, and so is Jónsson trivially. Similarly, if $\dim(V)$ and $\mathbb{F}$ are both finite, then by Recalled 1 (1 • 7), V is finite, and so trivially Jónsson. ⊣

Again, this says that being a Jónsson vector space is very rare, and the ones that are Jónsson are uninteresting: being finite or else a line. Now despite being vector spaces, related notions like Jónsson algebras are much more difficult to characterize since not all subspaces will be subalgebras. Even in the case of group algebras it's not always clear, since subalgebras don't necessarily correspond to subgroups. Yet there's more we can say about other structures. In particular, there are rich results for modules and groups, as Section 2 describes. This section ends with a note about prime fields, and the discussion of Jónsson fields will be picked back up in Section 3.

1 • 9. Example

Consider $\mathbb{Q}$ as a field.

We know that $\mathbb{Q}$ is not a Jónsson group, since the integers $\mathbb{Z} \leqslant \mathbb{Q}$ are a countable subgroup. We do know, however, that $\mathbb{Q}$ is a Jónsson $\mathbb{Q}$-vector space. But as a field, we can also show that $\mathbb{Q}$ is Jónsson as an immediate corollary to the following result. Because $\mathbb{Q}$ has no proper subfields, it is trivially a Jónsson field.

1 • 10. Result

$\mathbb{Q}$ has no proper subfields.

Proof .:.

Let $\mathbb{F} \subseteq \mathbb{Q}$ be a subfield of $\mathbb{Q}$. Any $f \in \mathbb{F}$ must have $1/f \in \mathbb{F}$ so that $1 \in \mathbb{F}$. Hence being closed under addition yields that $\mathbb{Z} \subseteq \mathbb{F}$. Therefore $1/n \in \mathbb{F}$ for any $n \in \mathbb{Z}$ so that $m/n \in \mathbb{F}$ for any $m, n \in \mathbb{Z}$. Thus $\mathbb{Q} \subseteq \mathbb{F}$ and we conclude equality. ⊣

So there are Jónsson fields on $\aleph_0$, and so on all $n < \aleph_1$. An interesting result is that there are no uncountable Jónsson fields at all. Proving this is relegated to Section 3, and relies on results about transcendental elements.

Note that the above result together with Section 3 tells us that $\mathbb{Q}$ is the only Jónsson field of characteristic 0.

Section 2. Jónsson Groups and Modules

So we've given a few examples of infinite Jónsson structures, but they haven't all been very complicated. This is because Jónsson structures are actually quite difficult to construct, and quite difficult to check that they are really Jónsson. Despite these difficulties, however, there are still interesting results about such structures. Some of these can even help characterize other notions. In particular, we will look at results involving Jónsson groups and modules in this section, concluding with the characterization of infinite, abelian, Jónsson groups: any such group is either finite or a $\mathbb{Z}(p^\infty)$ group.

Despite this focus on modules and groups, often these results can be thought of as results about the underlying ring. In some sense, the results allow us to talk a little more about the rings themselves through their Jónsson modules, and hence talk about Jónsson modules through their ring's structure. This in turn will allow us to talk about Jónsson, abelian groups as $\mathbb{Z}$-modules, and draw on results about $\mathbb{Z}$ as a ring.

Despite how simple Jónsson vector spaces are, Jónsson modules are much more complicated. In general, there are only partial results that characterize Jónsson modules. For example, we have the following result.

2 • 1. Result

Let M be a module. If M is infinite and Jónsson, then M is indecomposible.

Proof .:.

Let $M = N \oplus H$ for proper submodules $N, H \subsetneq M$. As M is infinite, one of the two N, H must be infinite. But through basic cardinal arithmetic,

$$|M| = |N \oplus H| = |N| \cdot |H| = \max(|N|, |H|).$$

Since M is Jónsson, both $|N| < |M|$ and $|H| < |M|$ so that $\max(|N|, |H|) < |M|$. The resulting $|M| < |M|$ is of course a contradiction. ⊣

More interesting results will follow when we restrict our view to somewhat "nice" rings: commutative rings. The following are two results about Jónsson modules over commutative rings. We will always restrict our focus from now on to commutative rings, because $\mathbb{Z}$ is one of these, and abelian groups are $\mathbb{Z}$-modules.

2 • 2. Result

Let R be a commutative ring, and M a (left) R-module. If M is infinite and Jónsson, then every $r \in R$ has $rM = \{0_M\}$ or $rM = M$.

Proof .:.

Let $r \in R$ and consider rM, a submodule of M because R is commutative: $rn + s \cdot (rm) = r \cdot (n + sm) \in rM$.

Consider $N = \{n \in M : rn = 0_M\}$. Note that as a kernel of the homomorphism $\varphi = m \mapsto rm$, we get that $M/N \cong rM = \operatorname{im} \varphi$. This then implies that $|rM||N| = |M/N||N| = |M|$.

Now since we're dealing with infinite cardinals, $|rM||N| = \max(|rM|, |N|)$. But as infinite cardinals, this implies $|N| = |M|$ or $|rM| = |M|$. Because M is Jónsson, this means either $N = M$ or $rM = M$. In the first case, $rM = \{0_M\}$, and in the second, $rM = M$. ⊣

This result allows us to conclude things about the rings by viewing them as modules over themselves. The next result is just a neat aside that characterizes infinite fields.

2 • 3. Result

Let R be an infinite, commutative ring. Thus R is a field iff R is a Jónsson R-module.

Proof .:.

(only if) Suppose R is a field. Thus R, as an R-module, is a 1-dimensional vector space. So by Result 1 • 8, R is a Jónsson R-module.

(if) If R is a Jónsson R-module, then by Result 2 • 2, every $r \in R$ has $rR = \{0_R\}$ or $rR = R$. Fix an arbitrary $r \in R \setminus \{0\}$. Since $1_R \in R$, we have $r \in rR$, meaning that $rR \neq \{0_R\}$, and so $rR = R$. But then there is some $\rho \in R$ where $r\rho = 1_R$ for $r \neq 0_R$. So every element of $R \setminus \{0\}$ is a unit, and R is a field. ⊣

This next result makes a push towards a remarkable characterization of infinite, abelian, Jónsson groups. Again, we can have results about the ring through Jónsson modules. This also marks a shift in focus towards Jónsson groups. In particular, we will consider abelian groups.

2 • 4. Result

Let R be a commutative ring, and M a (left) R-module. If M is infinite and Jónsson, then

$$\text{Ann}_R(M) = \{r \in R : rM = \{0_M\}\} \lhd R$$

is a prime ideal of R.

Proof .:.

It's clear this is an ideal of R: $r, s \in \text{Ann}_R(M)$ implies $(\rho r + s)M = \rho(rM) + sM = \{0_M\}$ for any $\rho \in R$. It's also clear that $\text{Ann}_R(M) \neq R$, since otherwise $M = 1_R \cdot M = \{0_M\}$, contradicting that M is infinite.

It follows very quickly from Result 2 • 2 that $\text{Ann}_R(M)$ is prime. Explicitly, suppose that $rsM = \{0_M\}$, but $r, s \notin \text{Ann}_R(M)$. By Result 2 • 2, $rM = sM = M$. Thus $rsM = rM = M$, which is not $\{0_M\}$ since M is infinite, a contradiction with the hypothesis that $rsM = \{0_M\}$. Thus r or $s \in \text{Ann}_R(M)$, meaning $\text{Ann}_R(M) \lhd R$ is prime. ⊣

Again, the major result for us here is that these $\mathbb{Z}(p^\infty)$ are the only infinite, abelian, Jónsson groups. To prove this, note that any abelian group can be viewed as a $\mathbb{Z}$-module by taking $n \cdot g = g + \cdots + g$ (or else $-g - \cdots - g$) for $n \in \mathbb{Z}$, g in the group. Using this operation, an abelian group is Jónsson iff it's a Jónsson $\mathbb{Z}$-module.

2 • 5. Result

Let G be an abelian group. Thus G is Jónsson iff G is a Jónsson $\mathbb{Z}$-module.

Proof .:.

(only if) Let G be a Jónsson group. Let $H \subsetneq G$ be an arbitrary proper $\mathbb{Z}$-submodule. H is closed under the group operation of addition (and subtraction), so that H is a subgroup. Because G is a Jónsson group, $|H| < |G|$. Because H was arbitrary, G is a Jónsson $\mathbb{Z}$-module.

(if) Suppose G is a Jónsson $\mathbb{Z}$-module. Let $H < G$ be an arbitrary proper subgroup which is then closed under the group operation of addition (and subtraction). For every $n \in \mathbb{Z}$ and $h_1, h_2 \in H$, $nh_1 + h_2 = \pm h_1 \pm \cdots \pm h_1 + h_2 \in H$. So H is a proper submodule. Since G is a Jónsson $\mathbb{Z}$-module, $|H| < |G|$. Because H was arbitrary, G is a Jónsson group. ⊣

The following result then gives us the characterization of infinite, abelian, Jónsson groups via the results given above. This characterization shows that all infinite, abelian, Jónsson groups are countable. This does not mean, however, that there are no uncountable Jónsson structures which can be thought of as abelian groups, Example 1 • 5 for instance. First recall two results. The first is relatively straightforward, but he second is a much more difficult result proven in Appendix C.

2 • 6. Result (Recalled 2)

$I \lhd \mathbb{Z}$ is a prime ideal iff $I = \{0\}$, or there is some prime $p \in \mathbb{N}$ where $I = \mathbb{Z}p$.

Proof .:.

(if) Clearly $I = \{0\}$ is a prime ideal. $\mathbb{Z}p$ is a prime ideal since p is prime: $mn \in \mathbb{Z}p$ means $p \mid mn$ so that $p \mid m$ or $p \mid n$.

(only if) Suppose $I \lhd \mathbb{Z}$ is prime. If $I \neq \{0\}$, then there is a least $p \in I$. Clearly $\mathbb{Z}p \subseteq I$. Moreover, if $m, n \in I$ then $\gcd(m, n) \in I$ since $\gcd(m, n)$ is given by a $\mathbb{Z}$-linear combination of m and n, and I is closed under $\mathbb{Z}$-linear combinations of its elements. Hence p is the gcd of all of I because any $\gcd(I) \neq p$ is less than p, contradicting that p is the least element of I. ⊣

This also tells us that the maximal ideals of $\mathbb{Z}$ are the sets $p\mathbb{Z}$ when $p \in \mathbb{N}$ is prime.

2 • 7. Result (Recalled 3)

Let G be an infinite, abelian group. Suppose that for all $n \in \mathbb{Z} \setminus \{0\}$, and $g \in G$, $n \cdot x = g$ has a solution of $x \in G$. Therefore, there are cardinals n, m (possibly infinite), and primes $p_i \in \mathbb{N}$ for $i \leq n$ where $G \cong \bigoplus_{i \leq n} \mathbb{Z}(p_i^\infty) \oplus \bigoplus_m \mathbb{Q}$.

If you know the terminology, this says a divisible abelian group is the direct sum of copies of various $\mathbb{Z}(p^\infty)$ and copies of $\mathbb{Q}$. This is why the seemingly arbitrary $\mathbb{Z}(p^\infty)$ is important in our characterization.

2 • 8. Result

Let G be an infinite, abelian group. Thus G is Jónsson iff there is some prime $p \in \mathbb{N}$ where $G \cong \mathbb{Z}(p^\infty)$.

Proof .:.

Result 1 • 4 gives the "if" direction. So we must show if G is Jónsson, then $G \cong \mathbb{Z}(p^\infty)$ for a prime $p \in \mathbb{N}$.

Suppose G is a Jónsson group. By Result 2 • 5, G is a Jónsson $\mathbb{Z}$-module. Since G is infinite, by Result 2 • 4, $\mathrm{Ann}_{\mathbb{Z}}(G) = \{n \in \mathbb{Z} : nG = \{0_G\}\}$ is a prime ideal of $\mathbb{Z}$. Recalled 2 (2 • 6) implies that either $\mathrm{Ann}_{\mathbb{Z}}(G) = \{0\}$, or there is some prime $p \in \mathbb{N}$ where $\mathrm{Ann}_{\mathbb{Z}}(G) = \mathbb{Z}p$.

Claim 1

There is no prime $p \in \mathbb{N}$ where $\mathrm{Ann}_{\mathbb{Z}}(G) = \mathbb{Z}p$.

Proof .:.

Suppose not: $\mathrm{Ann}_{\mathbb{Z}}(G) = \mathbb{Z}p$ for some prime $p \in \mathbb{N}$. Note that then $\mathbb{Z}/p\mathbb{Z}$ is a finite field. We can then consider G as a vector space over $\mathbb{Z}/p\mathbb{Z}$. But G is a Jónsson module, and so a Jónsson vector space. By Result 1 • 8, G is either finite or else 1-dimensional.

Since G is infinite by hypothesis, G is 1-dimensional. But $\mathbb{Z}/p\mathbb{Z}$ is a finite field. By Recalled 1 (1 • 7), $|G| = |\mathbb{Z}/p\mathbb{Z}|^1 < \aleph_0$, contradicting that G is infinite. ⊣

Thus we must have $\mathrm{Ann}_{\mathbb{Z}}(G) = \{0\}$, and so for all $n \in \mathbb{Z}$, $nG = G$. This implies that we can always solve the equation $n \cdot x = g$ for any fixed $0 \neq n \in \mathbb{Z}$ and $g \in G$. So by Recalled 3 (2 • 7), we get that G is the direct sum of copies of various $\mathbb{Z}(p_i^\infty)$s, and $\mathbb{Q}$:

$$G \cong \bigoplus_{i \leq n} \mathbb{Z}(p_i^\infty) \oplus \bigoplus_m \mathbb{Q}$$

for primes $p_i \in \mathbb{N}$. How many copies of $\mathbb{Z}(p_i^\infty)$s and $\mathbb{Q}$, you might ask? Well since G is an infinite Jónsson $\mathbb{Z}$-module, Result 2 • 1 tells us that G is indecomposible. So there is really only one copy: G is isomorphic to either $\mathbb{Z}(p^\infty)$ for some prime $p \in \mathbb{N}$, or $\mathbb{Q}$.

But $\mathbb{Q}$ has an infinite subgroup: $\mathbb{Z} < \mathbb{Q}$. Hence $\mathbb{Q}$ isn't Jónsson, and so $G \ncong \mathbb{Q}$. Therefore $G \cong \mathbb{Z}(p^\infty)$ for some prime $p \in \mathbb{N}$. ⊣

As said before, the above result tells us via Result 1 • 3 that any abelian, Jónsson group G is either finite, or $|G| = |\mathbb{Z}(p^\infty)| = \aleph_0$ is countably infinite. And so in either case, G is countable. But what about uncountable and non-abelian groups? Are there any countable non-abelian Jónsson groups? Are there any uncountable Jónsson groups? The answer to both these questions was answered "yes", the first by Ol'shanskii in [3], and the second by Shelah in [5], but the proofs of these are far too involved to present here.

So there are no uncountable abelian Jónsson groups, but there are uncountable Jónsson groups. A remarkable result shown in the next section Section 3 shows that this answer differs, however, for fields: there are no uncountable Jónsson fields at all.

Section 3. *Uncountable Fields*

The goal of this section will be to show that there are no uncountable, Jónsson fields. The heart of the proof of the result relies on looking at transcendence bases over the prime field of the characteristic of the field in question. In preparation for this, we must prove some lemmas on this background material.

3 • 1. Result

Let $\mathbb{F}$ be a field of characteristic p. If $p = 0$, then $\mathbb{Q}$ embedds into $\mathbb{F}$. Otherwise $\mathbb{Z}/p\mathbb{Z}$ embedds into $\mathbb{F}$.

Proof .:.

The essence of this proof is to consider the field generated by $1_{\mathbb{F}}$, being $\mathbb{Q}$ if $p = 0$, and $\mathbb{Z}/p\mathbb{Z}$ otherwise.

Let $\varphi : \mathbb{Z} \to \mathbb{F}$ be defined by $\varphi(n) = n \cdot 1_{\mathbb{F}} = \pm 1_{\mathbb{F}} \pm \cdots \pm 1_{\mathbb{F}}$ repeated addition (or subtraction). This is easily checked to be a homomorphism. By the first isomorphism theorem for rings, $\ker \varphi \lhd \mathbb{Z}$, and $\operatorname{im} \varphi \cong \mathbb{Z}/\ker \varphi$.

If $p > 0$, then $\ker \varphi = p\mathbb{Z}$, a maximal ideal of $\mathbb{Z}$, and so $\operatorname{im} \varphi \cong \mathbb{Z}/p\mathbb{Z}$ is a subfield of $\mathbb{F}$.

If $p = 0$, then $\ker \varphi = \{0\}$. Now consider the homomorphism $\psi : \mathbb{Q} \to \mathbb{F}$ defined by $\psi(m/n) = \varphi(m) \cdot \varphi(n)^{-1}$. Note that $\psi(m/n) = 0$ iff $\varphi(m) = 0$ iff $m \in \ker \varphi = \{0\}$. Hence $\ker \psi = \ker \varphi = \{0\}$. Again by the first isomorphism theorem for rings, $\operatorname{im} \psi \cong \mathbb{Q}/\ker \psi = \mathbb{Q}/\ker \varphi \cong \mathbb{Q}$. ⊣

In essence, we're showing the existence of the minimal subfield generated by $1_{\mathbb{F}}$. The other elements of the field $\mathbb{F}$ then won't be "reachable" by $1_{\mathbb{F}}$ in a sense described below.

3 • 2. Definition

Let $\mathbb{F}$ be a field, and $\mathbb{E} \subseteq \mathbb{F}$ be a subfield. $B \subseteq \mathbb{F}$ is a <u>transcendental basis</u> of $\mathbb{F}$ over $\mathbb{E}$ iff

(1) for all polynomials $p \in \mathbb{E}[x_1, x_2, ...]$ and $b_1, ..., b_n \in B$, $p(b_1, ..., b_n) = 0_{\mathbb{F}}$ iff $p = 0_{\mathbb{F}}$; and

(2) $\mathbb{F}$ is algebraic over $\mathbb{E}(B)$.

Useful for us is that every field has a transcendental basis over any subfield. This will be useful in calculating cardinality. To clarify, the notation $\mathbb{E}(B)$ is the field generated by adjoining B to $\mathbb{E}$. The polynomial ring $\mathbb{E}[B]$ then uses a slightly different notation, but is connected, since $\mathbb{E}(B)$ is isomorphic to the field of fractions of $\mathbb{E}[B]$.

3 • 3. Result

Let $\mathbb{F}$ be a field, and $\mathbb{E} \subseteq \mathbb{F}$ a subfield. Therefore, there is a transcendental basis $B \subseteq \mathbb{F}$ over $\mathbb{E}$.

Proof .:.

We explicitly construct one via transfinite recursion. If $\mathbb{F}$ is algebraic over $\mathbb{E}$, then we are done. Otherwise, for each ordinal α, define

$$b_\alpha \in \mathbb{F} \setminus \mathbb{E}\big(\{b_\beta : \beta < \alpha\}\big),$$

where b_α is not the root of any non-zero polynomial $p(x)$ with coefficients in $\mathbb{E}[\{b_\beta : \beta < \alpha\}][x]$. If no such b_α exists, then $\mathbb{F}$ is algebraic over $\mathbb{E}(\{b_\beta : \beta < \alpha\})$.

This sequence of $b_\alpha \in \mathbb{F}$ will have some length δ. Furthermore, any polynomial $p \in \mathbb{E}[x_1, ..., x_n]$ satisfying $p(b_{\alpha_1}, ..., b_{\alpha_n}) = 0_{\mathbb{F}}$ will have a maximal α among these b_α. So the polynomial replacing b_α with x,

$$\pi(x) = p(b_{\alpha_1}, ..., x, ..., b_{\alpha_n}) \in \mathbb{E}[\{b_\beta : \beta < \alpha\}][x],$$

has $\pi(b_\alpha) = 0_{\mathbb{F}}$, contradicting our choice of b_α. Hence $B = \{b_\alpha : \alpha < \delta\}$ is a transcendental basis over $\mathbb{E}$. ⊣

The above proof is essentially the same as the proof that every vector space has a basis. The two ideas are linked together, but ultimately aren't explored here. It will be useful to actually construct the field $\mathbb{E}(B)$ from $\mathbb{E}$ and B and prove some things about it.

3 • 4. Result

Let $\mathbb{F}$ be a field, $\mathbb{E} \subseteq \mathbb{F}$ a subfield, and $B \subseteq \mathbb{F}$ a non-empty subset. Therefore $|\mathbb{E}(B)| \leq |\mathbb{E}| \cdot |B| \cdot \aleph_0$.

Proof .:.

Because $\mathbb{E}(B)$ is isomorphic to the field of fractions of $\mathbb{E}[B]$, we have that $|\mathbb{E}(B)| \leq |\mathbb{E}[B]|^2$. After multiplying by $\aleph_0$, we get by basic cardinal arithmetic that

$$|\mathbb{E}(B)| \leq |\mathbb{E}[B]|^2 \cdot \aleph_0 = |\mathbb{E}[B]| \cdot \aleph_0.$$

So now we need to bound the cardinality of $\mathbb{E}[B]$.

Note that every element of $\mathbb{E}[B]$ will be a polynomial of multiple variables with coefficients in $\mathbb{E}$ evaluated at elements of B. Each such polynomial can be identified with a finite sequence of elements of $\mathbb{E}$. In the case that $\mathbb{E}$ is finite, the number of such polynomials is $\aleph_0$. In the case that $\mathbb{E}$ is infinite, the number of such polynomials is at most

$$\sum_{n \in \mathbb{N}} |\mathbb{E}|^n = \sum_{n \in \mathbb{N}} |\mathbb{E}| = |\mathbb{E}| \cdot \aleph_0.$$

Hence the number of such polynomials is at most $|\mathbb{E}| \cdot \aleph_0$. Similarly, each polynomial can be evaluated by a finite sequence of elements of B. The same reasoning tells us that the number of such evaluations is at most $|B| \cdot \aleph_0$. Hence

$$|\mathbb{E}(B)| \leq |\mathbb{E}[B]|^2 \leq |\mathbb{E}|^2 \cdot |B|^2 \cdot \aleph_0 = |\mathbb{E}| \cdot |B| \cdot \aleph_0 \dashv$$

Now a result not proven here is that the cardinality of any transcendental basis of a fixed $\mathbb{F}$ over a fixed $\mathbb{E} \subseteq \mathbb{F}$ is the same. This cardinality is referred to as the transendence degree, and is denoted $\operatorname{trdeg}_{\mathbb{E}} \mathbb{F}$. Instead, to avoid proving this result directly, we will just fix a B, and talk about $|B|$.

That said, the following result will tell us that $\operatorname{trdeg}_{\mathbb{E}} \mathbb{F}$ is always the same for an infinite field $\mathbb{F}$ when $|\mathbb{E}| < |\mathbb{F}|$, and $\mathbb{F}$ is uncountable.

3 • 5. Result

Let $\mathbb{F}$ be a field, $\mathbb{E} \subsetneq \mathbb{F}$ a subfield, and B a transcendental basis of $\mathbb{F}$ over $\mathbb{E}$. Suppose $\mathbb{F}$ is infinite. Therefore $|\mathbb{F}| = |\mathbb{E}| \cdot |B| \cdot \aleph_0$.

Proof .:.

Clearly $|\mathbb{E}| \cdot |B| \cdot \aleph_0 = \max(|\mathbb{E}|, |B|, \aleph_0) \leq |\mathbb{F}|$ as $\mathbb{E}, B \subseteq \mathbb{F}$ and $|\mathbb{F}|$ is infinite. So it suffices to show the other inequality: $|F| \leq |\mathbb{E}| \cdot |B| \cdot \aleph_0$.

As a transcendental basis, F is algebraic over $\mathbb{E}(B)$. Hence the elements of $\mathbb{F}$ can be identified as the roots of polynomials in $\mathbb{E}(B)[x]$. Every polynomial in $\mathbb{E}(B)[x]$ will have finitely many solutions. The number of polynomials with coefficients in $\mathbb{E}(B)$ is $|\mathbb{E}(B)| \cdot \aleph_0$. Hence by Result 3 • 4,

$$|\mathbb{F}| \leq |\mathbb{E}(B)| \cdot \aleph_0 \leq |\mathbb{E}| \cdot |B| \cdot \aleph_0.$$

And so we get equality. $\dashv$

Now we can show the main result for fields.

3 • 6. Result

Let $\mathbb{F}$ be a field. Suppose $|\mathbb{F}| > \aleph_0$. Therefore $\mathbb{F}$ isn't Jónsson.

Proof .:.

Let $\mathbb{E} \subseteq \mathbb{F}$ be as in Result 3 • 1 with B be a transcendental basis of $\mathbb{F}$ over $\mathbb{E}$ as in Result 3 • 3. Since $|\mathbb{E}| \leq \aleph_0 < |\mathbb{F}|$, basic cardinal arithmetic with Result 3 • 5 tells us that $|B| = |\mathbb{F}|$.

Let $b_\alpha \in B$ for $\alpha < \delta$. Consider $P = B \setminus \{b_\alpha\}$. Note that $\mathbb{E}(P) \subseteq \mathbb{E}(B) \subseteq \mathbb{F}$ is a subfield.

Furthermore, $b_\alpha \notin \mathbb{E}(P)$, since this would contradict construction of B as in Result 3 • 3. Explicitly, let $b_\alpha = p(b_1, ..., b_n)/q(b_1, ..., b_n)$ for $p, q \in \mathbb{E}[x_1, ..., x_n]$. The non-zero polynomial

$$\pi(x_1, ..., x_{n+1}) = p(x_1, ..., x_n) - x_{n+1} \cdot q(x_1, ..., x_n) \in \mathbb{E}[x_1, ..., x_{n+1}]$$

then has $\pi(b_1, ..., b_n, b_\alpha) = 0_{\mathbb{F}}$, contradicting that B is a trascendental basis of $\mathbb{F}$ over $\mathbb{E}$.

Since $|B| = |\mathbb{F}| > \aleph_0$ is infinite, $|P| = |B|$. Result 3 • 4 tells us that

$$|\mathbb{E}(P)| \le |\mathbb{E}| \cdot |P| \cdot \aleph_0 = |P|.$$

Since $P \subseteq \mathbb{E}(P)$, $|P| \le |\mathbb{E}(P)|$. So $|\mathbb{E}(P)| = |P| = |\mathbb{F}|$. But then $\mathbb{E}(P) \subsetneq \mathbb{F}$ is a subfield of $\mathbb{F}$ of the same cardinality. Hence $\mathbb{F}$ isn't Jónsson. ⊣

The result can be seen fairly easily for things like $\mathbb{C}$, since $\mathbb{R} \subsetneq \mathbb{C}$ and $|\mathbb{R}| = |\mathbb{C}|$. But we can keep reducing in this fashion for any field of any uncountable cardinality. As said before, in the face of Example 1 • 9, this tells us that the only Jónsson fields of characteristic 0 are isomorphic to $\mathbb{Q}$.

The above proof can also be generalized to certain other kinds of rings. Regardless, this continues the point that such large Jónsson structures are quite rare to find, and are very difficult to construct outright. It seems many common notions of algebraic structures, like abelian groups, fields, and vector spaces, are almost never Jónsson. Coming up with large examples of such structures ranges from impossible to requiring incredible creativity.

Appendix 1. *Cardinal Arithmetic Background*

People should be familiar with what cardinals are at this point, but this appendix will still give the general idea. After this necessary background, some basic results are given, but are not proven here. Mostly only a few results are used, but they are used here rather frequently.

Cardinal numbers can be thought of as the canonical elements of the equivalence classes of the universe modulo bijection. More concretely, however, they are the sets

$$0, 1, 2, 3, ..., \aleph_0, \aleph_1, ..., \aleph_\omega, \aleph_{\omega+1}, ..., \aleph_{\omega+\omega}, \aleph_{\omega+\omega+1}, ...$$

which have no upper bound: for every cardinal, there is a larger one. In fact, there is a successor cardinal: $\kappa < \kappa^+$. The $\aleph$ numbers are the infinite cardinals. $\aleph_0 = |\mathbb{N}|$ is the first infinite cardinal. $\aleph_1 = \aleph_0^+$ is the next, and so on. They are indexed by ordinal numbers, which are just canonical elements of the equivalence classes of well-orderings. For example, the order of $\mathbb{N}$ is ω. This is just notation, however.

The following defintions are used for operations. Note that $A \sqcup B = (A \times \{0\}) \cup (B \times \{1\})$ denotes the disjoint union: tagging the elements of A with a 0, and the elements of B with a 1 so that the tagged sets are disjoint. For larger unions, we just do the same thing, but with more tags. $A \times B$ denotes the cartesian product.

1 • 1. Definition

Let κ, λ, and κ_i for $i \in I$ be cardinals. Define

$$\begin{aligned} \kappa + \lambda &= |\kappa \sqcup \lambda| \\ \kappa \cdot \lambda &= |\kappa \times \lambda| \\ \sum_{i \in I} \kappa_i &= \left| \bigsqcup_{i \in I} \kappa_i \right| \\ \prod_{i \in I} \kappa_i &= \left| \prod_{i \in I} \kappa_i \right| \text{ (the cardinality of the cartesian product)} \\ [\kappa]^{<\omega} &= \{X \subseteq \kappa : |X| < \aleph_0\}. \end{aligned}$$

The following results aren't horribly difficult to prove, but can be quite long.

1 • 2. Result (Cardinal Arithmetic Basics)

Let $n \in \mathbb{N} \setminus \{0\}$ be a finite cardinal, κ, κ_i for $i \in I$ be infinite cardinals, and c an arbitrary cardinal (finite or infinite). Therefore

1. $+$ and $\cdot$ are associative, commutative, and distributive;
2. $c \cdot \kappa = c^n \cdot \kappa^n = c + \kappa = \max(c, \kappa)$;
3. $\sum_{i \in I} \kappa_i \leq \prod_{i \in I} \kappa_i$ (König's theorem);
4. $\left|[\kappa]^{<\omega}\right| = \kappa$;
5. $c < 2^c$ for $c \neq 0$.

Appendix 2. Vector Space Cardinality

2 • 1. Result (Recalled 1)

For V a vector space over a field $\mathbb{F}$ of dimension $\dim V = d$.

$$|V| = \begin{cases} |\mathbb{F}|^d & \text{if } d < \aleph_0 \\ \max(|\mathbb{F}|, d) & \text{if } d \geq \aleph_0 \end{cases}.$$

Proof .:.

If $d < \aleph_0$, then let $B = \{v_1, ..., v_d\}$ be a basis of V. We then have that any element of V can be written uniquely as a sum $\sum_{i=1}^{d} c_i v_i$. Hence we can associate $v \in V$ with the d-tuple $(c_1, ..., c_d)$ for $c_i \in \mathbb{F}$. This yields a bijection from V to $\mathbb{F}^d$. The cardinality of $\mathbb{F}^d$ is just $|\mathbb{F}|^d$ so that $|V| = \mathbb{F}^d$, confirming the result for finite dimensional vector spaces.

Suppose V is infinite dimensional, and let $B = \{v_i : i < d\}$ be a basis so that $|B| = d > \aleph_0$. Each element of V is still uniquely determined by the coefficients of basis elements. Hence for each $v \in V$ there is a unique function $\mathfrak{v}$ from d to $\mathbb{F}$ which satisfies $v = \sum_{i<d} \mathfrak{v}(i) v_i$. But not every function in ${}^d\mathbb{F} = \{f : d \to \mathbb{F}\}$ corresponds to an element $v \in V$, since we're only taking finite sums. Hence each element of v corresponds to a function $\mathfrak{v} \in {}^d\mathbb{F}$ with finite support. Let

$$\mathfrak{V} = \left\{ f : d \to \mathbb{F} : \left|\{\alpha < d : f(\alpha) \neq 0_{\mathbb{F}}\}\right| < \aleph_0 \right\},$$

so that $|V| = |\mathfrak{V}|$.

Let $[X]^{<\omega}$ be the set of finite subsets of a set X. Each function $f \in \mathfrak{V}$ is given by f restricted to the set $\{\alpha < d : f(\alpha) \neq 0_{\mathbb{F}}\} \in [d]^{<\omega}$. Hence $\mathfrak{V}$ is in bijection with the union

$$\mathfrak{W} := \bigcup_{S \in [d]^{<\omega}} {}^S\big(\mathbb{F} \setminus \{0_{\mathbb{F}}\}\big),$$

which can be seen by extending any $f \in \mathfrak{W}$ to a function on d by setting all values not in the domain of f to $0_{\mathbb{F}}$. Hence $|V| = |\mathfrak{V}| = |\mathfrak{W}|$.

For each $S \in [d]^{<\omega}$, there are exactly $|\mathbb{F}|^{|S|}$ elements. Through basic cardinal arithmetic, $|[d]^{<\omega}| = d$, and the cardinality of the union is less than the sum of the cardinalities:

$$|\mathfrak{W}| \leq \sum_{S \in [d]^{<\omega}} |\mathbb{F}|^{|S|}.$$

Assuming that $\mathbb{F}$ is finite, $|\mathbb{F}|^{|S|} \leq \aleph_0$ for any $S \in [d]^{<\omega}$. Hence in this case, because $d \geq \aleph_0$,

$$|V| = |\mathfrak{W}| \leq \sum_{S \in [d]^{<\infty}} \aleph_0 = \sum_{\alpha < d} \aleph_0 = d\aleph_0 = d = \max(|\mathbb{F}|, d).$$

Assuming that $\mathbb{F}$ is infinite, $|\mathbb{F}|^{|S|} = |\mathbb{F}|$ for $S \in [d]^{<\omega}$. Hence in this case

$$|V| = |\mathfrak{W}| \leq \sum_{S \in [d]^{<\infty}} |\mathbb{F}| = \sum_{\alpha < d} |\mathbb{F}| = d|\mathbb{F}| = \max(|\mathbb{F}|, d).$$

So that we always have $|V| \leq \max(|\mathbb{F}|, d)$ for $d \geq \aleph_0$.

But $|V| \geq \max(|\mathbb{F}|, d)$, since any non-zero $v \in V$ will yield $\mathbb{F}v \subseteq V$ so that $|\mathbb{F}v| = |\mathbb{F}| \leq |V|$. And $B \subseteq V$ yields $|B| = d \leq |V|$. Hence $|V| = \max(|\mathbb{F}|, d)$. ⊣

Appendix 3. *Divisible, Abelian Groups*

Now before we get into proving the result of Recalled 3 (2 • 7), it will be useful to define what it means for a group to be divisible. It will be also very useful to prove several lemmas. To emphasize what is important at a glance, the lemmas, definitions, and results are enclosed in black rectangles instead of grey ones. The following definition is given only for abelian groups, but the idea makes sense in general. Note that multiplication by an integer is just repeated addition of the group element.

3 • 1. Definition

Let G be an abelian group. G is divisible iff for every $g \in G$, and $n \in \mathbb{Z} \setminus \{0\}$, there is some $x \in G$ where $n \cdot x = g$.

Now we present two lemmas which tell us why Recalled 3 (2 • 7) talks about $\mathbb{Q}$ and $\mathbb{Z}(p^\infty)$ groups. Both of these lemmas are quite long, and are the meat of the structure theorem called Recalled 3 (2 • 7). The lemmas talk about the building blocks of divisible, abelian groups. First we will show that the torsion free building blocks are isomorphic to $\mathbb{Q}$ under addition.

3 • 2. Lemma

Let G be an infinite, abelian, divisible group. Suppose G is torsion free, and G has no divisible, proper, non-trivial subgroups. Therefore $G \cong \mathbb{Q}$ under addition.

Proof .:.

Fix $g \in G \setminus \{e_G\}$. Because G is divisible, for any $m/n \in \mathbb{Q}$, $n \cdot x = m \cdot g$ has a solution. Through choice, let $\gamma_{m/n}$ witness $n \cdot \gamma_{m/n} = m \cdot g$. With this, define the map

$$\varphi(1) = g,$$
$$\varphi\left(\frac{m}{n}\right) = \gamma_{m/n}.$$

The idea being that $\gamma_{m/n}$ is like $m/n \cdot g$, and $n\varphi(m/n) = mg$. This map φ is well-defined, since if $m/n = w/u$, then $mu = wn$, and so, because mu and wn are non-zero,

$$mu \cdot \gamma_{m/n} = wn \cdot \gamma_{m/n} = wm \cdot g = m(w \cdot g) = mu \cdot \gamma_{w/u}.$$
$$\therefore \gamma_{m/n} = \gamma_{w/u}.$$

From this we can show that φ is in fact an isomorphism. First we must show that φ is a homomorphism.

Claim 1

φ is a homomorphism.

Proof .:.

First we must show that $\varphi(0) = e_G$. Clearly if $m = 0$, then $m \cdot g = e_G$ and so $n \cdot \gamma_{0,n} = e_G$. Since G is torsion-free, this implies $\gamma_{0,n} = e_G$, and hence $\varphi(0) = \gamma_{0,n} = e_G$.

Now we must show $\varphi(m/n + w/u) = \varphi(m/n) + \varphi(w/u)$. Note that $nu \neq 0$ since both $n, u \neq 0$.

$$nu \cdot \varphi\left(\frac{m}{n} + \frac{w}{u}\right) = nu \cdot \varphi\left(\frac{mu + wn}{nu}\right) = (mu + wn) \cdot g = mu \cdot g + wn \cdot g$$
$$= un \cdot \varphi\left(\frac{m}{n}\right) + nu \cdot \varphi\left(\frac{w}{u}\right) = nu \cdot \left(\varphi\left(\frac{m}{n}\right) + \varphi\left(\frac{w}{n}\right)\right) \dashv$$

Claim 2

φ is a bijection.

Proof .:.

To show that φ is injective, suppose that $\varphi(m/n) = \varphi(w/u)$. This implies that

$$nu \cdot \varphi(m/n) = mu \cdot g$$
$$nu \cdot \varphi(w/u) = wn \cdot g$$

Therefore $mu \cdot g = wn \cdot g$ so that $(mu - wn) \cdot g = e_G$. Since $g \neq e_G$ and G is torsion free, this implies $mu - wn = 0$ and hence $mu = wn$: $m/n = w/u$.

To show that φ is surjective, note that otherwise $\operatorname{im} \varphi < G$ is a divisible subgroup of G, contradicting that G has no non-trivial, divisible, proper subgroups. ⊣

Thus φ is an isomorphism, and so $G \cong \mathbb{Q}$. ⊣

Now we will show that the non-torsion-free building blocks are isomorphic to some $\mathbb{Z}(p^\infty)$ group. After that, we can start to decompose infinite, abelian, divisible groups into building blocks: minimal divisible subgroups.

3 • 3. Lemma

Let G be an infinite, abelian, divisible group. Suppose G is not torsion free, and G has no divisible, proper, non-trivial subgroups. Therefore there is some prime $p \in \mathbb{Z}$ where $G \cong \mathbb{Z}(p^\infty)$.

Proof .:.

There are many different presentations of $\mathbb{Z}(p^\infty)$. For this proof, note that $\mathbb{Z}(p^\infty)$ is isomorphic to the free abelian group

$$\langle g_1, g_2, \ldots \ : \ p \cdot g_{i+1} = g_i, \ \& \ p \cdot g_1 = e \rangle.$$

The proof will proceed in three major steps. First, we will show every element has some order p^i for a fixed prime $p \in \mathbb{N}$. Second, we show every p^n is the order of some element of G. Third, we build an isomorphism from $\mathbb{Z}(p^\infty)$ to G.

Claim 1

The order of every element of G is finite.

Proof .:.

Let $F \subseteq G$ be the set of elements of G with infinite order along with e_G:

$$F := \{ f \in G : \forall n \in \mathbb{Z}(n \cdot f \neq e_G) \} \cup \{e_G\}.$$

If F is trivial, then we are done. So suppose $F \neq \{e_G\}$. Our goal is to show that F is divisible.

Let $f \in F \setminus \{e_G\}$ and $n \in \mathbb{Z}$ be fixed. Suppose $n \cdot x = f$ has no solution $x \in F$. Since G is divisible, there is then a solution $x \in G \setminus F$. Therefore x has finite order χ, whence $e_G = n\chi \cdot x = \chi \cdot f$ contradicts that f has infinite order.

Thus F is divisible. Since G has no divisible, non-trivial, proper subgroups, this implies $F = G$, contradicting that G is not torsion free. ⊣

Claim 2

There is some prime $p \in \mathbb{N}$ such that the order of every $g \in G$ is a power of p.

Proof .:.

For each prime $p \in \mathbb{N} \setminus \{0\}$ let $P_p = \{g \in P : \exists n \in \mathbb{N}(p^n \cdot g = e_G)\}$. This is a subgroup $P_p \leqslant G$, since if $g, h \in P_p$, then for $p^{n_g} \cdot g = p^{n_h} \cdot h = e_G$, we have

$$p^{n_g+n_h}(g-h) = p^{n_h} \cdot e_G - p^{n_g} \cdot e_G = e_G.$$

By Claim 1, all elements have finite order. In particular, applying the Sylow theorems to any $\{e_G\} < \langle g \rangle < G$, not all P_p are trivial.

Let $p > 0$ be the least such that $P_p \neq \{e_G\}$. We will show that P_p is divisible, implying that $P_p = G$, and hence the claim.

Fix $g \in P_p \setminus \{e_G\}$ of order p^π, and let $n > 0$ be the least such that $n \cdot x = g$ has no solution $x \in P_p$. Since G is divisible, let $x \in G \setminus P_p$ be a solution to $n \cdot x = g$ with order χ. Thus

$$e_G = \chi n \cdot x = \chi \cdot g \quad \text{so that} \quad p^\pi \mid \chi,$$
$$e_G = p^\pi g = p^\pi n \cdot x \quad \text{so that} \quad \chi \mid p^\pi n.$$

In particular, write $\chi = p^\pi m$ for $m > 0$, and $p^\pi n = \chi w$ for $w > 0$. These two tell us that $n = mw$.

Note that $w \cdot y = g$ has a solution $y \in P_p$ by the minimality of $n > w$. Let p^γ be the order of y. Again, we have that

$$e_G = p^\pi g = p^\pi w \cdot y$$

so that $p^y \mid p^\pi w$. This implies that w is a power of p. By the same argument, m is a power of p. Thus $n = mw$ is a power of p, and finally, $\chi \mid p^\pi n$ implies that χ is a power of p, contradicting that $x \notin P_p$. Hence no such n can exist, and P_p is divisible, meaning that $G = P_p$ since G has no proper, non-trivial, divisible subgroups. ⊣

We can then conclude that G is a p-group. Define by recursion a sequence

$$x_0 = \{e_G\},$$
$$x_1 \in G \setminus \{e_G\} \text{ has order } p,$$
$$x_{i+1} \in G \text{ satisfies } p \cdot x_{i+1} = x_i.$$

Such an x_1 exists, because G is a p-group. Since G is a divisible group, such a sequence exists. Note that $\langle x_1, \ldots \rangle$ is a divisible group. Hence, because G has no proper, non-trivial, divisible subgroups, $G = \langle x_1, x_2, \ldots \rangle$. But then

$$G = \langle x_1, x_2, \ldots \rangle \cong \langle g_1, g_2, \ldots \ : \ p \cdot g_{i+1} = g_i, \ \& \ p \cdot g_1 = e \rangle \cong \mathbb{Z}(p^\infty) \dashv$$

The next several lemmas will be about getting divisible groups out of old ones.

3 • 4. Lemma

Let G be a group, and $H < G$ a subgroup. Therefore there is a maximal $K \leqslant G$ with $H \cap K = \{e_G\}$.

Proof .:.

This can be seen through Zorn's lemma: consider the set of subgroups $\mathcal{H} := \{K \leqslant G : H \cap K = \{e_G\}\}$.

Trivially, $\{e_G\} \in \mathcal{H}$. Moreover, any chain of subgroups $K_1 \leqslant K_2 \leqslant \cdots \in \mathcal{H}$ has the union as a subgroup of G of trivial intersection with H, meaning the union is in $\mathcal{H}$. Hence by Zorn's lemma, there is a $\subseteq$-maximal element $K \in \mathcal{H}$. ⊣

3 • 5. Lemma

Let G be a divisible, abelian group. If $H \leqslant G$ is divisible, there is a $K \leqslant G$ where $G = H + K \cong H \oplus K$.

Proof .:.

As per Lemma 3 • 4, let $K \leqslant G$ with $H \cap K = \{e_G\}$ be maximal. Note that then $H \oplus K \cong H + K$, and so it suffices to show $G = H + K$. We consider two cases on K.

Claim 1

If $K = \{e_G\}$, then $G = H + K = H$.

Proof .:.

Suppose $K = \{e_G\}$ but $H \subsetneq G$, and let $g \in G \setminus H$ witness this. Note that $H \cap \langle g \rangle \neq \{e_g\}$ since otherwise $\langle g \rangle$ contradicts the maximality of $K = \{e_G\}$. Hence there is some least natural number $n > 0$ where $n \cdot g \in H$.

By hypothesis, H is divisible, and so there is some $x \in H$ with $n \cdot x = n \cdot g$ so that $e_G = n \cdot (x - g)$. Note that $x - g \notin H$ so we can consider the subgroup $\langle x - g \rangle < G$. Note that $h \in H \cap \langle x - g \rangle$ iff $h = z(x - g)$ for some $z \in \mathbb{Z}$. But then $zg = zx - h \in H$. This then implies $z \geq n$. Division yields $z = qn + [z]$ for some $[z] < n$. But then we still have

$$z(g - x) = qn \cdot (g - x) + [z](g - x) = e_G + [z](g - x) = [z](g - x),$$

and hence $[z]g = [z]x - h \in H$, contradicting that n is the least such that $n \cdot g \in G$. Hence no such g exists, and $G = H + \{e_G\} = H + K$. ⊣

Claim 2

If $K \neq \{e_G\}$, then $G = H + K$.

Proof .:.

Suppose $G \neq H + K$. Note that the quotient $H \cong (H + K)/K < G/K$ is a subgroup. By Lemma 3 • 4, there is a maximal $M \leqslant G/K$–and by the third isomorphism theorem, a $C/K \leqslant G/K$ where $K \leqslant C \leqslant G$–where

$$\{e_{G/K}\} = \frac{H + K}{K} \cap \frac{C}{K} = \frac{(H \cap C) + K}{K}.$$

Hence $H \cap C \subseteq K$ so that $H \cap C \subseteq H \cap K = \{e_G\}$. Since $K \leqslant C$ is maximal, $C = K$. But since $(H + K)/K \cong H$, the same proof as in Claim 1 applies to tell us that $C/K = K/K = \{e_{G/K}\} \ncong \{e_G\}$, a contradiction. ⊣

In either case, $G = H + K$, which is isomorphic to $H \oplus K$ since $H \cap K = \{e_G\}$. ⊣

3 • 6. Lemma

Let G be a divisible, abelian group, and $H \leqslant G$ a subgroup. Therefore G/H is divisible.

Proof .:.

G/H is a group since G is abelian so that any subgroup $H \leqslant G$ is normal in G.

Let $g + H \in G/H$, and $n \in \mathbb{N}$. Since G is divisible, $n \cdot x = g$ has a solution $x \in G$. But because G is abelian, it follows that $n \cdot (x + H) = n \cdot x + H = g + H$. Hence G/H is divisible. ⊣

3 • 7. Lemma

Let G be an infinite, divisible, abelian group. Therefore there is a subgroup $0 < H \leqslant G$ with no divisible subgroup $\{e_G\} < K \leqslant H$.

Proof .:.

Consider the set $\mathscr{H} = \{\{e_G\} < H \leqslant G : H \text{ is divisible}\}$, which is non-empty since $G \in \mathscr{H}$ and $G \neq \{e_G\}$. We will apply Zorn's Lemma to $\mathscr{H}$ ordered by reverse-inclusion: the maximal elements are $\subseteq$-minimal. Consider any chain $\{H_n : n < \kappa\}$ of length κ in $\mathscr{H}$: for all $\alpha, \beta < \kappa$,

$$\alpha < \beta \to H_\beta < H_\alpha.$$

By Lemma 3 • 4, for each $n < \kappa$, there is a $C_n \leqslant G$ where $G \cong H_n \oplus C_n$. Since the H_ns are decreasing, and $C_n \cap H_n = \{e_G\}$ for all $n < \kappa$, these C_ns are increasing: for all $\alpha, \beta < \kappa$,

$$\alpha < \beta \to C_\alpha < C_\beta.$$

By Lemma 3 • 6, each $C_n \cong G/H_n$ is divisible. Hence the union $C = \bigcup_{n<\kappa} C_n$ is also divisible. Therefore, by Lemma 3 • 5, there is an $H \leqslant G$ where $G = H + C \cong H \oplus C$. By Lemma 3 • 6, H is divisible. Moreover, $H < H_\alpha$ for each α by construction of C and the C_ns.

Therefore, by Zorn's lemma, there is a maximal ($\subseteq$-minimal) element in $\mathscr{H}$. Such an element $H \leqslant G$ has no divisible subgroup $\{e_G\} < K \leqslant H$. ⊣

In essence, this Lemma 3 • 7 says that every infinite, abelian group can be broken down into divisible groups with no divisible subgroups. With this, we can actually begin to prove Recalled 3 (2 • 7), also called the divisible, abelian group structure theorem. Note that although the result is stated only for infinite groups, it's not too difficult to see that any divisible group is either trivial or else infinite. So the result can be easily generalized.

3 • 8. Result (Recalled 3)

Let G be an infinite, abelian group. Suppose G is divisible. Therefore, there are cardinals n, m (possibly infinite), and primes $p_i \in \mathbb{N}$ for $i \leq n$ where

$$G \cong \bigoplus_{i \leq n} \mathbb{Z}(p_i^\infty) \oplus \bigoplus_m \mathbb{Q}.$$

Proof .:.

By Lemma 3 • 5, For each $H \leqslant G$, let $C(H) \leqslant G$ be such that $G = H + C(H) \cong H \oplus C(H)$. Note that by Lemma 3 • 6, $C(H) \cong G/H$ is divisible. Similarly, for each divisible group $K > \{e_G\}$, let $M(K) \leqslant K$ be a subgroup with no non-trivial, divisible subgroup as per Lemma 3 • 7. Now define by transfinite recursion

$$H_0 = M(G)$$
$$H_\alpha = \begin{cases} M\left(C\left(\sum_{\xi<\alpha} H_\xi\right)\right) & \text{if } \sum_{\xi<\alpha} H_\alpha \neq G \\ G & \text{otherwise} \end{cases}$$

By construction, $\sum_{\xi<\alpha} H_\xi \cong \bigoplus_{\xi<\alpha} H_\xi$ for $H_\alpha \neq G$. This is because once $\sum_{\xi<\alpha} H_\alpha = G$, then $H_\gamma = G$ for all $\gamma \geq \alpha$. If $H_\alpha \neq G$, then for $\xi < \alpha$, $H_\xi \leqslant C(\sum_{\gamma<\xi} H_\gamma)$ must have trivial intersection with each H_γ for $\gamma < \xi$.

Note also that there must be some α for which $H_\alpha = G$. This is because $H + C(H) = G$, where $\{e_G\} < H < G$, implies $\{e_G\} < C(H) < G$, meaning that $M(C(H))$ exists and is non-trivial. In essence, $C_\gamma = G \setminus_{\xi<\gamma} H_\xi$ is a strictly decreasing sequence of subsets of G, which must have length less than, say, $2^{|G|}$.

So consider the least α for which this happens. We then have that $G \cong \bigoplus_{\xi<\alpha} H_\xi$ since by construction, $\sum_{\xi<\alpha} H_\xi = G$, and the argument given above tells us that for $\xi, \gamma < \alpha$, $H_\xi \cap H_\gamma = \{e_G\}$ for $\xi \neq \gamma$. But note that by Lemma 3 • 2 and Lemma 3 • 3, each $H_\gamma \in \{H_\xi : \xi < \alpha\}$ must be isomorphic to either $\mathbb{Q}$, or to $\mathbb{Z}(p_\gamma^\infty)$ for some prime $p_\gamma \in \mathbb{N}$. Hence by reordering, and taking the appropriate cardinals for the ones isomorphic to $\mathbb{Q}$, and the ones isomorphic to a $\mathbb{Z}(p^\infty)$, we can conclude

$$G \cong \bigoplus_{\xi<\alpha} H_\xi \cong \bigoplus_{i \leq n} \mathbb{Z}(p_i^\infty) \oplus \bigoplus_m \mathbb{Q} \dashv$$

References

[1] C.C. Chang and H.J. Keisler, *Model Theory*, 3rd ed., Studies in Logic and the Foundations of Mathematics, vol. 73, Dover Publications, 1990.

[2] Eoin Coleman, *Jonsson Groups, Rings and Algebras*, Irish Mathematical Society Bulletin **36** (1996), 34–45.

[3] A. Ju. Ol'shanskii, *Infinite groups with cyclic subgroups*, Doklady Akademii Nauk SSSR **245** (1979), 785–787.

[4] Greg Oman, *Jónsson and HS Modules over Commutative Rings*, International Journal of Mathematics and Mathematical Sciences **2014** (2014), 14.

[5] S. Shelah, *On a problem of Kurosh, Jonsson groups, and some applications*, Word Problems II: the Oxford Book (S. I. Adian, W. W. Boone, and G. Higman, eds.), Studies in Logic and the Foundations of Mathematics, vol. 95, 1980, pp. 373–394.