7. INFINITE ABELIAN GROUPS

§7.1. Examples of Infinite Abelian Groups

Many of the groups which arise in various parts of mathematics are abelian. That is, they satisfy the commutative law: $xy = yx$.

If we're working in a totally abelian environment it is usual to use additive notation: $x + y$. The reason for this is that while multiplication of various mathematical objects (matrices, functions etc.) is non-commutative, addition invariably commutes. So by using additive notation the commutativity seems perfectly natural.

In additive notation we use the symbol 0 to represent the identity element. In a particular example it might be the number 0, the zero matrix O, or the zero vector **0**, but in an abstract setting we just use the symbol 0. And the inverse of an element x is written additively as $-x$.

Powers become multiples in additive notation. And if n is the smallest positive integer such that $nx = 0$ we say that x has **order** n. If no such n exists we say

that x has **infinite order**. In the group $\mathbb{Z}_2 \oplus \mathbb{Z}$ there are elements of order 2 and elements of infinite order.

In a previous chapter we studied finitely generated abelian groups and we proved that they are direct sums of cyclic groups. But the more interesting abelian groups are the ones that are not just infinite, but are infinitely generated. Some are direct sums of cyclic groups (with infinitely many direct summands) but many others have a more complicated structure, including some very familiar examples.

Many of these can be found within the complex number field, either as groups under addition or under multiplication. Under addition we have the group $\mathbb{C}$ of all complex numbers. It has many interesting subgroups, such as the group $\mathbb{R}$ (of real numbers), $\mathbb{Q}$ (of rational numbers) and $\mathbb{Z}$ (integers), plus many, many more. Other examples occur as quotients of these, most notably the group $\mathbb{Q}/\mathbb{Z}$.

Under multiplication we must exclude zero. We have the group $\mathbb{C}^{\#}$ of all non-zero complex numbers, $\mathbb{R}^{\#}$ (non-zero real numbers), $\mathbb{R}^{+}$ (positive reals), $\mathbb{Q}^{\#}$ (non-zero

rationals) and $\mathbb{Q}^+$ (positive rationals). Of course the non-zero integers do *not* form a group!

Some more exotic examples can be constructed as groups of sequences, where the terms are drawn from a collection of groups. This construction is called the **unrestricted direct product**.

If G_1, G_2, ... is an infinite sequence of abelian groups (written additively) we define $\oplus\Sigma G_n$ to be the set of all infinite sequences $(g_1, g_2, ...)$ with $g_n \in G_n$ for each n.

Addition is component-wise with:

$$(g_1, g_2, ...) + (h_1, h_2, ...) = (g_1 + h_1, g_2 + h_2, ...)$$

where the additions being performed in the respective G_n. We could take all the G_n to be the same group, for example:

$$\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \ldots$$

or we could make them different, for example:

$$\mathbb{Z}_p \oplus \mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^3} \times \ldots$$

Note that in the first example every element has finite order. But in the second example, even though the summands are all finite, there are elements of infinite order such as (1, 1, ...).

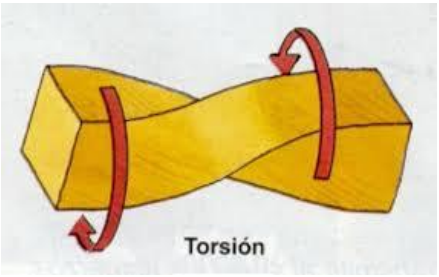
§7.2. The Torsion Subgroup

A **periodic** (or **torsion**) group is one where every element has finite order. At the other extreme we have the **torsion-free** groups where only 0 has finite order. The set of elements of finite order in the abelian group G

is denoted by **τG** and is known as the **torsion subgroup** of G. (The following theorem shows that it's indeed a subgroup.) So G is periodic if τG = G and torsion-free if τG = 0, meaning {0}. A group that is neither, such as $\mathbb{Z}_2 \oplus \mathbb{Z}$, is called **mixed**.

Theorem 1: (1) τG is a subgroup of G
(2) G/τG is torsion-free.

Proof: (1) Clearly 0 has finite order and if $ng = 0$ then $n(-g) = 0$. It remains, for the first part, to show that G is closed under addition.



If $g, h \in \tau G$ the for some $m, n \in \mathbb{Z}^+$, $mg = 0$ and $nh = 0$. Since $mn(g + h) = 0$, $g + h \in \tau G$.

(2) Suppose $g + \tau G$ is an element of finite order in G/τG. Then for some $n \in \mathbb{Z}^+$,
$n(g + \tau G) = \tau G$. Thus $ng \in \tau G$ and so for some $m \in \mathbb{Z}^+$, $m(ng) = (mn)g = 0$. Hence $g \in \tau G$ and so $g + \tau G$ is the zero coset τG.

Examples 1:
(1) $\mathbb{Q}$ and $\mathbb{Z}$ are torsion-free.
(2) Finite groups are periodic.
(3) $\mathbb{R}^{\#}$, the group of non-zero real numbers under multiplication is a mixed group. Because we use

multiplicative notation for this group, x has finite order if and only if $x^n = 1$ for some positive integer n. Hence $t\mathbb{R}^\# = \{\pm 1\}$.

(4) The torsion subgroup of $\mathbb{R}/\mathbb{Z}$ is $\mathbb{Q}/\mathbb{Z}$.

If G is finitely-generated, and so a direct sum of cyclic groups, τG is the direct sum of those cyclic factors that are finite. In such cases therefore τG is a direct summand of G, meaning that $G = \tau G \oplus H$ for some subgroup H.

Example 2: If $G = \mathbb{Z}_{60} \oplus \mathbb{Z}_{100} \oplus \mathbb{Z} \oplus \mathbb{Z}$ then

$$\tau G = \{(x, y, 0, 0)\} \cong \mathbb{Z}_{60} \oplus \mathbb{Z}_{100} \text{ and}$$

$$G = \tau G \oplus H \text{ where } H = \{(0, 0, x, y)\} \cong \mathbb{Z} \oplus \mathbb{Z}.$$

The torsion subgroup is a direct summand in many cases even when the group is not a direct sum of cyclic groups.

Example 3: $\tau\mathbb{Q}^\# = \{\pm 1\} \cong \mathbb{Z}_2$ and $\mathbb{Q}^\# = \tau\mathbb{Q}^\# \oplus \mathbb{Q}^+$.
Note that $\mathbb{Q}^+$ is torsion-free.

While it is very often the case that the torsion subgroup is a direct summand there are cases where it is not. Before we exhibit such an example we'll define another useful subgroup. Recall that if G is an abelian group nG = $\{ng \mid g \in G\}$.

The **prime subgroup** is defined to be:

$$\wp G = \cap pG,$$

with the intersection taken over all primes p.

Example 4: $\wp\mathbb{Z} = 0$ and $\wp\mathbb{Q} = \mathbb{Q}$.
When it comes to an abelian group G that is written multiplicatively we need to rewrite $\wp$G as $\cap G^p$.
If $G = \mathbb{R}^{\#}$, the group of non-zero real numbers under multiplication, then $G^p = G$ if p is an odd prime (all real numbers have a p-th root if p is odd) but $G^2 = \mathbb{R}^+$ and so $\wp\mathbb{R}^{\#} = \mathbb{R}^+$.

Theorem 2: Let $G = \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_{11} \oplus \ldots$, the unrestricted direct sum of one copy of $\mathbb{Z}_p$ for each prime p. The elements of G are infinite sequences the form:

$$(x_2, x_3, x_5, \ldots) \text{ where each } x_p \in \mathbb{Z}_p$$

then tG is not a direct summand of G.
Proof: Note that G is not periodic since, for example, (1, 1, 1, …) has infinite order. In fact tG is the set of all (x_2, x_3, x_5, …) where only finitely many x_p's are non-zero.

Clearly $\wp$G = 0. We shall show that $\wp(G/\tau G) \neq 0$.
Let x = (1, 1, ...) and let p be a prime.
For all primes $q \neq p$ there exists an integer x_q such that $px_q \equiv 1 (\text{mod } q)$. Define the missing x_p to be 0 and let

$$y_p = (x_2, x_3, x_5, x_7, x_{11}, \ldots).$$

Then py_p differs from x in just one position and so

$$p(y_p + \tau G) = x + \tau G.$$

It follows that $x + \tau G$ is a non-zero element of $\wp(G/tG)$. But since $\wp G = 0$, $G/\tau G$ cannot be isomorphic to a subgroup of G. This means that τG cannot be a direct summand of G, for if $G = \tau G \oplus H$ then $G/\tau G \cong H$.

§7.3. Divisible Groups

An abelian group *G* is **divisible** if $nG = G$ for all $n \in \mathbb{Z}^+$. The multiplicative version of divisibility is $G^n = G$ for all $n \in \mathbb{Z}^+$, meaning that every element has *n*'th roots for all *n*.

Example 5: No finite abelian group is divisible. Among the familiar infinite abelian groups, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}^\#$ and $\mathbb{R}^+$ are divisible but $\mathbb{R}^\#$, $\mathbb{Q}^+$ and $\mathbb{Z}$ are not. For example, -1 has no square roots in $\mathbb{R}^\#$, 2 has no square roots in $\mathbb{Q}^+$ and 3 is not divisible by 2 in $\mathbb{Z}$.

Theorem 3: A quotient of a divisible group is divisible.
Proof: Suppose *G* is divisible and $H \leq G$. Let $gH \in G/H$ and $n \in \mathbb{Z}^+$.
Since G is divisible
$g = nh$ for some $h \in H$ and hence $g + H = n(h + H)$. Hence G/H is divisible.

Example 6: $\mathbb{Q}/\mathbb{Z}$ is divisible. This is our first example of a periodic divisible group.
It's periodic because, if $q = m/n \in \mathbb{Q}$, then $nq \in \mathbb{Z}$ and so $n(q + \mathbb{Z}) = \mathbb{Z}$.

A subgroup of a divisible group needn't be divisible. For example $\mathbb{Z}$ is a subgroup of $\mathbb{Q}$ but, while $\mathbb{Q}$ is divisible, $\mathbb{Z}$ is not. So the class of divisible groups is closed under quotients, but not under subgroups. It is, however, closed under sums.

Theorem 4: The sum of two divisible subgroups of an abelian group is divisible.
Proof: Suppose $H, K \leq G$ where H, K are divisible.
Let $g = h + k$ where $h \in H$ and $k \in K$.
Let $n \in \mathbb{Z}^+$.
Then $h = ny$ and $k = nz$ for some $y \in H$, $z \in K$.
Thus $g = n(y + z)$.

In a similar way we can show that the sum of any collection of divisible subgroups is divisible. We define the **divisible subgroup** of an abelian group G, to be the sum of all the divisible subgroups of G and we denote it by $\delta\mathbf{G}$. If $\delta G = \{0\}$ we say that G is **reduced**.

Example 7: $\delta\mathbb{R}^{\#} = \mathbb{R}^+$. This is because, for every integer n, every positive real has an n'th root while no negative real has square roots in $\mathbb{R}^{\#}$. Also $\delta\mathbb{Q}^{\#} = \{0\}$ so $\mathbb{Q}^{\#}$ is reduced.

I proved that τG is not always a direct summand of G. What about δG? The answer is a qualified "yes". I shall prove that for every abelian group G, δG is a direct

summand, meaning that $G = \delta G \oplus H$ for some subgroup H.

So what do I mean by saying that the answer is a *qualified* "yes". The reason is that the theorem depends on something called **Zorn's Lemma**. Now no-one has ever proved that Zorn's Lemma is true. So why are we justified in assuming it? Well, no-one has ever proved it false. So what?

Well, it has been proved that **no-one can ever prove that it is true** and also it has been proved that **no-one can ever prove it to be false.**

It is an *undecidable* statement. You are logically free to assume it or deny it. Like the majority of mathematicians I choose to assume it. Therefore I can prove the statement about δG always being a direct summand.

This result takes us right down to the very foundations of mathematics. We must now confront the question "how do we know that something in mathematics is true?"

§7.4. Truth in Mathematics

The great thing about mathematics is that you always know where you stand. Everything in mathematics is either true or false. If it's true, you know it is true because you can prove it. It's not like religion where you have to believe something that you can't prove.

If only things were this simple. It's true that mathematics validates theorems by providing proofs, but remember that to begin with we have to agree on the logic that underlies it all. And even then, every statement in mathematics depends on certain fundamental assumptions. You can't prove something out of nothing.

Let's start with logic. We take this for granted. We assume that every statement is either true or false, and that no statement can be both. But what is a statement? Clearly questions or commands can't be considered as statements. Now we think we know what a statement is. It is a sentence that asserts something.

However the sentence "This sentence is false" appears to be a statement. Yet a moment's thought will reveal that if it is true it is false and if it's false then it's true. So we have to rule it out from being a statement. But on what grounds?

Perhaps we should rule it out on the grounds of self-referentiality. It is saying something about itself. So we should rule out self-referential statements.

But you can get two or more "statements", none of which refers to itself. Yet, taken together there may be self-referentiality. So we have to rule out self-referentiality, either direct or indirect.

But consider the following infinite list of "statements".

1. ONE OF THE NEXT STATEMENTS IS FALSE
2. ONE OF THE NEXT STATEMENTS IS FALSE
3. ONE OF THE NEXT STATEMENTS IS FALSE
……

Here I've abbreviated them so that each can fit on one line. What I mean is by each of these statements is that at least one of the statements that follow it is FALSE.

There is certainly no self-referentiality here, either direct or indirect. These appear to be identical copies of the same statement, but since 'the next statements' refers to an ever decreasing list they are not all equal. Each statement says something about the following ones but none, either directly or indirectly, say anything about themselves.

Case I Statement 1 is TRUE: Then for some $m > 1$ statement m is FALSE. Now statement m being FALSE it follows that statement n is TRUE for all $n > m$.

In particular statement $n + 1$ is TRUE. So for some $k > n + 1$, **statement k is FALSE**.

But $k > n + 1 > n > m$. Hence, by what I said earlier, **statement k is TRUE**. This is a contradiction. But don't panic. We still have Case II.

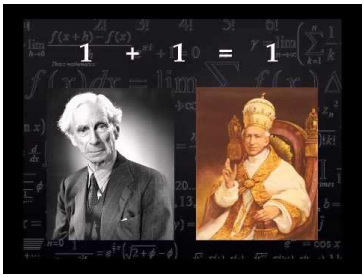
Case II Statement 1 is FALSE:
Hence for all $n > 1$, statement n is TRUE.
In particular statement 2 is TRUE.
Hence for some $m > 2$, statement m is FALSE.

Again this gives a contradiction!

This is an example of the pitfalls that are possible with logic.

However we're mathematicians, not logicians, and so we'll assume that we avoid such paradoxes as the one above. Every proof in mathematics is finite, which avoids the above sort of paradox, and if we avoid self-referential statements we should be OK. But if a contradiction arises in mathematics that we believe is not due to shonky logic, then we are in real trouble!

Now a contradiction is something that cannot be allowed in mathematics. In ordinary life we somehow live with contradictions but in mathematics, if just a single contradiction is allowed in one can prove everything.



Bertrand Russell was once challenged about this claim. "Assuming that 1 + 1 = 1 prove that you are the Pope," he was asked. Russell gave an argument along the following lines:

Suppose that 1 + 1 = 1.
Now by definition, 1 + 1 = 2.
Therefore 1 = 2.
The Pope and I are two people.
Therefore the Pope and I are one person.
Therefore I am the Pope!

So although we're ignoring potential difficulties with our logic there's an even bigger problem with our fundamental assumptions about sets. Set theory provides a suitable foundation for mathematics. Numbers can be defined as sets, and points can be defined as pairs of numbers. In fact it's possible to define every mathematical concept as a set. The elements of these sets will be sets, and so on. Don't we have to have some actual "things" to start with? Not really, it can all be created out of nothing.

The empty set $\varnothing$ is a thing that we can consider as being the number 0. We can then define 1 as {0}, 2 as {0, 1}, 3 as {0, 1, 2} and so on. It might seem a very strange way to define positive integers, but notice that the set that defines the integer *n* does have *n* elements. It is possible to define addition and multiplication of these 'integers' and to prove the standard facts about them.

It would take too long to describe how we can define negative integers, rational numbers, real and complex numbers. It can be done, and all these numbers will be sets of sets of sets, … all built up from the empty set.

It all sounds very biblical. In the beginning was the empty set. On the first day God created 1 as {0} etc. Or perhaps this makes you think of the big bang in which the universe begins with something very small.

It is possible to define functions of a complex variable, infinite series, polygons – indeed everything that can be talked about in mathematics can be considered as

a set of sets of sets. And all theorems in mathematics can be proved from these definitions.

This may not be the best way to learn mathematics. Mathematical intuition is a very useful tool. But if you are interested in whether it is all really true then you can fall back on this very rigorous development.

In the nineteenth and early twentieth centuries mathematicians were concerned with the foundations of the subject, and philosophers were concerned with the nature of truth. They developed mathematics on the basis of set theory. There was basically only one axiom about sets that needed to be used to create this mighty edifice.

Axiom of Extensionality: For every property P there is a set that consists of all sets that have that property. In symbols: $\{x \mid Px\}$ is always a set. (Here Px means 'x has the property P')

The empty set is a set because it's $\{x \mid x \neq x\}$.
Here Px = '$x \neq x$'.

$\{a, b\}$ is a set because it's $\{x \mid x = a \text{ or } x = b\}$.

We can define $x^+ = \{x, \{x\}\}$ and hence we can define the integers by considering n^+ as $n + 1$ (though addition and multiplication would yet have to be defined).

In the early 1900s as the great philosopher Frege was preparing the second volume of his book on the

foundations of mathematics, building everything on the basis of the axiom of extensionality. But just before it was published, the noted philosopher Bertrand Russell wrote to him pointing out the following paradox, now known as Russell's Paradox.

Russell's Paradox:
Let $S = \{x \mid x \notin x\}$.
Suppose $S \in S$. Then $S \notin S$, a contradiction.
Suppose $S \notin S$. Then $S \in S$, a contradiction.

The contradiction that arises from Russell's Paradox shows that the foundation which underpinned Frege's book was invalid. The book had to be withdrawn from publication. Mathematics was in danger of collapsing! A few mathematicians, those interested in the foundations of mathematics, tried to prop it up. Most mathematicians simply ignored the problem and just got on with it.

The rescue came with replacing the one axiom by a set of axioms that avoided the Russell Paradox. Several axiom systems have been proposed, but they have all been shown to be equivalent to all the others. One of the most widely used sets of axioms is the **Zermelo-Fraenkel axioms**. This allows $\{x \mid Px\}$ to be a set only for certain specified properties and these will avoid the property $x \notin x$.

Now, in stating these axioms I choose to use capital letters. When you first learnt about sets you may have

used capital letters to denote sets and lower case letters to denote elements. But this distinction is artificial. To do things properly we have to acknowledge that in mathematics all objects can be considered as sets. But properties are not sets and therefore I will use the CASTELLAR font to denote properties. So $\mathbb{P}$ is a property.

Sets are nouns and properties are adjectives. We tend to think that every adjective can be turned into a noun. The adjective 'beautiful' can be made into the noun phrase 'beautiful people' . But the thrust of the Russell Paradox is that not every adjective can be turned into a noun. There are properties that don't correspond to sets.

Zermelo-Fraenkel (ZF) Axioms:

(1) $0 = \{X \mid X \neq X\}$ is a set.

(2) If A, B are sets then so is

$$\{A, B\} = \{X \mid X = A \text{ or } X = B\}.$$

(3) If Z is a set so is $\cup Z = \{X \mid \exists Y[X \in Y \text{ and } Y \in Z]$.

For example if $Z = \{A, B, C\}$ then $\cup Z = A \cup B \cup C$.

(4) If S is a set then $\wp S = \{X \mid X \subseteq S\}$ is a set.

$\wp s$ is the set of all subsets of s.

(5) If S is a set and $\mathbb{P}$ is a property then $\{X \in S \mid \mathbb{P}X\}$ is a set. This may look like the single axiom that gave rise to the Russell Paradox, but the difference is that the elements have to belong to a set.

If we try to create the Russell Paradox we get:
Let $T = \{X \in S \mid X \notin X\}$.
Suppose $T \in T$. Then $T \notin T$, a contradiction.
Suppose $T \notin T$.
Now if $T \in S$ we get $T \notin T$, a contradiction.
But all this shows is that $T \notin S$.

So far so good. We seem to have avoided Russell's Paradox. But so far all our sets will be finite. If our set theory is going to be any good as a foundation for mathematics we'd better allow some infinite sets.

(6) There's a set that contains 0, and whenever it contains N it contains $N^+ = N \cup \{N\}$.

Finally we assume:
(7) If S is a set and $\mathbb{F}$ is a function, then $\mathbb{F}[S]$ is a set.

You've probably been taught that every function can be considered as a set. The function $f: \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ can be though of as the set

$$\{(x, y) \mid x, y \in \mathbb{R} \text{ and } y = x^2\}$$

But again there are things called generalised functions and not all of these can be considered as a set of ordered pairs. This is why I have written the function as $\mathbb{F}$ in axiom 7.

Do you agree to accept these axioms? If so you can proceed and develop most of what is called mathematics. We've avoided the Russell Paradox, but might there not

be a further paradox lurking out there that someone might one day stumble across?

In technical language we're asking "are the above seven axioms consistent?" The answer is "we don't know". Nobody has ever proved that they are consistent, and by their fundamental nature, it seems unlikely that anybody ever will. However we don't know that a proof of consistency is impossible. So another paradox might one day emerge.

Does this sound unsatisfactory? Is mathematics teetering on a precipice? Not really. If a further paradox should ever arise, mathematicians won't cut their throats, or jump off tall buildings in despair. Most will simply ignore the paradox, and those who are interested in the foundations will simply modify the axioms to get around the problem! Mathematicians have more faith in their intuition than in the logical foundations that underpin the subject.

In some ways mathematics can be likened to a religious belief. At the end of the day mathematicians can no more prove that their mathematics is true than a believer can prove the existence of God. They just have faith in their subject.

Of course the big difference is that there are almost as many different religions as there are believers, whereas by and large mathematics has a catholic unity. But that may reflect more on the different types of knowledge that mathematics and theology investigate.

Now here's where it gets interesting. A little while ago I said that on the basis of these seven axioms we can develop most of what we know as mathematics. There are some theorems that require us to go a step further – to assume a further axiom.

Axiom of Choice: Given a set of non-empty set of non-empty sets, there exists a generalised function that maps each of these sets to one of its elements.

Put more simply it says that if you have a set of boxes, and none of them is empty, you can select one object from each box. (The slight difference is that the sets that are represented by the 'boxes' might overlap and we are allowed to choose the same element many times.)

Example 7: Consider the following set of non-empty sets, where S = {A, B, C}, A = {1, 3, 7}, B = {2, 4}, and C = {1, 2, 6, 7, 8}. The Axiom of Choice asserts that it is possible to choose one element from each set and put them together in a set. This amounts to setting up a function
f:S$\rightarrow \cup$S = {1, 2, 3, 4, 6, 7, 8}. An example of such a function is f(A) = 7, f(B) = 4, f(C) = 2.
Another possibility is g(A) = 1, g(B) = 4, g(C) = 1,

Such an axiom seems intuitively obvious. If you have a collection of boxes, with at least one ball in each, it's certainly possible to choose one ball from each box. Indeed the axiom of choice is both true and obvious if

there are only finitely many sets from which to choose. But is it possible to make infinitely many choices, or even uncountably many?

Even if one cannot prove the Axiom of Choice it seems a harmless enough assumption to make. But be warned, one of its consequences is highly non-intuitive. One can prove, using the Axiom of Choice, that a solid sphere can be cut up into a small number of pieces and reassembled to form two complete solid spheres, each the same size as the one you started with!

But before you say that this contradicts the principle of conservation of volume remember that volumes can't be meaningfully assigned to every subset of $\mathbb{R}^3$. The 'pieces' we're talking about are not the sort one could make with a sharp knife. They are highly fragmented, like the 'piece' that consists of those points whose coordinates are rational numbers.

We don't know whether the Axiom of Choice is true or false, but what has been shown is that no proof or disproof is logically possible! In technical language it has been shown that the Axiom of Choice is consistent with, and independent of, the other seven axioms of set theory.

"Consistent with" means that if you accept the Axiom of Choice and a paradox ever does arise, it would have done so without the Axiom of Choice. "Don't blame me" it would say, pointing to the other axioms, "it must be their fault".

"Independent of" means that the negation of the Axiom of Choice is also consistent with the other seven axioms.

Should one accept the Axiom of Choice? Does it mean that there are two mathematical 'sects', those who believe in the Axiom of Choice and those who deny it? As far as I know there are no mathematical atheists (if that is the right word – if there were such mathematicians we would have to coin a word). There are mathematical believers and mathematical agnostics. Oh, and as with religious faith there is the majority of those who just ignore the question. Believers in the Axiom of Choice are happy to use it on aesthetic grounds. It makes for cleaner sounding theorems. The Axiom of Choice agnostics bend over backwards not to use it.

There are many other statements in set theory that are undecidable. These have to be taken as additional axioms, or rejected depending on personal taste.

So do we have as many varieties of mathematics as there are religions or denominations? Possibly. But there's an enormous overlap between these alternative mathematics. The fact that you've never encountered this problem before is because all the mathematics you've ever learnt is common to all these mathematicsl 'sects'. Indeed all the mathematical creeds must inevitably agree on any fact involving a specific concrete mathematical example. Essentially they only differ in the form in which

their theorems are stated (and then only in a tiny minority of theorems).

Under one assumption a theorem might need to be stated in a very complicated way, while under the alternative assumption it may be stated more cleanly. But on the specific examples covered by those theorems they must agree.

Rest assured that building is going to collapse because the engineer believes, or doesn't believe, in the Axiom of Choice. In the end it comes down simply to aesthetics! The version based on the Axiom of Choice is usually nicer than that based on its denial.

§7.5. Zorn's Lemma

We shall be assuming the Axiom of Choice, but in a form called Zorn's Lemma. Zorn's Lemma has been proved to be equivalent to the Axiom of Choice. Each can be used to prove the other. Zorn's Lemma has to do with 'partially ordered sets'.

I will drop back into the 'upper case – lower case' notation that we have been used to. And I won't be using fancy fonts for properties, relations and functions because in what follows all of these can be thought of as sets. In particular I will use the familiar notation xRy to denote the fact that x has the relation R with y.

A **partially ordered set** is a set, S, on which there is a relation R which satisfies the following three properties:

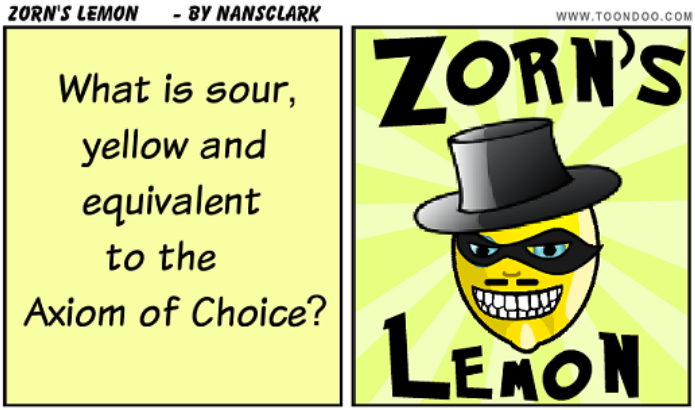
(1) **Reflexive:** $x\mathrm{R}x$ for all $x \in \mathrm{S}$;
(2) **Anti-symmetric:** $x\mathrm{R}y$ and $y\mathrm{R}x$ imply $x = y$;
(3) **Transitive:** $x\mathrm{R}y$ and $y\mathrm{R}z$ imply $x\mathrm{R}z$.

The standard example is the natural $\leq$ ordering on the real numbers but a more important example is the subset relation, $\subseteq$, among sets.

In fact we will use the familiar notation $x \leq y$ even if the relation has nothing to do with the size of real numbers, and $x < y$ will mean $x \leq y$ and $x \neq y$.

If $\leq$ is a partial ordering on a set S and $x, y \in \mathrm{S}$ with $x < y$, we'll say that y is **larger than** x. A **maximal element** one for which nothing in S is larger. A **largest element** is one which is larger than every other element. If there's a largest element it's clearly maximal and there's at most one largest element. On the other hand there can be more than one maximal element, in which case, there's no largest.

Example 8: If S is the set of proper subgroups of $\mathbb{Z}$ then $p\mathbb{Z}$ is maximal if and only if p is prime and so S has no largest. This is because the subgroups of $\mathbb{Z}$ all have the form $n\mathbb{Z}$, and $m\mathbb{Z} \subseteq n\mathbb{Z}$ if and only if $n \mid m$. But if S is now the set of *all* subgroups of $\mathbb{Z}$ then $\mathbb{Z}$ itself is the (unique) largest element of S.



A partially ordered set, S, is a **chain** if for every pair of distinct elements of *S* one is larger than the other. A subset, T, of a partially ordered set, S, has an **upper bound** *u* if *u* is greater than every element of T. The upper bound needn't be an element of the subset, but if it is, it's its largest element.

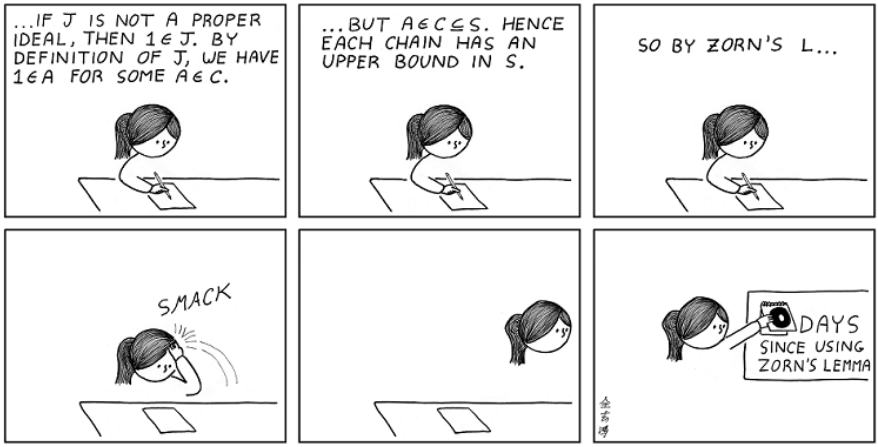
Example 9: The real numbers, under the partial ordering ≤, is a chain. The subset $\mathbb{Z}$ doesn't have any upper bounds in $\mathbb{Q}$. The open interval (0, 1) in $\mathbb{R}$ has no maximum element but has many upper bounds, of which 1 is the least upper bound.

Zorn's Lemma: Every partially ordered set in which every chain has an upper bound has a maximal element.

An argument that makes Zorn's Lemma plausible runs along the following lines. "If an element isn't

maximal there's a larger one. Either it is maximal or there's an element that's even larger. Continuing in this way we get an infinite chain which, by assumption, has an upper bound. Either it is a maximal element or there's an element larger still. Then we start all over again. Eventually we must reach a maximal element."

If you feel that this argument falls short of the rigour we've come to expect from a mathematical proof, you're right. In fact Zorn's Lemma *cannot* be proved! But nor can its negation! For it has been proved to be consistent with, yet independent of, the other axioms of set theory.



§7.6. Divisible Subgroups are Direct Summands

We now come to a quite deep theorem. Funnily enough the proof has 39 steps. Remember the proof of the fact that groups of order 2*p* are cyclic or dihedral? However don't think that every deep proof in group theory consists of 39 steps!

This proof needs Zorn's Lemma to prove it. It's up to you whether or not you're prepared to accept Zorn's Lemma (which is really an axiom rather than a lemma) or its equivalent, the Axiom of Choice. You are logically free to reject it, but this is really a very nice theorem and it would be a pity not to have it.

But is it really true? Well, consider the following meta-logical argument. You'll never encounter a specific infinite abelian group where the divisible subgroup is *not* a direct summand. Why not? Well the existence of such a counter example would mean that the theorem is false and as a consequence Zorn's Lemma would be false. But as I said earlier, it has been proved that Zorn's Lemma can never be proved false.

This "proof" of Zorn's Lemma is not a proof in the true sense of the word – at least not one that can be derived from the seven basic axioms. But it's good enough for me!

Theorem 7: A divisible subgroup of an abelian group is a direct summand.

Proof: Let H be a divisible subgroup of the abelian group G. We need to find a subgroup K that such that:

- K is disjoint from H, ie $H \cap K = \{0\}$ and
- $H + K = G$.

We divide the proof into a number of parts, in which we make a large number of definitions.

(A) CHOICE OF Δ, *K*

(1) Let Δ be the set of subgroups of *G* that are disjoint from *H*.

(2) Δ is partially ordered by inclusion (that is, under the partial order $\subseteq$).

(3) Every chain in Δ has an upper bound (namely the union of all the subgroups in the chain).

(4) By Zorn's Lemma there exists a maximal element $K \in \Delta$. We shall prove that this is a suitable K. It's clear that K is disjoint from H so it remains to show that $H + K = G$.

SUPPOSE THAT H + K is a proper subgroup of G. What we want now is a contradiction.

(B) CHOICE OF K_1

(4) Choose $x \in G$ such that $x \notin H + K$. (Possible because of our assumption.)

(5) Let $K_1 = K + \mathbb{Z}x$.

(6) Therefore K is a proper subgroup of K_1.

(7) Hence $K_1 \not\subseteq \Delta$. (If it was then K is not maximal.)

(8) Therefore K_1 is not disjoint from H and so $K_1 \cap H$ contains a non-zero element.

(C) CHOICE OF *g*, k_0, r, *n*, *h*, *k*

(9) Choose $0 \neq g \in K_1 \cap H$.

(10) Hence $g \in H$.

(11) So $g = k_0 + rx$ for some $k_0 \in K$, $r \in \mathbb{Z}$.

(12) Therefore $rx = g - k_0 \in H + K$.
(As $g \in H$ and $k_0 \in K$.)

(13) Let n be the smallest positive integer such that $nx \in H + K$.

(14) Hence $n \geq 2$. (Remember that $x \notin H + K$.)

(15) Let $nx = h + k$ for $h \in H$, $k \in K$.

(D) CHOICE OF p, y, h_1, u

(16) Let p be a prime divisor of n.
(This exists because $n \neq 1$.)

(17) Let $y = \left(\frac{n}{p}\right) x$, so that $py = nx$.

(18) Let $h_1 \in H$ such that $ph_1 = h$. (H is divisible.)

(19) Let $u = y - h_1$.

(20) Thus $pu = py - ph_1 = py - h = nx - h = k$.

(E) DEFINITION OF K_2

(21) Suppose that $u \in K$.

(22) Hence $y = \left(\frac{n}{p}\right) x = h_1 + u \in H + K$.

(As $h_1 \in H$ and $u \in K$.)

(23) This contradicts the minimality of n.

(24) Therefore $u \notin K$.

(25) Let $K_2 = K + \mathbb{Z}u$.

(26) Therefore K is a proper subgroup of K_2.

(27) Hence K_2 is not disjoint from H, that is, $K_2 \cap H$ contains a non-zero element.

(This is because K_2 is bigger than K and so can't be in Δ.)

(F) DEFINITION OF h_2, k_2, m

(28) Let $0 \neq h_2 \in K_2 \cap H$.

(29) Hence $h_2 \in K + \mathbb{Z}u$. (Since $h_2 \in K_2$.)

(30) Therefore $h_2 = k_2 + mu$ for some $k_2 \in K$ and some $m \in \mathbb{Z}$.

(G) p, m ARE COPRIME

(31) Suppose $p \mid m$.

(32) Therefore $mu \in K$.

(Since $pu = k \in K$.)

(33) Hence $h_2 \in K \cap H = 0$, a contradiction.

(Because k_2, $mu \in K$, $h_2 \in K$.)

(34) Thus p does not divide m.

(35) It follows that $1 = am + bp$ for some $a, b \in \mathbb{Z}$.

(H) FINAL CONTRADICTION

(36) Therefore $u = (am)u + (bp)u$.

(37) Now $amu = a(h_2 - k_2) \in H + K$ and $pu = k \in K$.

(38) Hence $u \in H + K$.

(39) So $\left(\frac{n}{p}\right) x = y = u + yh_1 \in H + K$,

a contradiction.

WARNING: In checking back to previous steps remember that (22) and (23) as well as (32) and (33) are based on further assumptions which are later shown to be contradictions. For example you can't use the statement $mu \in K$ that appears in (32) in step (37) and (38) to conclude that $u \in K$. That's why the statements that are based on these further assumptions are indented.

Theorem 8: Every abelian group is a direct sum of a divisible group and a reduced group.

Proof: By Theorems 7, $G = \delta G \oplus H$ for some H. Since $H = \delta H \oplus K$ for some K we have

$$G = \delta G \oplus \delta H \oplus K.$$

But $\delta G \oplus \delta H$ is a divisible group of G, yet δG is the largest divisible subgroup of G. Hence $\delta G \oplus \delta H = \delta G$ and so $\delta H = 0$, which means that H is reduced.

Recall that we showed that the torsion subgroup of an infinite abelian group need not be a direct summand. But for divisible groups the torsion subgroup is always a direct summand.

Theorem 9: The torsion subgroup of a divisible group is a direct summand.
Proof: Suppose G is divisible. Let $g \in \tau G$ and suppose $mg = 0$. Let $n \in \mathbb{Z}^+$. Then $g = nh$ for some $h \in G$. Since $(mn)h = 0$, h is in fact in τG. Thus τG is divisible and so by Theorem 7 it's a direct summand.

Theorem 10: A torsion-free divisible abelian group, G, is a direct sum of copies of $\mathbb{Q}$.
Proof: Suppose $g \in G$ and $m/n \in \mathbb{Q}$. Since G is divisible there exists $h \in G$ such that $nh = g$. Since G is torsion-free, h is unique (if $nh' = g$ we'd have $n(h - h') = 0$). Define $(m/n)g = mh$. In this way we have made G into a vector space over $\mathbb{Q}$ and so it is a direct sum of copies of $\mathbb{Q}$.

Actually we've cheated a bit here. We're assuming that every vector space over $\mathbb{Q}$ is a direct sum of copies of $\mathbb{Q}$. This is equivalent to the statement that every vector space has a basis. Probably you have only ever seen this proved for finite-dimensional vector spaces. It can be proved for arbitrary vector spaces but only if we assume Zorn's Lemma (or equivalently, the Axiom of Choice).

§7.7. Sylow *p*-Subgroups

If p is a prime, a ***p*-group** is one where the order of every element is a power of p. A p-group need not be finite, but if it is, its order must be a power of p.

The **Sylow p-subgroup** of a periodic abelian group G is the set of all elements whose order is a power of p. We shall denote it by $\mathbf{Syl}_p\mathbf{(G)}$. (It's easy to check that this set is a subgroup.)

Theorem 11: Every periodic group is the direct sum of its Sylow subgroups.

Proof: Let G be periodic and let $g \in$ G.

Suppose g has order $n = p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k}$ where the p_i are distinct primes and each $n_i \geq 1$.

For each i let $q_i = n/p^i$.

These q_i are coprime and so, for some integers h_i, we have $h_1q_1 + h_2q_2 + \ldots + h_kq_k = 1$.

For each i let $g_i = (h_iq_i)g$.

Then $g = g_1 + g_2 + \ldots + g_k$ and each $g_i \in \mathrm{Syl}_{p_i}(G)$.

§7.8. The Prüfer Groups

The groups $\mathbb{Q}/\mathbb{Z}$ and $\mathbb{R}/\mathbb{Z}$ are two very important examples of infinite abelian groups. The group $\mathbb{R}/\mathbb{Z}$ consists of real numbers modulo 1. There's a representative of each coset in the interval [0, 1) and it's usual to represent these cosets by their representative. We

do a similar thing for $\mathbb{Q}/\mathbb{Z}$ with the representatives consisting of the rational numbers in this interval.

Example 10: In $\mathbb{Q}/\mathbb{Z}$, or $\mathbb{R}/\mathbb{C}$:

$\frac{1}{2} + \frac{1}{3} = \frac{5}{6}$ (as in ordinary arithmetic)

$\frac{3}{4} + \frac{2}{3} = \frac{5}{12}$ (since in ordinary arithmetic their sum is $\frac{17}{12} = 1\frac{5}{12}$

$7\left(\frac{3}{7}\right) = 0.$

$7\left(\frac{1}{\sqrt{2}}\right) = \frac{7}{\sqrt{2}} - 4$ (since $4 \leq \frac{7}{\sqrt{2}} < 5$).

Clearly every element of $\mathbb{Q}/\mathbb{Z}$ has finite order. All other elements of $\mathbb{R}/\mathbb{Z}$ have infinite order.

The **circle group**, T, is the subgroup of $\mathbb{C}^{\#}$ consisting of those complex numbers with modulus 1. They're represented in the complex plane by the points on the unit circle. This group is isomorphic to $\mathbb{R}/\mathbb{Z}$ by the map f: $\mathbb{R}/\mathbb{Z} \to$ T defined by $f(x) = e^{2\pi ix}$.

The image of the subgroup $\mathbb{Q}/\mathbb{Z}$ under this isomorphism is $\{e^{2\pi im/n} \mid m \in \mathbb{Z}, n \in \mathbb{Z}^+\}$ which is the set of roots of unity. We'll show later that $\mathbb{R}/\mathbb{Z}$ is isomorphic to the direct sum of one copy of $\mathbb{Q}/\mathbb{Z}$ and uncountably many copies of $\mathbb{Q}$. Most of the interest in $\mathbb{R}/\mathbb{Z}$ lies in its $\mathbb{Q}/\mathbb{Z}$ factor, so we'll concentrate on that.

For each prime p, the **Prüfer p-group** is defined to be the Sylow p-subgroup of $\mathbb{Q}/\mathbb{Z}$, that is, the set of all elements of $\mathbb{Q}/\mathbb{Z}$ whose order is a power of p. It's denoted by $\mathbb{Z}_{p^\infty}$.

Example 11: Denoting each coset by its representative in the interval [0, 1):
$\mathbb{Z}_{2^\infty}$ = {1/2, 1/4, 3/4, 1/8, 3/8, 5/8, 7/18, 1/16, ...}
$\mathbb{Z}_{3^\infty}$ = {1/3, 2/3, 1/9, 2/9, 4/9, 5/9, 7/9, 8,9, 1/27, ...}

We'll show later that $\mathbb{Z}_{p^\infty}$ needs infinitely many generators. It has a presentation

$$\langle x_1, x_2, \ldots \mid px_1 = 0, px_2 = x_1, px_3 = x_2, \ldots \rangle.$$

The subgroup generated by a finite number of these generators is a finite cyclic group, because each one generates all preceding ones. What is remarkable about these Prüfer groups is that these finite subgroups are its only proper subgroups. So here we have an infinite, non-cyclic group whose proper subgroups are all finite and cyclic.

Theorem 12: Every proper subgroup of $\mathbb{Z}_{p^\infty}$ is finite and cyclic.
Proof: Let H be a subgroup of $\mathbb{Z}_{p^\infty}$. If the elements of H have a largest denominator, p^n, it's generated by $1/p^n$. If there's no largest denominator then for all n there's an element of H with denominator p^N for some $N > n$ in which case $H = \mathbb{Z}_{p^\infty}$.

Theorem 13: A divisible p-group is a direct sum of copies of $\mathbb{Z}_{p^\infty}$.

Proof: Let G be a non-trivial divisible p-group. We first show that G has a subgroup isomorphic to $\mathbb{Z}_{p^\infty}$.

Let $x_1 \in$ G have order p. Choose x_2 so that $px_2 = x_1$. Continuing in this way we construct a sequence $x_1, x_2, \ldots$ such that for each $i \geq 1$, $px_{i+1} = x_i$.

The subgroup generated by these is isomorphic to $\mathbb{Z}_{p^\infty}$, with $x_r \to r/p + \mathbb{Z}$.

This subgroup, being divisible, is a direct summand. We could simply say "continue by induction" but will the process ever terminate? What is needed is yet another appeal to Zorn's Lemma.

Let S denote the set of all subgroups isomorphic to $\mathbb{Z}_{p^\infty}$ and let T denote all the subsets $X \subseteq S$ in which the sum of the subgroups in X is a direct sum. T is partially ordered by inclusion and every chain has an upper bound (their union). By Zorn's Lemma T has a maximal element X. Let H be the (direct) sum of the subgroups in X. Being the direct sum of Prüfer groups, H is divisible and so $G = H \oplus K$ for some K.

If K is non-trivial it contains a subgroup, P, isomorphic to $\mathbb{Z}_{p^\infty}$. But then $X \cup \{P\} \in T$ and is larger than X, contradicting the maximality of X. Hence $K = 1$ and $G = H$ is a direct sum of copies of $\mathbb{Z}_{p^\infty}$.

Theorem 14: Every divisible group is isomorphic to a direct sum of copies of $\mathbb{Q}$ and $\mathbb{Z}_{p^\infty}$ for various primes p.

Proof: Let G be divisible. Then $G = \tau G \oplus H$ where H is torsion-free. By Theorem 10, H is isomorphic to a direct sum of copies of $\mathbb{Q}$. By theorem 4, τG is a direct sum of divisible p-groups. By theorem 13 each of these divisible p-groups is a direct sum of copies of $\mathbb{Z}_{p^\infty}$.

EXERCISES FOR CHAPTER 7

EXERCISE 1: For each of the following determine whether it is true or false.

(1) A periodic abelian group must be finite.

(2) $\mathbb{Q}^{\#}$, the group of rational numbers under multiplication, is torsion-free.

(3) If G is an infinite abelian group, tG is periodic.

(4) The non-trivial elements of G/tG have infinite order.

(5) $\mathbb{Q}/\mathbb{Z}$ is periodic.

(6) If G is an infinite abelian group then $G = tG \oplus H$ for some torsion-free subgroup H.

(7) $\mathbb{Q}/\mathbb{Z}$ is the direct sum of Prüfer groups.

(8) Zorn's Lemma cannot be proved true or false using the standard axioms of set theory.

(9) If G is an infinite abelian group then $G = dG \oplus H$ for some subgroup H.

(10) $\mathbb{R}^{\#}$, the group of non-zero real numbers under multiplication, is a divisible group.

EXERCISE 2: Find the orders of the following elements in $\mathbb{R}/\mathbb{Z}$:

(a) $\frac{3}{4} + \mathbb{Z}$; (b) $\frac{22}{68} + \mathbb{Z}$; (c) $\frac{1}{\sqrt{2}} + \mathbb{Z}$.

EXERCISE 3:

(a) What is the order of (1, 2, 3, 4, …) in the unrestricted direct sum

$$\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_5 \oplus \ldots$$

(b) What is the order of (1, 2, 4, 8, …) in the unrestricted direct sum

$$\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_{16} \oplus \ldots$$

(c) What is the order of (1, 2, 3, …, 10, 0, 0, …) in the unrestricted direct sum

$$\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_{11} \oplus \ldots$$

SOLUTIONS FOR CHAPTER 7

EXERCISE 1: (1) FALSE; (2) FALSE; (3) TRUE; (4) TRUE; (5) TRUE; (6) FALSE;
(7) TRUE; (8) TRUE; (9) TRUE; (10) FALSE.

EXERCISE 2: (a) 4; (b) 34; (c) ∞.

EXERCISE 3: (a) ∞; (b) 2; (c) 10!.