Projects (MATH0109)

Richard Hill and John Talbot

November 18, 2025

Contents

1 Introduction

This document describes the end of module projects for MATH0109 Theorem Proving in Lean. For each project there is a page or so of description of the mathematics. Each project also has an associated Lean file for you to work on.

You should choose one project and submit your edited version of the project file via Moodle. (See Moodle for details of deadline etc.)

The code for the projects is in the directory `UCLMATH0109/Projects/` where it is arranged by area of mathematics and title.

For example, the code for the Analysis project on the Cantor set can be found in: `UCLMATH0109/Projects/Analysis/CantorSet`

These projects are open-ended and vary in difficulty. Most projects have suggested extensions, and you may submit either more or less than the original outline. We encourage students to tackle something challenging, even if that means leaving parts of it incomplete.

2 Algebra (`Algebra`)

2.1 Central group extensions (`CentralGroupExtensions`)

This is a very open ended project in group theory.

Let G and K be groups and assume that K is abelian. A *cocycle* on G with values in K is a function

$$\sigma : G \times G \to K,$$

satisfying the following relation for all $x, y \in G$:

$$\sigma(x, y)\sigma(xy, z) = \sigma(x, yz)\sigma(y, z).$$

The cocycles on G with values in K form an abelian group with the operation of pointwise multiplication:

$$(\sigma_1 * \sigma_2)(x, y) := \sigma_1(x, y)\sigma_2(x, y).$$

A. If we choose a cocycle σ, then we may define a new group $\tilde{G}_\sigma$, whose elements are pairs (g, k) with $g \in G$ and $k \in K$, where multiplication is defined by

$$(g, k)(g', k') = (gg', kk'\sigma(g, g')).$$

For example, the associativity axiom is proved like this:

$$\begin{aligned}
\big((g_1, k_1)(g_2, k_2)\big)(g_3, k_3) &= (g_1g_2, k_1k_2\sigma(g_1, g_2))(g_3, k_3) \\
&= (g_1g_2g_3, k_1k_2k_3\sigma(g_1, g_2)\sigma(g_1g_2, g_3)) \\
&= (g_1g_2g_3, k_1k_2k_3\sigma(g_1, g_2g_3)\sigma(g_2, g_3)) \\
&= (g_1, k_1)(g_2g_3, k_2k_3\sigma(g_2, g_3)) \\
&= (g_1, k_1)\big((g_2, k_2)(g_3, k_3)\big).
\end{aligned}$$

The group $\tilde{G}_\sigma$ is sometimes called a *covering group* of G, or sometimes a *central extension* of G.

For example, in the case that σ is the identity element (i.e. $\sigma(x, y) = 1$ for all x, y, we have $\tilde{G}_\sigma \cong G \times K$, where $G \times K$ is the direct sum.

There is a surjective homomorphism $\pi : \tilde{G}_\sigma \to G$, taking (g, k) to g. The kernel of π is contained in the centre of $\tilde{G}_\sigma$ (the centre of a group is the set of elements which commute with all other elements of the group), and is isomorphic to K.

B. Conversely, suppose we have a group $\tilde{G}$ and a surjective homomorphism $\tilde{G} \to G$, whose kernel is isomorphic to K and is in the centre of $\tilde{G}$. Then there is a cocycle σ and an isomorphism $\tilde{G} \cong \tilde{G}_\sigma$. To define a cocycle σ, we choose for each element $x \in G$ a preimage $s(x) \in \tilde{G}$; in other words $s : G \to \tilde{G}$ is a right-inverse of π. The cocycle is defined by

$$\sigma(x, y) = s(x)s(y)s(xy)^{-1} \in \ker \pi.$$

(The cocycle σ depends on the choice of s.)

Here is the proof that $\sigma(x,y) \in \ker \pi$:

$$\begin{aligned}\pi(\sigma(x,y)) &= \pi(s(x)s(y)s(xy)^{-1}) \\ &= \pi(s(x))\pi(s(y))\pi(s(xy)^{-1}) \\ &= xy(xy)^{-1} \\ &= 1.\end{aligned}$$

and here is the proof that σ is a cocycle:

$$\begin{aligned}\sigma(x,y)\sigma(xy,z) &= (s(x)s(y)s(xy)^{-1})(s(xy)s(z)s(xyz)^{-1}) \\ &= s(x)s(y)s(z)s(xyz)^{-1} \\ \sigma(x,yz)\sigma(y,z) &= \sigma(x,yz)s(xyz)s(yz)^{-1}\sigma(y,z)s(yz)s(xyz)^{-1} \\ &= (s(x)s(yz)s(xyz)^{-1})s(xyz)s(yz)^{-1}(s(y)s(z)s(yz)^{-1})s(yz)s(xyz)^{-1} \\ &= s(x)s(y)s(y)s(z)s(xyz)^{-1}.\end{aligned}$$

The isomorphism $\Phi : \tilde{G}_\sigma \to \tilde{G}$ is the function

$$\Phi(g,k) = s(g)k = ks(g).$$

(Note that k commutes with $s(g)$ because it is in the centre of $\tilde{G}$). It's easy to show that this is a bijection; here is the proof that the map is a group isomorphism:

$$\begin{aligned}\Phi((g_1,k_1)(g_2,k_2)) &= \Phi(g_1g_2, k_1k_2\sigma(g_1,g_2)) \\ &= k_1k_2\sigma(g_1,g_2)s(g_1g_2) \\ &= k_1k_2s(g_1)s(g_2)s(g_1g_2)^{-1}s(g_1g_2) \\ &= k_1k_2s(g_1)s(g_2) \\ &= (k_1s(g_1))(k_2s(g_2)) \\ &= \Phi(g_1,k_1)\Phi(g_2,k_2).\end{aligned}$$

C. If $\tau : G \to K$ is any function, then the *coboundary* of τ is the function $\partial\tau$ defined by

$$\partial\tau(x,y) = \tau(x)\tau(y)\tau(xy)^{-1}.$$

Theorem. *$\partial\tau$ is a cocycle on G with values in K.*

Proof.

$$\begin{aligned}\partial\tau(x,y)\partial\tau(xy,z) &= (\tau(x)\tau(y)\tau(xy)^{-1})(\tau(xy)\tau(z)\tau(xyz)^{-1} \\ &= \tau(x)\tau(y)\tau(z)\tau(xyz)^{-1} \\ &= (\tau(x)\tau(yz)\tau(xyz)^{-1})(\tau(y)\tau(z)\tau(yz)^{-1}) \\ &= \partial\tau(x,yz)\partial\tau(y,z)\end{aligned}$$

□

The set of all coboundaries $\partial\tau$ is a subgroup of the group of cocycles; in fact ∂ is a homomorphism from the group $(G \to K)$ to the group of cocycles.

D. Suppose σ and σ' are two cocycles on G with values in K, which differ by a coboundary, i.e. $\sigma = \sigma' \cdot \partial\tau$ for some function $\tau : G \to K$. Then the groups $\tilde{G}_\sigma$ and $\tilde{G}_{\sigma'}$ are isomorphic.

Proof. The isomorphism is the function $\Psi : \tilde{G}_\sigma \to \tilde{G}_{\sigma'}$ defined by

$$\Psi(g, k) = (g, k\tau(g)).$$

It's easy to see that this is a bijection. It is an isomorphism by this calculation:

$$\begin{aligned}
\Psi((g_1, k_1)(g_2, k_2)) &= \Psi(g_1 g_2, k_1 k_2 \sigma(g_1, g_2)) \\
&= (g_1 g_2, k_1 k_2 \sigma(g_1, g_2)\tau(g_1 g_2)) \\
&= (g_1 g_2, k_1 k_2 \sigma'(g_1, g_2)\partial\tau(g_1, g_2)\tau(g_1 g_2)) \\
&= (g_1 g_2, k_1 k_2 \sigma'(g_1, g_2)\tau(g_1)\tau(g_2)\tau(g_1 g_2)^{-1}\tau(g_1 g_2)) \\
&= (g_1 g_2, k_1 \tau(g_1) k_2 \tau(g_2)\sigma'(g_1, g_2)) \\
&= (g_1, k_1\tau(g_1))(g_2, k_2\tau(g_2)) \\
&= \Psi(g_1, k_1)\Psi(g_2, k_2).
\end{aligned}$$

□

E. An example Let $G = \{1, x\}$ be the cyclic group of order 2, generated by an element x, and let $K = \{y^n : n \in \mathbb{Z}\}$ by the infinite cyclic group generated by an element y. Then the following is a cocycle on G with values in K:

$$\sigma(g_1, g_2) = \begin{cases} 1 & \text{if } g_1 = 1 \text{ or } g_2 = 1, \\ y & \text{if } g_1 = g_2 = x. \end{cases}$$

Theorem. *For the cocycle σ defined above, the covering group $\tilde{G}_\sigma$ is an infinite cyclic group generated by the element $(x, 1)$.*

Proof. It's trivial to check that $(x, 1)^2 = (1, y)$. We can then prove by induction that $(1, y^n) = (x, 1)^{2n}$. This implies $(x, y^n) = (x, 1)^{2n+1}$. Hence every element of $\tilde{G}_\sigma$ is a power of $(x, 1)$. □

Theorem. *The cocycle σ defined above is not a coboundary.*

Proof. Suppose $\sigma = \partial\tau$. By the result in D, the groups $\tilde{G}_\sigma$ and $\tilde{G}_1$ are isomorphic. The group $\tilde{G}_1$ is the product group $G \times K$, which has an element $(x, 1)$ of order 2. On the other hand $\tilde{G}_\sigma$ is an infinite cyclic group, so has no element of finite order apart from the identity element. This gives a contradiction. □

2.2 Dual Numbers (`DualNumbers`)

This project is quite open ended, so you can do as much or as little as you want. Parts A, B and C are independent of each other. The start of part B (the `Algebra` $\mathbb{R}$ `D` instance) is used in part D.

Roughly speaking, the dual numbers are a ring formed from $\mathbb{R}$ by adding an infinitesimally small positive number "dx". More precisely, a "dual number" is an expression of the form $a + b \cdot dx$ with $a, b \in \mathbb{R}$. We'll write D for the set of dual numbers. The dual numbers form a ring, where addition is defined by

$$(a + b \cdot dx)(a' + b' \cdot dx) = (a + a') + (b + b') \cdot dx.$$

Multiplication is defined by setting $dx^2 = 0$; in other words

$$(a + b \cdot dx)(a' + b' \cdot dx) = aa' + (ab' + ba') \cdot dx.$$

Lemma. *A dual number $a + b \cdot dx$ is invertible if and only if $a \neq 0$.*

Proof. If $(a + b \cdot dx)(a' + b' \cdot dx) = 1$ then by comparing coefficients we find $aa' = 1$. Therefore $a \neq 0$.

Conversely if $a \neq 0$, then we can check that $a^{-1} - a^{-2}b \cdot dx$ is an inverse of $a + b \cdot dx$. □

A. We can define an "ordering" on the dual numbers by defining $a + b \cdot dx \leq a' + b' \cdot dx$ to mean that either $a < a'$ or $a = a'$ and $b < b'$. It's easy to show that D satisfies the axioms of an "ordered ring" for all dual numbers r, s, t:

- $r \leq r$.
- If $r \leq s$ and $s \leq t$ the $r \leq t$.
- If $r \leq s$ and $s \leq r$ then $r = s$.
- If $r \leq s$ then $r + t \leq s + t$.
- $0 \leq 1$.
- If $0 \leq r$ and $0 \leq s$ then $0 \leq rs$.

With this definition, you can prove that the dual number dx is positive but smaller than every positive real number.

Using the ordering, we can try doing some analysis in the ring D. For example, we can define what it means for a sequence $a_n \in D$ to converge to a limit $x \in D$:

$$\forall \epsilon \in D,\ \epsilon > 0 \ \rightarrow\ \exists N \in \mathbb{N},\ \forall n \in \mathbb{N},\ N \leq n \ \rightarrow\ x - \epsilon < a_n < x + \epsilon.$$

The difference between convergence in D and the usual definition of convergence is that we can take ϵ to be infinitesimally small (for example we could take $\epsilon = dx$).

Theorem. *If $a_n \to x$ and $b_n \to y$ then $a_n + b_n \to x + y$.*

The proof is just the same as for the real numbers:

Proof. Choose any positive $\epsilon \in D$. Show that $\epsilon/2$ is positive. Hence there exist natural numbers N and M for which

$$N \leq n \quad \to \quad x - \epsilon/2 < a_n < x + \epsilon/2,$$

$$M \leq n \quad \to \quad y - \epsilon/2 < b_n < y + \epsilon/2.$$

If $\max(N, M) \leq n$, then we can deduce that

$$x + y - \epsilon < a_n + b_n < x + y + \epsilon.$$

□

In a similar way, one can prove the following:

- Limits of sequences are unique. I.e. if $a_n \to x$ and $a_n \to y$ then $x = y$.
- If $a_n \to x$ and $b_n \to y$ then $a_n b_n \to xy$.
- If $a_n \to x$ and x is invertible in D then for sufficiently large n, a_n is invertible and $a_n^{-1} \to x^{-1}$.

On the other hand, some things in D are quite different from the real numbers. You can prove the following:

Theorem. *Not every bounded increasing sequence in D converges.*

Proof. For example, the sequence

$$0,\ dx,\ 2 \cdot dx,\ 3 \cdot dx, \ldots$$

is bounded above (by 1) and increasing. If we assume that this converges to a limit x, then (taking $\epsilon = dx$) there must exist a natural number N for which

$$N \leq n \quad \to \quad x - dx < n \cdot dx < x + dx.$$

In particular we have

$$x - dx < N \cdot dx, \qquad (N + 2) \cdot dx < x + dx.$$

These two inequalities give a contradiction. □

Theorem. *Not every bounded non-empty set has a least upper bound.*

Proof. The set $\{c \cdot dx : c \in \mathbb{R}\}$ is bounded (for example all elements are less than 1. However if $a + b \cdot dx$ is an upper bound then a must be positive. But then $a/2$ is a smaller upper bound. □

Theorem. *Suppose a_n is a sequence of real numbers which converges to a limit $x \in D$ in the sense defined above. Then the limit x is a real number and all but finitely many of the terms a_n are equal to x.*

Proof. Suppose $x = u + v \cdot \epsilon$ with $v \neq 0$. By taking $\epsilon = |v| \cdot dx$ we can easily get a contradiction. Therefore $x = u \in \mathbb{R}$.
Now take $\epsilon = dx$. There is an N such that for all $n \geq N$ we have

$$x - dx < a_n < x + dx.$$

Since x and a_n are real numbers, it follows that $a_n = x$ for all $n \geq N$. □

B. The ring D is also a vector space over $\mathbb{R}$, where the scalar multiplication by a real number λ is defined by

$$\lambda \bullet (a + b \cdot dx) = \lambda a + (\lambda b) \cdot dx.$$

You can also prove that D is an algebra over $\mathbb{R}$; this means that there is a ring homomorphism $\phi : \mathbb{R} \to D$, such that

$$\lambda \bullet (a + b \cdot dx) = \phi(\lambda)(a + b \cdot dx).$$

(The ring homomorphism ϕ is defined by $\phi(\lambda) = \lambda + 0 \cdot dx$.)
Once we have defined D as an algebra over $\mathbb{R}$, lean can understand the meaning for $f(r)$ for a polynomial $f \in \mathbb{R}[X]$ and a dual number r. The notation for $f(r)$ in lean is "`aeval r f`". In particular you will be able to prove this:

Theorem. *Let f be a polynomial with real coefficients. The for any real number x we have*

$$f(x + dx) = f(x) + f'(x) \cdot dx.$$

(Here f' is the derivative of f).

Proof. The proof in general can be deduced from the case where f is the monomial x^n. In that special case, we need to prove that

$$(x + dx)^n = x^n + nx^{n-1} \cdot dx.$$

This can be proved either by induction on n or by the binomial theorem (which is `add_pow` in Mathlib). □

C. Recall that an ideal in D is a non-empty subset $I \subseteq D$, such that for all $r, s \in I$ and all $t \in D$, we have $r + ts \in I$. In particular, ideals are closed under multiplication by elements of D.

Theorem. *The ring D has only three ideals. They are 0, D and the principal ideal generated by dx.*

Proof. Let I be an ideal of D and assume that I is neither 0 nor D. Suppose that $r \in I$. If r is invertible, then every element of D is a multiple of r; hence every element of D is in I. This is a contradiction since $I \neq D$, so r cannot be invertible. Hence every element of I has the form $c \cdot dx$ for some $c \in \mathbb{R}$.

Since I is not the zero ideal, we can choose a non-zero element $c_0 \cdot dx \in I$. But then every element $c \cdot dx$ is a multiple of $c_0 \cdot dx$ by c/c_0. Therefore every element $c \cdot dx$ is in I.

We've shown that I is the set of elements of the form $c \cdot dx$, which is the principal ideal generated by dx. □

D. An automorphism of D (as an algebra over $\mathbb{R}$) is a bijective function $\sigma : D \to D$ satisfying the following properties for all $r, s \in D$ and $\lambda \in \mathbb{R}$:

- $\sigma(r + s) = \sigma(r) + \sigma(s)$,
- $\sigma(rs) = \sigma(r)\sigma(s)$,
- $\sigma(\lambda r) = \lambda\sigma(r)$.

The notation in Mathlib for the automorphisms of D is "$D \simeq_a [\mathbb{R}]D$". This is a structure whose fields consist of the actual function σ, its inverse function and proofs of axioms above. Mathlib knows that $D \simeq_a [\mathbb{R}]D$ is a group with the operation of composition of functions (you can think of this as being a bit like a Galois group, except that D is not a field).

For any non-zero real number c, we can define an automorphism σ_c of D by

$$\sigma_c(a + b \cdot dx) = a + cb \cdot dx.$$

It turns out that every automorphism of D is equal to σ_c for some $c \in \mathbb{R}^\times$. In fact the map $c \mapsto \sigma_c$ is a group isomorphism between $\mathbb{R}^\times$ and $D \simeq_a [\mathbb{R}]D$.

2.3 Free abelian groups (`FreeAbelian`)

Roughly speaking, we define a free abelian group to be an additive group isomorphic to $\mathbb{Z}^n$ for some $n \in \mathbb{N}$ (it would be more accurate to call such groups "finitely generated free abelian groups" but this takes too long to type). The aim of the project is to prove (with the definition given) that every subgroup of a free abelian group is a free abelian group.

The project is on additive commutative groups (the class AddCommGroup in Mathlib). We define a "free abelian group" as an inductive type with the following three constructors:

`zero` The zero group is a free abelian group.

`step` If G is a free abelian group then the product group $G \times \mathbb{Z}$ is a free abelian group.

`isomorphism` If G is a free abelian group and G is isomorphic to H then H is a free abelian group.

Lemma. *$\mathbb{Z}^n$ is a free abelian group.*

Proof. This is proved by induction on n. The base case is `zero` and the inductive step is `step`. □

Theorem. *Let G be an additive commutative group. Then G is a free abelian group if and only if G is isomorphic to $\mathbb{Z}^n$ for some natural number n.*

Proof. Suppose first that G is isomorphic to $\mathbb{Z}^n$. We already know from the lemma that $\mathbb{Z}^n$ is free abelian. Hence by `isomorphism` G is free abelian.

Conversely, assume that G is free abelian. We'll prove "by induction on G" that G is isomorphic to $\mathbb{Z}^n$ for some n.

`zero` If G is the zero group then G is isomorphic to $\mathbb{Z}^0$.

`step` If $G = H \times \mathbb{Z}$ and H is isomorphic to $\mathbb{Z}^n$ then G is isomorphic to $\mathbb{Z}^{n+1}$.

`isomorphism` If G is isomorphic to H and H is isomorphic to $\mathbb{Z}^n$ then G is isomorphic to $\mathbb{Z}^n$.

□

Lemma. *If G is a non-zero subgroup of $\mathbb{Z}$, then G is isomorphic to $\mathbb{Z}$.*

Proof. Since G is non-zero, it must contain a non-zero element x. Replacing x by $-x$ if necessary, we see that G must contain a positive integer. Let n be the smallest positive integer in G.

Since G is closed under addition and subtraction, all integers of the form nx are in G for $x \in \mathbb{Z}$. In fact these are all the elements of G. To see why this is true,

suppose $g \in G$. Dividing with remainder, we see that there exist integers q, r such that $g = qn + r$ and $0 \leq r < g$. Since g and qn are in G, it follows that $r \in G$, so our choice of n forces r to be zero. Hence $g = nx$.

Since $G = \{nx : x \in \mathbb{Z}\}$, there is an isomorphism $G \cong \mathbb{Z}$, which takes nx to n. □

Alternative Proof. Since G is a subgroup of $\mathbb{Z}$, it follows easily that $ng \in G$ for all $n \in \mathbb{Z}$ and $g \in G$. Therefore G is an ideal of $\mathbb{Z}$. It is proved in Mathlib that $\mathbb{Z}$ is a principal ideal domain, so G is a principal ideal. Hence there is some element $g \in G$ such that $g = \{ng : n \in \mathbb{Z}\}$. The bijection $n \mapsto ng$ is an isomorphism between $\mathbb{Z}$ and G. □

Lemma. *Let G be an additive commutative group and let $\phi : G \to \mathbb{Z}$ be a surjective homomorphism. Then there is an isomorphism $G \cong \ker \phi \times \mathbb{Z}$.*

Proof. Since ϕ is surjective, we can choose an element $g_1 \in G$ such that $\phi(g_1) = 1$.

Define a map $\Phi : \ker \phi \times \mathbb{Z} \to G$ by

$$\Phi(g, n) = g + n \cdot g_1.$$

It's easy to check that Φ is a group homomorphism.

For any element $h \in G$ we define $h' = h - \phi(h) \cdot g_1$.

$$\phi(h') = \phi(h) - \phi(h) \cdot \phi(g_1) = 0.$$

Therefore $h' \in \ker \phi$. The map $h \mapsto (h', \phi(h))$ is the inverse function of Φ, so Φ is a bijection. □

Theorem. *If G is a subgroup of $\mathbb{Z}^d$, then G is isomorphic to $\mathbb{Z}^e$ for some $e \leq d$.*

Proof. We'll prove by induction on d that G is a free abelian group. The case $d = 0$ is trivial, so assume $d \geq 0$. There is a homomorphism $\phi : G \to \mathbb{Z}$, which takes every element of G to its d-th coordinate.

Case 1. If $\phi(g) = 0$ for all $g \in G$, then G is (isomorphic to) a subgroup of $\mathbb{Z}^{d-1}$. By the inductive hypothesis G is isomorphic to $\mathbb{Z}^e$ for some $e \leq d - 1$.

Case 2. If $\phi(g) \neq 0$ for some $g \in G$, then the image of ϕ is a non-zero subgroup H of $\mathbb{Z}$ and the kernel K of ϕ is a subgroup of $\mathbb{Z}^{d-1}$. An earlier lemma implies that H is isomorphic to $\mathbb{Z}$. Composing ϕ with this isomorphism, we get a surjective homomorphism $\phi' : G \to \mathbb{Z}$, whose kernel is also K.

By the previous lemma, there is an isomorphism $G \cong K \times \mathbb{Z}$. The inductive hypothesis implies that K is isomorphic to $\mathbb{Z}^e$ for some $e \leq d - 1$. Hence G is isomorphic to $\mathbb{Z}^{e+1}$ and $e + 1 \leq d$. □

Theorem. *Every subgroup of a free abelian group is a free abelian group.*

Proof. Let G be a subgroup of a free abelian group. We've proved above that all free abelian groups are isomorphic to $\mathbb{Z}^d$, so we can assume that G is a subgroup of $\mathbb{Z}^d$. By the previous theorem, G is isomorphic to $\mathbb{Z}^e$ for some e. Therefore G is a free abelian group. □

If you'd like to take this further, then you could try defining the rank of a free abelian group, and proving that the rank is well-defined (i.e. prove that $\mathbb{Z}^n$ is not isomorphic to $\mathbb{Z}^m$ unless $n = m$).

2.4 Galois Theory (`Galois`)

Let $\mathbb{F}$ be a field. We'll write Gal$\mathbb{F}$ for the group of field automorphisms of $\mathbb{F}$. The set Gal$\mathbb{F}$ is a group with the operation of composition. The aim of the project is to calculate the group Gal$\mathbb{F}$ for some fields $\mathbb{F}$. Here are some examples that you could consider:

Lemma. *Let $\sigma \in \mathrm{Gal}(\mathbb{F})$. Then for all natural numbers n we have $\sigma(\uparrow n) = \uparrow n$. (Here $\uparrow n$ is the cast of n into the field $\mathbb{F}$).*

Proof. By induction on n. Clearly $\sigma(0) = 0$ since σ is ahomomorphism. Assuming $\sigma(n) = n$, we have

$$\sigma(n+1) = \sigma(n) + \sigma(1) = \sigma(n) + 1 = n + 1.$$

□

Lemma. *Let $\sigma \in \mathrm{Gal}(\mathbb{F})$. Then for all integers numbers n we have $\sigma(\uparrow n) = \uparrow n$. (Here $\uparrow n$ is the cast of n into the field $\mathbb{F}$).*

Proof. If $n \geq 0$ then this follows from the previous lemma. If $n < 0$ then we have $n = -m$ for some natural number m. By the previous lemma be have

$$\sigma(n) = \sigma(-m) = -\sigma(m) = -m = n.$$

□

Lemma. *Let $\sigma \in \mathrm{Gal}(\mathbb{F})$. Then for all rational numbers x we have $\sigma(\uparrow x) = \uparrow x$. (Here $\uparrow x$ is the cast of x into the field $\mathbb{F}$).*

Proof. Let $x = n/m$ with integers n, m. By the previous lemma we have

$$\sigma(x) = \sigma(n/m) = \sigma(n)/\sigma(m) = n/m = x.$$

□

Theorem. $\mathrm{Gal}(\mathbb{Q})$ *is the trivial group.*

Proof. The previous lemma proves that every element σ is equal to the identity element. □

Theorem. $\mathrm{Gal}(\mathbb{R})$ *is the trivial group.*

Proof. Let $\sigma \in \mathrm{Gal}(\mathbb{R})$. have already proved that $\sigma(x) = x$ for all $x \in \mathbb{Q}$.

Next, we can prove that σ takes positive real numbers to positive real numbers. This uses the fact that $x \geq 0$ iff x has a square root in $\mathbb{R}$.

Finally we prove that $\sigma(x) = x$ for all real x: if this were not true, then there would be a rational number y between x and $\sigma(x)$. From this we can get a contradiction since $x - y$ would have the opposite sign to $\sigma(x - y)$. □

Prove that complex conjugation is a non-trivial element of $\mathrm{Gal}(\mathbb{C})$. Define what it means for an element of $\mathrm{Gal}(\mathbb{C})$ to be continuous.

Theorem. *Every continuous element of* $\mathrm{Gal}(\mathbb{C})$ *is either the identity or complex conjugation.*

Proof. Since $i^2 = -1$, we must have $\sigma(i)^2 = \sigma(-1) = -1$. Therefore $\sigma(i) = \epsilon \cdot i$ for some $\epsilon = \pm 1$.

If x and y are rational numbers then one of our earlier lemmas implies

$$\sigma(x + iy) = \sigma(x) + \sigma(i)\sigma(y) = x + \epsilon iy.$$

Using the continuity of σ, we can extend this formula to all real x, y by choosing sequences of rationals $x_n \to x$ and $y_n \to y$. □

The field $\mathbb{F}_4 = \{0, 1, a, a+1\}$ is defined by setting $a^2 = a + 1$. This implies that addition and multiplication are given by

$+$	0	1	a	$a+1$
0	0	1	a	$a+1$
1	1	0	$a+1$	a
a	a	$a+1$	0	1
$a+1$	$a+1$	a	1	0

$\times$	0	1	a	$a+1$
0	0	0	0	0
1	0	1	a	$a+1$
a	0	a	$a+1$	1
$a+1$	0	$a+1$	1	a

.

Theorem. $\mathrm{Gal}(\mathbb{F}_4) = \{1, \sigma\}$*, where* $\sigma(x) = x^2$ *for all* x *in* $\mathbb{F}_4$*.*

Proof. To check that $\sigma \in \mathrm{Gal}(\mathbb{F}_4)$, we need to check that it is a field automorphism:

$$\sigma(0) = 0, \quad \sigma(1) = 1, \quad \sigma(x + y) = \sigma(x) + \sigma(y), \qquad \sigma(xy) = \sigma(x)\sigma(y).$$

The only one of these four equations which is not obvious is the third one, which is proved like this:

$$\sigma(x + y) = (x + y)^2 = x^2 + (1 + 1)xy + y^2 = x^2 + y^2 = \sigma(x) + \sigma(y).$$

(We used the fact that $1 + 1 = 0$ in $\mathbb{F}_4$.)

To see why 1 and σ are the only two elements of the Galois group, suppose τ is any element of the Galois group. We have $\tau(0) = 0$ and $\tau(1) = 1$. Since τ is a bijection, it either takes a to a and $a + 1$ to $a + 1$, or it swaps those two elements over. □

2.5 Semi-direct products (`SemiDirectProduct`)

This is a project on group theory, which follows some of the material in MATH0053. For a group G, we define the type `Aut G` of automorphisms of G as follows:

```
structure Aut (G : Type) [Group G] where
  homomorphism : G →* G
  bijective    : homomorphism.toFun.Bijective
```

Lemma. *`Aut G` is a group with the operation of composition of functions.*

Proof. Composition of functions is an associative operation. The identity function is an automorphism, and is an identity element for the operation of composition of functions. If σ is an automorphism, then by definition σ is a bijective function, so it has an inverse function, and it's easy to show that the inverse function is also a group homomorphism. □

There is a different definition of the automorphisms of G in Mathlib, which is written `MulEquiv G G`, and abbreviated:

```
G ≃* G
```

We can prove that the groups `Aut G` and `MulEquiv G G` are isomorphic.

For some small groups G we can calculate the group $\mathrm{Aut}(G)$. For example:

Lemma. *The only automorphism of the cyclic group $C_2 = \{1, x\}$ is the the identity function.*

Proof. If σ is an automorphism of C_2 then $\sigma(1) = 1$. Since σ is a bijection we must also have $\sigma(x) = x$. □

Lemma. *The cyclic group $C_3 = \{1, x, x^2\}$ has exactly two automorphisms. They are the identity and the the automorphism σ defined by $\sigma(g) = g^2$ for all g in C_3.*

Proof. Similar to the previous proof. □

Definition. *For any element $g \in G$, the function $x \mapsto gxg^{-1}$ is an automorphism of G. This kind of automorphism is called an* inner automorphism. *Define a homomorphism `inn : G →* Aut G` by setting `inn g` to be the inner automorphism $x \mapsto gxg^{-1}$.*

Theorem. *The set of inner automorphisms of G is a normal subgroup of `Aut G`.*

Proof. This set is certainly a subgroup, since it is the image of a homomorphism. To see why it is a normal subgroup, suppose that ϕ is the inner automorphism

$x \mapsto gxg^{-1}$ and ψ is any other automorphism of G. We need to check that $\psi \circ \phi \circ \psi^{-1}$ is an inner automorphism. We have

$$\begin{aligned}\psi \circ \phi \circ \psi^{-1}(x) &= \psi(\phi(\psi^{-1}(x))) \\ &= \psi(g\psi^{-1}(x)g^{-1}) \\ &= \psi(g)x\psi(g)^{-1}) \\ &= hxh^{-1},\end{aligned}$$

where $h = \psi(g)$. □

Given a homomorphism $\phi : H \to \mathrm{Aut}(G)$, the semi-direct product $G \rtimes_\phi H$ is a group defined to be the set $G \times H$, with multiplication given by

$$(g, h)(g', h') = (g\phi(h)(g'), hh').$$

Definition. *Given homomorphisms $\phi, \psi : H \to \mathrm{Aut}(G)$, we shall call ϕ and ψ equivalent if $\phi = \psi \circ p$ for some automorphism p of H. This relation is an equivalence relation.*

Theorem. *If ϕ and ψ are equivalent, then the semi-direct products $G \rtimes_\phi H$ and $G \rtimes_\psi H$ are isomorphic.*

Proof. It's easy to check that the function $(g, h) \mapsto (g, p(h))$ is an isomorphism between the semi-direct products. □

We can find all the semi-direct products for small groups G and H. For example:

Theorem. *There are exactly two homomorphisms $C_2 \to \mathrm{Aut}(C_3)$. One of these takes every element of C_2 to the identity, and the other takes the non-trivial element of C_2 to the the automorphism $g \mapsto g^2$ of C_3. The semi-direct products corresponding to these two homomorphism are not isomorphic (one of them is cyclic of order 6 and the other is isomorphic to S_3).*

2.6 Groups of small order (`SmallGroups`)

This project is about describing groups of small order up to isomorphism.

Theorem. *If G is a group of order 4 then either G is either cyclic or a direct sum of two cyclic subgroups of order 2.*

Proof. If G has an element x of order 4, then G is the cyclic group generated by x. If this is not the case, then every element apart from the identity has order 2.

Let a and b be two distinct elements of G of order 2. The subgroups generated by a and b are both normal, since they have index 2. These subgroups have trivial intersection. Therefore G is the direct sum of these two subgroups. □

Recall that the dihedral group of order $2n$ is defined as

$$D_{2n} = \langle x, y | x^n = y^2 = 1, y^{-1}xy = x^{-1} \rangle.$$

The elements of this group are $x^r y^s$ with $0 \leq r < n$ and $0 \leq s < 2$. We can think of these elements as the symmetrices of a regular n-gon, where x as a rotation by an angle $2\pi/n$ and y as a reflection.

The group D_{2n} is defined in Mathlib as `DihedralGroup n`. There are many useful facts about this group proved in the file *Mathlib.GroupTheory.SpecificGroups.Dihedral*.

Theorem. *If G is a group of order 6 then either G is cyclic or G is isomorphic to the dihedral group of order 6.*

Proof. Since 2 and 3 are prime, we may choose elements x of order 3 and y of order 2.

The subgroup $\langle x \rangle$ generated by x has index 2, so this is a normal subgroup. It follows that G is a semi-direct product of the subgroups $\langle x \rangle$ and $\langle y \rangle$. Hence all elements of G are of the form $x^r y^s$.

Since $\langle x \rangle$ is normal, $y^{-1}xy$ is also in this subgroup, and is not 1. Therefore $y^{-1}xy$ is either x or x^2.

If $y^{-1}xy = x$, then x and y commute, and it's easy to check that xy has order 6, so G is cyclic.

If $y^{-1}xy = x^2$, then the map taking y to a reflection and x to a rotation by $2\pi/3$ extends to an isomorphism between G and the dihedral group. □

The quaternion group of order $4n$ is defined by

$$Q_{4n} = \langle a, x | a^{2n} = 1, x^2 = a^n, x^{-1}ax = a^{-1} \rangle.$$

This group is defined in Mathlib as `QuaternionGroup n`, and there are some useful facts in Mathlib in the file *Mathlib.GroupTheory.SpecificGroups.Quaternion*.

Theorem. *If G is a group of order 8 and is non-abelian then G is isomorphic to the dihedral group of order 8 or the quaternion group of order 8.*

The proof of this is slightly more involved. There is a simple description *at this link*. In the same link, you can also see a proof that, up to isomorphism there are exactly five groups of order p^3 for any prime p, which you could try to prove in lean if you want to take the project further.

2.7 Direct Summands of Groups (`Summand`)

This project is on group theory. If G and H are groups, then the set $G \times H$ can be made into a group is the obvious way (called the "direct sum") by defining

$$(g, h) * (g', h') := (g * g', h * h').$$

Mathlib is aware of this construction, so that if we give lean the instances `Group G` and `Group H`, then it automatically infers `Group (G × H)`.

Definition. *We'll call G a* direct summand *of H if there exists a group G' and an isomorphism*

$$G \times G' \cong H.$$

This definition is included in the .lean file as `Summand G H`*, and is abbreviated* `G |⊕ H`.

The aim of the project is to prove facts about the relation `Summand`. Here are some examples.

Lemma. *The summand relation is reflexive, i.e. if G is a group then G is a summand of G.*

Proof. There is an isomorphism $G \times 1 \cong G$ which takes $(g, 1)$ to g. □

(Note that in Mathlib, the group 1 with one element is called `Unit`. Mathlib knows that `Unit` is a group, and that every element in `Unit` is the identity element `1`; a proof that such an element is 1 is `rfl`.)

Lemma. *The summand relation is transitive. I.e. if G_1 is a summand of G_2 and G_2 is a summand of G_3 then G_1 is a summand of G_3.*

Proof. Suppose we have isomorphisms $G_1 \times H_1 \cong G_2$ and $G_2 \times H_2 \cong G_3$. Putting these together, we can get an isomorphism

$$G_1 \times (H_1 \times H_2) \cong (G_1 \times H_1) \times H_2 \cong G_3.$$

□

Lemma. *The trivial group 1 is a summand of every group G.*

Proof. There is an isomorphism $1 \times G \cong G$. □

Lemma. *If $G \cong G'$ and $H \cong H'$ then G is a summand of H if and only if G' is a summand of H'.*

Proof. Let $\phi_G : G \to G'$ and $\phi_H : H \to H'$ be isomorphisms, and assume that G is a direct summand of H. I.e. there is another group K and an isomorphism $\Phi : G \times K \cong H$. We can construct an isomorpism $\Phi' : G' \times K \to H'$ by

$$\Phi'(g', k) = \phi_H(\Phi(\phi_G^{-1}(g'), k)).$$

Therefore G' is a direct summand of H'. □

Lemma. *G is a summand of 1 if and only if G is isomorphic to 1.*

Proof. The proof from right to left follows from the previous two lemmas. Conversely, if G is a summand of 1, then there is an isomorphism $G \times H \cong 1$. Using this, we show that every element of G is equal to 1. Hence the map $G \to 1$ which takes every element to 1 is an isomorphism. □

Lemma. *If G and H are finite groups and G is a summand of H then $|G|$ is a factor of $|H|$.*

Proof. If $G \times G'$ is isomorphic to H then $|H| = |G| \cdot |H|$. □

Lemma. *If G and H are finite group such that G is a summand of H and H is a summand of G then G is isomorphic to H.*

Proof. We have isomorphisms $G \times G' \cong H$ and $H \times H' \cong G$. Putting these together we get a bijection

$$G \times G' \times H' \cong G.$$

This implies $|G| \cdot |G'| \cdot |H'| = |G|$, so G' and H' each have only one element. This implies $G \times G' \cong G$, and therefore $G \cong H$. □

Lemma. *G is a summand of H if and only if there exist homomorphisms $\phi : G \to H$ and $\psi : H \to G$, such that (i) the image of ϕ is a normal subgroup of H, and (ii) $\psi \circ \phi = id_G$.*

Proof. Assume first that $H = G \times G'$. Then we can define $\phi : G \to H$ and $\psi : H \to G$ by

$$\phi(g) = (g, 1), \qquad \psi(g, g') = g.$$

It's easy to check that these are group homomorphisms with the required properties.

Conversely, assume that we have homomorphisms ϕ and ψ with these properties. We can define an isomorphism $\Phi : G \times \ker(\psi) \to H$ by

$$\Phi(g, k) = \phi(g)k.$$

(Note that elements of im ϕ and $\ker \psi$ commute with each other by the result `Subgroup.commute_of_normal_of_disjoint` in Mathlib). The inverse is given by

$$\Phi^{-1}(h) = (\psi(h), \phi(\psi(h))^{-1}h).$$

□

A group is called *simple* is it has no normal subgroups apart from 1 and itself. The next theorem shows that finite simple groups have a property similar to prime numbers.

Theorem. *Let G be a finite simple group and let A and B be groups. Then G is a summand of $A \times B$ if and only if G is a summand of A or G is a summand of B (or both).*

Proof. The theorem is obviously true if $G = 1$, so let's assume G has at least one other element $g \neq 1$.

By the lemma, we have homomorphisms $f_1 : G \to A \times B$ and $f_2 : A \times B \to G$, such that $f_2 \circ f_1 = id$ and the image of f_1 is normal in $A \times B$. We also have projection homomorphisms $\pi_A : A \times B \to A$, $\pi_B : A \times B \to B$ and inclusion homomorphisms $\iota_A : A \to A \times B$ and $\iota_B : B \to A \times B$.

Define homomorphisms $\phi_A : G \to A$ and $\psi_A : A \to G$ by

$$\phi_A = \pi_A \circ f_1, \qquad \psi_A = f_2 \circ \iota_A.$$

Similarly, define $\phi_B : G \to B$ and $\psi_B : B \to G$. The statement $f_2 \circ f_1 = id$ implies that

$$g = \psi_A(\phi_A(g)) * \psi_B(\phi_B(g)).$$

Since $g \neq 1$, it follows that $\psi_A(\phi_A(g))$ and $\psi_B(\phi_B(g))$ are not both 1.

Without loss of generality, let's assume $\psi_A(\phi_A(g)) \neq 1$. Therefore $\ker(\psi_A \circ \phi_A) \neq G$. Since the kernel is a normal subgroup of G and G is simple, we must have $\ker(\psi_A \circ \phi_A) = 1$. Therefore the homomorphism $\psi_A \circ \phi_A : G \to G$ is injective. Since G is finite, this homomorphism must also be surjective, so it is an isomorphism.

The homomorphisms $\phi_A : G \to A$ and $(\psi_A \circ \phi_A)^{-1} \circ \psi_A : A \to G$ satisfy the conditions of the lemma above, so G is a summand of A. □

3 Analysis (`Analysis`)

Metric Spaces

A *metric space* is a pair (X, d) where X is a set and $d : X \times X \to \mathbb{R}$ is a distance, satisfying three axioms:

- $\forall x, y \in X,\ d(x, y) \geq 0$ with $d(x, y) = 0$ iff $x = y$.
- $\forall x, y \in X,\ d(x, y) = d(y, x)$.
- $\forall x, y, z \in X,\ d(x, z) \leq d(x, y) + d(y, z)$.

A sequence $\{x_n\} \subseteq X$ *converges* to $l \in X$ iff

$$\forall \epsilon > 0, \exists N \in \mathbb{N}, \forall n \geq N, d(x_n, l) < \epsilon.$$

A sequence $\{x_n\} \subseteq X$ is said to be *Cauchy* iff

$$\forall \epsilon > 0, \exists N \in \mathbb{N}, \forall m \geq N, d(x_m, x_N) < \epsilon.$$

A metric space is said to be *complete* iff every Cauchy sequence in (X, d) converges to a limit in X. For example $\mathbb{R}$, with $d(x, y) = |x - y|$ is a complete metric space.
Given $a \in X$ and $r \geq 0$ the *open ball* centre a and radius r is

$$B_r(a) = \{x \in X \mid d(x, a) < r\},$$

while the *closed ball* centre a and radius r is

$$B_r[a] = \{x \in X \mid d(x, a) \leq r\}.$$

A set $A \subseteq X$ is *open* iff $\forall a \in A, \exists r > 0, B_r(a) \subseteq A$.

3.1 Cantor's Intersection theorem (`CantorIntersection`)

Prerequisites: MATH0051 Analysis 4.
This project is on metric spaces. See page 23 for a quick recap of the definition of a metric space.

Let $B_r[c] = \{x \in X \mid d(x,c) \leq r\}$ denote the *closed ball* with centre c and radius r in the metric space (X,d). Recall that a metric space (X,d) is *complete* iff every Cauchy sequence in (X,d) converges to a limit in X.

There are three parts to this project. First, prove Cantor's intersection theorem.

Theorem (Cantor)**.** *If (X,d) is a complete metric space and $\{B_{r_n}[c_n]\}$ is a decreasing sequence of closed balls whose radii are nonnegative and tend to zero, then*

$$\bigcap_{n=0}^{\infty} B_{r_n}[c_n] \neq \emptyset.$$

You could start the proof of Cantor's theorem by proving the following lemma.

Lemma. *If x_n converges to l and there exists a closed ball $B_r[c]$ and $N \in \mathbb{N}$ such that $\forall n \geq N,\ x_n \in B_r[c]$ then $l \in B_r[c]$.*

Proof: By contradiction. If $l \notin B_r[c]$ then $d(l,c) > r$. Let $\epsilon = d(l,c) - r > 0$ then, since $x_n \to l$, there exists $N_\epsilon \in \mathbb{N}$ such that $d(x_n, l) < \epsilon$ for $n \geq N_\epsilon$. But then for $n \geq \max\{N, N_\epsilon\}$ we have the following contradiction:

$$d(l,c) \leq d(l,x_n) + d(x_n,c) < \epsilon + r = d(l,c).$$

□

Proof of Cantor's theorem: First show that the centres of the balls form a Cauchy sequence. Use completeness of (X,d) to deduce that they converge to a limit $l \in X$. Finally use the lemma to deduce the result. □

The second part of the project is to establish that the following function defines a complete metric on $\mathbb{N}$:

$$\texttt{Ndist}(m,n) := \begin{cases} 0, & m = n \\ 1 + 1/(m+n), & m \neq n. \end{cases}$$

You should start this part by stating and proving basic definitional lemmas about `Ndist`, building up to proving that the axioms of a metric space hold. Once you have proved that $(\mathbb{N}, \texttt{Ndist})$ is a metric space you need to show that it is complete. To help with this you could prove that any Cauchy sequence in $(\mathbb{N}, \texttt{Ndist})$ is eventually constant. (A sequence x_n is *eventually constant* iff $\exists N \in \mathbb{N},\ \forall n \geq N,\ x_n = x_N$.)

The third part of the project is an example to show that the condition "radii tend to zero" is necessary in Cantor's theorem. We prove that the sets

$$\texttt{NBall}(n) := \{n, n+1, \ldots\} \subseteq \mathbb{N}$$

form a strictly decreasing sequence of nonempty closed balls in $(\mathbb{N}, \texttt{Ndist})$ whose radii do not tend to zero and whose intersection is empty.

You should state and prove the following results.

Lemma. $\forall n \in \mathbb{N}, \exists c_n \in \mathbb{N}, \exists r_n \geq 1,\ \texttt{Nball}(n) = B_{r_n}[c_n]$ *is a non-empty closed ball of radius at least one.*

Lemma. *The sequence* $\{\texttt{Nball}(n)\}_{n\in\mathbb{N}}$ *is strictly decreasing, i.e.*

$$\forall n,\ \texttt{Nball}\ (\texttt{n} + \texttt{1}) \subset \texttt{Nball}\ \texttt{n}.$$

Finally we show that the conclusion of Cantor's intersection theorem fails.

Lemma. *The intersection of these balls is empty:*

$$\bigcap_{n=0}^{\infty} \texttt{Nball}(n) = \emptyset.$$

Possible extension: prove that we cannot replace *closed balls* by *open balls* in Cantor's Intersection theorem by giving an example of a complete metric space X and a decreasing sequence of non-empty open balls in X whose radii tend to zero and have empty intersection.

3.2 Cantor Set (`CantorSet`)

Prerequisites: MATH0003 Analysis 1. This project involves first year level analysis (infinite sums).

In this project we will explore ternary (base 3) expansions and the Cantor set.

Given an ternary sequence $f : \mathbb{N} \to \{0, 1, 2\}$ we define the associated real ternary expansion:

$$\texttt{texp}(f) = \sum_{n=0}^{\infty} \frac{f(n)}{3^{n+1}}.$$

We say that a ternary sequence is *Cantor* if it contains only 0s and 2s.

Note that different ternary sequences can correspond to the same expansion, e.g. $0.120\overline{2}$ and $0.121\overline{0}$ both correspond to $16/27$. But (as you will prove below) if the expansions only involve 0s and 2s then the representation is unique.

We will give the lexicographic ordering to ternary sequences, this means we consider them in "dictionary order". More formally, if f and g are ternary sequences and $f \neq g$ then $f < g$ iff $\exists N \in \mathbb{N}$, $\forall i < N$, $f(i) = g(i)$ and $f(N) < g(N)$. Note that this is a linear order, i.e. for any two ternary sequences f and g, either $f < g$, $f = g$ or $f > g$.

Our main theorem is the following.

Theorem. *The function* `texp` *is injective on the set of all Cantor sequences.*

This follows almost immediately from the following result.

Theorem. *If we order ternary sequences lexicographically and f, g are Cantor sequences satisfying $f < g$ then* $\texttt{texp}(f) < \texttt{texp}(g)$.

Proof: By the definition of the lexicographic ordering if $f < g$ there exists $N \in \mathbb{N}$ such that $f(i) = g(i)$ for $i < N$ and $f(N) < g(N)$. Since f and g are Cantor sequences we must have $f(N) = 0$ and $g(N) = 2$. So

$$\begin{aligned}
\texttt{texp}(g) - \texttt{texp}(f) &= \sum_{n=0}^{\infty} \frac{g(n) - f(n)}{3^{n+1}} \\
&= \frac{2}{3^{N+1}} + \sum_{n=N+1}^{\infty} \frac{g(n) - f(n)}{3^{n+1}} \\
&\geq \frac{2}{3^{N+1}} - \sum_{n=N+1}^{\infty} \frac{2}{3^{n+1}} \\
&= \frac{2}{3^{N+1}} \left(1 - \sum_{n=0}^{\infty} \frac{1}{3^{n+1}}\right) \\
&= \frac{1}{3^{N+1}} \\
&> 0.
\end{aligned}$$

Our third main result is the following. (This is Cantor's diagonal argument.)

Theorem. *There is no surjection from* $\mathbb{N}$ *to the set of all Cantor sequences.*

Proof: Let $F : \mathbb{N} \to \{f \mid f \text{ is a Cantor sequence}\}$. Consider the Cantor sequence defined by

$$c(n) = \begin{cases} 0, & \text{if the } n\text{th term of } F(n) \text{ is } 2, \\ 2, & \text{otherwise.} \end{cases}$$

Prove that c has no preimage under F, and hence F is not surjective. □

Putting these together and writing $\#A$ for the cardinality of a set A, we can prove that $\mathbb{R}$ is uncountable.

Theorem. *The reals are uncountable since:*

$$\#\mathbb{N} < \#\{f \mid f \ \texttt{Cantor}\} = \#\texttt{texp}(\{f \mid f \ \texttt{Cantor}\}) \leq \#\mathbb{R}.$$

Possible extension: state and prove a result characterizing when two distinct ternary sequences have expansions that sum to the same value.

3.3 Contraction maps on $(\mathbb{N}, d_2)$ (`ContractionMap`)

Prerequisites: MATH0051 Analysis 4.
This project is on metric spaces using some very elementary number theory. See page 23 for a quick recap of the definition of a metric space.

A metric space (X, d) is *complete* iff every Cauchy sequence in X converges to a limit in X.

A map $f : X \to X$ is a *contraction* iff there exists $0 \leq K < 1$ such that $\forall x, y \in X,\ d(f(x), f(y)) \leq Kd(x, y)$.

We say that $x \in X$ is a *fixed point* of $f : X \to X$ iff $f(x) = x$.

Theorem (Banach)**.** *If (X, d) is a complete metric space and $f : X \to X$ is a contraction then f has a fixed point.*

In this project we will define the 2-adic metric d_2 on $\mathbb{N}$ by

$$d_2(m, n) = \begin{cases} 0, & m = n \\ 1/2^{\log_2 |m-n|}, & m \neq n, \end{cases}$$

where (for $n \neq 0$), $\log_2 n = \max\{k \in \mathbb{N} \mid 2^k \text{ divides } n\}$.

For example,

$$d_2(31, 79) = 1/2^{\log_2 |31-79|} = 1/2^{\log_2 48} = 1/2^4 = 1/16.$$

You should work out proofs of all the metric space axioms for d_2 on paper (they are straightforward).

After proving that $(\mathbb{N}, d_2)$ is a metric space we will consider maps of the form $T : \mathbb{N} \to \mathbb{N}$, $T(n) = an + b$ and prove that if $a, b \neq 0$ then such a map has no fixed points. We will also prove that for $a = 2$ such a map is a contraction. From these results we can use Banach's Fixed Point theorem to deduce our main result.

Theorem. $(\mathbb{N}, d_2)$ *is not complete.*

In the Lean file we define $\log_2 n$ recursively as follows:

```
def log₂ : ℕ → ℕ
  | 0 => 0
  | succ n =>
    if 2 ∣ succ n then log₂ (succ n / 2) + 1 else 0
```

Our first main goal is to prove that for $n \neq 0$ this satisfies

$$\texttt{log}_2 n = \max\{k \in \mathbb{N} \mid 2^k \mid n\}.$$

Next we define $\texttt{ndist}(m, n) = |m - n|$, where we want to consider m and n as integers rather than natural numbers. The easiest way to do this is to use Mathlib's `Nat.dist` which is defined as follows:

```
def dist (n m : ℕ) := (n - m) + (m - n)
```

We then define the d_2 metric on $\mathbb{N}$:

```
def d₂ : ℕ → ℕ → ℝ := fun m n =>
    if  (m = n)  then 0 else (1 / 2 ^ log₂ (ndist m n))
```

In Lean the definitions of contraction and fixed point are as follows.

```
def ContractingWith (K : ℝ≥0) (f : α → α) :=
     K < 1 ∧ LipschitzWith K f

def IsFixedPt (f : α → α) (x : α) := f x = x
```

Before starting this project work out a proof on paper. You will probably need to add quite a few intermediate lemmas to the Lean file.

Possible extension: prove that in $(\mathbb{N}, d_2)$ any polynomial with coefficients in $\mathbb{N}$ is continuous everywhere.

3.4 Set of points of continuity (`GdeltaCts`)

Prerequisites: MATH0051 Analysis 4.
This project is on metric spaces. See page 23 for a quick recap of the definition.

In Analysis 1 you saw the Thomae function $\tau : \mathbb{R} \to \mathbb{R}$, given by

$$\tau(x) = \begin{cases} 0, & x \notin \mathbb{Q}, \\ 1/q, & x = p/q \in \mathbb{Q},\ \gcd(p,q) = 1. \end{cases}$$

This function is continuous at $x \in \mathbb{R}$ iff x is irrational. So we say that the *set of points of continuity* of τ is $\mathbb{R} \setminus \mathbb{Q}$.

A natural follow-up question is to ask what other sets can occur as the set of points of continuity of a function? We will consider this question in the setting of metric spaces.

Let (X, d) be a metric space. Recall that the *open ball* with centre $a \in X$ and radius $r > 0$ is the set

$$B_r(a) = \{x \mid d(a, x) < r\}.$$

A set $U \subseteq X$ is said to be *open* iff for every point $u \in U$ there exists $\epsilon > 0$ such that $B_\epsilon(u) \subseteq U$.

Let (X, d_X) and (Y, d_Y) be metric spaces. A function $f : X \to Y$ is *continuous* at x iff

$$\forall \epsilon > 0, \exists \delta > 0 \text{ such that } d_X(a, x) < \delta \implies d_Y(f(a), f(x)) < \epsilon.$$

We will prove two theorems in this project, the first characterizes the set of points of continuity of a function mapping between metric spaces.

Theorem. *Let (X, d_X) and (Y, d_Y) be metric spaces. If $f : X \to Y$ then there exists a sequence of open sets, $\{V_n\}_{n\in\mathbb{N}}$, such that the set of points of continuity of f is $\bigcap_{n\in\mathbb{N}} V_n$.*

Proof: Given $f : X \to Y$ and $n \in \mathbb{N}$ define

$$V_n = \{x \in X \mid \exists \delta > 0, \forall a, b \in X, \text{ if } d_X(x, a) < \delta \text{ and } d_X(x, b) < \delta \text{ then } d_Y(f(a), f(b)) < 1/(n+1)\}.$$

We will prove that f is continuous at x iff $x \in \bigcap_{n\in\mathbb{N}} V_n$.

First suppose that f is continuous at x and let $n \in \mathbb{N}$. Taking $\epsilon = 1/2(n+1) > 0$ in the definition of continuity of f at x we obtain $\delta > 0$ such that if $d_X(x, a) < \delta$ then $d_Y(f(a), f(x)) < 1/2(n+1)$. Hence, if both $d_X(x, a) < \delta$ and $d_X(x, b)$ hold then, using the triangle inequality in (Y, d_Y),

$$\begin{aligned} d_Y(f(a), f(b)) &\leq d_Y(f(a), f(x)) + d_Y(f(x), f(b)) \\ &< 1/2(n+1) + 1/2(n+1) \\ &= 1/(n+1). \end{aligned}$$

Hence $x \in V_n$. Since n was arbitrary we deduce that $x \in \bigcap_{n\in\mathbb{N}} V_n$.

Conversely, if $x \in \bigcap_{n\in\mathbb{N}} V_n$ we can prove that f is continuous at x as follows. If $\epsilon > 0$ then there exists $N \in \mathbb{N}$ such that $1/(N+1) < \epsilon$. Since $x \in V_N$, the definition of V_N implies the existence of $\delta > 0$ such that if $d_X(x,a) < \delta$ and $d_X(x,b) < \delta$ then $d_Y(f(a), f(b)) < 1/(N+1) < \epsilon$. In particular if $b = x$ then $d_Y(f(a), f(x)) < \epsilon$. So f is continuous at x □

For our second theorem we consider the special case of $X = Y = \mathbb{R}$, and prove the following converse.

Theorem. *If $\{U_n\}_{n\in\mathbb{N}}$ is a sequence of open sets in $\mathbb{R}$ then there exists a function $\texttt{func}_U : \mathbb{R} \to \mathbb{R}$ whose set of points of continuity is $\bigcap_{n\in\mathbb{N}} U_n$.*

We define $\texttt{func}_U$ as follows. (Note that if $x \notin \bigcap U_n$ then $\min\{n \mid x \notin U_n\}$ is well-defined.)

$$\texttt{func}_U(x) = \begin{cases} 0, & x \in \bigcap U_n, \\ 1/(N+1), & x \text{ is irrational and } N = \min\{n \mid x \notin U_n\}, \\ -1/(N+1), & x \text{ is rational and } N = \min\{n \mid x \notin U_n\}. \end{cases}$$

Proof (sketch): We need to show that $\texttt{func}_U(x)$ is continuous at x iff $x \in \bigcap U_n$. If $x \in \bigcap U_n$ then $\texttt{func}_U(x) = 0$. Given $\epsilon > 0$, we can choose $N \in \mathbb{N}$ such that $1/(N+1) < \epsilon$. Since each U_n is open there exist $\delta_n > 0$ such that $B(x, \delta_n) \subseteq U_n$. Setting $\delta = \min\{\delta_i \mid i \leq N\} > 0$ we can show that $|f(a)| \leq 1/(N+1) < \epsilon$ for any a satisfying $d(x,a) < \delta$ and hence $\texttt{func}_U$ is continuous at x.

Conversely suppose that $\texttt{func}_U$ is continuous at x. We need to prove that $x \in \bigcap U_n$. Suppose, for a contradiction that $x \notin \bigcap U_n$, and let N be minimal such that $x \notin U_N$. By definition $|\texttt{func}_U(x)| = 1/(N+1)$. By choosing an appropriate value of ϵ and considering the cases of whether or not x is rational we can derive a contradiction. (The details will use the fact that between any two distinct real numbers we can find a rational/irrational number.) □

Possible extension: give an example of a metric space (X, d) and a sequence of open sets $\{U_n\}_{n\in\mathbb{N}}$ in X such that for any function $f : X \to \mathbb{R}$ we have

$$\bigcap_{n\in\mathbb{N}} U_n \neq \texttt{SetOfContinuousAt}(f).$$

3.5 Measure Theory (`MeasureTheory`)

3.5.1 Vitali Set (`VitaliSet`)

Prerequisites: MATH0003 Analysis 1. This project does not actually require any measure theory or analysis beyond Year 1.

In this project we will formalize Vitali's proof that, with any sensible definition of a measure, not all subsets of $\mathbb{R}$ can be measurable.

Recall that the *powerset* of a set X is $\mathcal{P}(X) = \{A \mid A \subset X\}$. We say that a function $\mu : \mathcal{P}(\mathbb{R}) \to [0, +\infty]$ *is a Vitali-measure* if it has the following properties.

- Monotone: $\forall s, t \subseteq \mathbb{R},\ s \subseteq t \implies \mu(s) \leq \mu(t)$
- Unit: $\mu([0, 1]) = 1$ (the unit interval has length 1)
- Translation invariance: $\forall s \subseteq \mathbb{R},\ \forall x \in \mathbb{R}, \mu(s + x) = \mu(s)$ (where $s + x = \{y + x \mid y \in s\}$).
- Countably additive: if $\{F_n\}_{n=0}^{\infty}$ is a countable sequence of pairwise disjoint sets, then
$$\mu\left(\bigcup_{n=0}^{\infty} F_n\right) = \sum_{n=0}^{\infty} \mu(F_n).$$

The main goal of this project is to prove that no Vitali-measure exists. We do this by constructing a pathological subset of the reals called the *Vitali set* $\mathcal{V}$.

We start by defining a relation on $\mathbb{R}$ by $x \sim y \iff x - y \in \mathbb{Q}$. We prove that this is an equivalence relation and show that every equivalence class contains an element in $[0, 1/2]$.

We define the Vitali set $\mathcal{V}$ by choosing a single element in $[0, 1/2]$ from each equivalence class. We then establish that:

(A) $\mathcal{V} \subseteq [0, 1/2]$.

(B) $\bigcup_{q \in \mathbb{Q}} (\mathcal{V} + q) = \mathbb{R}$.

(C) If $p, q \in \mathbb{Q}$ and $p \neq q$ then $\mathcal{V} + p$ and $\mathcal{V} + q$ are disjoint.

Proof: (A) follows immediately from the definition of $\mathcal{V}$.

For (B): if $x \in \mathbb{R}$ then, by definition of $\mathcal{V}$, there is an element y of the equivalence class of x in $\mathcal{V}$. Hence $q = x - y \in \mathbb{Q}$ and $x = y + q \in \mathcal{V} + q$.

For (C): if not there exist $a, b \in \mathcal{V}$ such that $a + p = b + q$. But then $a - b = q - p \in \mathbb{Q}$ so $a \sim b$. Hence, by the definition of $\mathcal{V}$, $a = b$ and so $p = q$. $\square$

Note that (A) implies that for all $n \in \mathbb{N}$, $\mathcal{V} + \frac{1}{n+2} \subseteq [0, 1]$. Hence we also have

(D) $\bigcup_{n=0}^{\infty}\left(\mathcal{V}+\frac{1}{n+2}\right)\subseteq[0,1]$.

We can now prove our main theorem.

Theorem. *No Vitali-measure exists.*

Proof. Suppose that μ is a Vitali-measure. Using translation invariance; countable additivity with (C); monotonicity with (D) and the fact that $\mu([0,1])=1$ we have

$$\sum_{n=0}^{\infty}\mu(\mathcal{V})=\sum_{n=0}^{\infty}\mu\left(\mathcal{V}+\frac{1}{n+2}\right)=\mu\left(\bigcup_{n=0}^{\infty}\mathcal{V}+\frac{1}{n+2}\right)\leq\mu([0,1])=1.$$

But the LHS is an infinite sum of constant nonnegative terms, hence $\mu(\mathcal{V})=0$. Using the fact that $\mathbb{Q}$ is countable, (B) and (C), together with translation invariance and countable additivity imply

$$\mu(\mathbb{R})=\mu\left(\bigcup_{q\in\mathbb{Q}}\mathcal{V}+q\right)=\sum_{q\in\mathbb{Q}}\mu(\mathcal{V})=\sum_{q\in\mathbb{Q}}0=0.$$

Which contradicts monotonicity, since $\mu([0,1])\subseteq\mathbb{R}$ and $\mu([0,1])=1$. □

Possible extension: explore what happens if we weaken the condition of *countably additive* to *finitely additive*.

3.6 Sum of reciprocals of primes (`SumReciprocalsPrimes`)

Prerequisites: MATH0003 Analysis 1 and MATH0006 Algebra 2.
This project is in elementary number theory (uniqueness of prime factorisation) and basic analysis (infinite sums).

The aim of this project is to formalize the following result.

Theorem. *If $m \in \mathbb{N}$ then the sum of the reciprocals of the primes less than $2^{4m}+1$ satisfies*

$$\log(m+1/2) \leq \sum_{p<2^{4m}+1} \frac{1}{p}.$$

Let $f : \mathbb{N} \to \mathbb{R}$ satisfy $f(0) = 0$, $f(1) = 1$ and $\forall a, b$, $f(ab) = f(a)f(b)$. In Lean such a function is called a `MonoidWithZeroHom`.

Most of the results we prove below hold for any nonnegative `MonoidWithZeroHom` f, but we will need to specialize to the function $k \mapsto 1/k$ to obtain our main theorem.

We call $k \in \mathbb{N}$ *squarefree* if the only square that divides k is 1.

Given $n \in \mathbb{N}$ we define

$$\texttt{PrimesLt}(n) = \{p \mid p < n \text{ and } p \text{ prime}\},$$

$$\texttt{SqFreesLt}(n) = \{k \mid k < n \text{ and } k \text{ squarefree}\}.$$

If $n = \prod_{i=1}^{k} p_i^{\alpha_i} \geq 1$ is a product of distinct primes then we define

$$\texttt{sqf}(n) = \prod_{\alpha_i \text{ odd}} p_i, \quad \text{and} \quad \texttt{squ}(n) = \prod_{i=1}^{k} p_i^{\lfloor \alpha_i/2 \rfloor}.$$

For $n = 1$ these are both the empty product so equal 1. We extend these definitions to $n = 0$ by $\texttt{sqf}(0) = 1$ and $\texttt{squ}(0) = 0$.

Lemma. (A) *If $n \in \mathbb{N}$ then $n = \texttt{sqf}(n)\texttt{squ}(n)^2$.*

Proof: Easy to check for $n = 0, 1$. So suppose $n \geq 2$. If p_i is a prime factor of n with multiplicity α_i then either α_i is even and so $\alpha_i = 2 * \lfloor \alpha_i/2 \rfloor$ or α_i is odd and so $\alpha_i = 2 * \lfloor \alpha_i/2 \rfloor + 1$. The result follows from the definitions of $\texttt{sqf}(n)$ and $\texttt{squ}(n)$. □

Lemma. (B) *Let $f : \mathbb{N} \to \mathbb{R}$ be a nonnegative `MonoidWithZeroHom`. If $n \in \mathbb{N}$ and $n \geq 2$ then*

$$\log\left(\sum_{k \in \texttt{SqFreesLt}(n)} f(k)\right) \leq \sum_{p \in \texttt{PrimesLt}(n)} f(p).$$

Proof: If $k \in \texttt{SqFreesLt}(n)$ then k has no repeated prime factors and hence k is equal to the product of its set of distinct prime factors F_k. Moreover the map $k \mapsto F_k$ is injective. Hence, using the fact that f is a nonnegative `MonoidWithZeroHom`, we have

$$\begin{aligned}\sum_{k \in \texttt{SqFreesLt}(n)} f(k) &\leq \sum_{B \subseteq \texttt{PrimesLt}(n)} f\left(\prod_{p \in B} p\right) \\ &= \sum_{B \subseteq \texttt{PrimesLt}(n)} \prod_{p \in B} f(p) \\ &= \prod_{p \in \texttt{PrimesLt}(n)} (1 + f(p)).\end{aligned}$$

Finally use the bound $1 + x \leq \exp x$ and take logarithms. □

Our other main intermediate result is the following:

Lemma. (C) *Let $f : \mathbb{N} \to \mathbb{R}$ be a nonnegative `MonoidWithZeroHom`. If $n \in \mathbb{N}$ then*

$$\sum_{k<n} f(k) \ \leq \left(\sum_{a \in \texttt{SqFreesLt}(n)} f(a)\right)\left(\sum_{b<n} f(b^2)\right).$$

This follows from the Lemma (A) decomposition $n = \texttt{sqf}(n)\texttt{squ}(n)^2$, the properties of f and the fact the map $n \mapsto (\texttt{sqf}(n), \texttt{squ}(n))$ is injective.

For the main theorem we set $f(n) = 1/n$ and prove the following simple bounds.

Lemma. (D) *If $m \in \mathbb{N}$ then*

$$\frac{m}{2} + 1 \ \leq \ \sum_{k=0}^{2^m} \frac{1}{k}.$$

Lemma. (E) *If $m \in \mathbb{N}$ then*

$$\sum_{k=0}^{m} \frac{1}{k^2} \leq 2.$$

Proof of main theorem: Lemmas (C), (D), (E) and dividing through by 2 gives

$$m + \frac{1}{2} \leq \frac{1}{2} \sum_{k<2^{4m}+1} \frac{1}{k} \leq \sum_{a \in \texttt{SqFreesLt}(2^{4m}+1)} \frac{1}{k}.$$

The result now follows from Lemma (B) after taking logarithms. □

You should work out the entire proof on paper before starting.

3.7 Topology (`Topology`)

3.7.1 Alexandrov topology and orders (`Alexandrov`)

Prerequisites: MATH0051 Analysis 4. This project is on topological spaces.

In this project you will explore the Alexandrov topology and the relationship between orders and topologies.

In particular you will show how to construct a *preorder* from a topology and how to construct a topology from a preorder; characterising when these constructions are inverses of each other.

A *topology* τ on a set X is a collection of subsets of X satisfying:

(1) $X \in \tau$,

(2) $U, V \in \tau \implies U \cap V \in \tau$,

(3) If $\sigma \subseteq \tau$ then $\bigcup_{U \in \sigma} U \in \tau$.

Note that by taking σ to be the empty subfamily in (3) we always have $\emptyset \in \tau$.

We call the members of τ the *open* sets of the topological space (X, τ). The properties can be summarised as: (1) the whole space is open; (2) pairwise intersections of open sets are open; (3) arbitrary unions of open sets are open.

Given (X, τ), a topological space, we say that $F \subseteq X$ is *closed* iff $X \setminus F$ is open.

A topological space is *discrete* iff every set is open.

In any topological space every *union* of open sets is open. A space in which every *intersection* of open sets is open is said to be *Alexandrov*.

In an Alexandrov space the intersection of all the open sets containing a point x is itself open (and hence is the unique smallest open set containing x). We call this $\mathtt{In}(x)$:

$$\mathtt{In}(x) = \bigcap_{x \in U,\ U \text{ open}} U.$$

In fact we have the following characterisation of Alexandrov spaces.

Theorem. *A topological space X is Alexandrov iff $\forall x \in X$, $\mathtt{In}(x)$ is open.*

Proof: If X is Alexandrov then for any $x \in X$ we have $\mathtt{In}(x)$ is open since it is the intersection of open sets.

Conversely suppose that $\forall x \in X$, $\mathtt{In}(x)$ is open. Let S be a family of open subsets of X, we need to show that $V := \bigcap_{U \in S} U$ is open. This will follow if we prove that $V = \bigcup_{v \in V} \mathtt{In}(v)$, since any union of open sets is open.

Clearly $V \subseteq \bigcup_{v \in V} \mathtt{In}(v)$, since for any $x \in X$, $x \in \mathtt{In}(x)$.

To see that $\bigcup_{v \in V} \mathtt{In}(v) \subseteq V$ suppose that $x \in \bigcup_{v \in V} \mathtt{In}(v)$. There exists $v \in V$ such that $x \in \mathtt{In}(v)$. By definition of $\mathtt{In}(v)$, x belongs to every open set

containing v. In particular, since $v \in V = \bigcap_{U \in S} U$ and all the sets in S are open, x belongs to all the sets in S. Hence $x \in V$. □

Separation axioms are a way of imposing conditions on a topological space that tell us how easy it is to distinguish between points (or sets) using the topology.

They start with T_0-spaces and go up to T_5-spaces. We will only really consider T_0 and T_1-spaces.

A T_0-space is a topological space in which $\forall x, y,\ x \neq y$ implies there exists an open set U such that either $x \in U$ and $y \notin U$ or $x \notin U$ and $y \in U$.

A T_1-space is a topological space in which $\forall x, y,\ x \neq y$ implies there exists an open set U such that $x \in U$ and $y \notin U$.

Theorem. *Any Alexandrov T_1-space is discrete.*

Proof: We prove that if X is an Alexandrov T_1-space then for any $x \in X$, we have $\texttt{In}(x) = \{x\}$. Since $\texttt{In}(x)$ is open this implies that every subset $A \subseteq X$ is open since it a union of open sets:

$$A = \bigcup_{a \in A} \{a\} = \bigcup_{a \in A} \texttt{In}(a).$$

Since $x \in \texttt{In}(x)$ always holds we need to prove that if $x \neq y$ then $y \notin \texttt{In}(x)$. Suppose that $x \neq y$. Using the T_1-space property there is an open set U such that $x \in U$ and $y \notin U$. Hence $y \notin \texttt{In}(x)$ as required. □

One important place in which Alexandrov spaces arise is when constructing a topological space from a preorder.

Given a topological space (X, τ) we can define a "$\leq$" called `toPre` on X by

$$a \leq b \quad \text{iff} \quad \texttt{In}(b) \subseteq \texttt{In}(b).$$

Theorem. *If (X, τ) is a topological space then `toPre` X is a preorder. Moreover if X is a T_0-space then `toPre` is a partial order*

We can also define a topology given a preorder. To define a topology we need to describe the open sets. Given a preorder $(X, \leq)$ we define a topology on X called `toTop` X as follows:

$$U \text{ is open iff } \ \forall x \in U, \text{ if } x \leq y \text{ then } y \in U.$$

Theorem. *Given a preorder $(X, \leq)$ the topological space `toTop` is Alexandrov, moreover if the preorder we start with is a partial order then `toTop` is a T_0-space.*

A natural question to ask is when are these constructions inverses of each other?

We prove first that if we start with a preorder Y and form `toPre (toTop Y)` then we recover the original preorder on Y. In Lean this is:

```
theorem toPre_of_toTop_eq_Pre [Preorder Y] (a b : Y) :
    a ≤ b ↔ (In b ⊆ In a)
```

Since `toTop` is Alexandrov we cannot hope to prove an analogous result starting from a general topological space. However we have the next best thing. If we start with an Alexandrov space Y and form the preorder `toPre Y` and then form the topological space from this preorder, i.e. `toTop (toPre Y)` we recover the original topological space. In Lean this is:

```
theorem toTop_of_toPre_eq_Top_of_Alexandrov [TopologicalSpace Y]
  (hA : IsAlexandrov Y) (s : Set Y):
  IsOpen s ↔ ∀ {|x|}, x ∈ s → ∀ {|y|}, x ≤ y → y ∈ s
```

Possible extension: consider the two element type `Point`:

```
inductive Point where
| bot : Point
| top : Point
```

Construct a topological space on `Point` by giving it an order with `bot` $\leq$ `bot`, `bot` $\leq$ `top` and `top` $\leq$ `top` and have Lean infer the topology from this using `toTop`. Prove that this is a T_0-space but not a T_1-space

Prove that given any topological space X there is a equivalence between the open sets in the topology of X and the continuous functions `f : X → Point`.

```
{s : Set X // IsOpen s} ≃ {f : X → Point // Continuous f}
```

For this you need to use the definition of a continuous function between topological spaces. If $f : X \to Y$ with X and Y topological spaces, then f is *continuous* iff the preimage of every open set in Y is open in X.

3.7.2 Infinitude of primes (`Furstenberg`)

Prerequisites: MATH0006 Algebra 2 for very elementary facts about primes. You will need to use the definition of a topology given below but you don't need to have taken MATH0051 Analysis 4.

Formalize Furstenberg's topological proof that there exist infinitely many primes.

A *topology* τ on a set X is a collection of subsets of X satisfying:

(1) $X \in \tau$,

(2) $U, V \in \tau \implies U \cap V \in \tau$,

(3) If $\sigma \subseteq \tau$ then $\bigcup_{U \in \sigma} U \in \tau$.

Note that by taking σ to be the empty subfamily in (3) we always have $\emptyset \in \tau$.

We call the members of τ the *open* sets of the topological space (X, τ). The properties can be summarised as: (1) the whole space is open; (2) pairwise intersections of open sets are open; (3) arbitrary unions of open sets are open.

Given (X, τ), a topological space, we say that $F \subseteq X$ is *closed* iff $X \setminus F$ is open.

For any $a, b \in \mathbb{N}$ we define the associated arithmetic progression starting at b with common difference a:

$$AP(a, b) = \{n \in \mathbb{N} \mid \exists k \in N, n = ak + b\}.$$

For example $AP(3, 7) = \{7, 10, 13, 16, \ldots\}$.

Before introducing a topology on $\mathbb{N}$ we establish two main results.

Lemma. (A) *The union of the arithmetic progressions of the form $AP(p, 0)$, where p is prime satisfies:*

$$\mathbb{N} \setminus \{1\} = \bigcup_{p \text{ prime}} AP(p, 0).$$

Proof: If $n \in \mathbb{N} \setminus \{1\}$ then n has a prime divisor p and so $n \in AP(p, 0)$. Conversely, if $m \in AP(p, 0)$, with p prime, then there exists $k \in \mathbb{N}$ such that $m = kp$ so $m \neq 1$. □

Lemma. (B) *If $a, b \in \mathbb{N}$ and $b < a$ then we can express the arithmetic progression $AP(a, b)$ as the complement of a union of arithmetic progressions:*

$$AP(a, b) = \mathbb{N} \setminus \bigcup_{j<a,\ j \neq b} AP(a, j).$$

Proof: If $b < a$ then $a \neq 0$ and $AP(a, b)$ is the set of natural numbers that are congruent to b modulo a. This set is the complement of all the other congruence classes modulo a. □

We now define the *Furstenberg topology* on $\mathbb{N}$ by declaring that a set $U \subseteq \mathbb{N}$ is open iff $\forall n \in U$, $\exists a, a \neq 0$ such that $AP(a, n) \subseteq U$.

We need to prove that this does indeed define a topology on $\mathbb{N}$.

Lemma. (C) *The Furstenberg topology is a topology on* $\mathbb{N}$.

Proof (sketch): Most of the axioms of a topological space are easy to check. The only slightly tricky part is showing that if U and V are open then so is $U \cap V$. A useful intermediate result is to prove that for any $a_1, a_2, b \in \mathbb{N}$ we have

$$AP(a_1 a_2, b) \subseteq AP(a_1, b) \cap AP(a_2, b).$$

□

We establish some simple facts about arithmetic progressions in this topology.

Lemma. (D) *If* $a, b \in \mathbb{N}$ *and* $a \neq 0$ *then* $AP(a, b)$ *is open.*

Proof: This follows almost immediately from the definition of an open set. □

Lemma. (E) *If* $a, b \in \mathbb{N}$ *and* $b < a$ *then* $AP(a, b)$ *is closed.*

Proof: Since $b < a$ we have $a \neq 0$ and hence $AP(a, j)$ is open for each j by Lemma (D). Then Lemma (B) implies that $AP(a, b)$ is the complement of a union of open sets, and hence is closed. □

We now consider whether $\{1\}$ is open in this topology and prove the key result.

Theorem. *If there were only finitely many primes then* $\{1\}$ *would be open.*

Proof: If there are only finitely many primes then Lemma (A) implies that $\mathbb{N} \setminus \{1\}$ is finite union of $AP(p, 0)$, which are all closed by Lemma (E). Hence $\mathbb{N} \setminus \{1\}$ is closed and so $\{1\}$ is open. □

Corollary. *There exist infinitely many primes.*

Proof: If there are only finitely many primes then $\{1\}$ is open by our previous result. But if $\{1\}$ is open then there exists $a \neq 0$ such that $AP(a, 1) \subseteq \{1\}$, which is impossible. □

Possible extension (requires MATH0051 Analysis 4): explore the topological properties of $\mathbb{N}$ (with the Furstenberg topology). For example prove that it is (i) a Hausdorff space and (ii) it is not compact.

A topological space X is *Hausdorff* iff $\forall x \neq y$, $\exists U_x, U_y$ disjoint open sets, such that $x \in U_x$ and $y \in U_y$.

A space X is *compact* iff given any collection of open sets whose union is X there is a finite subcollection whose union is X.

To show that $\mathbb{N}$ is a Hausdorff let $m \neq n$, so wlog $m < n$, then setting $d = 2(n - m)$ we can use $U_m = AP(d, m)$ and $U_n = AP(d, n)$ as the required disjoint open sets.

For non-compactness of $\mathbb{N}$ it is easier to use the following equivalent definition, known as the *finite intersection property* for closed sets. (This result is in Mathlib.)

Lemma. *A topological space X is compact iff given any collection $\mathcal{F}$ of closed sets whose intersection is empty there is a finite subcollection whose intersection is empty.*

Let $C_n = AP(p_n, n+1)$ be the arithmetic progression starting from $n+1$ and with common difference the nth prime. (So $p_0 = 2$, $p_1 = 3$ etc.)

$$C_0 = AP(2,1),\ C_1 = AP(3,2), \ldots, C_5 = AP(13,6), \ldots,$$

The Chinese Remainder theorem guarantees that any finite subcollection of these closed sets has nonempty intersection. But the intersection of all the C_n is empty. Thus $\mathbb{N}$ is not compact.

4 Combinatorics (`Combinatorics`)

Most of the following projects in combinatorics are related to results from MATH0029 Graph Theory and Combinatorics. If you are interested in doing any other graph theory or combinatorics projects please just ask and we can help you with this.

4.1 Greedy Graph Colouring (`Greedy`)

Prerequisites: MATH0029 Graph Theory and Combinatorics

Theorem. *If $G = (V, E)$ is a finite graph with maximum degree Δ then the chromatic number of G satisfies $\chi(G) \leq \Delta + 1$.*

The natural proof of this result is via the so-called "Greedy Colouring Algorithm".

In this project you will formalize this proof by implementing the algorithm.

If $V(G) = \{v_0, v_1, \ldots, v_n\}$ and our set of colours is $\{0, 1, \ldots \Delta\}$ then the greedy algorithm produces a $(\Delta + 1)$-colouring c of G as follows:

`zero` Set $c(v_0) := 0$.

`succ` If $c(v_j)$ has been defined for $0 \leq j \leq i$ then we choose the colour of v_{i+1} *greedily*

$$c(v_{i+1}) := \min\{b \in \{0, \ldots, \Delta\} \mid \forall j \in \Gamma(v_{i+1}),\ j \leq i \implies c(v_j) \neq b\}.$$

Since $d(v_{i+1}) \leq \Delta$ and we have $\Delta + 1$ colours this value is well-defined (it is the minimum of a non-empty subset of $\{0, 1, \ldots, \Delta\}$).

There are two fundamentally different ways to implement the `succ` step of this algorithm in Lean. It can either be computable or noncomputable.

The computable version: first prove that the set of possible colors is a non-empty subset of the finite set $\{0, 1, \ldots, \Delta\}$ and then compute its minimum using `Finset.min'`.

The noncomputable version: given a proof `(h : ∃ b, p b)`, using the axiom of choice, `Classical.choose h` will magically produce an element `b` satisfying `p b`. (In our case `p` would be the proposition that $\forall j \in \Gamma(v_{i+1}),\ j \leq i \implies c(v_j) \neq b$.)

The computable version will allow us to actually compute examples of greedy colorings, so if possible try to make your greedy algorithm computable.

Possible extensions: (these are independent of each other and you should only attempt at most one of them.)

(1) Consider a graph G with vertex set $\mathbb{N}$. For $n \in \mathbb{N}$ define

$$\mathrm{degLT}_G(n) = \#\{m \in \mathbb{N} : m \text{ is a neighbor of } n \text{ and } m < n\}.$$

So $\text{degLT}_G(n)$ is the number of neighbors of the vertex n that come before n in the usual ordering of $\mathbb{N}$. Prove the following theorem

Theorem. *If G is a graph with vertex set $\mathbb{N}$ and $\forall n, \text{degLT}_G(n) \leq \Delta$ then G is $(\Delta+1)$-colorable.*

Bonus points: make your proof of the previous theorem constructive by defining a computable $(\Delta+1)$-coloring of such a graph.

(2) Prove the following theorem. [Requires some topology: namely compactness and product spaces.]

Theorem. *(De Bruijn–Erdős) A graph $H = (V, E)$ is k-colorable iff every finite induced subgraph is k-colorable*

Proof: If H is k-colorable and $A \subseteq V$ is finite, then any k-coloring of H is also a k-coloring of $H[A]$ (the subgraph of H induced by A).

Conversely suppose that for every finite subset $A \subseteq V$ we know that $H[A]$ is k-colorable. Consider the set $X := V \to [k]$ endowed with the product topology. By Tychonoff's theorem this space is compact. (Note that in Lean the compactness will be inferred as an instance so you won't need to prove this!)

For any finite subset $A \subseteq V$ let

$$X_A = \{f \in X \mid f \text{ is a legal } k\text{-coloring of } H[A]\}.$$

We can prove that (1) each X_A is a closed subset of X and (2) the family of subsets of X

$$\mathcal{F} = \{X_A \mid A \subseteq V,\ A \text{ finite }\},$$

has the *finite intersection property* (i.e. the intersection of any finite subfamily of $\mathcal{F}$ is nonempty).

By compactness of X this implies that $\bigcap_{F \in \mathcal{F}} F$ is nonempty. You can then check that any element of this intersection is a legal k-coloring of H. □

Corollary. *If $H = (V, E)$ is a graph satisfying $\forall v \in V$, $d(v) \leq \Delta$ then H is $(\Delta+1)$ -colorable.*

Proof: By the previous theorem this follows if we prove that all finite induced subgraphs of H are $(\Delta+1)$ -colorable. This in turn follows by using the greedy algorithm. □

4.2 Intersecting Families of sets (`Intersecting`)

Prerequisites: MATH0029 Graph Theory and Combinatorics

We say that a family of sets $\mathcal{A}$ is *intersecting* if $A, B \in \mathcal{A}$ implies $A \cap B \neq \emptyset$.

Given a finite nonempty set α let $\mathcal{P}(\alpha) = \{A \mid A \subseteq \alpha\}$ denote its powerset. We say that a family $\mathcal{A} \subseteq \mathcal{P}(\alpha)$ is a *maximally intersecting family* iff $\mathcal{A}$ is intersecting and $\mathcal{A}$ is not properly contained in any larger intersecting family from $\mathcal{P}(\alpha)$.

The main aim of this project is to prove the following theorem.

Theorem. (Main) *If $\mathcal{A} \subseteq \mathcal{P}(\alpha)$ is a maximally intersecting family then*

$$|\mathcal{A}| = 2^{|\alpha|-1}.$$

Given a family $\mathcal{A}$ we need some notation for the family of the complements of members of $\mathcal{A}$. This is not, in general, the same as the complement of $\mathcal{A}$ in $\mathcal{P}(\alpha)$ but we will abuse notation by defining this to be

$$\mathcal{A}^c := \{A^c \mid A \in \mathcal{A}\}.$$

As a warm-up we first prove an upper bound on the size of any intersecting family.

Theorem. *If $\mathcal{A} \subseteq \mathcal{P}(\alpha)$ is an intersecting family then*

$$|\mathcal{A}| \leq 2^{|\alpha|-1}.$$

Proof: Given any member A of an intersecting family $\mathcal{A}$ we know that $A^c \notin \mathcal{A}$ (since A and A^c are disjoint). This implies (with our abuse of notation) that $\mathcal{A}$ and $\mathcal{A}^c$ are disjoint as families of sets in $\mathcal{P}(\alpha)$. Moreover $|\mathcal{A}| = |\mathcal{A}^c|$ since the map $A \mapsto A^c$ is bijective. The bound then follows from the fact that $|\mathcal{P}(\alpha)| = 2^{|\alpha|}$. □

Proof of Main Theorem: This result will follow if we prove that any maximally intersecting family $\mathcal{A}$ satisfies $\mathcal{P}(\alpha) = \mathcal{A} \cup \mathcal{A}^c$. This in turn will follow if we prove that for any $B \in \mathcal{P}(\alpha)$ either $B \in \mathcal{A}$ or $B^c \in \mathcal{A}$.

Suppose that $\mathcal{A} \subseteq \mathcal{P}(\alpha)$ is a maximally intersecting family and let $B \in \mathcal{P}(\alpha)$. If $\mathcal{A} \cup \{B\}$ is intersecting then the maximality of $\mathcal{A}$ implies that $B \in \mathcal{A}$ so suppose that $\mathcal{A} \cup \{B\}$ is not intersecting. So there is $C \in \mathcal{A}$ such that $B \cap C = \emptyset$. Hence $C \subseteq B^c$. But this implies that $\mathcal{A} \cup \{B^c\}$ is intersecting, and hence by maximality $B^c \in \mathcal{A}$. □

Possible extension:

Let $\alpha_n = \{0, 1, \ldots, n\}$. We will describe a computable function that, when given an intersecting family $\mathcal{A} \subseteq \mathcal{P}(\alpha_n)$, returns a maximal intersecting family containing $\mathcal{A}$.

Given a family $\mathcal{A} \subseteq \mathcal{P}(\alpha_n)$ let $\uparrow \mathcal{A} = \{B \subseteq \alpha_n \mid \exists A \in \mathcal{A},\ A \subseteq B\}$ denote the family of all super-sets of members of $\mathcal{A}$.

We will call a set $B \in \mathcal{P}(\alpha_n)$ *big* iff either $|B^c| < |B|$ or ($|B^c| = |B|$ and $n \in B$). Let $\mathcal{B}(\alpha_n)$ denote the family of big sets in $\mathcal{P}(\alpha_n)$. It is easy to check that $\mathcal{B}(\alpha_n)$ is intersecting.

Given a family of sets $\mathcal{A} \subseteq \mathcal{P}(\alpha_n)$ we define

$$\mathcal{B}(\mathcal{A}) = \{B \in \mathcal{B}(\alpha_n) \mid \forall A \in \mathcal{A}, A \cap B \neq \emptyset \text{ and } A \cap B^c \neq \emptyset.\}.$$

Theorem. *For any intersecting family $\mathcal{A} \subseteq \mathcal{P}(\alpha_n)$ the family*

$$\max(\mathcal{A}) := \uparrow \mathcal{A} \cup \mathcal{B}(\mathcal{A}),$$

is a maximally intersecting family containing $\mathcal{A}$.

4.3 Mycielskian (`Mycielskian`)

Prerequisites: MATH0029 Graph Theory and Combinatorics

Given a graph G of order n, the *Mycielskian* of G is the graph $M(G)$ of order $2n+1$ defined as follows. If $V(G) = \{v_1, v_2, \ldots, v_n\}$ then $M(G)$ has vertex set

$$V(G) \,\dot\cup\, \{u_1, u_2, \ldots, u_n\} \,\dot\cup\, \{w\}.$$

The edges of $M(G)$ are

$$E(G) \,\dot\cup\, \{wu_i \mid 1 \le i \le n\} \,\dot\cup\, \{u_i v_j \mid v_i v_j \in E(G)\}.$$

The first aim of this project is to prove the following results.

Theorem. *If G is K_3-free then its Mycielskian is K_3-free.*

Proof: Check all possible subsets of size three in $V(M(G))$ and see that none of them form a copy of K_3 (assuming that G is K_3-free). □

Theorem. *The graph G is k-colourable iff its Mycielskian is $(k+1)$-colourable.*

Proof: If c is a k-coloring of G we can form a $(k+1)$-coloring of $M(G)$ by setting $d(v_i) = c(v_i)$, $d(u_i) = c(v_i)$ and $d(w) = k+1$. You can check that this is a legal $(k+1)$-coloring of $M(G)$.
Conversely if $M(G)$ is $(k+1)$-colorable then (by swapping colors if necessary) take a $(k+1)$-coloring c of $M(G)$ with $c(w) = k+1$. Now define a k-coloring of G as follows: if $c(v_i) = k+1$ then let $d(v_i) = c(u_i)$ otherwise let $d(v_i) = c(v_i)$. You can check that d is a legal k-coloring of G. □

The Mycielskian can be used to construct triangle-free graphs with arbitrarily large chromatic number. In particular if we define $M_0 = K_2$ (a single edge) and then define $M_{k+1} = M(M_k)$ then we can prove the following result.

Theorem. *For each $n \ge 0$, M_n has order $3 \cdot 2^n - 1$, is K_3-free, and has chromatic number $n+2$.*

Proof: The fact that M_n is K_3-free and has chromatic number $n+2$ follows from the earlier results by induction. The fact that it has order $3 \cdot 2^n - 1$ is a straightforward induction. □

Possible extension: computing the exact number of edges in M_n for all n would be messy (but not impossible), but we can compute the number of edges in some non-trival examples. For instance you could prove the following result (replacing X with a correct value).

Theorem. *There exists a K_3-free graph of order 95, with chromatic number 7 and X edges.*

4.4 Ramsey Theory (`Ramsey`)

Prerequisites: MATH0029 Graph Theory and Combinatorics

There are three possible projects in Ramsey theory, all contained in the same file `Ramsey.lean`. Each project forms a separate section of the file.

4.4.1 Ramsey's theorem for two colours (`section twocolour`)

The aim of this project is to prove Ramsey's theorem for graphs. (See MATH0029 lecture notes for definitions.)

Theorem (Ramsey)**.** *For $s, t \geq 2$ there exists $n \in \mathbb{N}$ such that any red-blue edge-coloured K_n contains either a red K_s or a blue K_t. Moreover if $R(s,t)$ denotes the smallest such n then*

$$R(s,t) \leq \binom{s+t-2}{s-1}.$$

Proof: (By induction on $m = s+t$.) Clearly $R(2,t) = t = \binom{2+t-2}{1}$ and $R(s,2) = s = \binom{s+2-2}{s-1}$ (since any red-blue edge-colouring of K_t either contains a red edge or is entirely blue and similarly for $R(s,2)$). In particular the result holds for $s+t = 4$.

Suppose the result holds for all pairs (s',t') with $s'+t' = m \geq 4$, let $s+t = m+1$ we need to prove the result holds for (s,t). (Note we may also assume that $s,t \geq 3$ since we already checked the result in the cases $s = 2$ or $t = 2$.)

Our inductive hypothesis allows us to assume the result holds for any pair with sum m, in particular we can assume that the theorem holds for $(s-1,t)$ and $(s,t-1)$. (And both of these cases make sense since $s,t \geq 3$.)

Let $n = R(s-1,t) + R(s,t-1)$ (these both exist by our inductive hypothesis) and suppose we have a red-blue edge-colouring of K_n. Consider a vertex v. Since $d(v) = n-1 = R(s-1,t) + R(s,t-1) - 1$ and $d(v) = d_{\text{red}}(v) + d_{\text{blue}}(v)$ then either (1) $d_{\text{red}}(v) \geq R(s-1,t)$ or (2) $d_{\text{blue}}(v) \geq R(s,t-1)$. In case (1) $\Gamma_{\text{red}}(v)$ contains a blue K_t or a red K_{s-1} which, together with v, forms a red K_s. In case (2) $\Gamma_{\text{blue}}(v)$ contains a red K_s or a blue K_{t-1} which, together with v, forms a red K_t.

Hence any red-blue edge-coloured K_n contains a red K_s or a blue K_t. So $R(s,t)$ exists and satisfies (using our inductive hypothesis in the second inequality below)

$$\begin{aligned} R(s,t) &\leq R(s-1,t) + R(s,t-1) \\ &\leq \binom{(s-1)+t-2}{(s-1)-1} + \binom{s+(t-1)-2}{s-1} \\ &= \binom{s+t-2}{s-1}. \end{aligned}$$

□

The proof of this result in Lean follows the same basic structure, but rather than defining $R(s,t)$ as the minimum of a potentially empty set we instead define a predicate on $\mathbb{N}$ saying that `RamseyOf`(n,s,t) is true, iff every red/blue edge coloring of K_n contains a red K_s or blue K_t.

In Lean it is easier to prove the result for all $s,t \geq 1$ rather than just $s,t \geq 2$ so we need to think about what it means for an edge-coloring of K_n to contain a monochromatic K_1? Well, it means there exists a K_1 in K_n all of whose edges have the same colour. Since K_1 has no edges this is true of any K_1 in K_n so holds for any $n \geq 1$. This change actually simplifies the proof since we no longer need to consider the cases $R(s,2)$ and $R(2,t)$ separately.

Rather than doing the induction on $s+t$ in the main theorem we can instead do a double induction on s and then on t. This is sketched out in the Lean file.

Possible extension: prove some constructive lower bounds for small values of s and t.

4.4.2 Ramsey's theorem for k colours (`section kcolours`)

We will assume Ramsey's theorem for two colours and establish Ramsey's theorem for k colours.

For $k \geq 1$ and $s_1, \ldots, s_k \geq 2$ define $R_k(s_1, s_2, \ldots, s_k)$ to be the smallest integer n such that for any edge-colouring of K_n with k colours $c_1, \ldots, c_k$, there exists a c_i-coloured copy of K_{s_i} for some $1 \leq i \leq k$.

Theorem. *For all $k \geq 1$ and $s_1, \ldots, s_k \geq 2$, $R_k(s_1, \ldots, s_k)$ is well defined.*

Proof: By induction on k. True for $k = 1, 2$ (for $k = 2$ by Ramsey's theorem (see previous section). Suppose that $k \geq 2$ and let $s_1, \ldots, s_{k+1} \geq 2$ we will show that $R_{k+1}(s_1, \ldots, s_k, s_{k+1})$ is well-defined.

Let $n = R(R_k(s_1, s_2, \ldots, s_k), s_{k+1}))$, which exists by Ramsey's theorem for two-colours and by our inductive hypothesis. Take an edge-colouring of K_n with $k+1$ colours $c_1, \ldots, c_{k+1}$. We first consider this as an edge-colouring with 2 colours by pretending to be colour-blind. We consider anything coloured with $c_1, c_2, \ldots, c_k$ as having a new colour c^*, so we have a edge-colouring of K_n with colours c^* and c_{k+1}.

By our choice of n and Ramsey's theorem for two colours we either have a c^*-coloured copy of $K_{R_k(s_1, s_2, \ldots, s_k)}$ or we have a c_{k+1}-coloured copy of $K_{s_{k+1}}$. In the latter case we are done. In the former case we now stop being colour-blind and realise that we have a k-edge colouring of $K_{R_k(s_1, s_2, \ldots, s_k)}$ with colours $c_1, \ldots, c_k$, which by our inductive hypothesis contains a c_i-coloured copy of K_{s_i} for some $1 \leq i \leq k$. □

Possible extension: prove some constructive lower bounds for $k = 3$, or use your result to prove Schur's theorem in the next section.

4.4.3 Schur's theorem (`section schur`)

Let $R_k(3)$ denote the k-color Ramsey number for triangles. I.e. $R_k(3)$ is the smallest integer n such that any k-coloring of the edges of K_n contains a monochromactic triangle. (See previous section for proof that this exists.)

Theorem (Schur)**.** *For any $k \in \mathbb{N}$ there exists $N \in \mathbb{N}$ such that in any k-colouring of $\mathbb{N}$, $c : \mathbb{N} \to \{1, 2, \ldots, k\}$ there exist $x, y, z \in \{1, \ldots, N\}$ such that $x + y = z$ and $c(x) = c(y) = c(z)$.*

Proof: Let $n \geq R_k(3)$ and consider a k-colouring of $\{1, 2, \ldots, n\}$ given by $c : [n] \to [k]$. We define a colouring γ of the edges of K_n by $\gamma(xy) = c(|x - y|)$. By our choice of n and the definition of $R_k(3)$ there is a monochromatic triangle in K_n. Suppose its vertices are $x > y > z$ and $\gamma(xy) = \gamma(xz) = \gamma(yz) = c^*$. Let $u = x - y$, $v = y - z$, $w = x - z$. Then $u + v = x - y + y - z = x - z = w$ and $c(u) = c(v) = c(w) = c^*$. □

Schur's theorem follows quite easily from the k-colour version of Ramsey's theorem which we will assume.

Possible extensions:

1. Prove some constructive lower bounds for small values of k.
2. Generalise the result to other equations.
3. Prove the following theorem (see MATH0029 notes for details).

   Theorem. *For every integer $n \geq 1$ there exists p_n such that for any prime $p \geq p_n$ the congruence*

   $$x^n + y^n = z^n \mod p$$

   has a non-trivial solution (i.e. a solution with $x, y, z \neq 0 \mod p$).

5 Linear Algebra (`LinearAlgebra`)

5.1 Gaussian Elimination (`GaussElim`)

Prerequisites: MATH0005 Algebra 1

A square matrix is *upper triangular* iff all entries below its diagonal are zero.

Given an $n \times n$ matrix M over a field $\mathbb{F}$ we will consider the computational problem of reducing M to *upper triangular form* using elementary row operations.

Our Gaussian elimination algorithm (`GaussStep`) works as follows.

(Input) M an $n \times n$ matrix over a field $\mathbb{F}$.

(Check) If M is upper triangular then stop.

(Find J) Identify the first column containing a non-zero entry below the diagonal and call the index of this column J.

(Find I) Identify the first non-zero entry in column J below the diagonal and call its row index I.

(GaussStep) If $M_{J,J} = 0$ then swap rows I and J else subtract $M_{I,J}M_{J,J}^{-1}$ times row J from row I. Return to (Check).

The main goal of this project is to prove that this algorithm terminates with an upper triangular matrix after at most $n^2 - 1$ iterations.

See below for an example of applying this algorithm (over $\mathbb{Q}$), at each step the pivot is underlined.

$$\begin{pmatrix} 1 & 2 & 1 & 0 \\ 0 & 1 & 2 & 1 \\ \underline{1} & 3 & 3 & 0 \\ 2 & 4 & 1 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 1 & 0 \\ 0 & 1 & 2 & 1 \\ 0 & 1 & 2 & 0 \\ \underline{2} & 4 & 1 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 1 & 0 \\ 0 & 1 & 2 & 1 \\ 0 & \underline{1} & 2 & 0 \\ 0 & 0 & -1 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 1 & 0 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & \underline{-1} & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 1 & 0 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & -1 & 2 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

Our main theorem is as follows.

Theorem. *Given any $n \times n$ matrix M over a field $\mathbb{F}$ the Gaussian elimination algorithm will terminate with an upper triangular matrix after at most $n^2 - 1$ iterations.*

Proof (sketch): If M is an $n \times n$ not upper triangular (NUT) matrix we define its weight to be $I + nJ$, where (I, J) is the pivot described above. We will show (see lemmas below) that any application of `GaussStep` either increases

this weight by at least one, or produces an upper triangular matrix. It is easy to check that the weight is bounded above by $n^2 - 1$ (since $I, J \leq n - 1$) and this implies that the algorithm repeats at most $n^2 - 1$ times. □

Lemma. *If M is a NUT matrix with pivot (I, J) and $M_{J,J} = 0$ then* `GaussStep`(M)*, the matrix given by swapping rows I and J is either upper triangular or it is NUT and satisfies*

$$\text{weight}(\texttt{GaussStep}(M)) \geq \text{weight}(M) + 1.$$

Lemma. *If M is a NUT matrix with pivot (I, J) and $M_{J,J} \neq 0$ then* `GaussStep`(M)*, the matrix given by subtracting $M_{I,J}M_{J,J}^{-1}$ times row J from row I is either upper triangular or it is NUT and satisfies*

$$\text{weight}(\texttt{GaussStep}(M)) \geq \text{weight}(M) + 1.$$

Proof of lemmas: In both cases either the matrix `GaussStep`(M) is upper triangular, or, if it is NUT, then it has a new pivot (I', J') which satisfies $J < J'$ or ($J = J'$ and $I < I'$) and hence has strictly larger weight. □

Possible extension: Describe a function that computes the transition matrix P such that PM is the upper triangular form of M (and prove that P is invertible).

5.2 Steinitz Exchange Lemma (`SteinitzExchange`)

Prerequisites: MATH0006 Algebra 2

The main goal of this project is to prove the Steinitz Exchange Lemma for complex vector spaces and deduce that any two bases in a finite dimensional complex vector space have the same size.

Let V be a complex vector space.

Theorem (Steinitz)**.** *If $A, B \subseteq V$ are finite with*

(i) A is linearly independent,

(ii) $\mathrm{span}(A) \subseteq \mathrm{span}(B)$*,*

then there exists a finite set $C \subseteq B$ such that $|A \cup C| = |B|$ and $\mathrm{span}(A \cup C) = \mathrm{span}(B)$*.*

The following simple lemma is useful for the proof Steinitz's theorem.

Lemma. *If $A, B \subseteq V$ are finite, $v \notin \mathrm{span}(A)$ and $v \in \mathrm{span}(B)$ then there exist coefficients $\lambda_b \in \mathbb{R}$, $b \in B$ and $\hat{b} \in B \setminus A$ such that $\lambda_{\hat{b}} \neq 0$ and*

$$v = \sum_{b \in B} \lambda_b b.$$

Proof: Since $v \in \mathrm{span}(B)$ there exist coefficients $\lambda_b \in \mathbb{R}$, for $b \in B$, such that

$$v = \sum_{b \in B} \lambda_b b = \sum_{b \in B \setminus A} \lambda_b b + \sum_{b \in A \cap B} \lambda_a a.$$

If $\lambda_b = 0$ for all $b \in B \setminus A$ then $v \in \mathrm{span}(A \cap B) \subseteq \mathrm{span}(A)$, a contradiction, hence there exists $\hat{b} \in B \setminus A$ with $\lambda_{\hat{b}} \neq 0$. □

Proof of Steinitz: By induction on $|A|$. If $|A| = 0$ then $A = \emptyset$ and we can take $C = B$.

So suppose $|A| = n+1$ and the result holds for $|A| = n$. Let $A = A' \cup \{v\}$, where $v \notin A'$, satisfy A is linearly independent and $\mathrm{span}(A) \subseteq \mathrm{span}(B)$. We can apply our inductive hypothesis to A' and obtain $C' \subseteq B$ such that $|A' \cup C'| = |B|$ and $\mathrm{span}(A' \cup C') = \mathrm{span}(B)$. If $v \in C'$ then we are done so suppose that $v \notin C'$.

We know that $v \notin \mathrm{span}(A')$ since $A = A' \cup \{v\}$ is linearly independent so by our lemma (since $v \notin \mathrm{span}(A')$ and $v \in \mathrm{span}(A' \cup C')$) there exist coefficients $\lambda_w \in \mathbb{R}$, for $w \in A' \cup C'$, and $\hat{w} \in (A' \cup C') \setminus A'$ such that $\lambda_{\hat{w}} \neq 0$ and

$$v = \sum_{w \in A' \cup C'} \lambda_w w. \tag{1}$$

We claim that we can take $C = C' \setminus \{\hat{w}\}$. Clearly $C \subseteq C' \subseteq B$ and

$$|A \cup C| = |A' \cup \{v\} \cup (C' \setminus \{\hat{w}\})| = |A' \cup C'| + 1 - 1 = |B|$$

since $v \notin A' \cup C'$ while $\hat{w} \in C' \setminus A'$.

Finally we need to check that $\mathrm{span}(A \cup C) = \mathrm{span}(B)$. This is equivalent to checking that $\mathrm{span}(A' \cup \{v\} \cup C' \setminus \{\hat{w}\}) = \mathrm{span}(A' \cup C')$.

That $\mathrm{span}(A' \cup \{v\} \cup C' \setminus \{\hat{w}\}) \subseteq \mathrm{span}(A' \cup C')$ follows from the fact that $v \in \mathrm{span}(A' \cup C')$.

Conversely if $u \in \mathrm{span}(A' \cup C')$ then we can use (1) to express u as a linear combination of elements of $A' \cup \{v\} \cup C' \setminus \{\hat{w}\}$ as follows. First we use the fact that $\lambda_{\hat{w}} \neq 0$ to write

$$\hat{w} = \lambda_{\hat{w}}^{-1} v - \sum_{x \in (A' \cup C') \setminus \{\hat{w}\}} \lambda_{\hat{w}}^{-1} \lambda_x x.$$

So if $u = \sum_{x \in A' \cup C'} \mu_x x$ then

$$u = \mu_{\hat{w}} \lambda_{\hat{w}}^{-1} v + \sum_{x \in (A' \cup C') \setminus \{\hat{w}\}} (\mu_x - \mu_{\hat{w}} * \lambda_{\hat{w}}^{-1} \lambda_x) x.$$

Hence $u \in \mathrm{span}(A' \cup \{v\} \cup C' \setminus \{\hat{w}\})$. □

We say that a V is *finite dimensional* iff there exists a finite set of vectors B that spans V.

As a corollary of Steinitz's theorem we obtain the following result.

Theorem. *If A and B are bases of a finite dimensional vector space V then $|A| = |B|$.*

Proof: Steinitz implies that if A is an independent set and B is a finite spanning set then $|A| \leq |B|$.

If A and B are bases of a finite dimensional vector space then they are both independent spanning sets. Thus $|A| \leq |B|$ and $|B| \leq |A|$ and we deduce that $|A| = |B|$. □

There are many possible extensions:

For example you could define a structure `Subspace V` and construct `span A` as a term of type `Subspace V`.

Define an instance of `Add (Subspace V)` (the sum of two subspaces).

Define an instance of `Inter (Subspace V)` (the intersection of two subspaces).

Prove the dimension formula: $\dim(A + B) + \dim(A \cap B) = \dim A + \dim B$.

6 Number Theory (NumberTheory)

6.1 Convergence of continued fractions (ContinuedFrac)

Let $a_0, a_1 \ldots$ be a sequence of positive integers. The (finite) continued fraction $CFrac([a_0, \ldots, a_n])$ is defined to be the number

$$CFrac([a_0, \ldots, a_n]) := a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots + \frac{1}{a_n}}}}.$$

In lean this is defined as follows

```
def CFrac : List ℝ → ℝ
| []      => 0
| x :: xs => x + 1 / (CFrac xs)
```

The aim of this project is to prove that all infinite continued fractions converge, i.e.

Theorem. *Then the sequence $CFrac([a_0, \ldots, a_n])$ converges as $n \to \infty$.*

To prove the theorem, we first define the "numerator" and "denominator" of the continued fraction $CFrac([a_0, \ldots, a_n])$ as follows:

$$numer(n) = \begin{cases} a_0 & n = 0 \\ a_0 a_1 + 1 & n = 1 \\ a_{n+2} \cdot numer(n-1) + numer(n-2) & n \geq 2, \end{cases}$$

$$denom(n) = \begin{cases} 1 & n = 0 \\ a_1 & n = 1 \\ a_{n+2} \cdot denom(n-1) + denom(n-2) & n \geq 2. \end{cases}$$

In lean this definition is:

```
def numer : ℕ → ℕ+
| 0   => a 0
| 1   => (a 0) * (a 1) + 1
| n+2 => a (n+2) * numer (n+1) + numer n

def denom : ℕ → ℕ+
| 0   => 1
| 1   => (a 1)
| n+2 => a (n+2) * denom (n+1) + denom n
```

Lemma. *For any positive real number α we have*

$$CFrac([a_0, \ldots, a_{n+1}, \alpha]) = \frac{numer(n+1)\alpha + numer(n)}{denom(n+1)\alpha + denom(n)}.$$

Proof. This follows easily by induction on n. □

Lemma.

$$CFrac([a_0, \ldots, a_n]) = \frac{numer(n)}{denom(n)}.$$

Proof. This as a special case of the previous lemma. (The reason why the more general lemma is stated is because it is easier to prove by induction than this special case.) □

Lemma. *For all n we have:*

$$numer(n+1) \cdot denom(n) - numer(n) \cdot denom(n+1) = (-1)^n.$$

Proof. This follows by induction on n. □

Lemma. *For al n we have*

$$CFrac([a_0, \ldots, a_{n+1}]) - CFrac([a_0, \ldots, a_n]) = \frac{(-1)^n}{denom(n) \cdot denom(n+1)}.$$

Proof. This follows from the previous two lemmas. □

Lemma.

$$CFrac([a_0, \ldots, a_{n+1}]) = a_0 + \sum_{i=0}^{n} \frac{(-1)^i}{denom(i) \cdot denom(i+1)}$$

Proof. This follows from the previous lemma by induction. □

Proof of the Theorem. This follows from the previous lemma by the alternating series test. (Note that $denom(n)$ is a strictly increasing sequence of natural numbers, so $denom(i) \cdot denom(i+1) \to \infty$.) □

As an example, you could prove that in the case $a_0 = a_1 = \ldots = 1$, the continued fraction

$$1 + \cfrac{1}{1 + \cfrac{1}{1 + \ddots}}$$

converges to to "golden ratio" $\alpha = \frac{1+\sqrt{5}}{2}$. In this case the sequences $numer(n)$ and $denom(n)$ are the Fibonacci numbers, and the limit is calculated using the following formula for the Fibonacci sequence:

$$F_n = \frac{(\frac{1+\sqrt{5}}{2})^n - (\frac{1-\sqrt{5}}{2})^n}{\sqrt{5}}.$$

You can prove by a similar method that

$$2 + \cfrac{1}{2 + \cfrac{1}{2 + \ddots}} \text{ converges to } 1 + \sqrt{2}.$$

If you'd like to extend the project further, then you could prove that every real number $\alpha > 1$, there is a sequence of positive integers a_n, whose continued fraction converges to α. The sequence a_n is defined recursively as follows:

$$\alpha_0 = \alpha, \qquad \alpha_{n+1} = \frac{1}{\alpha_n - \lfloor \alpha_n \rfloor}, \qquad a_n = \lfloor \alpha_n \rfloor.$$

6.2 The Eisenstein integers (`EisensteinIntegers`)

The aim of the project is to construct the ring of Eisenstein integers and prove that this ring is norm-Euclidean.

Let $\omega = \frac{1+\sqrt{-3}}{2}$. An Eisenstein integer is a complex number of the form $x + y\omega$, where x and y are integers. The set of all of these numbers is written $\mathbb{Z}[\omega]$. We can define the Eisenstein integers as a structure as follows:

```
structure EisensteinInt : Type where
  x : ℤ
  y : ℤ
notation "ℤ[ω]" => EisensteinInt
```

- Define operations of addition and multiplication on the Eisenstein integers and prove that they form a commutative ring. I.e. create an instance

  ```
  instance : CommRing ℤ[ω] := sorry
  ```

- Define a function which takes an Eisenstein integer to the corresponding complex number. Prove that this function is a ring homomorphism.
- Define the norm function $N(x + y\omega) = x^2 - xy + y^2$. Prove that $N(A) = |A|^2$.
- Prove that if $A, B \in \mathbb{Z}[\omega]$ with $B \neq 0$, then there exist $Q, R \in \mathbb{Z}[\omega]$, such that $A = QB + R$ and $N(R) < N(B)$. Using this lemma, create an instance

  ```
  instance : EuclideanDomain ℤ[ω] := sorry
  ```

The key lemma above is the following:

Lemma. *Let $A, B \in \mathbb{Z}[\omega]$ with $B \neq 0$, then there exist $Q, R \in \mathbb{Z}[\omega]$, such that $A = QB + R$ and $N(R) < N(B)$.*

Proof. Let $\frac{A}{B} = x + y\omega$ with $x, y \in \mathbb{Q}$. Choose the nearest integer b to y, so that $|b - y| \leq \frac{1}{2}$. This implies $|\Im(x + (y - b)\omega)| \leq \frac{\sqrt{3}}{4}$. Then choose the nearest integer a to $x + (y - b)\omega$. Then we have $|\Re((x - a) + (y - b)\omega| \leq \frac{1}{2}$. As a consequence of this, we have

$$N\left(\frac{A}{B} - (a + b\omega)\right) = |((x - a) + (y - b)\omega|^2 \leq \left(\frac{1}{2}\right)^2 + \left(\frac{\sqrt{3}}{4}\right)^2 < 1.$$

If we set $Q = a + b\omega$ and $R = A - QB$, then we have $A = QB + R$. We have from the inequality above:

$$N\left(\frac{R}{B}\right) = N\left(\frac{A}{B} - (a + b\omega)\right) < 1,$$

and this implies $N(R) < N(B)$. $\square$

If you'd like to take this further, then you could prove the "Disappointing Theorem" from MATH0034, which says that $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ is a Euclidean ring for $d = -3, -7, -11, 5, 13$ and $\mathbb{Z}[\sqrt{d}]$ is a Euclidean ring for $d = -1, -2, 2$. Alternatively, you could prove that if p and q are distinct odd primes then $\mathbb{Z}[\sqrt{-pq}]$ is not a Euclidean ring. The reason for this is because the elements p, q and $\sqrt{-pq}$ are all irreducible in this ring, so we have two different factorizations into irreducibles:

$$p \cdot q = -\sqrt{-pq} \cdot \sqrt{-pq}.$$

6.3 Units in the Ring $\mathbb{Z}[\frac{1+\sqrt{13}}{2}]$ (`QuadraticRingUnits`)

This material is on material from MATH0034. The aim of this project is to find the units in the ring $\mathbb{Z}[\frac{1+\sqrt{13}}{2}]$.

Let $\alpha = \frac{1+\sqrt{5}}{2}$. The set of all numbers $x + y\alpha$ with $x, y \in \mathbb{Z}$ is written $\mathbb{Z}[\alpha]$. This set is a ring with the usual operations of addition and multiplication. This ring has infinitely many invertible elements. For example the element $1 + \alpha$ is invertible, with inverse $\alpha - 2$, because $(1 + \alpha)(\alpha - 2) = 1$. More generally, the powers $(1 + \alpha)^n$ is invertible. The aim of the project is to prove that all the invertible elements of this ring have the form $\pm(1 + \alpha)^n$ for some $n \in \mathbb{Z}$. This is equivalent to finding all solutions to the Diophantine equations

$$x^2 + xy - 3y^2 = \pm 1.$$

We define the *conjugate* of an element $A = x + y \cdot \alpha$ to be

$$\bar{A} = x + y \cdot (1 - \alpha),$$

Lemma. *For all $A, B \in \mathbb{Z}[\alpha]$ we have*

$$\overline{A + B} = \bar{A} + \bar{B}, \qquad \overline{A \cdot B} = \bar{A} \cdot \bar{B}, \qquad \bar{\bar{A}} = A.$$

Proof. These are all easy to check. □

The norm, $N(A)$ of an element $A = x + y \cdot \alpha$ is defined by

$$N(A) = x^2 + xy - 3y^2.$$

Lemma. *For all elements $A, B \in \mathbb{Z}[\alpha]$ we have*

$$N(A) = A \cdot \bar{A}, \qquad N(AB) = N(A)N(B).$$

Lemma. *$N(A) = 0$ if and only if $A = 0$.*

Proof. It's trivial to check that $N(0) = 0$. Conversely, suppose $N(A) = 0$ with some $A = x+y\alpha \neq 0$. Dividing through by $\gcd(x, y)$ if necessary, we can assume that x and y are coprime. Multiplying the equation $N(A) = 0$ by 4, we get

$$(2x + y)^2 + 13y^2 = 0.$$

Hence 13 is a factor of $(2x+y)^2$. Since 13 is prime, it follows that 13 is a factor of $2x+y$. This implies that 13 is a factor of y^2, and hence also of y. Since 13 is a common factor of $2x+y$ and y, it must also be a factor of x. This contradicts our assumption that x and y are coprime. □

Lemma. *Let A be an element of $\mathbb{Z}[\alpha]$. Then A is a unit (i.e. invertible) if and only if $N(A) = \pm 1$.*

Proof. If $N(A) = \pm 1$ then $A\bar{A} = \pm 1$. Therefore $\pm\bar{A}$ is an inverse of A.

Conversely suppose $AB = 1$ then $N(AB) = N(1) = 1$. This implies $N(A)N(B) = 1$, so $N(A)$ is invertible in $\mathbb{Z}$. Therefore $N(A) = \pm 1$. □

We can check that the element $u_1 = 1 + \alpha$ has norm -1, and is therefore a unit in $\mathbb{Z}[\alpha]$; its inverse is $\alpha - 2$. The powers of u_1 are also units in $\mathbb{Z}[\alpha]$. We can prove a formula for these powers as follows: Define two sequences of integers recursively as follows:

$$x_0 = 1, \qquad x_1 = 1, \quad x_{n+2} = x_n + 3x_{n+1},$$

$$y_0 = 0, \qquad y_1 = 1, \quad y_{n+2} = y_n + 3y_{n+1}.$$

Lemma. *For all natural numbers n we have $u^n = x_n + y_n\alpha$.*

Proof. We can easily prove by induction on n that $x_{n+1} = x_n + 3y_n$ and $y_{n+1} = x_n + 2y_n$ for all natural numbers n. Using this result, we can prove the lemma by induction. The result is easy to check for $n = 0$, and we have

$$\begin{aligned} u_1^{n+1} &= (1 + \alpha)u_1^n \\ &= (1 + \alpha)(x_n + y_n\alpha) \\ &= (x_n + 3y_n) + (x_n + 2y_n)\alpha. \end{aligned}$$

□

Lemma. *Let $U > 1$ be a unit in $\mathbb{Z}[\alpha]$. Then $U \geq u_1$.*

Proof. Let $U = x + y\alpha$. Since $U\bar{U} = \pm 1$, we must have $-1 < \bar{U} < 1$. This implies

$$2x + y = U + \bar{U} > 0, \qquad \sqrt{13}y = U - \bar{U} > 0.$$

Suppose for the sake of argument that $U < u_1$. Combining this with the two inequalities above, we can deduce that $y = 1$. Since $x^2 + xy + 3y^2 = N(U) = \pm 1$. it follows that x is a solution to one of the two quadratic equations:

$$x^2 + x - 2 = 0, \qquad x^2 + x - 4 = 0.$$

The second of these has no integer solutions. The first has solutions $x = -2$ and $x = 1$. In these cases we have $U = u_1$ and $u = u_1^{-1}$ respectively. Both of these cases contradict the assumption $1 < U < u_1$. □

Theorem. *Let U be a unit in $\mathbb{Z}[\alpha]$. Then $U = u_1^n$ for some $n \in \mathbb{Z}$.*

Proof. Without loss of generality, we'll assume $U > 0$. We'll show that $U = u_1^n$ for some $n \in \mathbb{Z}$.

Note that $u_1^n \to \infty$ as $n \to \infty$ and $u_1^n \to 0$ as $n \to -\infty$. Hence there exists an integer n such that $u_1^{n-1} < U \leq u_1^n$. Let $V = u_1^{1-n}U$. Then V is a unit in $\mathbb{Z}[\alpha]$ and $1 < V \leq u_1$. By the previous lemma, $V = u_1$. Therefore $U = u_1^n$. □

Theorem. *Let (x, y) be a solution in natural numbers to the equation*

$$x^2 + xy - 3y^2 = 1.$$

Then there is an even natural number n such that $x = x_n$ and $y = y_n$.

Proof. Let $U = x + y\alpha$. The equation implies that U is a unit in the ring $\mathbb{Z}[\alpha]$. Hence by the theorem $U = \pm u_1^n$ for some $n \in \mathbb{Z}$. Since $U > 0$, the sign is $+1$. Since x and y are ≥ 0 we have $U \geq 1$, and therefore $n \geq 0$. Since U has norm 1 it follows that n is even. □

Theorem. *Let (x, y) be a solution in natural numbers to the equation*

$$x^2 + xy - 3y^2 = -1.$$

Then there is an odd natural number n such that $x = x_n$ and $y = y_n$.

Proof. The proof is the same as for the previous theorem, except that $N(U) = -1$, which implies that n is odd. □

6.4 A Thue equation (`ThueEquation`)

This project requires some knowledge of algebraic number theory (MATH0035).

A *Thue equation* is a Diophantine equation of the form

$$f(x, y) = c,$$

where $f \in \mathbb{Z}[x, y]$ is irreducible, homogeneous, and has degree at least 3. Each Thue equation has only finitely many solutions in integers.

In this project, consider the Thue equation

$$x^3 - 2y^3 = 1.$$

The aim of the project is to prove in lean that the only solutions in integers are $(1, 0)$ and $(-1, -1)$.

As a first step, we let $\alpha = \sqrt[3]{2}$. The equation can be rewritten as

$$N(x - y\alpha) = 1,$$

where N is the norm of an element of $\mathbb{Z}[\alpha]$. Therefore $x - y\alpha$ is a unit in $\mathbb{Z}[\alpha]$. One can prove that $u = 1 + \alpha + \alpha^2$ is a fundamental unit in $\mathbb{Z}[\alpha]$, which means that every unit is (up to a sign) a power of u, and every unit with norm 1 is a power of u. We then need to prove that the only powers u^n which have α^2-coefficient equal to zero are

$$u^0 = 1, \qquad u^{-1} = \alpha - 1.$$

These give the two solutions to the Thue equation

To do this in lean, you will need to begin by defining the ring $\mathbb{Z}[\alpha]$ together with its field embeddings in the complex numbers, and proving the properties of its norm. Proving that u is a fundamental unit involves some careful inequalities. The final step of finding which powers of n have zero α^2-coefficient can be done by congruences.

Theorem. *Every element of $\mathbb{Z}[\alpha]$ with norm 1 is a power of u.*

Proof. We'll write α for the real cube root of 2. There are also two complex cube roots of 2, which are $\omega\alpha$ and $\bar{\omega}\alpha$, where $\omega = e^{2\pi i/3}$. There are two ring homomorphisms $\sigma : \mathbb{Z}[\alpha] \to \mathbb{R}$ and $\tau : \mathbb{Z}[\alpha] \to \mathbb{C}$, where $\sigma(\alpha)$ is the real cube root α and $\tau(\alpha) = \omega\alpha$. The complex conjugate $\bar{\tau} : \mathbb{Z}[\alpha] \to \mathbb{C}$ is also a ring homomorphism. Recall that we have

$$N(A) = \sigma(A)\tau(A)\bar{\tau}(A) = \sigma(A)|\tau(A)|^2.$$

If A has norm 1 then clearly $\sigma(A) > 0$. Dividing A by a power of u, we may assume that

$$1 \leq \sigma(A) < \sigma(u).$$

This implies $|\tau(A)| \leq 1$.
If $A = a + b\alpha + c\alpha^2$ then we have

$$\begin{aligned}\sigma(A) &= a + b\alpha + c\alpha^2,\\ \tau(A) &= a + b\omega\alpha + c\bar{\omega}\alpha^2,\\ \bar{\tau}(A) &= a + b\bar{\omega}\alpha + c\omega\alpha^2.\end{aligned}$$

Solving these linear equations in a, b, c, we get

$$\begin{aligned}3a &= \sigma(A) + \tau(A) + \bar{\tau}(A),\\ 3\alpha b &= \sigma(A) + \bar{\omega}\tau(A) + \omega\bar{\tau}(A),\\ 3\alpha^2 c &= \sigma(A) + \omega\tau(A) + \bar{\omega}\bar{\tau}(A).\end{aligned}$$

From the inequalities above, we can see that $3a$, $3\alpha b$ and $3\alpha^2 c$ are all in the interval $[-2, \sigma(u) + 2)$. Since $\sigma(u) < 4$ and $\alpha > 1$, it follows that

$$a, b, c \in \{0, 1\}.$$

Here is a table of values of the norm in these cases.

a	b	c	$N(a + b\alpha + c\alpha^2)$
0	0	0	0
0	0	1	4
0	1	0	2
0	1	1	6
1	0	0	1
1	0	1	5
1	1	0	3
1	1	1	1

As we are assuming that $N(A) = 1$, we must have either $A = 1$ or $A = 1 + \alpha + \alpha^2 = u$. □

We are now left with the task of checking which powers of u have the form $x + y\alpha$.

Lemma. $u^3 \equiv 1 \bmod 3$.

(This is easy to check).

Lemma. *If $u^n = x - y\alpha$ then n is congruent to 0 or -1 modulo 3.*

Proof. If n congruent to 1 modulo 3, then the previous lemma shows that $u^n \equiv 1 + \alpha + \alpha^2 \bmod 3$, and hence the α^2-coefficient is not zero. □

Lemma. *For all natural numbers $n \geq 1$ we have $u^{3^n} \equiv 1 + 3^n(\alpha^2 - \alpha) \bmod 3^{n+1}$.*

Proof. We prove this by induction on n. If $n = 1$, then this is trivial to check. Assume the result for n. then we have for some $c \in \mathbb{Z}[\alpha]$,

$$u^{3^n} = 1 + 3^n(\alpha^2 - \alpha + 3c),$$

Therefore

$$u^{3^{n+1}} = (1 + 3^n(\alpha^2 - \alpha + 3c))^3.$$

Expanding this out, we find that

$$u^{3^{n+1}} \equiv 1 + 3^{n+1}(\alpha^2 - \alpha) \bmod 3^{n+2}.$$

□

Theorem. *If $u^n = x + y\alpha$ and n is congruent to 0 modulo 3, then $n = 0$.*

Proof. We'll prove by induction on r that n is a multiple of 3^r. If this is true for all r then we must have $n = 0$.

The case $r = 1$ is a hypothesis of the theorem.

Assume $n = 3^r a$. We must prove that a is a multiple of 3. We have by the previous lemma:

$$\begin{aligned} x - y\alpha &= (u^{3^r})^a \\ &\equiv (1 + 3^r(\alpha^2 - \alpha))^a \bmod 3^{r+1} \\ &\equiv 1 + 3^r a(\alpha^2 - \alpha) \bmod 3^{r+1} \end{aligned}$$

Comparing coefficients of α^2, we get

$$0 \equiv 3^r a \bmod 3^{r+1}$$

Therefore a is a multiple of 3. □

Theorem. *If $u^n = x + y\alpha$ and n is congruent to -1 modulo 3, then $n = -1$.*

Proof. We'll prove by induction on r that $n + 1$ is a multiple of 3^r. If this is true for all r then we must have $n = -1$.

The case $r = 1$ is a hypothesis of the theorem.

Assume $n = 3^r a - 1$. We must prove that a is a multiple of 3. We have by the previous lemma:

$$\begin{aligned} x - y\alpha &= (u^{3^r})^a u^{-1} \\ &\equiv (1 + 3^r(\alpha^2 - \alpha))^a u^{-1} \bmod 3^{r+1} \\ &\equiv (1 + 3^r a(\alpha^2 - \alpha))u^{-1} \bmod 3^{r+1}. \end{aligned}$$

Since $u^{-1} = \alpha - 1$, it follows that

$$x + y\alpha \equiv \alpha + 3^r a(2 - \alpha^2) - (1 + 3^r a(\alpha^2 - \alpha))$$

Comparing coefficients of α^2, we get

$$0 \equiv -2 \times 3^r a \bmod 3^{r+1}$$

Therefore a is a multiple of 3. □

Putting all of this together, we have

Theorem. *If $x^3 - 2y^3 = 1$ then $x + y\alpha$ is either 1 or $u^{-1} = \alpha - 1$.*

Proof. If we set $A = x + y\alpha$ then the norm of A is 1. We've proved above that such an A must be u^n for some integer n We also showed that n must be congruent to 0 or -1 modulo 3. In the case $n \equiv 0 \bmod 3$, we proved that $n = 0$. In the case $n \equiv -1 \bmod 3$, we proved that $n = -1$. □