A Gentle Introduction on Lean

Moti Ben-Ari

ORCiD ID: 0000-0002-2091-5107

`http://www.weizmann.ac.il/sci-tea/benari/`

January 26, 2024

Contents

1 Introduction

Lean 4 is a *proof assistant*. You enter your proof into Lean in a formal language and the system checks the correctness of the proof. It displays the current set of hypotheses and goals, and it is capable of performing many simple proofs automatically. This tutorial is, as its name states, a gentle introduction to Lean intended for students and others who have no previous experience with a proof assistant, though a basic knowledge of propositional and first-order logic is assumed.

Constructs of Lean are explained and demonstrated within complete proofs of theorems of arithmetic and logic. The source code is heavily commented and additional explanations are given. As you gain more experience with Lean, fewer comments are given. Proof tactics are introduced one at a time as needed and only standard tactics are used. Tables of keyboard shortcuts, tactics and tips are given in the appendices.

The Lean source code of the proofs and the XƎLaTeX source of this document can be found at

`https://github.com/motib/gentle-lean`.

Installation

To install Lean, follow the instructions for your operating system at
`https://leanprover-community.github.io/get_started.html`.

The Lean community uses *Visual Studio Code (VSC)*
`https://code.visualstudio.com/`
It is a versatile environment with lots of features, so be sure to study VSC tutorials before starting to work with Lean.

You must work within a project framework as described in
`https://leanprover-community.github.io/install/project.html`.
Once you have created a project, open the project folder and create new source files with the extension `lean`.

Syntax

Lean uses two types of comments:

- Line comments start with `--` and continue to end of the line.
- Range comments start with `/-` and continue to `-/`.

The convention is to use spaces around each operator:
```
a ≤ b ∧ b ≤ a → a = b
```
and I will do so in this tutorial. You may ignore this convention in your proofs.

There is also a convention for naming theorems: the name is written in lower case with underscores between the parts of the name. The name specifies the meaning of the theorem in a few words or abbreviations, for example, `min_le_right` is `min a b ≤ b` and `min_le_left` is `min a b ≤ a`.

Tips for working with Lean

Tip: Infoview

Enter `ctrl-shift-enter` to open the Lean Infoview where hypotheses, goals and errors are displayed. To understand the effect of applying a tactic, place the cursor just before the source line and then alternate `Home` and `End` while looking at Infoview.

Tip: tactic

If you hover over a tactic its specification will be displayed.

Tip: theorem

If you hover over a theorem the stattement of the theorem will be displayed.

Theorems are defined to be widely applicable, so initially you will not be able to understand the full statement of a theorem in the library. In this tutorial only natural numbers and integers are used, so you can interpret the theorems narrowly, for example,

```
dvd_mul_right (a b : Nat) : a ∣ a * b
```

Preamble

The Lean community has developed a mathematical library called `Mathlib`. You will work with the definitions and theorems defined there, which are imported in the first lines of your Lean source file. Preambles do not appear in the examples here but can be found in the source files.

1. The library of proof tactics:
   ```
   import Mathlib.Tactic
   ```
2. Other libraries contain the definitions and theorems of data types:
   ```
   import Mathlib.Data.Nat.Prime
   ```
3. `namespace` ensures that the names you give do not clash with the names of theorems in `Mathlib`. The examples in this tutorial use the same names as those in `Mathlib` so be sure to retain the `namespace`.
   ```
   namespace gentle
   ```
   Alternatively, you can modify the names of the theorems, for example, replace `gcd_comm` by `my_gcd_comm`.

4. You can open a namespace so that you do not have to write a full name: `factorial` instead of `Nat.factorial`:
   ```
   open Nat
   ```

References

Lean resources

- J. Avigad and P. Massot. *Mathematics in Lean*.
  `https://leanprover-community.github.io/mathematics_in_lean/`
  This is a comprehensive presentation on the use of Lean to prove mathematical theorems. Most of the proofs in this tutorial are based on examples given there.

- The website of the Lean Community contains links to important resources and to the Zulip chat where you can ask questions.
  `https://leanprover-community.github.io/`

- J. Avigad, L. de Moura, S. Kong and S. Ullrich. *Theorem Proving in Lean 4*.
  `https://lean-lang.org/theorem_proving_in_lean4/`
  A formal presentation of Lean.

Learning materials on Lean

- The games on the Lean Game Server are a fun way to start learning Lean.
  `https://adam.math.hhu.de/`

- D. J. Velleman. *How to Prove It with Lean*.
  `https://djvelleman.github.io/HTPIwL/`
  This is a textbook on methods of proof in mathematics. To simplify learning it uses tactics developed by the author.

- H. Macbeth. *The Mechanics of Proof*.
  `https://hrmacbeth.github.io/math2001/`
  This is a textbook on methods of proof in mathematics. To simplify learning it uses tactics developed by the author.

Mathematical logic

- M. Ben-Ari. *Mathematical Logic for Computer Science (Third Edition)*, Springer, 2012.
  An introduction to mathematical logic including both syntactical and semantic proof methods, as well as sections on temporal logic and program verification.

- M. Huth and M. Ryan. *Logic in Computer Science: Modelling and Reasoning about Systems (Second Edition)*, Cambridge University Press, 2004.
  An introduction to mathematical logic with emphasis on natural deduction, temporal logic and model checking.

Acknowledgment

I am deeply indebted to the members of the Lean Community for their patience and help as I took my first steps in Lean.

2 Commutativity of gcd

A theorem is declared like a function in a programming language with the name of the theorem, its parameters and the statement of the theorem.The keyword `by` introduces a *tactic proof*, which we will be using exclusively in this tutorial.

Tip `example`

`example` is used to state an unnamed theorem.

It is common in writing about Lean to demonstrate constructs using unnamed theorems, but `example` is not used in this tutorial except briefly in Appendix B.

The first theorem we prove is the commutativity of the greatest common denominator.

```
1 theorem gcd_comm (m n : ℕ) :
2     Nat.gcd m n = Nat.gcd n m := by
```

The parameters `m n` have a logical meaning as universally quantified variables.

$$\forall m, n \in N : (\mathrm{gcd}(m, n) = \mathrm{gcd}(n, m)) \, .$$

The proof of the theorem uses the fact that the division operator is antisymmetric: if $m|n$ and $m|n$ then $m = n$. Applying this theorem results in two new goals.

```
3   apply Nat.dvd_antisymm
4     -- dvd_antisymm: (m ∣ n ∧ n ∣ m) → m = n,
5     --   where m = gcd m n, n = gcd n m
6     -- Two new goals: gcd m n ∣ gcd n m, gcd n m ∣ gcd m n
```

When you place the cursor before line 6, Lean Inforview will display the *tactic state*:

```
m n : ℕ
⊢ Nat.gcd m n = Nat.gcd n m
```

This gives the *context* that `m n` are natural numbers and the current *goal* following the turnstile symbol ⊢. After the theorem `Nat.dvd_antisymm` is applied, there are two goals.

```
case a
m n : ℕ
⊢ Nat.gcd m n ∣ Nat.gcd n m
case a
m n : ℕ
⊢ Nat.gcd n m ∣ Nat.gcd m n
```

Tactic: `apply`

If you have a theorem `P→Q` and the goal matches `Q` then `apply P→Q` removes the goal `Q` and adds `P` as the new goal.

If you have a theorem `Q` and the goal matches `Q` then `apply Q` removes the goal and there are no more goals.

gcd(m, n) will divide gcd(n, m) only if it divides both n and m, so we again have two new subgoals. Then, by definition, gcd(m, n) is a common divisor so it divides both the left parameter m and the right parameter n.

```
  -- First goal
  apply Nat.dvd_gcd
      -- dvd_gcd: (k ∣ m ∧ k ∣ n) → k ∣ gcd m n,
      --   where k = gcd m n, m = n, n = m
      -- New goals are gcd m n ∣ n and gcd m n ∣ m
  apply Nat.gcd_dvd_right
      -- gcd_dvd_right: gcd m n ∣ n,
      --   where m = m, n = n
  apply Nat.gcd_dvd_left
      -- gcd_dvd_left: gcd m n ∣ m
      --   where m = m, n = n
```

Repeat the same proof for the second subgoal gcd$(n, m) |$ gcd(m, n).

```
  -- Second goal
  apply Nat.dvd_gcd
      -- dvd_gcd: k ∣ m ∧ k ∣ n → k ∣ gcd m n,
      --   where k = gcd n m, m = m, n = n
      -- New goals are gcd n m ∣ m and gcd n m ∣ n
  apply Nat.gcd_dvd_right
      -- gcd_dvd_right: gcd m n ∣ n,
      --   where m = n, n = m
  apply Nat.gcd_dvd_left
      -- gcd_dvd_left: gcd m n ∣ m
      --   where m = n, n = m
  done
```

Tip: done

All proofs should be terminated by `done`. This is not necessary but if your proof is not complete, `done` will display a message.

Tip: Division

The division operator in Lean is not the | symbol on your keyboard, but a similar Unicode symbol ∣ obtained by typing `\|`.

3 Commutativity of minimum

To prove that the minimum operator is commutative, a hypothesis named `h` is introduced. Of course we have to prove the hypothesis before we can use it.

```
theorem min_comm (a b : ℕ) :
    min a b = min b a := by
  have h : ∀ x y : ℕ, min x y ≤ min y x := by
    -- Hypothesis: For all natural numbers x y,
    --   min x y ≤ min y x
```

Tactic: `have`

Introduces a new named hypothesis for use in the proof.

Tip: indentation

All statements used to prove a hypothesis must be uniformly indented.

The hypothesis is $\forall m, n \in N : \min(m, n) = \min(n, m)$. For the bound variables m, n, free variables must be substituted. The tactic `intro x y` introduces new free variables `x y` for `m n`.

```
    intro x y
      -- Introduce arbitrary x y in place of ∀
```

Tactic: `intro`

Introduces free variables in place of bound variables in a universally quantified formula. A universally bound variable means that the formula has to hold for an arbitrary value so we substitute a variable that is this arbitrary value.

If the goal is is `P→Q`, `intro` introduces `P` as a hypothesis. If `Q` is proven then the hypothesis can be *discharged* and `P→Q` is proven.

The first step of the proof of the hypothesis uses the theorem that $c \leq a \wedge c \leq b \rightarrow c \leq \min(a, b)$. The Lean theorem `le_min` is applied to obtain two subgoals whose proofs complete the proof of the hypothsis `h`.

```
    apply le_min
      -- le_min: for all natural numbers c,
      --   (c ≤ a ∧ c ≤ b) → c ≤ min a b
      --   where a = y, b = x, c = min x y
      --   New goals are min x y ≤ y and min x y ≤ x
    apply min_le_right
      -- min_le_right: min a b ≤ b
      --   where a = x, b = y
      -- Solves goal min x y ≤ y
    apply min_le_left
      -- min_le_left: min a b ≤ a
      --   where a = y, b = x
    -- This completes the proof of h
```

Now that h has been proved, the indentation is removed to continue the proof the main theorem.

le_antisymm is applied to the goal creating two subgoals which are proved by applying the hypothesis h.

```
  apply le_antisymm
    -- le_antisymm: (a ≤ b ∧ b ≤ a) → a = b
    --   where a = min a b, b = min b a
    --   New goals are min a b ≤ min b a and min b a ≤ min a b
  apply h
    -- Apply h with x = a and y = b
  apply h
    -- Apply h with x = b and y = a
  done
```

4 Cancellation

Here we prove theorems of arithmetic related to cancellation properties:

$$-a + (a + b) = b\,, \quad a + c = a + c \rightarrow b = c\,, \quad a * 0 = 0.$$

The library `import Mathlib.Data.Int.Basic` is imported because negative numbers are integers, not natural numbers.

Tip: associativity

The associativity of the operators `+` and `*` is defined to be *left*:
`a + b + c` is `(a + b) + c` and `a * b * c` is `(a * b) * c`.
Use `add_assoc` and `mul_assoc` to change the associativity of an expression.

In order to prove $-a + (a + b)$ we first need to proof that it equals $(-a + a) + b)$ and then set $-a + a = 0$.

This proof uses the tactic `rw` that *rewrites* an expression with another expression that has already been proved to be equal to it. After two rewrites, applying the theorem `zero_add b` results in exactly the expression needed to proof the goal.

```
theorem neg_add_cancel_left (a b : Int) :
    -a + (a + b) = b := by
  rw [← add_assoc]
    -- add_assoc: a + b + c = a + (b + c)
    -- Addition is left associative: a + b + c = (a + b) + c
    -- New goal is -a + a + b = b
  rw [add_left_neg]
    -- add_left_neg: -a + a = 0
    -- New goal is 0 + b = b
  exact zero_add b
    -- zero_add: 0 + a = a, where a = b
  done
```

Tactic: `rw`

`rw [eqn]`, where `eqn` is an equation or an equivalence, rewrites the goal by replacing occurrences of the the left-hand side of `eqn` with the right-hand side.
`rw [← eqn]` rewrites the goal by replacing occurrences of the right-hand side of `eqn` with the left-hand side.
`rw [eqn] h` and `rw [← eqn] h` rewrite expressions in the hypothesis `h`.

Tactic: `exact`

The tactic `exact h` is used when `h` is exactly the statement of the current goal, so the goal is now proved. `exact` is similar to `apply` but limited because it can only be used if the hypothesis exactly matches the goal.

The parameter `h : a + b = a + c` in the theorem `add_left_cancel` is a hypothesis.

```
13 theorem add_left_cancel {a b c : Int}
14     (h : a + b = a + c) : b = c := by
15   rw [← neg_add_cancel_left a b]
16     -- neg_add_cancel (above): -a + (a + b) = b
17     -- New goal is -a + (a + b) = c
18   rw [h]
19     -- New goal is -a + (a + c) = c
20   exact neg_add_cancel_left a c
21     -- neg_add_cancel (above): -a + (a + b) = b, where b = c
22   done
```

The theorem `add_left_cancel` has four parameters: `a b c` of type `Int` and a hypothesis `h`. To use the theorem we can write

```
apply add_left_cancel i j k h
```

for some values `i j k` of type `Int` and a hypothesis `h`. When the theorem is used in line 36 below, `h` has been replaced by its definition in line 25:

```
exact add_left_cancel (a * 0 + a * 0 = a * 0 + 0)
```

but the integer parameters are not given. When the hypothesis is matched against `a + b = a + c` in the statement of the theorem, we have

```
a = a * 0   b = a * 0   c = 0.
```

Clearly, all three expressions are of type `Int` so Lean can infer their values and types when they are used:

```
exact add_left_cancel (a * 0) (a * 0) 0 h
```

Tip: implicit

Parameters declared with braces, such as `{a b c : Int}` state that `a b c` are *implicit* bound variables in the theorem whose actual names and types can be inferred when the theorem is used.

The proof of the following theorem is similar to the previous two. First the hypothesis `h` is proved using `rw` three times and it is then used as a hypothesis in the application of `add_left_cancel`.

```
theorem mul_zero {a : Int} :
    a * 0 = 0 := by
  have h : a * 0 + a * 0 = a * 0 + 0 := by
    rw [← mul_add]
      -- Distribute multiplcation over addition (reversed)
      -- mul_add: a * (b + c) = a * b + a * c,
      --   where a = a, b = 0, c = 0
      -- New goal is a * (0 + 0) = a * 0 + 0
    rw [add_zero]
      -- add_zero: a + 0 = 0
      -- New goal is a * 0 = a * 0 + 0
    rw [add_zero]
      -- h is proved
  exact add_left_cancel h
    -- add_left_cancel (above): if a + b = a + c then b = c,
    --   where a = a * 0, b = 0, c = 0
  done
```

5 An infinite number of prime numbers

To prove that there are an infinite number of prime numbers, assume to the contrary that there are finitely many prime numbers $p_1, p_2, \ldots, p_n$. Consider $q = (p_1 p_2 \cdots p_n) + 1$. For any $1 < m < q$, m does not divide q because the remainder is 1. Therefore, q is a prime since it is divisible only by 1 and q.

There are two ways to define primes in Lean:

- `Nat.prime_def_lt`: p is prime if and only if $(2 \leq p) \wedge \forall m < p (m|p \rightarrow m = 1)$.
- `Nat.Prime.eq_one_or_self_of_dvd`: p is prime only if $m|p \rightarrow (m = 1 \vee m = p)$.[1]

The proof above follows the definition `Nat.prime_def_lt`, but the proof using

`Nat.Prime.eq_one_or_self_of_dvd`

is easier, because we need only work the hypothesis $m|p$ and not with the quantifier $\forall m < p$.

The proof starts with the *definition* of p as the smallest prime factor of $n! + 1$. A major part of the proof is to show that such a p does exist.

```
theorem exists_infinite_primes (n : ℕ) :
    ∃ p, n ≤ p ∧ Nat.Prime p := by
      -- For all natural numbers n,
      --   there exists a natural number p,
      --   such that n ≤ p and p is a prime
  let p := minFac (n ! + 1)
    -- if n ! + 1 ≠ 1, p is its smallest prime factor
```

Tactic: `let`

`let` introduces a definition whose scope is local.

Now we prove the hypothesis that $n! + 1 \neq 1$.

```
  have f1 : n ! + 1 ≠ 1 := by
    apply Nat.ne_of_gt <| succ_lt_succ <| factorial_pos _
      -- factorial_pos: n ! > 0
      -- succ_lt_succ: m < n → succ m < succ n
      --   where m = 0, n = n !
      --   succ(essor of) n is the formal definition of n + 1
      -- ne_of_gt: b < a → b ≠ a
      --   where b = 1 and a = n ! + 1
      -- <| means that the formula on its right is
      --   the input to the one on its left
```

Let us look at `apply Nat.ne_of_gt <| succ_lt_succ <| factorial_pos _` in detail.

- `factorial_pos _` is the theorem that the value of any factorial is positive, here, $0 < n!$.
- `succ_lt_succ` uses the definition of $+1$ as the successor function. It takes $0 < n!$ from `factorial_pos _` and proves that $0 + 1 < n! + 1$.

[1]This definition is *not* "if and only if," because $p = 1$ satisfies the right-hand side but 1 is not a prime.

- `Nat.ne_of_gt` is the simple theorem that if $1 < n! + 1$ then $1 \neq n! + 1$, which is the hypothesis `f1` that we want to prove.

Tip: right-to-left

The symbol `<|` means to compute the expression to its right and pass it to the left.

From the hypothesis `f1` it follows that $n! + 1$ has a smallest prime factor and therefore p exists.

```
  have pp : Nat.Prime p := by
    apply minFac_prime f1
      -- minFac_prime: if n ≠ 1 then
      --   the smallest prime factor of n prime,
      --   where n = n ! + 1
      -- f1 proves pp
```

To prove $n \leq p$, we will prove the equivalent formula $\neg(n \geq p)$ which itself if equivalent to $(n \geq p) \rightarrow \mathit{False}$. The method is to introduce $n \geq p$ as a new hypothesis and derive a contradiction.

```
  have np : n ≤ p := by
    apply le_of_not_ge
      -- le_of_not_ge: ¬a ≥ b → a ≤ b
      --   where a = n, b = p
      -- New goal is ¬n > p
    intro h
      -- By definition of negation, n ≥ p implies False
      -- Assume n ≥ p and make False the new goal
      --   to prove np by contradiction
```

Tip: negation

A negation `¬p` is defined as `p → False` so it is proved by introducing `p` as a hypothesis and then showing that this results in a contradiction by proving `False`.

On page 8 we noted that the tactic `intro` is applicable to goals or hypotheses of the form `P → Q`, as is done here with `p → False`.

Two final hypotheses are needed: $p|n!$ and $p|1$.

In the proof of the first hypothesis, the theorem `dvd_factorial` takes two parameters: the fact that the minimum prime factor of any number (_) is positive and the hypothesis `h` that `n ≥ p`.

```
    have h₁ : p ∣ n ! := by
      apply dvd_factorial (minFac_pos _) h
        -- minFac_pos: 0 < minFac n,
        --   where _ means that this holds for any n
        -- dvd_factorial: (0 < m ∨ m ≤ n) → m ∣ n !
        --   where m = p
        -- p is natural so 0 < m and
        -- p ≤ n by assumption (intro) h
        -- h₁ is proved
```

To prove the second hypothesis we use the theorem `Nat.dvd_add_iff_right` whose main operator is if-and-only-if $a \leftrightarrow b$. This theorem can be used in two ways:

- Modus ponens (`mp`): $a \rightarrow b$, assume a and prove b.
- Modus ponens reversed (`mpr`): $a \leftarrow b$, assume b and prove a.

Here reversed modus ponens is used.

```
    have h₂ : p ∣ 1 := by
      apply (Nat.dvd_add_iff_right h₁).mpr (minFac_dvd _)
        -- minFac_dvd: minFac n ∣ n,
        --   where _ means that this holds for any n
        -- dvd_add_iff_right: k ∣ m → (k ∣ n ↔ (k ∣ m) + n)
        --   where k = p, m = n !, n = 1
        --   p ∣ n ! by h₁, so p | 1 iff p ∣ n ! + 1
        -- mpr (MP reverse): p ∣ n ! + 1 → p | 1
        --   p ∣ n ! + 1 by definition
        --   since pp shows that p is prime
        -- p ∣ is proved
```

Applications of the hypotheses `pp` and `h₂` complete the proof of `np`.

```
    apply Nat.Prime.not_dvd_one pp
      -- if p is a prime (true by pp) then ¬p ∣ 1
      --   which is p | 1 → False
    exact h₂
      -- Use MP with h₂, proving False and
      --   thus np by contradiction,
      --   since by definition a prime is ≥ 2
    -- The proof of np : np: n ≤ p is (finally) complete
```

The current goal is `∃ p, n ≤ p ∧ Nat.Prime p`. The existentially quantified variable `p` must be replaced with a specific value, here also `p`, by the tactic `use`. We can split the conjunction `n ≤ p ∧ Nat.Prime p` into two subgoals that are proved using the hypotheses `np` and `pp`.

```
  use p
    -- Introduce free variable p for the bound variable p
    --   to get n ≤ p ∧ Nat.Prime p
    -- Since both conjuncts are hypotheses,
    --   the proof is complete
  done
```

Tactic: `use`

Given an existential goal `∃ c A(c)`, this tactic introduces a free variable for the bound variable `c` to form a new goal. It will also attempt to prove the goal using the hypotheses.

Even without the comments the proof is not short. When proving complex theorems it is convenient to assume that certain lemmas are true, and then when the main proof is complete to return to prove the lemmas. In Lean the tactic `sorry` is accepted as a proof of anything. For example, the eight-line proof of the hypothesis `np` can be proved by `sorry`. Lean will issue a stern warning to tell you not to rest on your laurels.

```
theorem exists_infinite_primes_sorry (n : ℕ) :
    ∃ p, n ≤ p ∧ Nat.Prime p := by
  let p := minFac (n !  + 1)
  have f1 : n ! + 1 ≠ 1 := by
    apply Nat.ne_of_gt <| succ_lt_succ <| factorial_pos _
  have pp : Nat.Prime p := by
    apply minFac_prime f1
  have np : n ≤ p       := by sorry
  use p
  done
```

Tactic: `sorry`

Proves any theorem.

6 Square root of two is irrational

To prove that $\sqrt{2}$ is rational, suppose that it is rational so that $\sqrt{2} = m/n$. Without loss of generality, assume that m, n are *coprime*, that is, they have no common factor. Then $m^2/n^2 = 2$ and $m^2 = 2n^2$, so 2 must divide m. Therefore, 2^2 must divide $2n^2$ and hence n is also divisible by 2, contracting the assumption that m, n are coprime. This section contains a Lean proof of the central claim of the proof that if m, n are coprime then $m^2 \neq 2n^2$.

A `lemma` is just a different name for a `theorem`. This lemma proves that $a^2 = a \cdot a$ using `rw` on the successor function and the base case of the definition for taking the power of a number.

```
lemma pow_two (a : ℕ) : a ^ 2 = a * a := by
  rw [Nat.pow_succ]
    -- Nat.pow_succ:  n ^ succ m = n ^ m * n,
    --   where n = a, m = 1, succ m = 1 + 1
    -- New goal is a ^ 1 * a = a * a
  rw [pow_one]
    -- pow_one: a ^ 1 = a
  done
```

The second lemma proves that if $2|m^2$ then $2|m$ using the first lemma and the theorem that if there is a prime factor of $a * b$ then it is a prime factor of either a or b. When the hypothesis `h` which is now $2|m \cdot m$ is rewritten, the hypothesis becomes the disjunction $2|m \vee 2|m$ since $a = b = m$.

```
lemma even_of_even_sqr (m : ℕ)
      (h : 2 ∣ m ^ 2) : 2 ∣ m := by
  rw [pow_two] at h
    -- pow_two (lemma): a ^ 2 = a * a,
    --   where a = m
    -- New goal is 2 ∣ m
  rw [prime_two.dvd_mul] at h
    -- prime_two: 2 is prime
    -- dvd_mul: if p is prime
    --   then p ∣ m * m ↔ p ∣ m ∨ p ∣ m,
    --   where p = 2, m = m,
    -- Apply to h : 2 | m * m → (2 | m ∨ 2 | m)
    -- h is now 2 | m ∨ 2 | m, goal is still 2 ∣ m
```

Split the disjunctive hypothesis $2|m \vee 2|m$ into two identical hypotheses; each one is exactly the goal of the lemma.

```
  rcases h with h₁ | h₁
    -- Splits disjunctive hypothesis h:
    --   2 | m ∨ 2 | m  into
    --   two (identical) subformulas 2 ∣ m, 2 ∣ m
```

Prove both the (identical) subformulas.

```
  · exact h₁
      -- 2 ∣ m proves 2 ∣ m
  · exact h₁
      -- 2 ∣ m proves 2 ∣ m
  done
```

Tactic: `rcases`

Given a hypothesis or goal that is a disjunction `A∨B` the tactic `rcases` splits it into two sub-hypotheses or subgoals `A` and `B`.

For a disjunctive hypothesis, prove the goal under both sub-hypotheses. For a disjunctive goal, prove one of the subgoals.

To prove the theorem, we assume $m^2 = 2n^2$ and prove a contradiction.

```
theorem sqr_not_even (m n : ℕ) (coprime_mn : Coprime m n) :
    m ^ 2 ≠ 2 * n ^ 2 := by
  intro sqr_eq
    -- Assume sqr_eq: m ^ 2 = 2 * n ^ 2 and
    --   prove a contradiction
```

Add the hypothesis $2|m$. By the lemma `apply even_of_even_sqr`, it is sufficient to prove $2|m^2$ which becomes the new goal. Rewrite using the assumption $m^2 = 2n^2$ that was introduced to prove a contradiction and apply the trivial theorem that $a|a \cdot b$ proving the hypothesis.

```
  have two_dvd_m : 2 ∣ m := by
    apply even_of_even_sqr
      --  even_of_even_sqr (lemma): 2 ∣ m ^ 2 → 2 ∣ m
      --  New goal is 2 ∣ m ^ 2
    rw [sqr_eq]
      -- sqr_eq: m ^ 2 = 2 * n ^ 2.
      -- Apply to the current goal.
      -- The new goal is 2 ∣ 2 * n ^ 2
    apply dvd_mul_right
      -- dvd_mul_right: a ∣ a * b,
      --   where a = 2, b = n ^ 2
      -- Apply to the current goal to prove two_dvd_m : 2 ∣ m
```

The definition of divisibility is: $a|b \leftrightarrow \exists c(a \cdot c = b)$. In Lean this is expressed by the forward direction (`mp`) of `dvd_iff_exists_eq_mul_left` applied to the hypothesis `2 ∣ m`. The goal is now to find such a c.

```
  have h : ∃ c, m = c * 2 := by
    apply dvd_iff_exists_eq_mul_left.mp two_dvd_m
      -- dvd_iff_exists_eq_mul_left: a ∣ b ↔ ∃ c, b = c * a
      --   where a = 2, b = m, c = c
      -- Use MP with two_dvd_m: 2 ∣ m to prove h
```

Given an existential formula such as $\exists c P(c)$, let c be some value that satisfies P.

```
  rcases h with ⟨k, meq⟩
    -- h : ∃ c, m = c * 2 is an existential formula
    --   rcases on h:
    --     k is the free variable for the bound variable c
    --     meq : m = k * 2 is a new hypothesis
    -- Type ⟨ ⟩ using \< \>
```

Tactic: `rcases`

`rcases h with ⟨v, h'⟩` means given a hypothesis `h`, let `v` be a value such that the new goal is `h'`.

We now prove a sequence of five hypotheses.

```
  have h₁ : 2 * (2 * k ^ 2) = 2 * n ^ 2 := by
    rw [← sqr_eq]
      -- sqr_eq : m ^ 2 = 2 * n ^ 2
      -- New goal is 2 * (2 * k ^ 2) = m ^ 2
    rw [meq]
      -- Rewrite m = k * 2 in h₁
      -- New goal is  2 * (2 * k ^ 2) = (k * 2) ^ 2
    ring
      -- Prove goal by using the ring axioms
```

Tactic: `ring`

Proves equalities that can be proved directly from the axioms of a commutative ring without taking any hypotheses into account.

For the ring of integers, only addition, subtraction, multiplication and powers by natural numbers can be used; the division operation is not allowed because $1/2$ is not an integer.

$2(2k^2) = (k \cdot 2)^2$ can be proved using only the definition of positive powers of integers as repeated multiplication, and the laws of associativity and commutativity of the integers.

The theorem `mul_right_inj'` is applied assuming that $2 \neq 0$, but this is a simple property of natural numbers which can be proved by the tactic `norm_num`.

```
  have h₂ : 2 * k ^ 2 = n ^ 2 := by
    apply (mul_right_inj' (by norm_num : 2 ≠ 0)).mp h₁
      -- mul_right_inj': a ≠ 0 → (a * b = a * c ↔ b = c)
```

Tactic: `norm_num`

Proves numerical equalities and inequalities that do not use variables.

```
  have h₃ : 2 ∣ n := by
    apply even_of_even_sqr
      -- even_of_even_sqr (lemma) : 2 ∣ m ^ 2 → 2 ∣ m
      -- New goal is 2 ∣ n ^ 2
    rw [← h₂]
      -- New goal is 2 ∣ 2 * k ^ 2
    apply dvd_mul_right
      -- dvd_mul_right : a ∣ a * b

    have h₄ : 2 ∣ Nat.gcd m n := by
      apply Nat.dvd_gcd
        -- Nat.dvd_gcd : (k ∣ m ∧ k | m) → k ∣ gcd m n
        -- New goals are 2 ∣ m and 2 ∣ n
      · exact two_dvd_m
      . exact h₃
```

The sequence of hypotheses that have been proved terminates in `h₅ : 2 ∣ 1`, but `norm_num` can prove that this is the negation of the true formula `1 ∣ 2`, thereby deriving a contradiction.

```
  have h₅ : 2 ∣ 1 := by
    rw [Coprime.gcd_eq_one] at h₄
      -- if m and n are coprime then gcd m n = 1
      -- New goals are 2 ∣ 1 and m, n are coprime
    exact h₄
      -- Proves 2 ∣ 1
    exact coprime_mn
      -- Assumption that m, n are coprime
  norm_num at h₅
  done
```

7 Propositional logic

7.1 Conjunction and equivalence

When a theorem has equivalence (↔) as the main operator, it must be split into two subgoals, one for the modus ponens (`mp`) direction and one for the modus ponens reversed (`mpr`) direction.

```
theorem lt_iff_le_eq {a b : Int} :
    a < b ↔ a ≤ b ∧ a ≠ b := by
  rw [lt_iff_le_not_le]
    -- lt_iff_le_not_le : a < b ↔ (a ≤ b ∧ ¬b ≤ a)
  constructor
    -- Create two subgoals (mp and mpr) from the current iff goal
    -- First subgoal is (a ≤ b ∧ ¬b ≤ a) → (a ≤ b ∧ a ≠ b)
```

The current goal is an implication whose premise and conclusion are both conjunctions. We can use `intro` to introduce the premise as a hypothesis and then `rcases` (page 18) to split the conjunctive hypothesis into two subgoals to be proved.

```
intro h
rcases h with ⟨h0, h1⟩
```

It is possible to combine the two tactics into the tactic `rintro`.

We start with the implication of the modus ponens direction, where `rintro` introduces the hypothesis and then `constructor` splits the conjuctive goal into two subgoals.

```
  · rintro ⟨h0, h1⟩
    -- Introduces the premise as a hypothesis and split it
    --   into two sub-hypotheses a ≤ b and ¬b ≤ a

    constructor
      -- Creates two subgoals from the current conjunctive goal
    · exact h0
        -- Proves the second subgoal
    · intro h2
        -- a ≠ b is a = b → False
      apply h1
        -- Replace False with the negation of the hypothesis
      rw [h2]
```

The proof of the implication of the modus ponens reversed direction is similar.

```
  · rintro ⟨h0, h1⟩
    constructor
    · exact h0
    · intro h2
      apply h1
      apply le_antisymm h0 h2
        --  le_antisymm: (a ≤ b) → (b ≤ a) → a = b
  done
```

Tactic: `constructor`

Splits a goal into two subgoals: equivalence (↔) into two implications (Modus ponens and Modus ponens reversed) and conjunction (∧) into two conjuncts.

Tactic: `rintro`

Performs `intro` and then `rcases` to split the resulting hypothesis.

7.2 Disjunction

In the previous theorem, we first split the equivalence into two implications. Here, tactic `rcases` is used with a theorem to split on the sign of y.

```
theorem lt_abs {x y : Int} :
    x < |y| ↔ x < y ∨ x < -y := by
  rcases le_or_gt 0 y with h | h
    -- Absolute value depends on sign of y
    -- le_or_gt 0 y: a ≤ b ∨ a > b
```

The equivalence goal is unchanged, but we must prove it under both hypotheses: $0 \leq y$ and $0 > y$. First we prove the goal for $0 \leq y$, in which case we can rewrite $|y|$ by y.

```
  · rw [abs_of_nonneg h]
    -- abs_of_nonneg: 0 ≤ a → |a| = a
    constructor
      -- Split iff into mp and mpr
```

For the modus ponens direction, the premise is introduced as a hypothesis and the conclusion becomes the goal $x < y \vee x < -y$. When a *goal* is a disjunction, it is sufficient to prove one disjunct. Here we are smart enough to tell Lean that we want to prove the left disjunct, because the right one won't make any progress toward the proof.

```
    · intro h'
      left
      exact h'
```

For the modus ponens reversed direction, the *hypothesis* is a disjunction and we have to prove the goal for each disjunct. For the second disjunct, we have $0 \leq y$ and $x < -y$, and Lean can prove that this implies the goal $x < y$ using the tactic `linarith`.

```
    . intro h'
      rcases h' with h' | h'
      · exact h'
      . linarith
```

Tactic: `left`, `right`
If the goal is a disjunction, tell Lean which disjunction you want to prove.

Tactic: `linarith`
The tactic solves linear equalities and inequalities. Unlike `ring` it can use hypotheses and unlike `norm_num` it can solve equations with variables.

The proof for $y < 0$ is similar.

```
  · rw [abs_of_neg h]
    constructor
    · intro h'
      right
      exact h'
    . intro h'
      rcases h' with h' | h'
      · linarith
      . exact h'
  done
```

7.3 Implication

The following theorem is proved by contradiction using the tactic `by_contra`, after which the proof is straightforward.

```
theorem T1a {A : Prop} : (¬A → A) → A := by
  intro h1
  by_contra h2
    -- Prove A by contradction: assume A and prove False
  apply h2
  apply h1
  exact h2
  done
```

Tactic: `by_contra`
This tactic removes a goal `P`, adds the hypothesis `¬P` and creates a new goal `False`.

Here is another proof of the same theorem using contraposition instead of contradiction.

```
theorem T1b {A : Prop} : (¬A → A) → A := by
  intro h1
  contrapose! h1
    -- Replace h1 by its contrapositive and push negation inward
  constructor
  · exact h1
  · exact h1
  done
```

The result of using the tactic `contrapose` is not what you might expect from the way it is usually used in logic. Given the *hypothesis* $\neg A \to A$, it does not change the hypothesis into $\neg A \to \neg\neg A$. Instead, the hypothesis becomes the goal $\neg(\neg A \to A)$ and the goal A becomes the hypothesis $\neg A$. This makes sense by the deduction theorem.

$$\{H_1, H_2, \ldots, H_n\} \vdash G$$

means

$$\vdash H_1 \land H_2 \land \ldots \land H_n \to G$$

whose contrapositive is

$$\vdash \neg G \to \neg(H_1 \land H_2 \land \ldots \land H_n)\,,$$

which by the deduction theorem is

$$\neg G \vdash \neg(H_1 \land H_2 \land \ldots \land H_n)\,.$$

Although $\neg(\neg A \to A)$ doesn't simplify the proof, if we push negation inward (do the calculation yourself!) the result is $\neg A \land \neg A$ which is trivial to prove. The exclamation point in the tactic means that following the tactic `contrapose`, the tactic `push_neg` is called to push negation inward.

Tactic: `contrapose`

Transforms a goal into its contrapositive. Applied to a hypothesis, it makes the negation of the goal into a hypothesis and the negation of the hypothesis into the goal. An exclamation point following `contrapose` calls tactic `push_neg` on the resulting contrapositive.

The interesting step in the following proof is

```
    rcases h1 with ⟨h2, _⟩
```

The hypothesis `h1` is `A ∧ ¬B` while the goal is `A`. We use `rcases` to split the hypothesis into two, `A` and `¬B`. Since only one sub-hypothesis is sufficient to prove the goal, we don't even bother to give the sub-hypothesis `¬B` a name.

```
theorem T2 {A B : Prop} : ((A → B) → A) → A := by
  intro h1
  contrapose! h1

  constructor
  · contrapose! h1
      -- Make ¬(A → B) the hypothesis and A the goal
      -- Push negation inward
    rcases h1 with ⟨h2, _⟩
      -- Split the hypothesis
    · exact h2
      -- Only need to use left subformula
  · exact h1
  done
```

Tip: Don't care

When a name or value is syntactically required but you don't care what its value is, you can use the underscore symbol _ instead.

The theorem $(A \to B) \vee (B \to C)$ has a disjunction operator as its main operator. We prefer to carry out the proof using only the implication operator, so we first try to prove the hypthosis $\neg(A \to B) \to (B \to C)$. When the hypothesis has been proved, we use the `contrapose!` to negate the hypothesis and the goal, and then exchange them. Moving the negations inward results in a hypothesis that is exactly the goal.

```
theorem T3 {A B C : Prop} : (A → B) ∨ (B → C) := by
  have h1 : ¬(A → B) → (B → C) := by
    intro h2
    intro h3
    contrapose! h2
    intro
      -- No need to name the new hypothesis
    exact h3
  contrapose! h1
  exact h1
  done
```

7.4 Tautologies

Tautologies in propositional logic can be proved very easily using semantic methods such as truth tables and semantic tableaux. Lean can prove tautologies so the above theorems can be proved immediately using the tactic `tauto`.

```
theorem T1a {A : Prop}     : (¬A → A) → A       := by tauto
theorem T2  {A B : Prop}   : ((A → B) → A) → A := by tauto
theorem T3  {A B C : Prop} : (A → B) ∨ (B → C) := by tauto
```

Tactic: `tauto`

If a tautology can be formed from the hypotheses and the goal, the proof can be immediately completed using this tactic.

The following theorem shows that `tauto` works when the tautology is formed from both a hypothesis and a goal.

```
theorem T0a {A : Prop} (h : ¬A → A) : A := by tauto
```

This theorem shows that `tauto` works on substitution instances of a tautology.

```
theorem T0b {a : Nat} : ¬a = 0 ∨ a = 0 := by tauto
```

8 Induction

8.1 Sum of a sequence

The following theorem is the one usually used to introduce induction.

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}\,.$$

Here is the preamble for the proof of this theorem.

```
import Mathlib.Tactic
import Mathlib.Data.Nat.Basic
import Mathlib.Data.Finset.Basic
import Mathlib.Algebra.BigOperators.Basic
namespace gentle
open Nat Finset BigOperators
```

The library `Finset` supports finite sets and `BigOperators` enables the use of the operators for sum and product.

$$\sum_{x\in s} f(x)\,, \qquad \prod_{x\in s} f(x)\,.$$

Tip: `Finset`, `BigOperators`

Given a finite set of numbers `s` and a function `f` over these numbers, `Finset` defines the expressions `∑ x in s f x` and `∏ x in s f x`, where `BigOperators` enables the use of `∑` and `∏`.

Tip: `range`

`range n` is defined as the set of natural numbers less than `n`.

Since `range n` is $0, 1, 2, \ldots, n-1$, to get the set of natural numbers $0, 1, 2, \ldots, n$ the proof will use `range (n + 1)`.[2] We will use $r(n+1)$ to denote this sequence of numbers:

$$\sum_{i=r(n+1)} i = \frac{n(n+1)}{2}\,.$$

This first step in the proof is to replace the goal with the symmetric goal

$$\frac{n(n+1)}{2} = \sum_{i=r(n+1)} i\,.$$

```
theorem sum_id (n : ℕ) :
    ∑ i in range (n + 1), i = n * (n + 1) / 2 := by
  symm
```

Tactic: `symm`

Replace an equality `t = u` by `u = t`.

[2]The result of adding the numbers from $k = 0$ to $k = n$ is obviously the same as adding from $k = 1$ to $k = n$.

The next step is to prove the trivial hypothesis $0 < 2$. The hypothesis is *anonymous* and is subsequently accessed as `this`.

```
  have : 0 < 2 := by norm_num
```

Tip: Anonymous hypothesis

A hypothesis can be unamed and can subsequently be accessed as `this`.

Division is replaced by multiplication which is easier to work with.

$$n(n+1) = 2 \sum_{i=r(n+1)} i\,.$$

```
  apply Nat.div_eq_of_eq_mul_right this
    -- div_eq_of_eq_mul_right:
    --    (0 < n) ∧ (m = n * k) → m / n = k
```

The proof continues by induction, where `k` is the variable of induction and `ih` is the inductive hypothesis.

```
  induction' n with k ih
```

Tactic: `induction'`

To prove a goal with `n` by induction, specify an induction variable `k` and a name `ih` for the inductive hypothesis.

The base case $k = 0$ is proved using Lean's simplifier.

$$0(0+1) = 2 * \sum_{i=0(0+1)} i = 2 \cdot 0(0+1)$$

```
  · simp
```

Tactic: `simp`

The `simp` tactic uses lemmas and hypotheses in `Mathlib` to simplify a goal or hypothesis.

For the inductive step we assume that the theorem holds for k and prove that it holds for $k+1$. The proof starts by separating out the last term of the sum. The notation is a bit clumsy because we aren't replacing $(k+1)+1$ by $k+2$.

$$(k+1)((k+1)+1) = 2 \sum_{i=r((k+1)+1)} i = 2 \left(\sum_{i=r(k+1)} i + (k+1) \right)\,.$$

```
  · rw [Finset.sum_range_succ]
      -- Finset.sum_range_succ:
      --    ∑ x in range (n + 1), f x = ∑ x in range n, f x + f n
```

Next, the distributive law is used.

$$(k+1)((k+1)+1) = 2 \sum_{i=r(n)} i + 2(k+1)\,.$$

```
    rw [mul_add 2]
      -- mul_add: a * (b + c) = a * b + a * c
```

Substitute the inductive hypothesis.

$$(k+1)((k+1)+1) = k*(k+1) + 2(k+1)\,.$$

```
    rw [← ih]
```

Lean uses the successor function which is now changed to $+1$ and the proof concludes with a simple calculation that can be performed by the tactic `ring`.

```
    rw [succ_eq_add_one]
      -- succ_eq_add_one : succ n = n + 1
    ring
  done
```

8.2 Inductive definition of addition

Here is an inductive definition of natural numbers.[3]

```
inductive Nat
| zero : Nat
| succ : Nat → Nat
```

The next step is to defined addition inductively.

```
def add : Nat → Nat → Nat
  | x, zero => x
  | x, succ y => succ (add x y)
```

Although we normally think of addition as a function of two variables $add(a,b)$, there are advantages to defining it as a function that takes one variable $add(a)$ resulting in another function $add_a(b)$ that gives the sum of a and b.[4]

A proof that $0+n=n$. The proof is by induction and the base case $0+0=0$ follows from the base case of the definition of `add`.

```
theorem zero_add (n : Nat) :
    add zero n = n := by
  induction' n with k ih
  · rfl
```

[3]The program is enclosed in the namespace `gentle` to avoid clashing with predefined `Nat`. After defining `Nat` we open its namespace so that we can use `zero` and `succ` without the prefix `Nat`.

[4]This is called *currying* but an explanation is outside the scope of this tutorial.

Tactic: `rfl`

`rfl` solves a goal that is an equality if they are *definitionally equivalent*, that is, they define the same entity.

Consider the goal:

```
((m + k) + 1) + 1 = (m + (k + 1)) + 1
```

By definition of `add`, `(a + (b + 1)` is `(a + b) + 1` so the right-hand side of the equation `(m + (k + 1)) + 1` means `((m + k) + 1) + 1` which is the left-hand side. Therefore, the tactic `rfl` solves it.

The inductive step is to prove $0+(k+1) = (0+k)+1$. Using definition of `add` to rewrite the left-hand side, we get $(0+k)+1 = k+1$ which can be solved using the inductive hypothesis that $0+k=k$.

```
  · rw [add]
    rw [ih]
  done
```

A proof that $(m+1)+n = (m+n)+1$**.** The base case $(m+1)+0 = m+1$ is immediate from the base case of the definition of `add`.

```
theorem succ_add (m n : Nat) :
    add (succ m) n = succ (add m n) := by
  induction' n with k ih
  · rfl
```

The inductive step is to prove $(m+1)+(k+1) = (m+(k+1))+1$. From the definition of `add` it follows that $((m+1)+k)+1 = (m+(k+1))+1$.

```
  · rw [add]
```

Substituting the inductive hypothesis $(m+1)+k = (m+k)+1$ results in $((m+k)+1)+1 = (m+(k+1))+1$ which, as noted above can be solved by `rfl`.

```
    rw [ih]
    rfl
  done
```

8.3 Multiple steps in a proof

In this section we explain two ways to shorten proofs in Lean by performing more than one step in the same action. We start with the proof of $(m|n \vee m|k) \rightarrow m|mk$. Since the hypothesis is a disjunction, the goal must be proved separately for each disjunct using `rcases` to create separate hypotheses. Furthermore, since $m|n$ is defined as $\exists a(n = ma)$, new variables must be introduced (page 18).

```
theorem div_prod1 {m n k : ℕ} (h : m ∣ n ∨ m ∣ k) :
    m ∣ n * k := by
  rcases h with ⟨a, h1⟩ | ⟨b, h2⟩
```

The new hypotheses are `h1 : n = m * a` and `h2 : k = m * b` which can be used to rewrite the goals. The rest of the proof is straightforward.

```
  · rw [h1]
    rw [mul_assoc]
    apply dvd_mul_right
      -- dvd_mul_right: a ∣ a * b
  · rw [h2]
    rw [mul_comm]
    rw [mul_assoc]
    apply dvd_mul_right
  done
```

The proofs can be shortened by combining multiple rewrites into one `rw`.

```
· rw [h1, mul_assoc]
· rw [h2, mul_comm, mul_assoc]
```

The hypotheses `h1` and `h2` replace `m ∣ n` and `m ∣ k` by the definitionally equivalent `n = m * a` and `k = m * b`. `rfl` can be used to perform the substitutions without creating hypotheses.

```
theorem div_prod2 {m n k : ℕ} (h : m ∣ n ∨ m ∣ k) :
    m ∣ n * k := by
  rcases h with ⟨a, rfl⟩ | ⟨b, rfl⟩
  · rw [mul_assoc]
    apply dvd_mul_right
  · rw [mul_comm, mul_assoc]
    apply dvd_mul_right
  done
```

8.4 Calculating with equations and inequalities

This subsection discusses proofs of theorem with inequalities. We prove the following theorem on Fibonacci numbers.

$$\text{fib}(n) < (7/4)^n\,.$$

The base cases are $\text{fib}(0) = 0 < (7/4)^0$ and $\text{fib}(1) = 1 < (7/4)^1$.[5] The inductive step is:

$$\begin{aligned}\text{fib}(n+1) &= \text{fib}(n) + \text{fib}(n-1) < \left(\frac{7}{4}\right)^n + \left(\frac{7}{4}\right)^{n-1}\\ &= \left(\frac{7}{4}\right)^{n-1}\left(\frac{7}{4}+1\right) < \left(\frac{7}{4}\right)^{n-1}\left(\frac{7}{4}\right)^2 = \left(\frac{7}{4}\right)^{n+1}\,.\end{aligned}$$

[5]Fibonacci numbers are defined sometimes starting with 0 and sometimes starting with 1. Here, we start with 0.

The new aspects of the proof are: (a) two base cases and two inductive hypotheses, (b) an inductive hypothesis that is an inequality rather than an equality, and (c) calculations performed after using the inductive hypothesis.

We start with an inductive definition of the Fibonacci numbers. Normally, this is a function from natural numbers to natural numbers, but here the function is to rational numbers to enable comparison with 7/4.

```
def fib : ℕ → ℚ
  | 0 => 0
  | 1 => 1
  | n + 2 => fib (n + 1) + fib n
```

In the expression of the theorem 7/4 is labeled as being of type ℚ, otherwise it would be interpreted as division of natural numbers with remainder.

```
theorem seven_fourths (n : ℕ) : fib n < (7 / 4 : ℚ) ^ n := by
```

The tactic `twoStepInduction` creates three subgoals, two for the base cases and one for the inductive step. It also creates two inductive hypotheses: `ih1` for `fib(k)` and `ih2` for `fib(k+1)`.

```
  induction' n using Nat.twoStepInduction with k ih1 ih2
```

Tactic `twoStepInduction`

Proof by induction when there are two base cases and two inductive hypotheses.

First the two base cases are proved.

```
  ·  rw [fib] ; norm_num
  ·  rw [fib] ; norm_num
```

Tip Multiple tactics

A sequence of tactics can be written on one line with semicolons between them.

Next we prove two hypotheses that will be used in the proof.

```
  · have h1 : 0 < (7/4:ℚ)^k := by apply pow_pos ; norm_num
      -- pow_pos: 0 < a → 0 < a ^ n
    have h2 : 1+(7/4:ℚ) < (7/4)^2 := by norm_num
```

Look again at the mathematical proof above, which involves substitution of the inductive hypotheses that are inequalities and calculation with rational numbers:

$$e_1 = e_2 < e_3 = e_4 < e_5 = e_6 .$$

Of course each step in the calculation must be justified.

This calculation can be performing using `calc`, where uniform indentation must be observed.

```
calc e1 = e2 := by ...
     _ < e3  := by ...
     _ = e4  := by ...
     _ < e5  := by ...
     _ = e6  := by ...
```

The definition of `fib` is used to expand `fib(k+2)` and the inductive hypotheses are used. Since the hypotheses are inequalities, we cannot use the `rw` tactic; instead, the `rel` tactic is used which substitutes inequalities.

```
    calc fib (k + 2) = fib (k + 1) + fib k := by rw [fib]
       _ < (7/4)^(k+1) + (7/4)^k := by rel [ih1, ih2]
       _ = (7/4)^k * (1+(7/4)) := by ring
       _ < (7/4)^k * (7/4)^2 := by
           apply (mul_lt_mul_left  h1).mpr h2
             -- mul_lt_mul_left: 0 < a → a * b < a * c ↔ b < c
     _ = (7/4)^(k+2) := by ring
  done
```

Tactic `calc`[a]

A proof that is a sequence of expressions related by equality or inequality together with their proofs.

[a] `calc` is technically not a tactic, but I include it in the list of tactics for convenience.

Tactic `rel`

Given a hypothesis `h` which is a relation e_1 *rel_op* e_2, `rel [h]` will attempt to prove the current goal by substituting `h` into the goal.

A shorter proof uses the tactic `gcongr` which is similar to `rel` except that the hypotheses need not be specified because the tactic will find them if possible.

```
theorem seven_fourths_gcongr (n : ℕ) : fib n < (7 / 4 : ℚ) ^ n := by
  induction' n using Nat.twoStepInduction with k ih1 ih2
  ·  rw [fib] ; norm_num
  ·  rw [fib] ; norm_num
  · calc fib (k + 2) = fib (k + 1) + fib k := by rw [fib]
       _ < (7/4)^(k+1) + (7/4)^k := by gcongr
       _ = (7/4)^k * (1+(7/4)) := by ring
       _ < (7/4)^k * (7/4)^2 := by gcongr ; norm_num
       _ = (7/4)^(k+2) := by ring
  done
```

Given

```
fib (k + 2) = fib (k + 1) + fib k
```

the tactic `gcongr` will find the (inductive) hypotheses by itself so we have a proof of that

```
fib (k + 2) < (7/4)^(k+1) + (7/4)^k
```

Tactic `gcongr`

`gcongr` will attempt to prove the current goal by finding and substituting hypotheses of the form e_1 *rel_op* e_2 into the goal.

9 Groups

A group is a set of elements that satisfy some axioms. Here we show how a group can be defined in Lean, although in practice you will use the definitions in `Mathlib`. Groups are defined as *classes* which consist of a type of the elements of the group, a set of functions and a set of axioms.

9.1 Additive groups

To define an additive group like the integers, we need a function `add`, a (constant) function `zero` and a function `neg`. However, it would be weird use that notation; instead, we want to use the mathematical notation for additive structures. These are predefined in `Mathlib` and we can access them by extending the class `AddGroup` from the classes `Add`, `Zero`, `Neg`.

```
class AddGroup (α : Type*) extends Add α, Zero α, Neg α where
  add_assoc : ∀ x y z : α, x + y + z = x + (y + z)
  add_zero : ∀ x : α, x + 0 = x
  zero_add : ∀ x : α, 0 + x = x
  add_left_neg : ∀ x : α, -x + x = 0
```

Tip: Types

By convention types are denoted by Greek letters `α`

This class is a function that takes a type of elements and returns a type that is a group of those elements (see `#check AddGroup`). Declaring a variable `G` will create a group.

```
namespace AddGroup
variable {G : Type*} [AddGroup G]
```

Proving $a + (-a) = 0$. While `add_left_neg` is an axiom, `add_right_neg` is provable. Negation but not subtraction has been defined so we use the somewhat strange notation `a + (-a)`.

```
theorem add_right_neg (a : G) : a + (-a) = 0 := by
```

The proof starts with a hypothesis containing multiple expressions `a + (-a)` which are rearranged by associativity and then collapsed using negativity and the property of addition of zero.

```
  have h : -(a + (-a)) + (a + (-a) + (a + (-a))) = 0 := by
    rw [add_assoc]
    rw [← add_assoc (-a) a]
      -- After rewriting associativity new goal is
      --   -(a + -a) + (a + (-a + a -a)) = 0
      -- Now add_left_neg axiom can be used
    rw [add_left_neg]
    rw [zero_add]
    rw [add_left_neg]
```

Using the hypothesis to rewrite zero a new goal is obtained which is easy to prove.

```
  rw [← h]
    -- New goal is a + -a = -(a + -a) + (a + (-a + a -a))
  rw [← add_assoc]
  rw [add_left_neg]
  rw [zero_add]
  done
```

Proving that x and $-x$ cancel.

```
theorem add_neg_cancel_right (a b : G) : a + b + -b = a := by
  rw [add_assoc, add_right_neg, add_zero]
theorem neg_add_cancel_left (a b : G) : -a + (a + b) = b := by
  rw [← add_assoc, add_left_neg, zero_add]
```

Proving cancellation of equals.

```
theorem add_left_cancel {a b c : G}
    (h : a + b = a + c) : b = c := by
  rw [← neg_add_cancel_left a b, h, neg_add_cancel_left]
theorem add_right_cancel {a b c : G}
    (h : a + b = c + b) : a = c := by
  rw [← add_neg_cancel_right a b, h, add_neg_cancel_right]
```

Theorems on integers Once these theorems have been proved for groups in general, they are defined by inheritance for all groups in `Mathlib`. We can prove our own version of `add_right_neg` for integers using theorems in the library for `Int`.

```
theorem my_add_right_neg (a : ℤ) : a + (-a) = 0 := by
  have h : -(a + (-a)) + (a + (-a) + (a + (-a))) = 0 := by
    rw [Int.add_assoc, ← Int.add_assoc (-a) a,
        Int.add_left_neg, Int.zero_add, Int.add_left_neg]
  rw [← h, ← Int.add_assoc, Int.add_left_neg, Int.zero_add]
  done
```

9.2 Multiplicative groups

In algebra textbooks, groups are defined using multiplicative notation, while additive notation is reserved for abelian groups like the integers. The same class declaration can be used to define a group using multiplicative notation except that it extends `Mul`, `One` and `Inv`. The proofs are structurally identical to the proofs for the additive groups.

```
class Group (α : Type*) extends Mul α, One α, Inv α where
  mul_assoc : ∀ x y z : α, x * y * z = x * (y * z)
  mul_one : ∀ x : α, x * 1 = x
  one_mul : ∀ x : α, 1 * x = x
  mul_left_inv : ∀ x : α, x⁻¹ * x = 1

namespace Group
variable {G : Type*} [Group G]
theorem mul_right_inv (a : G) : a * a⁻¹ = 1 := by
  have h : (a * a⁻¹)⁻¹ * (a * a⁻¹ * (a * a⁻¹)) = 1 := by
    rw [mul_assoc, ← mul_assoc a⁻¹ a, mul_left_inv]
    rw [one_mul, mul_left_inv]
  rw [← h, ← mul_assoc, mul_left_inv, one_mul]
```

A Keyboard shortcuts

Lean uses Unicode symbols that are not on keyboards. The following table shows keyboard shortcuts that are used in VSC for entering the symbols. Enter a space or tab after a shortcut and the symbol will appear. If you hover over a symbol the shortcut will be displayed.

Unicode symbol	Keyboard shortcut
ℕ	`\N`
ℤ	`\Z`
ℚ	`\Q`
ℝ	`\R`
≤	`\le`, `\leq`
≥	`\ge`, `\geq`
≠	`\ne`, `\neq`
←	`\l`
→	`\r`, `\imp`
↔	`\iff`
∧	`\and`
∨	`\or`
∀	`\all`, `\forall`
∃	`\ex`, `\exists`
¬	`\n`, `\neq`
⟨	`\<`
⟩	`\>`
|	`\\|`
⊢	`\\|-`, `\vdash`
h_1	`h\1`
a^{-1}	`a\^-1`,`a\inv`
∑	`\sum`
∏	`\prod`
α	`\alpha`

B Tactics

Tactic	Page	Definition
`apply`	6	If you have a theorem `P→Q` and the goal matches `Q` then `apply P→Q` removes the goal `Q` and adds `P` as the new goal. If you have a theorem `Q` and the goal matches `Q` then `apply Q` removes the goal and there are no more goals.
`by_contra`	23	This tactic removes a goal `P`, adds the hypothesis `¬P` and creates a new goal `False`.
`calc`	33	A proof that is a sequence of expressions related by equality or inequality together with their proofs.
`contrapose`	24	Transforms a goal into its contrapositive. Applied to a hypothesis, it makes the negation of the goal into a hypothesis and the negation of the hypothesis into the goal. An exclamation point following `contrapose` calls tactic `push_neg` on the resulting contrapositive.
`constructor`	22	Splits a goal into two subgoals: equivalence (↔) into two implications (Modus ponens and Modus ponens reversed) and conjunction (∧) into two conjuncts.
`exact`	10	The tactic `exact h` is used when `h` is exactly the statement of the current goal, so the goal is now proved. `exact` is similar to `apply` but limited because it can only be used if the hypothesis exactly matches the goal.
`gcongr`	34	`gcongr` will attempt to prove the current goal by finding and substituting hypotheses of the form e_1 *rel_op* e_2 into the goal.
`have`	8	Introduces a new named hypothesis for use in the proof.
`induction'`	28	To prove a goal with `n` by induction, specify an induction variable `k` and a name `ih` for the inductive hypothesis.
`intro`	8	Introduces free variables in place of bound variables in a universally quantified formula. A universally bound variable means that the formula has to hold for an arbitrary value so we simply substitute a variable that is this arbitrary value. If the goal is `P→Q` then `intro` introduces `P` as a hypothesis. If `Q` is proven then the hypothesis can be *discharged* and `P→Q` is proven. For an existential goal `∃ a A(a)`, `intro c` introduces `A(c)` as the new goal.
`left, right`	23	If the goal is a disjunction, tell Lean which disjunction you want to prove.
`linarith`	23	Solves linear equalities and inequalities.
`norm_num`	19	Proves numerical equalities and inequalities that do not use variables.
`range`	27	`range n` is defined as the set of natural numbers less than *n*.
`rcases`	18	Given a hypothesis or goal that is a disjunction `A∨B` the tactic `rcases` splits it into two sub-hypotheses or subgoals `A` and `B`. For a disjunctive hypothesis, prove the goal under both sub-hypotheses. For a disjunctive goal, prove one of the subgoals.
`rcases`	19	`rcases h with ⟨v, h'⟩` means given a hypothesis `h`, let `v` be a value such that the new goal is `h'`.

`rel`	33	Given a hypothesis `h` which is a relation e_1 *rel_op* e_2, `rel [h]` will attempt to prove the current goal by substituting `h` into the goal.
`rfl`	30	`rfl` solves a goal that is an equality if they are *definitionally equivalent*, that is, they define the same entity.
`ring`	19	Proves equalities that can be proved directly from the axioms of a commutative ring without taking any hypotheses into account.
`rintro`	22	Performs `intro` and then `rcases` to split the resulting hypothesis.
`rw`	10	`rw [eqn]`, where `eqn` is an equation or an equivalence, rewrites the goal by replacing occurrences of the the left-hand side of `eqn` with the right-hand side. `rw [← eqn]` rewrites the goal by replacing occurrences of the right-hand side of `eqn` with the left-hand side. `rw [eqn] h` and `rw [← eqn] h` rewrite expressions in the hypothesis `h`.
`simp`	28	The `simp` tactic uses lemmas and hypotheses in `Mathlib` to simplify a goal or hypothesis.
`sorry`	16	Proves any theorem.
`symm`	27	Replace an equality `t = u` by `u = t`.
`twoStep-Induction`	32	Proof by induction when there are two base cases and two inductive hypotheses.
`use`	16	Given an existential goal `∃ c A(c)`, this tactic introduces a free variable for the bound variable `c` to form a new goal. It will also attempt to prove the goal using the hypotheses.

Comparison of numerical tactics The follow table and examples clarify the differences between the various tactics for proving numerical equalities and inequalities.

Tactic	Inequalities	Use hypotheses	Use variables
`linarith`	yes	yes	yes
`norm_num`	yes	yes	no
`ring`	no	no	no

```
example : 1 + 3 = 4 := by ring
example : 1 + 3 = 4 := by linarith
example : 1 + 3 = 4 := by norm_num

example : 1 + 3 < 5 := by ring      -- Error
example : 1 + 3 < 5 := by linarith
example : 1 + 3 < 5 := by norm_num

example (h : k = 3): 1 + k = 4 := by ring      -- Error
example (h : k = 3): 1 + k = 4 := by linarith
example (h : k = 3): 1 + k = 4 := by norm_num  -- Error
```

C Tips

Topic	Page	Tip
Anonymous hypothesis	28	A hypothesis can be unamed and can be subsequently accessed as `this`.
Associativity	10	The default associativity in Lean is *left*: `a + b + c` means `(a + b) + c`. Even if the operation is associative, you still have to prove associativity for a given expression.
Division	7	The division operator in Lean is not the `|` symbol on your keyboard, but a similar Unicode symbol `∣` obtained by typing `\\|`.
`done`	7	All proofs should be terminated by `done`. This is not necessary but if your proof is not complete, `done` will display a message.
Don't care	25	When a name or value is syntactically required but you don't care what its value is, you can use the underscore symbol _ instead.
`example`	6	`example` can be used to state an unnamed theorem.
`Finset`, `BigOperators`	27	Given a finite set of numbers `s` and a function `f` over these numbers, `Finset` defines the expressions `∑ x in s f x` and `∏ x in s f x`, where `BigOperators` enables the use of `∑` and `∏`.
Indentation	8	All statements used to prove a hypothesis must be uniformly indented.
Infoview	4	Enter `ctrl-shift-enter` to open the Lean Infoview where hypotheses, goals and errors are displayed. I have found it helpful to place the cursor just before the source line, and then to alternate between `Home` and `End` while looking at Infoview.
Implicit	11	Parameters declared with braces, such as `{a b c : Int}` state that `a b c` are *implicit* bound variables in the theorem whose actual names and types can be inferred when the theorem is used.
Multiple tactics	32	A sequence of tactics can be written on one line with semicolons between them.
Negation	14	A negation `¬p` is defined as `p → False` so it is proved by introducing `p` as a hypothesis and then showing that this results in a contradiction by proving `False`.
`range`	27	`range n` is defined as the set of natural numbers less than `n`.
Right-to-left	14	The symbol `<|` means to compute the expression to its right and pass it to the left.
Tactic	4	If you hover over a tactic its specification will be displayed.
Theorem	4	If you hover over a theorem the stattement of the theorem will be displayed.
Types	35	By convention types are denoted by Greek letters `α`