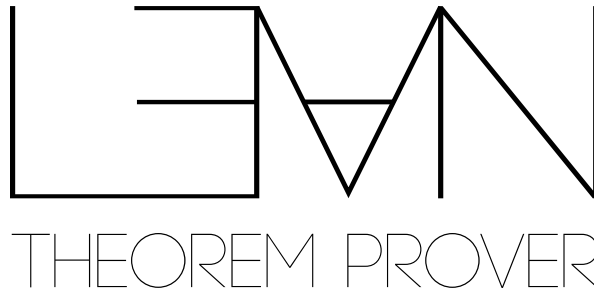


Schulmathematik mit dem



Peter Pfaffelhuber
Sommersemester 2023

universität freiburg

13. Mai 2023

Schulmathematik mit dem Lean Theorem Prover

Inhaltsverzeichnis

0	Vorbereitung zur Nutzung des Skriptes	3
1	Einleitung	3
2	Mathematik	5
2.1	Logik	5
3	Hinweise zu Lean und vscode	7
3.1	Dependent type theory	8
3.2	Von Universen, Typen und Termen	8
3.3	Gleichheit	8
3.4	Hinweise zu vscode	10
4	Taktiken	10
4.1	Cheatsheet	10
	apply	14
	assumption	15
	by_cases	16
	by_contra	17
	calc	18
	cases	20
	change	22
	clear	23
	exact	24
	exfalso	25
	have	26
	induction	27
	intro	28
	intros	29
	left	30
	induction	31
	library_search	32
	linarith	33

norm_num	34
nth_rewrite	35
obtain	36
push_neg	37
rcases	38
refine	39
refl	40
revert	41
right	42
ring	43
rintro	44
rw	45
simp	47
specialize	48
split	49
tauto	50
triv	51
use	52

0 Vorbereitung zur Nutzung des Skriptes

Dies sind die Notizen zu einem Kurs zum formalen Beweisen mit dem interaktiven Theorem-Prover Lean3 (im folgenden schreiben wir nur Lean) im Sommersemester 2023 an der Universität Freiburg. Um den Kurs sinnvoll durcharbeiten zu können, sind folgende technische Vorbereitungen zu treffen:

1. Lokale Installation von Lean und der dazugehörigen Tools: Folgen Sie bitte den Hinweisen auf https://leanprover-community.github.io/get_started.html.
2. Installation von vscode. Bitte befolgen Sie die Download-Hinweise auf <https://code.visualstudio.com/download>.
3. Installation des Repositories des Kurses: Navigieren Sie zu einem Ort, wo Sie die Kursunterlagen ablegen möchten und verwenden Sie `leanproject get https://github.com/pfaffelh/schulmathematik_mit_lean`
Dies sollte die Kursunterlagen herunterladen. Anschließend finden Sie das Manuskript unter `Manuskript/skript.pdf`, und Sie können die Übungen mit `code schulmathematik_mit_lean` öffnen. Die Übungen befinden sich dabei in `src`. Wir empfehlen, dieses Verzeichnis zunächst zu kopieren, etwa nach `mysrc`. Andernfalls kann es sein, dass durch ein Update des Repositories die lokalen Dateien überschrieben werden. Um die Kursunterlagen auf den neuesten Stand zu bringen, geben Sie `git pull` im Verzeichnis `schulmathematik_mit_lean` ein.

1 Einleitung

Der Kurs hat einen Fokus auf das Lehramts-Studium Mathematik an Gymnasien und hat mindestens zwei Ziele:

- Erlernen der Techniken zum interaktiven, formalen Beweisen mit Hilfe der funktionalen Programmiersprache Lean: In den letzten Jahren haben in der Mathematik Bemühungen drastisch zugenommen, computergestützte Beweise zu führen. Während vor ein paar Jahrzehnten eher das konsequente Abarbeiten vieler Fälle dem Computer überlassen wurde, sind interaktive Theorem-Prover anders. Hier kann ein sehr kleiner Kern dazu verwendet werden, alle logischen Schlüsse eines mathematischen Beweises nachzuvollziehen oder interaktiv zu generieren. Der Computer berichtet dann interaktiv über den Fortschritt im Beweis und wann alle Schritte vollzogen wurden.
- Herstellung von Verbindungen zur Schulmathematik: Manchmal geht im Mathematik-Studium der Bezug zur Schulmathematik verloren. Dieser Kurs ist der Versuch, diesen einerseits wieder herzustellen, und auf dem Weg ein tieferes Verständnis für die bereits verinnerlichte Mathematik zu bekommen. Um einem Computer zu *erklären*, wie ein Beweis (oder eine Rechnung oder ein anderweitiges Argument) funktioniert, muss man ihn

erstmal selbst sehr gut verstanden haben. Außerdem muss man den Beweis – zumindest wenn er ein paar Zeilen übersteigt – gut planen, damit die eingegebenen Befehle (die wir Taktiken nennen werden) zusammenpassen.

Formalisierung in der Mathematik

Obwohl Mathematik den Anspruch hat, sauber zu argumentieren, finden sich in mathematischen Veröffentlichungen Fehler. Oftmals sind diese nicht entscheidend für die Richtigkeit der Aussage, die zu beweisen war. Manchmal wird eine Voraussetzung vergessen, und manchmal gibt es auch echte Fehler. Stellt ein Theorem Prover die Richtigkeit eines Beweises fest, so ist die Glaubwürdigkeit deutlich größer. Zwar muss man sich immer noch auf die Fehlerfreiheit des Kerns (also etwa 10000 Zeilen Code) der Programmiersprache verlassen, sonst jedoch nur noch darauf, dass man die zu beweisende Aussage auch versteht und richtig interpretiert.

Heute wächst die Anzahl an Aussagen, die formal bewiesen werden, immer noch deutlich langsamer als die Anzahl an Veröffentlichungen in der Mathematik. Andererseits gibt es mittlerweile eine Community des formalen Beweisens, die von der Zukunftsfähigkeit von Theorem Provers überzeugt ist.

Interactive Theorem Prover

Mittlerweile gibt es einige Theorem Prover. Wir werden hier Lean (von Microsoft Research) verwenden. Grund für diese Wahl ist vor allem, dass es hier die größte Anzahl an Mathematikern gibt, die die `mathlib`, also die mathematische Bibliothek, die auf formal bewiesenen Aussagen mit dem Theorem Prover besteht, weiterentwickeln.

Momentan steht der Wechsel von Lean3 zu Lean4 an. Da insbesondere noch nicht die gesamte `mathlib` in Lean4 zur Verfügung steht, werden wir Lean3 verwenden.

Zum Inhalt

Dieses Manuskript gliedert sich in drei Abschnitte. In Kapitel 2 werden wir die Mathematik besprechen, die wir in den Übungen formal beweisen werden. Dies wird mit einfachen logischen Schlüssen anfangen, und am Ende werden einige Aussagen der Schulmathematik formal bewiesen. Dieser Teil ist der einzige Teil, den man von vorne nach hinten entlang der Übungsaufgaben abarbeiten sollte. Kapitel 3 gibt nützliche Hinweise zu Lean und `vscode`, von der Installation, über die Syntax, bis hin zu verwendeten Gleichheitsbegriffen. Im Kapitel 4 werden wir alle verwendeten Befehle (also die *Taktiken*) besprechen. Diese werden hier als Nachschlagewerk zur Verfügung gestellt, wobei in den Übungen jeweils darauf verwiesen wird, welche neuen Taktiken gerade zu erlernen sind.

2 Mathematik

2.1 Logik

Wir beginnen mit einfachen logischen Aussagen. Wir unterscheiden immer (wie auch in jedem mathematischen Theorem) zwischen den Hypothesen und der Aussage. Um unsere Hypothesen einzuführen, führen wir sie in allen `lean`-Dateien auf einmal mit `variables (P Q R S T: Prop)` ein. Für die Lean-Syntax bemerken wir, dass hier kein üblicher Doppelpfeil \Rightarrow verwendet wird, sondern ein einfacher \rightarrow . Wir gehen hier folgende logische Schlüsse durch:

- Blatt 01-a:
Die Aussage $\vdash P \rightarrow Q$ (d.h. aus P folgt Q) bedeutet ja, dass Q gilt, falls man annehmen darf, dass die Hypothese P richtig ist. Dieser Übergang von $\vdash P \rightarrow Q$ zur Hypothese $hP : P$ mit Ziel $\vdash Q$ erfolgt mittels `intro hP`. Mehrere `intro`-Befehle kann man mittels `intros h1 h2...` abkürzen.
Gilt die Hypothese $hP : P$, und wir wollen $\vdash P$ beweisen, so müssen wir ja nur hP auf das Ziel anwenden. Ist Ziel und Hypothese identisch, so geschieht dies mit `exact hP`. Etwas allgemeiner sucht `assumption` alle Hypothesen danach durch, ob sie mit dem Ziel definitorisch gleich sind.
- Blatt 01-b:
Will man $\vdash Q$ beweisen, und weiß, dass $hPQ : P \rightarrow Q$ gilt, so genügt es, $\vdash P$ zu beweisen (da mit hPQ daraus dann $\vdash Q$ folgt). Mit `apply hPQ` wird in diesem Fall das Ziel nach $\vdash P$ geändert.
Hinter einer Äquivalenz-Aussage $\vdash P \leftrightarrow Q$ stehen eigentlich die beiden Aussagen $\vdash P \rightarrow Q$ und $\vdash Q \rightarrow P$. Mittels `split` wandelt man das Ziel $\vdash P \leftrightarrow Q$ in zwei Ziele für die beiden Richtungen um.
Die logische Verneinung wird in Lean mit \neg notiert. Die Aussage $\neg P$ ist dabei definitorisch gleich $P \rightarrow \text{false}$, wobei `false` für eine falsche Aussage steht.
- Blatt 01-c: Aus falschem folgt Beliebiges ist eigentlich die Aussage $\vdash \text{false} \rightarrow P$. Ist das aktuelle Ziel $\vdash P$, und wendet man die Aussage $\vdash \text{false} \rightarrow P$ mittels `apply` an, so ist das äquivalent zur Anwendung von `exfalso`.
Die beiden Ausdrücke `false` und `true` stehen für zwei Aussagen, die falsch bzw. wahr sind. Also sollte `true` leicht beweisbar sein. Dies liefert die Taktik `triv`.
Bei einem Beweis durch Widerspruch beweist man statt $\vdash P$ die Aussage $\vdash \neg P \rightarrow \text{false}$ (was nach `intro h` zur Annahme $h : \neg P$ und dem neuen Ziel $\vdash \text{false}$ führt). Dies ist logisch korrekt, da P genau dann wahr ist, wenn $\neg P$ auf einen Widerspruch, also eine falsche Aussage, führt. Die

Umwandlung des Goals auf diese Art und Weise erreicht man mit der Taktik `by_contra` bzw. `by_contra h`.

- Blatt 01-d:

Für *und*- bzw. *oder*-Verknüpfungen von Aussagen stellt Lean die üblichen Bezeichnungen \wedge bzw. \vee zur Verfügung. Mit diesen Verbindungen verknüpfte Aussagen können sowohl in einer Hypothese als auch im Ziel vorkommen. Nun gibt es folgende vier Fälle:

$\vdash P \wedge Q$ Hier müssen also die beiden Aussagen P und Q bewiesen werden. Mit `split` werden genau diese beiden Ziele (mit denselben Voraussetzungen) erzeugt, also $\vdash P$ und $\vdash Q$. Sind diese beiden nämlich gezeigt, ist offebar auch $\vdash P \wedge Q$ gezeigt.

$\vdash P \vee Q$ Um dies zu zeigen, genügt es ja, entweder P zu zeigen, oder Q zu zeigen. Im ersten Fall wird mit `left` das Ziel durch $\vdash P$ ersetzt, mit `right` wird das Ziel mit $\vdash Q$. $h : P \wedge Q$ Offenbar zerfällt die Hypothese h in zwei Hypothesen, die beide gelten müssen. Mittels `cases h with hP hQ` wird aus $h : P \wedge Q$ zwei Hypothesen generiert, nämlich $hP : P$ und `leanstate` $hQ : Q$.

$h : P \vee Q$ Ähnlich wie im letzten Fall erzeugt `cases h with hP hQ` nun zwei neue Goals, nämlich eines bei dem $h : P \vee Q$ durch $hP : P$ ersetzt wurde, und eines bei dem $h : P \vee Q$ durch $hQ : Q$ ersetzt wurde. Dies ist logisch in Ordnung, weil man ja so gerade die Fälle, bei denen P oder Q gelten, voneinander treffen kann.

- Blatt 01-e:

Hier geht es um die Einführung neuer Hypothesen. Bei der `by_cases` - Taktik - angewandt auf eine Hypothese $h : P$ - werden alle Möglichkeiten durchgegangen, die P annehmen kann. Diese sind, dass P entweder `true` oder `false` ist. Mit `by_cases h : P` werden also zwei neue Ziele eingeführt, eines mit der Hypothese $h : P$ und eines mit der Hypothese $h : \neg P$.

Eine sehr allgemeine Taktik ist `have`. Hier können beliebige Hypothesen formuliert werden, die zunächst gezeigt werden müssen.

- Blatt 01-f:

Nun kommen wir zu abkürzenden Schreibweisen. Zunächst führen wir die abkürzenden Schreibweise (hP, hQ, hR) für die \wedge -Verknüpfung der Aussagen hP , hQ und hR . (Dies funktioniert ebenfalls mit nur zwei oder mehr als drei Hypothesen). Analog ist $(hP \mid hQ)$ eine Schreibweise für $hP \vee hQ$. Diese beiden Schreibweisen können ebenso verschachtelt werden. Die drei Taktiken, die wir hier besprechen, sind `rintros` für `intros` + `cases`, `rcases` für eine flexiblere Version von `cases`, bei der man die gerade eingeführten Schreibweisen verwenden kann, und `obtain` für `intros` + `have`.

- Blatt 01-g: Quantoren

Quantoren wie \forall und \exists sind (zwar nicht aus der Schule, aber) seit dem ersten Semester bekannt. Diese können ebenfalls in `lean` auftreten. Wir unterscheiden dabei, ob diese Quantoren im Goal oder einer Hypothese auftreten. Es folgt eine kleine Tabelle, welche Taktiken sich jeweils anbieten. Genaue Erklärungen sind in `01-g.lean`.

Quantor	im Goal	in Hypothese <code>h : _</code>
$\forall (x : X), _$	<code>intro x,</code>	<code>apply h _,</code> <code>specialize h _</code>
$\exists (x : X), _$	<code>use _</code>	<code>cases h,</code>

- Blatt 01-h:

Langsam aber sicher arbeiten wir uns zu Anwendungen mit *richtiger* Mathematik vor, aber ein paar Sachen fehlen noch. In diesem Blatt lernen wir, Gleichheiten mittels `refl` zu beweisen. Für das spätere Arbeiten mit `=` - oder \leftrightarrow -Aussagen ist `rw` sehr wichtig, weil man hier Sachen umschreiben kann, d.h. man kann propositionelle Gleichheiten verwenden. Da es in der `mathlib` sehr viele Aussagen bereits gibt, ist es gut, eine Art Suchfunktion zu haben. Diese wird durch `library_search` bzw. `suggest` bereitgestellt. Außerdem lernen wir, Funktionen zu definieren. Dies geschieht in `lean` mit der λ -Notation (übrigens genau wie an vielen Stellen in anderen Programmiersprachen, etwa `python`). Als Beispiel steht `$\lambda x, 2*x$` für die Funktion $x \mapsto 2x$. Hat man etwa `let f : X → X := $\lambda x, 2*x$` , so gibt `f 1` den Funktionswert bei $x = 1$.

Natürliche Zahlen

Definition

`rw`

`calc`

`simp`

Funktionsdefinition

`2n = n+n`

Induktion

`congr?`

3 Hinweise zu Lean und vscode

xxx naming convention

Klammern

In Abschnitt 0 haben wir uns bereits mit der Installation von Lean und `vscode` befasst. Hier folgt eine kurze, unzusammenhängende Einführung.

3.1 Dependent type theory

Lean ist eine funktionale Programmiersprache (d.h. es besteht eigentlich nur aus Funktionen) und basiert auf der *dependent type theory*. Typen in Programmiersprachen wie etwa Python sind `bool`, `int`, `double` etc. Lean lebt davon, eigene Typen zu definieren und zu verwenden. Wir werden sehen im Verlauf des Kurses sehen, dass man über die entstehenden Typen wie Mengen denken kann. Der Typ \mathbb{N} wird etwa die Menge der natürlichen Zahlen, und \mathbb{R} die Menge der reellen Zahlen sein. Allerdings steht \mathbb{N} in der Tat für eine unendliche Menge, die dadurch charakterisiert ist, dass sie `0` enthält, und wenn sie `n` enthält, so enthält sie auch den Nachfolger von `n` (der mit `succ n` dargestellt wird). Entsprechend sind die reellen Zahlen durch eine Äquivalenzrelation auf Cauchy-Folgen definiert, was schon recht aufwändig ist. Typen können dabei von anderen Typen abhängen, und deshalb sprechen wir von *dependent types*. Etwa ist der Raum \mathbb{R}^n abhängig von der Dimension `n`. Wie wir sehen werden, sind mathematische Aussagen ebenfalls solche Typen.

```
example : P → P :=  
begin  
  sorry,  
end
```

Zur Notation: Bei Mengen sind wir gewohnt, etwa $n \in \mathbb{N}$ zu schreiben, falls `n` eine natürliche Zahl ist. In der Typentheorie schreiben wir `n : \mathbb{N}` und sagen, dass `n` ein Term (Ausdruck) vom Typ \mathbb{N} ist. Etwas allgemeiner hat jeder Ausdruck einen Typ und bei der Einführung jedes Ausdrucks überprüft Lean dessen Typ.

Sehen wir uns den rechten Teil des vscode-Fensters an. Dieser heißt aktueller *proof state*.

3.2 Von Universen, Typen und Termen

In Lean gibt es drei Ebenen von Objekten: Universen, Typen und Terme. Wir befassen uns hier mit den letzten beiden. Von besonderem Interesse ist der Typ `Prop`, der aus Aussagen besteht, die wahr oder falsch sein können. Er umfasst mathematische Aussagen, also entweder die Hypothesen, oder das Goal dessen, was zu beweisen ist. Eine Hypothese in Lean hat die Form `hP : P`, was soviel sagt wie `P` gilt, und diese Aussage heißt `hP`. Es kann auch bedeuten, dass `P` gilt und `hP` ein Beweis von `P` ist. Dabei haben die Hypothesen hier Namen `P Q R S`, und die Namen der Hypothesen `hP hQ hR hS`. Alle Namen können beliebig sein. Weiter gibt es Hypothesen der Form `P → Q`, also die Aussage, dass aus `P` die Aussage `Q` folgt.

3.3 Gleichheit

In Lean gibt es drei Arten von Gleichheit:

- Syntaktische Gleichheit: Wenn zwei Terme Buchstabe für Buchstabe gleich sind, so sind sie syntaktisch gleich. Allerdings gibt es noch ein paar weitere Situationen, in denen zwei Terme syntaktisch gleich sind. Ist nämlich ein Term nur eine Abkürzung für den anderen (etwa ist $x=y$ eine Abkürzung für $\text{eq } x \ y$), so sind diese beiden Terme syntaktisch gleich. Ebenfalls gleich sind Terme, bei denen global quantifizierte Variablen andere Buchstaben haben. Etwa sind $\forall x, \exists y, f \ x \ y$ und $\forall y, \exists x, f \ y \ x$ syntaktisch gleich.
- Definitorische Gleichheit: Manche Terme sind in Lean per Definition gleich. Für $x : \mathbb{N}$ ist $x + 0$ per Definition identisch zu x . Allerdings ist $0 + x$ nicht definitorisch identisch zu x . Dies hat offenbar nur mit der internen Definition der Addition natürlicher Zahlen in Lean zu tun.
- Propositionelle Gleichheit: Falls es einen Beweis von $x = y$ gibt, so heißen x und y und propositionell gleich. Analog heißen Terme P und Q propositionell gleich, wenn man $P \leftrightarrow Q$ beweisen kann.

rw ist für syntaktische Gleichheit

Viele Taktiken arbeiten bis hin zur definitorischen Gleichheit.

xxx Extensionalität

Terms of Types


sorry-Taktik

Wir beginnen mit der Beschreibung zweier grundlegender Taktiken, nämlich `intro` und `exact`; bitte in Kapitel 4 nachlesen. Das denkbar einfachste Beispiel ist die Aussage $P \rightarrow P$, d.h. aus P folgt P . In Lean sieht das dann so aus:

```
example : P → P :=
begin
  sorry,
end
```

Der *proof state* verändert sich je nachdem, wo der cursor innerhalb des **begin end**-Blockes steht. Ist der Cursor direkt nach **begin**, so ist der *proof state*

```
P : Prop
├ P → P
```

Hier ist wichtig zu wissen, dass hinter \vdash die Behauptung steht, und alles darüber Hypothesen sind. (Im gezeigten Fall ist dies nur die Tatsache, dass P eine Behauptung/Proposition ist. Diese Darstellung entspricht also genau der Behauptung. Ist der Cursor nach dem `sorry`, so steht nun zwar **goals accomplished** , allerdings ist die `sorry`-Taktik nur da, um erst einmal unbewiesene Behauptungen ohne weitere Handlung beweisen zu können und es erfolgt eine Warnung in vscode. Löscht man das `sorry` und ersetzt es durch ein `intro hP`, so erhält man

```
P : Prop
hP : P
├ P
```

Wir haben also die Aussage $P \rightarrow P$ überführt in einen Zustand, bei dem wir $hP : P$ annehmen, und P folgern müssen. Dies lässt sich nun leicht mittels `assumption`, lösen (bitte das Komma nicht vergessen), und es erscheint das gewünschte **goals accomplished** 🏆. Die `assumption`-Taktik sucht nach einer Hypothese, die identisch mit der Aussage ist und schließt den Beweis. Etwas anders ist es mit der `exact`-Taktik. Hier muss man wissen, welche Hypothese genau gemeint und, und kann hier mit `exact hP` den Beweis schließen

Klammerung: In Lean wird die Anwendung von Funktionen, oder die Anwendung von Hypothesen, meist ohne Klammern geschrieben, also etwa $f\ x$ anstatt $f(x)$. Eine interne Klammerung erfolgt dabei immer nach rechts, d.h. $g\ f\ x$ ist eigentlich $g\ (f\ x)$. Analog ist bei Aussagen $P \rightarrow Q \rightarrow R$ zu lesen als $P \rightarrow (Q \rightarrow R)$.

3.4 Hinweise zu vscode

Hinweise zu vscode

Warnungen und Fehler

Eingabe von Sonderzeichen

Klammerung anzeigen lassen

(In vscode gibt man diese mit `\wedge` bzw. `\vee` ein.)

4 Taktiken

4.1 Cheatsheet

Binäre Operatoren wie *und* (\wedge), *oder* (\vee), *Schnittmengen* (\cap) und *Vereinigungsmengen* (\cup) sind rechts-assoziativ, also z.B. $P \wedge Q \wedge R := P \wedge (Q \wedge R)$.

Proof state	Kommando	Neuer proof state
$\vdash P \rightarrow Q$	<code>intro hP</code>	$hP : P$ $\vdash Q$
$f : \alpha \rightarrow \text{Prop}$ $\vdash \forall (x : \alpha), f\ x$	<code>intro x</code>	$f : \alpha \rightarrow \text{Prop}$ $x : \alpha$ $\vdash f\ x$
$h : P$ $\vdash P$	<code>exact h</code>	goals accomplished 🏆

Proof state	Kommando	Neuer proof state
$h : P$ $\vdash P$	assumption	goals accomplished 🏁
$h : P \rightarrow Q$ $\vdash Q$	apply h	$h : P \rightarrow Q$ $\vdash P$
$\vdash P \rightarrow Q \rightarrow R$	intros hP hQ	$hP : P$ $hQ : Q$ $\vdash R$
$\vdash P \wedge Q \rightarrow P$ ¹	tauto oder tauto!	goals accomplished 🏁
$\vdash \text{true}$	triv	goals accomplished 🏁
$h : P$ $\vdash Q$	exfalso	$h : P$ $\vdash \text{false}$
$\vdash P$	by_contra h	$h : \neg P$ $\vdash \text{false}$
$\vdash P$	by_cases h : Q	$h : Q$ $\vdash P$ $h : \neg Q$ $\vdash P$
$h : P \wedge Q$ $\vdash R$	cases h with hP hQ	$hP : P$ $hQ : Q$ $\vdash R$
$h : P \vee Q$ $\vdash R$	cases h with hP hQ	$hP : P$ $\vdash R$ $hQ : Q$ $\vdash R$
$h : \text{false}$ $\vdash P$	cases h	goals accomplished 🏁
$\vdash : P \rightarrow \text{false}$	change $\neg P$	$\vdash \neg P$
$\vdash P \wedge Q$	split	$\vdash P$ $\vdash Q$
$\vdash P \leftrightarrow Q$	split	$\vdash P \rightarrow Q$ $\vdash Q \rightarrow P$
$\vdash P \leftrightarrow P$ oder $\vdash P = P$	refl	goals accomplished 🏁
$h : P \leftrightarrow Q$	rw h	$h : P \leftrightarrow Q$



¹...oder ein anderes Statement, das mit Wahrheitstabellen lösbar ist.

Proof state	Kommando	Neuer proof state
$\vdash P$		$\vdash Q$
$h : P \leftrightarrow Q$ $\vdash Q$	<code>rw ← h</code>	$h : P \leftrightarrow Q$ $\vdash P$
$h : P \leftrightarrow Q$ $hP : P$	<code>rw h at hP</code>	$h : P \leftrightarrow Q$ $hP : Q$
$h : P \leftrightarrow Q$ $hQ : Q$	<code>rw ← h at hQ</code>	$h : P \leftrightarrow Q$ $hQ : P$
$\vdash P \vee Q$	<code>left</code>	$\vdash P$
$\vdash P \vee Q$	<code>right</code>	$\vdash Q$
$\vdash 2 + 2 < 5^2$	<code>norm_num</code>	goals accomplished 🏆
$f : \alpha \rightarrow \text{Prop}$ $y : \alpha$ $\vdash \exists (x : \alpha), f x$	<code>use y</code>	$f : \alpha \rightarrow \text{Prop}$ $y : \alpha$ $\vdash f y$
$x y : \mathbb{R}$ $\vdash x + y = y + x^3$	<code>ring</code>	goals accomplished 🏆
$\vdash P \rightarrow Q$	<code>intro hP</code>	$hP : P$ $\vdash Q$
$f : \alpha \rightarrow \text{Prop}$ $\vdash \forall (x : \alpha), f x$	<code>intro x</code>	$f : \alpha \rightarrow \text{Prop}$ $x : \alpha$ $\vdash f x$
$h1 : a < b$ $h2 : b \leq c$ $\vdash a < c^4$	<code>linarith</code>	goals accomplished 🏆
$h : P$ $\vdash Q$	<code>clear h</code>	$\vdash Q$
$f : \mathbb{N} \rightarrow \text{Prop}$ $h : \forall (n : \mathbb{N}), f n$ $\vdash P$	<code>specialize h 13</code>	$f : \mathbb{N} \rightarrow \text{Prop}$ $h : f 13$ $\vdash P$
$f : \mathbb{N} \rightarrow \mathbb{N} \rightarrow \text{Prop}$ $h : \forall (n : \mathbb{N}), \exists (m : \mathbb{N}), f n m$	<code>obtain { m, hm } := h 27,</code>	$f : \mathbb{N} \rightarrow \mathbb{N} \rightarrow \text{Prop}$ $h : \forall (n : \mathbb{N}), \exists (m : \mathbb{N}),$ $f n m$ $m : \mathbb{N}$

²...oder ein anderes Statement, das nur Rechnungen mit numerischen Werte beinhaltet.

³...oder ein anderes Statement, das nur Rechenregeln von kommutativen Ringen verwendet.
`ring` zieht Hypothesen nicht in Betracht.

⁴...oder eine Aussage, die nur $<$, \leq , \neq oder $=$ verwendet. `linarith` zieht Hypothesen in Betracht.

Proof state	Kommando	Neuer proof state
		hm : f 27 m
$\vdash R$	have h : P \leftrightarrow Q,	$\vdash P \leftrightarrow Q$ h : P \leftrightarrow Q $\vdash R$
h1 : a < b h2 : b < c $\vdash a < c$	library_search	goals accomplished  Try this: exact lt_trans h1 h2
hQ : Q $\vdash P \wedge Q$	refine (_, hQ)	hQ : Q $\vdash P$
$\vdash P \vee Q \rightarrow R$	rintro (hP hQ) = intro h , cases h with hP hQ	hP : P $\vdash P$ hQ : Q $\vdash Q$
$\vdash P \wedge Q \rightarrow R$	rintro (hP , hQ) = intro h , cases h with h1 h2	hP : P hQ : Q $\vdash Q$
h : P \wedge Q \vee P \wedge R $\vdash P$	rcases h with ((hP1,hQ) (hP2,hR))	hP1 : P hQ : Q $\vdash P$ hP2 : P hR : R $\vdash P$
$\vdash n + 0 = n$ ⁵	simp	goals accomplished 
h : n + 0 = m ⁵ $\vdash P$	simp at h	h : n = m $\vdash P$

xxx change xxx let

def f : $\mathbb{N} \rightarrow \mathbb{R} := \lambda n, n^2 + 3$

⁵...oder ein anderes Statement, das sich durch Äquivalenz-Aussagen der Bibliothek vereinfachen lassen.

apply

Zusammenfassung

Angenommen, das Goal ist $\vdash Q$, wobei bereits ein Beweis für $h : P \rightarrow Q$ zur Verfügung steht. Deshalb braucht man nur noch einen Beweis für $\vdash P$ zu finden. Diese Umwandlung passiert mit `apply h`.

Beispiele

Proof state	Kommando	Neuer proof state
$h : P \rightarrow Q$ $\vdash Q$	<code>apply h</code>	$h : P \rightarrow Q$ $\vdash P$
$h : \neg P$ $\vdash \text{false}$	<code>apply h</code>	$h : \neg P$ $\vdash P$

Die Taktik `apply` wendet sich iterativ an. Das bedeutet: liefert `apply h` (identisch mit `refine h _`) keinen Fortschritt, so wird es mit `refine h _ _` versucht:

Proof state	Kommando	Neuer proof state
$h : P \rightarrow Q \rightarrow R$ $\vdash R$	<code>apply h</code>	$h : P \rightarrow Q \rightarrow R$ $\vdash P$ $h : P \rightarrow Q \rightarrow R$ $\vdash Q$

Anmerkungen

1. `apply` arbeitet bis hin zur definitorischen Gleichheit. Dies kann man im zweiten Beispiel sehen, da $\neg P$ per Definition gleich $P \rightarrow \text{false}$ ist:
2. `apply h` ist identisch zu `refine h _`, bzw. (wie im zweiten Beispiel oben) zu `refine h _ _`.

assumption

Zusammenfassung

Ist eine der Annahmen identisch mit dem Goal, dann schließt `assumption`, das Goal.

Beispiele

Proof state	Kommando	Neuer proof state
$h : P$ $\vdash P$	<code>assumption</code>	goals accomplished 🏁
$h : \neg P$ $\vdash P \rightarrow \text{false}$	<code>assumption,</code>	goals accomplished 🏁

Anmerkungen

1. Wie andere Taktiken auch arbeitet `assumption` bis zur definitorischen Gleichheit.
2. Hier ein Trick: Verwendet man als Abschluss einer Taktik ein Semicolon `;`, so wird die nachfolgende Taktik auf alle Goals angewendet:

Proof state	Kommando	Neuer proof state
$hP : P$ $hQ : Q$ $\vdash : P \wedge Q$	<code>split; assumption,</code>	goals accomplished 🏁

by_cases

Zusammenfassung

Hat man einen Term $P : \text{Prop}$ als Hypothese, so liefert `by_cases hP : P` zwei Goals. Beim ersten gibt es zusätzlich $hP : P$, beim zweiten $hP : \neg P$. Diese Taktik ist also identisch mit `have hP : P \vee \neg P, exact em P, cases hP, .` (Der zweite Ausdruck ist $\text{em} : \forall (p : \text{Prop}), p \vee \neg p$).

Beispiele

Proof state	Kommando	Neuer proof state
$\vdash P$	<code>by_cases h : Q</code>	$h : Q$ $\vdash P$ $h : \neg Q$ $\vdash P$
$x : \text{bool}$ $\vdash x = \text{tt} \vee x = \text{ff}$	<code>by_cases x=tt,</code>	$x : \text{bool}$ $h : x = \text{tt}$ $\vdash x = \text{tt} \vee x = \text{ff}$ $x : \text{bool}$ $h : \neg x = \text{tt}$ $\vdash x = \text{tt} \vee x = \text{ff}$

Im zweiten Beispiel verwenden wir eine Variable vom Typ `bool`. Diese ist folgendermaßen definiert:

```
inductive bool : Type
| ff : bool
| tt : bool
```

Eine Bool'sche Variable hat also nur die Möglichkeiten `tt` (für `true`) und `ff` (für `false`).

Anmerkungen

1. Offenbar benutzt die `by_cases`-Taktik (genau wie `by_contradiction`), dass eine Aussage entweder wahr oder falsch ist. Dies ist auch bekannt unter dem Gesetz des ausgeschlossenen Dritten. In der Mathematik nennt man Beweise, die diese Regel nicht verwenden, konstruktiv.
2. Für Terme vom Typ `Prop` kann die Taktik `tauto` (bzw. `tauto!`) durch eine Wahrheitstabelle viele Schlüsse ziehen.

by_contra

Zusammenfassung

Die `by_contra`-Taktik stellt einen Beweis durch Widerspruch dar. Es wird deshalb angenommen (d.h. in eine Hypothese überführt), dass die Aussage (hinter \vdash) nicht wahr ist, und dies muss zu einem Widerspruch geführt werden, d.h. es muss ein Beweis von `false` gefunden werden.

Beispiele

Proof state	Kommando	Neuer proof state
$\vdash P$	<code>by_contra h</code>	$h : \neg P$ $\vdash \text{false}$
$h : \neg \neg P$ $\vdash P$	<code>by_contra hnegP,</code>	$h : \neg \neg P$ $hnegP : \neg P$ $\vdash \text{false}$

Anmerkungen

Diese Taktik ist stärker als `exfalso`. Dort wird ja schließlich das Goal nur in `false` überführt, ohne eine neue Hypothese hinzuzufügen. Bei `by_contra` ist das neue Goal zwar auch `false`, aber es gibt noch eine neue Hypothese.

calc

Zusammenfassung

Wie das Wort schon andeutet, geht es bei **calc** um konkrete Berechnungen. Dies ist kein Taktik, sondern ein `lean`-Modus. Das bedeutet, dass man diesen Modus betreten kann (mit dem Wort **calc**) Rechenschritte eingibt und Beweise dafür, dass jeder einzelne Rechenschritt stimmt.

Beispiele

Hier ein Beweis der ersten binomischen Formel, der nur durch Umschreiben von Recheneigenschaften aus der `mathlib` zustande kommt.

```
example (n : ℕ): (n+1)^2 = n^2 + 2*n + 1 :=  
begin  
  have h : n + n = 2*n,  
  {  
    nth_rewrite 0 ← one_mul n,  
    nth_rewrite 1 ← one_mul n,  
    rw ← add_mul,  
  },  
  calc (n+1)^2 = (n+1) * (n+1) : by { rw pow_two, }  
  ... = (n+1)*n + (n+1) * 1: by {rw mul_add, }  
  ... = n*n + 1*n + (n+1) : by {rw add_mul, rw mul_one (n+1),}  
  ... = n^2 + n + (n+1) : by {rw one_mul, rw ← pow_two,}  
  ... = n^2 + (n + n+1) : by {rw add_assoc, rw ← add_assoc n n 1,}  
  ... = n^2 + 2*n + 1 : by { rw ← add_assoc, rw ← h, },  
end
```

Dasselbe kann man auch ohne den **calc**-Modus erreichen, etwa so:

```
example (n : ℕ): (n+1)^2 = n^2 + 2*n + 1 :=  
begin  
  have h : n + n = 2*n, by { nth_rewrite 0 ← one_mul n,  
    nth_rewrite 1 ← one_mul n, rw ← add_mul, },  
  rw [pow_two, mul_add, add_mul, mul_one (n+1), one_mul,  
    ← pow_two, add_assoc, ← add_assoc n n 1,  
    ← add_assoc, ← h],  
end
```

Dies ist jedoch deutlich schlechter lesbar.

Anmerkungen

1. Wichtig ist die genaue Notation im **calc**-Modus, insbesondere die drei `...` und das `: by { }`.

2. Um einen Beweis im **calc**-Modus zu erzeugen, geht man am besten wie folgt vor (hier am Beispiel eines Beweises von $h : n + n = 2 * n$: Zunächst gibt man die einzelnen Rechenschritte an, und entschuldigt sich bei jedem Beweis:

```
example (n : ℕ) : n + n = 2 * n :=  
begin  
  calc n + n = 1 * n + 1 * n : by {sorry,}  
  ... = (1 + 1) * n : by {sorry, }  
  ... = 2 * n : by {sorry, }  
end
```

Anschließend kann man in jeder Klammer das **sorry**, mit dem richtigen Beweis schrittweise austauschen.

3. Der **calc**-Modus funktioniert nicht nur für Gleichungsketten, sondern auch für Ungleichungsketten, Teilmengenrelationen etc.
4. Deutlich einfacher löst man obiges Beispiel mit **linarith**, oder **ring**.

cases

Zusammenfassung

Ist eine Hypothese zusammengesetzt, d.h. lässt sich in zwei oder mehr Fälle erweitern, so liefert `cases` genau das. Dies kann nicht nur bei Hypothesen $h : P \vee Q$ oder $h : P \wedge Q$ angewendet werden, sondern auch bei Strukturen, die aus mehreren Fällen bestehen, wie $\exists \dots$ (hier gibt es eine Variable und eine Aussage) und $x : \text{bool}$ oder $n : \mathbb{N}$.

Beispiele

Proof state	Kommando	Neuer proof state
$h : P \wedge Q$ $\vdash R$	<code>cases h with hP hQ</code>	$hP : P$ $hQ : Q$ $\vdash R$
$h : P \vee Q$ $\vdash R$	<code>cases h with hP hQ</code>	$hP : P$ $\vdash R$ $hQ : Q$ $\vdash R$
$h : \text{false}$ $\vdash P$	<code>cases h</code>	goals accomplished 🏁
$P : \mathbb{N} \rightarrow \text{Prop}$ $h : \exists (m : \mathbb{N}), P\ m$ $\vdash Q$	<code>cases x with m h1,</code>	$P : \mathbb{N} \rightarrow \text{Prop}$ $m : \mathbb{N}$ $h1 : P\ m$ $\vdash Q$
$x : \text{bool}$ $\vdash x = \text{tt} \vee x = \text{ff}$	<code>cases x,</code>	$\vdash \text{ff} = \text{tt} \vee \text{ff} = \text{ff}$ $\vdash \text{tt} = \text{tt} \vee \text{tt} = \text{ff}$
$n : \mathbb{N}$ $\vdash n > 0$ $\rightarrow (\exists (k : \mathbb{N}), n = k + 1)$	<code>cases n,</code>	$\vdash 0 > 0$ $\rightarrow (\exists (k : \mathbb{N}), 0 = k + 1)$ $\vdash n.\text{succ} > 0$ $\rightarrow (\exists (k : \mathbb{N}),$ $n.\text{succ} = k + 1)$

Anmerkungen

1. Die Anwendung `cases n` für $n : \mathbb{N}$ ist strikt schwächer als die vollständige Induktion (siehe `induction`). Durch `cases` wird ja nur $n : \mathbb{N}$ in die beiden Fälle `0` und `succ n` umgewandelt, aber man darf nicht die Aussage für $n-1$ verwenden, um die Aussage für n zu beweisen.
2. Ein besonderer Fall ist es, wenn h unmöglich ist und damit gar keine

Konstrukturen hat. Ist etwa $h : \text{false}$, so schließt `cases h` jedes Goal.

3. Eine etwas flexiblere Version von `cases` ist `rcases`.

change

Zusammenfassung

Ändert das Goal (bzw. eine Hypothese) in ein Goal (bzw. eine Hypothese), das (die) definitorisch gleich ist.

Beispiele

Proof state	Kommando	Neuer proof state
$\vdash : P \rightarrow \text{false}$	change $\neg P$	$\vdash \neg P$
$h : \neg P$ $\vdash Q$	change $P \rightarrow \text{false}$ at h ,	$h : P \rightarrow \text{false}$ $\vdash Q$
$xs : x \in s$ $\vdash x \in f^{-1}(f \text{ '' } s)$	change $f x \in f \text{ '' } s$,	$xs : x \in s$ $\vdash f x \in f \text{ '' } s$

Anmerkungen

1. Wie man am vorletzten Beispiel sieht, funktioniert `change` auch bei Hypothesen.
2. Da viele Taktiken sowieso auf definitorische Gleichheit testen, ist `change` oftmals nicht nötig. Es kann aber helfen, den Beweis lesbarer zu machen.

clear

Zusammenfassung

Mit `clear h` wird die Hypothese `h` aus dem Goal state entfernt (vergessen).

Beispiele

Proof state	Kommando	Neuer proof state
<code>h : P</code> <code>└─ Q</code>	<code>clear h</code>	<code>└─ Q</code>

exact

Zusammenfassung

Ist das Goal durch einen einzigen Befehl zu lösen, dann durch die `exact` Taktik. Wie viele andere Taktiken auch funktioniert `exact` auch bei definitorischen gleichen Termen.

Beispiele

Proof state	Kommando	Neuer proof state
$h : P$ $\vdash P$	<code>exact h</code>	goals accomplished 🏆
$hP : P$ $hQ : Q$ $\vdash P \wedge Q$	<code>exact { hP, hQ },</code>	goals accomplished 🏆
$hP : P$ $hnP : P \rightarrow \text{false}$ $\vdash \text{false}$	<code>exact hnP hP,</code>	goals accomplished 🏆

Anmerkungen

Beim dritten Beispiel sollte man sich die Reihenfolge einprägen, in der die beiden Hypothesen `hP` und `hnP` angewendet werden. Die erste Hypothese nach `exact` ist immer die, deren rechte Seite mit dem Goal übereinstimmt. Benötigt diese weiteren Input, wird er danach fortgeschrieben.

exfalse

Zusammenfassung

Die Aussage $\text{false} \rightarrow P$ ist für alle P wahr. Ist das momentane Goal also $\vdash P$, und man würde diese wahre Aussage mittels `apply` anwenden, wäre das neue Goal $\vdash \text{false}$. Genau dies macht die `exfalse`-Taktik.

Beispiele

Proof state	Kommando	Neuer proof state
$h : P$ $\vdash Q$	<code>exfalse</code>	$h : P$ $\vdash \text{false}$
$hP : P$ $hnP : \neg P$ $\vdash Q$	<code>exfalse,</code>	$hP : P$ $hnP : \neg P$ $\vdash \text{false}$

Anmerkungen

Falls man diese Taktik anwendet, verlässt man den Bereich der konstruktiven Mathematik. (Diese verzichtet auf die Regel des ausgeschlossenen Dritten.)

have

Zusammenfassung

Mittels **have** führt man eine neue Behauptung ein, die man zunächst beweisen muss. Anschließend steht sie als Hypothese in allen weiteren Goals zur Verfügung. Dies ist identisch damit, zunächst ein Lemma h mit der Aussage nach **have** h : zu beweisen, und es dann an gegebener Stelle im Beweis wieder zu verwenden (etwa mit `apply` oder `rw`).

Beispiele

Proof state	Kommando	Neuer proof state
$\vdash R$	have $h : P \leftrightarrow Q$,	$\vdash P \leftrightarrow Q$ $h : P \leftrightarrow Q$ $\vdash R$
$\vdash P$	have $h1 : \exists (m : \mathbb{N}),$ $f \geq m, \dots$ cases $h1$ with $m \ hm$	$m : \mathbb{N}$ $hm : f \geq m$ $\vdash P$

Anmerkungen

1. Hat man zwei Goals (nennen wir sie $\vdash 1$ und $\vdash 2$), und benötigt man im Beweis von $\vdash 2$ die Aussage von $\vdash 1$, so kann man zunächst ein drittes Goal mit **have** $h := \vdash 1$ einführen (wobei $\vdash 1$ durch die Aussage zu ersetzen ist). Anschließend kann man $\vdash 1$ mit `exact` beweisen, und hat im Beweis von $\vdash 2$ die Aussage $\vdash 1$ zur Verfügung.

induction

Zusammenfassung

Beispiele

Anmerkungen

intro

Zusammenfassung

Ist das Goal von der Form $\vdash P \rightarrow Q$ oder $\forall (n : \mathbb{N}), P\ n$, so kann man mit `intro P` bzw. `intro n` weiterkommen.

Beispiele

Proof state	Kommando	Neuer proof state
$\vdash P \rightarrow Q$	<code>intro hP</code>	$hP : P$ $\vdash Q$
$f : \alpha \rightarrow \text{Prop}$ $\vdash \forall (x : \alpha), f\ x$	<code>intro x</code>	$f : \alpha \rightarrow \text{Prop}$ $x : \alpha$ $\vdash f\ x$

Anmerkungen

1. Mehrere `intro`-Befehle hintereinander fasst man am besten mit `intros` zusammen. Weiter ist `rintro` eine flexiblere Variante.
2. Eine Umkehrung von `intro` ist `revert`.

intros

Zusammenfassung

Dies ist genau wie bei `intro`, aber es können gleichzeitig mehrere `intro`-Befehle zu einem einzigen zusammengefasst werden. Etwas genauer ist `intros h1 h2 h3`, identisch mit `intro h1, intro h2, intro h3`.

Beispiele

Proof state	Kommando	Neuer proof state
$\vdash P \rightarrow Q \rightarrow R$	<code>intros hP hQ</code>	$hP : P$ $hQ : Q$ $\vdash R$
$P : \mathbb{N} \rightarrow \text{Prop}$ $\vdash \forall (n : \mathbb{N}), P\ n \rightarrow Q$	<code>intros n hP</code>	$P : \mathbb{N} \rightarrow \text{Prop}$ $n : \mathbb{N}$ $hP : P\ n \vdash Q$

Anmerkungen

`rintro` ist eine flexiblere Variante, bei der gleichzeitig `cases`-Anwendungen ausgeführt werden können.

left

Zusammenfassung

Die Anwendung von `left`, ist identisch mit `apply h`, für $h : P \rightarrow P \vee Q$. Hat man also eine Goal der Form $\vdash P \vee Q$, so bewirkt `left`, dass man nur noch das Goal $\vdash P$ hat. Schließlich genügt es ja, P zu zeigen, um das Goal zu schließen.

Beispiele

Proof state	Kommando	Neuer proof state
$\vdash P \vee Q$	<code>left</code>	$\vdash P$
$\vdash \mathbb{N}$	<code>left,</code>	goals accomplished 🏆

Das zweite Beispiel bedarf einer kleinen Erklärung. Zunächst muss man verstehen, dass beim Goal $\vdash \mathbb{N}$ zu zeigen ist, dass es einen Term vom Typ \mathbb{N} gibt, also dass es eine natürliche Zahl gibt. Nun muss man wissen, wie \mathbb{N} in Lean implementiert ist. Dies ist

```
inductive nat
| zero : nat
| succ (n : nat) : nat
```

zusammen mit

```
notation `N := nat
```

Das bedeutet: Der Typ \mathbb{N} ist definiert dadurch, dass `zero` ein Term von diesem Typ ist, und dass es eine Funktion $\text{succ} : \mathbb{N} \rightarrow \mathbb{N}$ gibt. Mit der Eingabe von `left`, im zweiten Beispiel wird das Goal also deshalb geschlossen, weil per Definition `zero : \mathbb{N}` gilt, insbesondere gibt es also einen Term vom Typ \mathbb{N} .

Anmerkungen

1. Siehe auch `right`, für die entsprechende Taktik, die äquivalent ist zu `apply h` für $h : Q \rightarrow P \vee Q$.
2. Wie im zweiten Beispiel lässt sich `left`, immer dann anwenden, wenn man einen induktiven Typ mit zwei Konstruktoren (so wie \mathbb{N}) vor sich hat.

library_search

Zusammenfassung

Es gibt ja sehr viele bereits bewiesene Aussage in `mathlib`. Bei der Verwendung von `library_search` wird die `mathlib` auf Aussagen hin durchsucht, deren Typen denen der zu beweisenden Aussage entsprechen. Führt dies nicht zum Erfolg, meldet Lean einen `timeout`. Im Fall eines Erfolges wird außerdem berichtet, welches Kommando gefunden wurde. Clickt man darauf, so wird dies an Stelle von `library_search` eingesetzt.

Beispiele

Proof state	Kommando	Neuer proof state
$h1 : a < b$ $h2 : b < c$ $\vdash a < c$	<code>library_search</code>	goals accomplished 🏆 Try this: <code>exact lt_trans h1 h2</code>

Anmerkungen

Die Taktik `suggest` ist ähnlich und funktioniert auch dann, wenn das Goal nicht geschlossen werden kann.

linarith

Zusammenfassung

Diese Taktik kann unter Zuhilfenahme der Hypothesen Gleichungen und Ungleichungen beweisen. Wichtig ist, dass die verwendeten Hypothesen ebenfalls nur Gleichungen und Ungleichungen sind. Hier wird also vor allem mit Transitivität von $<$ zusammen mit Rechenregeln gearbeitet.

Beispiele

Proof state	Kommando	Neuer proof state
$h1 : a < b$ $h2 : b \leq c$ $\vdash a < c$ ⁶	linarith	goals accomplished 🏆

Anmerkungen

norm_num

Zusammenfassung

Solange keine Variablen involviert sind, kann `norm_num` Rechnungen durchführen, die ein $=$, $<$, \leq , oder \neq beinhalten.

Beispiele

Proof state	Kommando	Neuer proof state
$\vdash 2 + 2 < 5$ ⁷	<code>norm_num</code>	goals accomplished 🏆
$\vdash (1 : \mathbb{R}) = 1$	<code>norm_num,</code>	goals accomplished 🏆

Anmerkungen

`norm_num` kennt noch ein paar andere Rechenoperationen, etwa die Betragsfunktion, siehe das zweite Beispiel.

nth_rewrite

Proof state	Kommando	Neuer proof state
$\vdash 2 + 2 < 5$ ⁸	norm_num	goals accomplished 🎉

Zusammenfassung

Diese Taktik ist verwandt zu `rw`. Der Unterschied ist, dass man angeben kann, auf das wievielte Vorkommen des zu ersetzenden Terms das `rw` angewendet werden soll. Die genaue Syntax ist `nth_rewrite k h`, wobei `k` die Nummer (beginnend mit 0) des zu ersetzenden Terms ist und `h` die zu ersetzende Hypothese. Wie bei `rw` muss diese von der Form `h : x=y` oder `h : A↔B` sein.

Beispiele

Proof state	Kommando	Neuer proof state
$n : \mathbb{N}$ $\vdash 0 + n = 0 + 0 + n$	<code>nth_rewrite 0 zero_add</code>	$n : \mathbb{N}$ $\vdash n = 0 + 0 + n$
$n : \mathbb{N}$ $\vdash 0 + n = 0 + 0 + n$	<code>nth_rewrite 1 zero_add</code>	$n : \mathbb{N}$ $\vdash 0 + n = n$
$n : \mathbb{N}$ $\vdash 0 + n = 0 + 0 + n$	<code>nth_rewrite 2 zero_add</code>	$n : \mathbb{N}$ $\vdash 0 + n = 0 + n$

Lean sieht in obigem Beispiel dreimal ein Term der Form `0 + _`: Nummer 0 ist auf der linken Seite, für Nummer 1 und 2 wird auf der rechten Seite (wegen der Klammerung `0 + 0 + n = (0 + 0) + n`) zunächst das zweite `=` gecheckt. Links davon steht `0 + 0`, was definitorisch identisch ist zu `0`. Wendet man das `rw zero_add` also hier an, wird der Term zu `n` umgewandelt. Für Nummer 2 sieht man das `0 + 0` an, stellt fest, dass es von der gewünschten Form ist und wandelt es in `0` um.

obtain

Zusammenfassung

Die `obtain`-Taktik kann man verwenden, um `have` und `cases` in einem Kommando zusammenzuführen.

Beispiele

Proof state	Kommando	Neuer proof state
$f : \mathbb{N} \rightarrow \mathbb{N} \rightarrow \text{Prop}$ $h : \forall (n : \mathbb{N}), \exists (m : \mathbb{N}), f\ n\ m$	<code>obtain (m, hm)</code> <code>:= h 27,</code>	$f : \mathbb{N} \rightarrow \mathbb{N} \rightarrow \text{Prop}$ $h : \forall (n : \mathbb{N}), \exists (m : \mathbb{N}),$ $\qquad\qquad\qquad f\ n\ m$ $m : \mathbb{N}$ $hm : f\ 27\ m$

push_neg

Zusammenfassung

In vielen Beweisschritten muss eine Negation durchgeführt werden. Um die entsprechenden Quantoren etc. ebenfalls zu verarbeiten und das Ergebnis besser weiterverwenden zu können, gibt es die Taktik `push_neg`.

Beispiele

Proof state	Kommando	Neuer proof state
$\vdash \neg(P \vee Q)$	<code>push_neg,</code>	$\vdash \neg P \wedge \neg Q$
$h : \neg(P \vee Q)$	<code>push_neg at h,</code>	$h : \neg P \wedge \neg Q$
$\vdash \neg(P \wedge Q)$	<code>push_neg,</code>	$\vdash P \rightarrow \neg Q$
$P : X \rightarrow \text{Prop}$ $\vdash \neg \forall (x : X), P x$	<code>push_neg,</code>	$P : X \rightarrow \text{Prop}$ $\vdash \exists (x : X), \neg P x$
$P : X \rightarrow \text{Prop}$ $\vdash \neg \exists (x : X), P x$	<code>push_neg,</code>	$P : X \rightarrow \text{Prop}$ $\vdash \forall (x : X), \neg P x$

Anmerkungen

Diese Taktik funktioniert auch bei anderen Objekten, etwa Mengen.

rcases

Proof state	Kommando	Neuer proof state
$h : P \wedge Q \vee P \wedge R$ $\vdash P$	<code>rcases h with</code> <code>((hP1,hQ) (hP2,hR))</code>	$hP1 : P$ $hQ : Q$ $\vdash P$ $hP2 : P$ $hR : R$ $\vdash P$

Zusammenfassung

`rcases` ist eine flexiblere Version von `cases`. Etwas genauer ist es hier erlaubt, mittels `(hP, hQ)` (bzw. `(hP | hQ)`) die durch \wedge (bzw. \vee) verknüpfte Hypothesen hP und hQ in ihre Fälle aufzuteilen. Wie man im obigen Beispiel sieht, ist dabei auch eine Schachtelung von `(.,.)` und `(.|.)` möglich.

Beispiele

Proof state	Kommando	Neuer proof state
$h : P \wedge Q$ $\vdash R$	<code>rcases h with</code> <code>(hP, hQ)</code>	$hP : P$ $hQ : Q$ $\vdash R$
$h : P \vee Q$ $\vdash R$	<code>rcases h with</code> <code>(hP hQ)</code>	$hP : P$ $\vdash R$ $hQ : Q$ $\vdash R$
$h : \exists (m : \mathbb{N}) (hg : 0 \leq m),$ $m < n$ $\vdash P$	<code>rcases h with</code> <code>(m, h1, h2),</code>	$n m : \mathbb{N}$ $h1 : 0 \leq m$ $h2 : m < n$ $\vdash 1 < n$

Anmerkungen

Im letzten Beispiel sieht man, wie man mit `rcases` einen \exists -Quantor in einer Hypothese, der mehr als eine Einschränkung hat (hier: $0 \leq m$) und $m < n$ direkt auflösen kann.

refine

Zusammenfassung

Die `refine`-Taktik ist wie `exact` mit Löchern. Etwas genauer: Wenn das Goal darin besteht, eine Kombination aus Hypothesen anzuwenden, so kann man das mittels `refine` machen und für jeden offene Term `_` schreiben. Dann erhält man jeden `_` als neues Ziel zurück (wobei solche mit definitorischer Gleichheit sofort gelöst werden).

Beispiele



Proof state	Kommando	Neuer proof state
$hQ : Q$ $\vdash P \wedge Q$	<code>refine { _, hQ }</code>	$hQ : Q$ $\vdash P$
$\vdash \exists (n : \mathbb{N}) (h : n > 0),$ $n^2 = 9$	<code>refine</code> <code>{3, _, by norm_num},</code>	$\vdash 3 > 0$

refl

Zusammenfassung

Diese Taktik beweist die Gleichheit (oder Äquivalenz) zweier definitorisch gleicher Terme.

Beispiele

Proof state	Kommando	Neuer proof state
$\vdash P \leftrightarrow P$ oder $\vdash P = P$	refl	goals accomplished 
$\vdash 1 + 2 = 3$	refl,	goals accomplished 

Anmerkungen

Das zweite Beispiel funktioniert deswegen, weil beide Seiten definitorisch gleich $\text{succ succ succ } 0$ sind.

revert

Zusammenfassung

revert ist das Gegenteil von intro: Es wird eine Hypothese des lokalen Kontextes genommen, und als Voraussetzung in das Goal eingefügt.

Beispiele

Proof state	Kommando	Neuer proof state
hP : P └─ Q	revert hP	└─ P → Q

Anmerkungen

revert wird selten benötigt; eigentlich nur dann, wenn man ein bereits bewiesenes Resultat exakt anwenden möchte und erst die richtige Form des Goals herstellen will.

right

Zusammenfassung

Siehe left , wobei die Anpassungen offensichtlich sind.

Beispiele



Proof state	Kommando	Neuer proof state
$\vdash P \vee Q$	right	$\vdash Q$

ring

Zusammenfassung

Durch `ring` werden Rechenregeln wie Assoziativität, Kommutativität, Distributivität angewandt, um das Goal zu erreichen.

Beispiele

Proof state	Kommando	Neuer proof state
$x\ y : \mathbb{R}$ $\vdash x + y = y + x$ ⁹	<code>ring</code>	goals accomplished 
$n : \mathbb{N}$ $\vdash (n+1)^2 = n^2 + 2*n + 1$	<code>ring,</code>	goals accomplished 

Anmerkungen

1. Das zweite Beispiel funktioniert, obwohl \mathbb{N} kein Ring (sondern nur ein Halbring) ist. Es würde auch mit $n : \mathbb{R}$ funktionieren (da in \mathbb{R} ja noch mehr Rechenregeln gelten als in \mathbb{N}).
2. `ring` wird nur verwendet, um das Goal zu schließen.

rintro

Zusammenfassung

Die `rintro`-Taktik wird dazu verwendet, mehrere `intro`- und `cases`-Taktiken in einer Zeile zu verarbeiten.

Beispiele

Proof state	Kommando	Neuer proof state
$\vdash P \vee Q \rightarrow R$	<code>rintro (hP hQ)</code> = <code>intro h ,</code> <code>cases h with hP hQ</code>	$hP : P$ $\vdash P$ $hQ : Q$ $\vdash Q$
$\vdash P \wedge Q \rightarrow R$	<code>rintro (hP , hQ)</code> = <code>intro h ,</code> <code>cases h with h1 h2</code>	$hP : P$ $hQ : Q$ $\vdash Q$

Anmerkungen

Hier können auch mehr als zwei \vee in einem Schritt in Fälle aufgeteilt werden:
Bei $A \vee B \vee C$ werden mit `rintro (A | B | C)` drei Goals eingeführt.

rw

Zusammenfassung

`rw` steht für *rewrite*. Für `rw h` muss `h` eine Aussage vom Typ `h : x=y` oder `h : A↔B` sein. In diesem Fall wird durch `rw h` jeder Term, der syntaktisch identisch zu `x` (bzw. `A`) ist durch `y` (bzw. `B`) ersetzt. Dies funktioniert auch, wenn `h` ein bereits bewiesenes Ergebnis (also ein **lemma** oder **theorem**) ist. Mit `rw ← h` wird `rw` von rechts nach links angewendet. (In obigem Beispiel wird also `y` durch `x` bzw. `B` durch `A` ersetzt.)

Beispiele

Proof state	Kommando	Neuer proof state
<code>h : P ↔ Q</code> <code>⊢ P</code>	<code>rw h</code>	<code>h : P ↔ Q</code> <code>⊢ Q</code>
<code>h : P ↔ Q</code> <code>⊢ Q</code>	<code>rw ← h</code>	<code>h : P ↔ Q</code> <code>⊢ P</code>
<code>h : P ↔ Q</code> <code>hP : P</code>	<code>rw h at hP</code>	<code>h : P ↔ Q</code> <code>hP : Q</code>
<code>h : P ↔ Q</code> <code>hQ : Q</code>	<code>rw ← h at hQ</code>	<code>h : P ↔ Q</code> <code>hQ : P</code>
<code>k m : ℕ</code> <code>⊢ k + m + 0 = m + k + 0</code>	<code>rw add_comm,</code>	<code>k m : ℕ</code> <code>⊢ 0 + (k + m)</code> <code>= m + k + 0</code>
<code>k m : ℕ</code> <code>⊢ k + m + 0 = m + k + 0</code>	<code>rw add_comm k m,</code>	<code>⊢ m + k + 0</code> <code>= m + k + 0</code>
<code>k m : ℕ</code> <code>⊢ k + m + 0 = m + k + 0</code>	<code>rw ← add_comm k m,</code>	<code>⊢ k + m + 0</code> <code>= k + m + 0</code>
<code>k m : ℕ</code> <code>⊢ k + m + 0 = m + k + 0</code>	<code>rw [add_zero,</code> <code>add_zero,]</code>	<code>k m : ℕ</code> <code>⊢ k + m = m + k</code>

Für die letzten vier Beispiele muss man erstmal wissen, dass `add_comm` und `add_zero` die Aussagen

```
add_comm : ∀ {G : Type} [_inst_1 : add_comm_semigroup G] (a b : G),  
          a + b = b + a  
add_zero : ∀ {M : Type} [_inst_1 : add_zero_class M] (a : M), a + 0 = a
```

sind. Im ersten der vier Beispiele wendet `rw` auf das erste Vorkommen eines Terms vom Typ `a + b` an. Durch die interne Klammerung steht auf der linken Seite `(k + m) + 0`, so dass das `rw` zu einem `0 + k + m` führt. Will man

stattdessen die Kommutativität im Term $k + m$ ausnutzen, so benötigt man das zweite (bzw. dritte) Beispiel, bei dem `rw add_comm k m` zum gewünschten Fortschritt führt. Im letzten Beispiel werden zunächst die beiden $+ 0$ -Terme durch `rw add_zero` beseitigt.

Anmerkungen

1. `rw` wird in der Praxis sehr oft verwendet, um Aussagen der `mathlib` anzuwenden (zumindest wenn Sie vom Typ `=` oder \leftrightarrow sind).
2. Will man mehrere `rw`-Kommandos kombinieren, so kann man das in eckigen Klammern machen, etwa `rw [h1, h2]` oder `rw [h1, \leftarrow h2, h3]`.
3. `rw` führt nach seiner Anwendung sofort ein `refl` durch. Das führt im zweiten und dritten Beispiel der Anwendungen von `add_comm` und `add_zero` dazu, dass der neue Proof state nicht wie angegeben ist, sondern **goals accomplished** 🎉
4. Will man nicht der Reihe nach ein `rw` durchführen (wie etwa bei der doppelten Beseitigung des $+0$ oben), so kann man mittels `nth_rewrite` gezielt das zweite Vorkommen eines Terms umschreiben.
5. Die `rw`-Taktik funktioniert nicht, wenn sie nach einem *Binder* steht, was etwa ein $\forall \exists \sum$ sein kann. In diesem Fall hilft hoffentlich `simp_rw` weiter.

simp

Zusammenfassung

In `mathlib` gibt es viele Lemmas mit `=` oder `↔`-Aussagen, die mit `rw` angewendet werden können und mit `@[simp]` gekennzeichnet sind. Diese gekennzeichneten Lemmas haben die Eigenschaft, dass auf der rechten Seite eine vereinfachte Form der linken Seite steht. Bei `simp` sucht `lean` nach passenden Lemmas und versucht sie anzuwenden.

Beispiele

Proof state	Kommando	Neuer proof state
$\vdash n + 0 = n$ ¹⁰	<code>simp</code>	goals accomplished 🏆
$h : n + 0 = m$ ⁵ $\vdash P$	<code>simp at h</code>	$h : n = m$ $\vdash P$

Anmerkungen

Will man wissen welche Lemmas genau angewendet wurden, so versucht man es mit `simp?` oder `squeeze_simp`. Dies liefert Hinweise.

Proof state	Kommando	Neuer proof state
$\vdash n + 0 = n$	<code>simp?</code> ,	goals accomplished 🏆 Try this: simp only [add_zero, eq_self_iff_true]
$\vdash n + 0 = n$	<code>squeeze_simp</code> ,	goals accomplished 🏆 Try this: simp only [add_zero]

specialize

Proof state	Kommando	Neuer proof state
$f : \mathbb{N} \rightarrow \text{Prop}$ $h : \forall (n : \mathbb{N}), f n$ $\vdash P$	specialize h 13	$f : \mathbb{N} \rightarrow \text{Prop}$ $h : f 13$ $\vdash P$

Zusammenfassung

Bei einer Hypothese $h : \forall n, \dots$ gilt \dots für alle n , aber für den Beweis des Goals benötigt man eventuell ja nur ein bestimmtes n . Gibt man `specialize h` gefolgt von dem Wert an, für den h benötigt wird, ändert sich die Hypothese entsprechend.

Beispiele

Proof state	Kommando	Neuer proof state
$h : \forall (n : \mathbb{N}), 0 < n + 1$ $\vdash 0 < 1$	specialize h 0,	$m : \mathbb{N}$ $h : 0 < 0 + 1$ $\vdash 0 < 1$

Anmerkungen

1. Genau wie bei `use` muss man aufpassen, dass das Goal beweisbar bleibt.
2. Will man zwei Werte der Hypothese h verwendet, so liefert `let h' := h` zunächst eine Verdopplung der Hypothese, so dass man anschließend `specialize` auf h und h' anwenden kann.

split

Zusammenfassung

Ist das Goal vom Typ $\vdash P \wedge Q$, so wird es durch `split` in zwei Goals $\vdash P$ und $\vdash Q$ ersetzt.

Beispiele

Proof state	Kommando	Neuer proof state
$\vdash P \wedge Q$	<code>split</code>	$\vdash P$ $\vdash Q$
$\vdash P \leftrightarrow Q$	<code>split</code>	$\vdash P \rightarrow Q$ $\vdash Q \rightarrow P$

Anmerkungen

Man beachte, dass $\vdash P \leftrightarrow Q$ identisch ist zu $\vdash (P \rightarrow Q) \wedge (Q \rightarrow P)$ ist.

tauto

Zusammenfassung

tauto löst alle Goals, die mit einer Wahrheitstabelle lösbar sind.

Beispiele

Proof state	Kommando	Neuer proof state
$\vdash P \wedge Q \rightarrow P$ ¹¹	tauto oder tauto!	goals accomplished 🎉
$\vdash ((P \rightarrow Q) \rightarrow P) \rightarrow P$	tauto!,	goals accomplished 🎉

Die Wahrheitstabellen für $\neg P$, $P \wedge Q$ bzw. $P \vee Q$ sehen wiefolgt aus; sind mehr Terme vom Typ **Prop** involviert, gibt es mehr Zeilen.

		P	Q	$(P \wedge Q)$	P	Q	$(P \vee Q)$
P	$\neg P$	true	true	true	true	true	true
true	false	false	true	false	false	true	true
false	true	true	false	false	true	false	true
		false	false	false	false	false	false

Anmerkungen

Der Unterschied zwischen tauto und tauto! ist, dass bei letzterer Taktik die Regel des ausgeschlossenen Dritten zugelassen ist. Das zweite Beispiel ist deshalb nur mit tauto!, aber nicht mit tauto lösbar.

triv

Zusammenfassung

triv löst ein Ziel, das definitorisch identisch zu true ist. Es löst ebenfalls Ziele, die mit refl lösbar sind.

Beispiele

Proof state	Kommando	Neuer proof state
$\vdash \text{true}$	triv	goals accomplished 🏆
$\vdash x=x$	triv,	goals accomplished 🏆

use

Proof state	Kommando	Neuer proof state
$f : \alpha \rightarrow \text{Prop}$ $y : \alpha$ $\vdash \exists (x : \alpha), f x$	use y	$f : \alpha \rightarrow \text{Prop}$ $y : \alpha$ $\vdash f y$

Zusammenfassung

Die `use`-Taktik kommt bei Goals zum Einsatz, die mit \exists beginnen. Hier wird durch Paramtere gesagt, welches durch \exists quantifizierte Objekt denn im Beweis weiter verwendet werden soll.

Beispiele

Proof state	Kommando	Neuer proof state
$\vdash \exists (k : \mathbb{N}), k * k = 16$	use 4,	$\vdash 4 * 4 = 16$
$\vdash \exists (k l : \mathbb{N}), k * l = 16$	use [8, 2],	$\vdash 8 * 2 = 16$

Anmerkungen

1. Man muss aufpassen, dass das Goal durch die Verwendung von `use` beweisbar (insbesondere wahr) bleibt. Im ersten Fall unter Beispiele hätten wir ja auch `use 3` schreiben können, und $3 * 3 = 16$ ist nicht beweisbar.
2. Man kann gleichzeitig mehr als eine Variable durch `use` angeben. Dies geschieht in eckigen Klammern; siehe das letzte Beispiel.