A Tutorial

Dalton Bentley

February 27, 2021

Contents

1 Square root of prime

We wrote an Isabelle tutorial[1] using a proof provided in the `HOL/ex/Sqrt.thy` file (developed by Markus Wenzel and Tobias Nipkow) of the Isabelle distribution. This proof demonstrates that the square root of a prime number cannot be a rational number.[2]

Our statement of the theory and proof is:

Theorem. *If p is prime, i.e., $p \in \mathbb{Z}_{>0}$ with $p > 1$ and having only factors 1 and itself, then $\sqrt{p} \notin \mathbb{Q}$, where $\mathbb{Q} = \{\frac{a}{b} | \, a \in \mathbb{Z} \text{ and } b \in \mathbb{Z} \text{ and } b \neq 0\}$ and there is a unique (reduced) representation such that $\gcd(a, b) = 1$, i.e., (a, b) are relatively prime.*

Proof. Assume on the contrary that $\sqrt{p} \in \mathbb{Q}$: Then $\exists m, n \in \mathbb{Z}$ with $n \neq 0$ such that $\sqrt{p} = m/n$ with $\gcd(m, n) = 1$, i.e., (m, n) are relatively prime. In that case, $m = |\sqrt{p}|n$. It follows that $m^2 = (\sqrt{p})^2 n^2$ and $m^2 = pn^2$. In that case we may say that $p|m^2$ and also that $p|m$, since a prime divisor of a product of integers must divide one of the integer factors, which are identical in the case of a square. That being so, there must be an integer k such that $m = pk$. Since we established that $m^2 = pn^2$ and we can square $m = pk$ to obtain $m^2 = p^2k^2$, we have $pn^2 = p^2k^2$. We can divide that last result by p to obtain $n^2 = pk^2$. That tells us that $p|n^2$ and therefore $p|n$ (as above, prime divisor of product of integers divides at least one of the factors). We

[1] https://github.com/AncientZygote/izzie/blob/main/IsabelleTutorial.pdf

[2] The authors present several such proofs in that theory document. We selected the proof that they described as using mostly linear forward-reasoning, that appearing more like a mathematical proof rather than a prover tactic script.

have therefore shown that p prime divides both m and n and therefore must divide the greatest common divisor of m, n, i.e., $p|\gcd(m,n)$. However, we stipulated that m, n are relatively prime, i.e., that $\gcd(m,n) = 1$. In that case, $p = 1$, a contradiction since we stated p is prime and must therefore be greater than 1, i.e., $p > 1$ by definition of primality. Our assumption that $\sqrt{p} \in \mathbb{Q}$ is therefore false and therefore $\sqrt{p} \notin \mathbb{Q}$. $\square$

2 Isabelle/Isar proof

The following is the actual Isabelle/Isar proof which we worked through step-by-step in our tutorial cited above. It must be emphasized that the words you are reading here are text inserted into the actual `SqrtTutor1.thy` theory file that executes as a formal proof in Isabelle/jEdit.

theorem
  assumes ‹*prime* (*p*::*nat*)›
  shows ‹*sqrt p* ∉ ℚ›
proof
  from ‹*prime p*› **have** *p*: ‹*1* < *p*› **by** (*rule prime-gt-1-nat*)

  assume ‹*sqrt p* ∈ ℚ›
  then obtain *m n* :: *nat* **where**
    n: ‹*n* ≠ *0* › **and** *sqrt-rat*: ‹|*sqrt p*| = *m*/*n*›
    and ‹*coprime m n*› **by** (*rule Rats-abs-nat-div-natE*)

  from *n* **and** *sqrt-rat* **have** ‹*m* = | *sqrt p* | ∗ *n* › **by** *simp*

  then have *m^2* = (*sqrt p*) ^*2* ∗ *n^2*
    by (*simp add*: *power-mult-distrib*)
  also have ‹(*sqrt p*) ^*2* = *p*› **by** *simp*

  also have ‹... ∗ *n^2* = *p* ∗ *n^2*› **by** *simp*

  finally have *eq*: ‹*m^2* = *p* ∗ *n^2*›
    using *of-nat-eq-iff* **by** *blast*

  then have ‹*p dvd m^2*› **..**

  with ‹*prime p*› **have** *dvd-m*: ‹*p dvd m*›
    using *prime-dvd-power-nat* **by** *blast*

  then obtain *k* **where** ‹*m* = *p* ∗ *k*› **..**

  with *eq* **have** ‹*p* ∗ *n^2* = *p^2* ∗ *k^2*›
  proof −
    show *?thesis*
    by (*metis* (*full-types*) ‹*m* = *p* ∗ *k*› ‹$m^2 = p * n^2$› *mult.commute mult.left-commute power2-eq-square*)

qed

with *p* **have** ‹*n^2 = p * k^2*›
proof −
have ¬ (*1*::*nat*) < *0*
by *blast*
then show *?thesis*
by (*metis* (*no-types*) ‹*1 < p*› ‹*p * n^2 = p^2 * k^2*› *mult.assoc nonzero-mult-div-cancel-left power2-eq-square*)
qed
then have ‹*p dvd n^2*› **..**
with ‹*prime p*› **have** ‹*p dvd n*› **by** (*rule prime-dvd-power-nat*)
with *dvd-m* **have** ‹*p dvd gcd m n*› **by** (*rule gcd-greatest*)
with ‹*coprime m n*› **have** ‹*p = 1*› **by** *simp*
with *p* **show** *False*
by *simp*
qed

3 How to print this theory document

Relevant Isabelle system documentation includes Chapter 2 and Chapter 3 of [2], and §4.2 in [1][3]. Let us assume you have a copy of this theory file `SqrtTutor1.thy`[4]) (or a theory file of your own making that you are interested in printing within Isabelle).

- Go to your home directory area, e.g., `/home/dalton/IsabelleStuff`.
- Open a terminal (we are going to use Linux-oriented language) session there.
- Execute the following command string in the terminal (is a single line): `isabelle mkroot -n TestSess -T "A Tutorial" -A "Dalton Bentley" Test`
- If you do not want a session name (e.g., `TestSess`) different from the directory name to be created (here the directory to be created is `Test`, the last token on the command string), do not want to specify the title of the pdf document (`"A Tutorial"` here), do not want to specify the author in the pdf (`"Dalton Bentley"` here) use instead the following command string in the terminal: `isabelle mkroot Test`

Your terminal output should indicate the result of the `mkroot` command (we used the first, longer line with options[5]):

[3]The cited document, *Isabelle/HOL: A Proof Assistant for Higher-Order Logic*, also accompanies the Isabelle distribution as `tutorial.pdf`.

[4]Downloaded at https://github.com/AncientZygote/izzie/

[5]See §3.2 in [2] for those options.

```
Preparing session "TestSess" in "Test"
creating "Test/ROOT"
creating "Test/document/root.tex"
```

We obtain a new directory (which will be the *session root*) named `Test` as we specified with the final token of the invocation line above. Place a copy of the `SqrtTutor1.thy` file[6] in the new `Test` directory. We see `mkroot` creates a `ROOT` file in that directory (the *session root* directory), along with a subfolder named `document` with a contained LaTeX file `root.tex`.

The `ROOT` file (a text file) has our optional session name `TestSess` differing from the root directory name itself `Test` in the default text inserted:

```
session TestSess = HOL +
  options [document = pdf, document_output = "output"]
(*theories [document = false]
    A
    B
  theories
    C
    D*)
  document_files
    "root.tex"
```

Edit the `ROOT` file, keeping the first two lines identifying the session and options, and insert our theory `SqrtTutor1` below a `theories` heading. Remove the `.thy` suffix or you will get complaints. Be sure to observe the indentations indicated, i.e., maintain the same block structure. We note that it is possible to edit `ROOT` files in Isabelle/jEdit[3] and thereby obtain syntax indentation and painting, however, we find it more convenient to simply use a text editor in the current context since we are using Isabelle batch mode facilities for theory document preparation.

We leave the `document_files` entry alone for now, knowing the Isabelle document commands default to looking in the `document` subdirectory of the root directory created by `mkroot` (if we used documents in other directories we could provide the path under a `document_files` heading in `ROOT`).[7] We

[6] Obtain at our GitHub area: https://github.com/AncientZygote/izzie/

[7] We note that the Isabelle distribution contains many `ROOT` files which provide examples of possible configurations, all considerably more sophisticated than our usage here. See `$ISABELLE_HOME/src/HOL/ROOT` and `$ISABELLE_HOME/src/Doc/ROOT`. `$ISABELLE_HOME` is the location of the top-level Isabelle distribution directory. You can see its value with terminal command `isabelle getenv ISABELLE_HOME`, typically it is `/usr/local/Isabelle2020`.

obtain in our ROOT then:

```
session TestSess = HOL +
  options [document = pdf, document_output = "output"]
  theories
    SqrtTutor1
  document_files
    "root.tex"
```

If we run `isabelle build -D Test` now (from our terminal open above the `Test` directory level), that will fail with error:

```
*** Cannot load theory "HOL-Computational_Algebra.Primes"
*** The error(s) above occurred in session "TestSess" (line 1 of
"/home/dalton/IsabelleStuff/Test/ROOT")
```

Why? We have hidden some of the theory file text to make this printed document cleaner. If you open this file `SqrtTutor1.thy` in your text editor (or jEdit), you will see that in the first few lines the theory imports a theory from a session not in the current namespace:

`imports Complex_Main "HOL-Computational_Algebra.Primes"`

Notice the format `HOL-`, signifying found within the `HOL` object logic folder. `Computational_Algebra` is a session folder within the `HOL` directory (but not part of the default `HOL` heap load). The period "." attaches the theory `Primes.thy` to its containing session `Computational_Algebra` (we do not include the `.thy` suffix when naming theory files in `imports` or `ROOT` lists). We must edit our `ROOT` file to inform Isabelle to include this session:[8]

```
session TestSess = HOL +
  options [document = pdf, document_output = "output"]
  sessions
    "HOL-Computational_Algebra"
  theories
     SqrtTutor1
  document_files
    "root.tex"
    "root.bib"
```

[8] Why are some of the entities enclosed in quotation marks? We do not have a specific answer, other than that, heuristically, the `build` may fail otherwise.

You see we inserted a `sessions` heading, indented to the same level as other major keywords below the initial new `session` declaration (we define a new session `TestSess` with parent session `HOL`).[9]

You also should notice that we inserted a bibliography file reference (it must be named `root.bib` if we want to obtain Isabelle default bibliography processing without having to write a `build` script) under the `document_files` heading. This seems a good time to take care of that requirement also and to discuss the required modifications to the default `root.tex` file. If you examine our theory file `SqrtTutor1.thy` in your text editor, you will see the form of the reference cites, e.g., `@{`*cite* `"isabelle-system"}`.

Download the `root.bib` file from our GitHub Isabelle-related area[10] if you have not done so. It is a text file that can be edited in a text editor or in a TEX editor like TEXworks. We will not digress to discuss BibTEX, but point you at the `$ISABELLE_HOME/src/Doc/manual.bib` file, which contains a BibTEXdatabase for the Isabelle documentation with on the order of 300 bibliography entries of all types (and the shell scripts in that directory illustrate how to specify bibliography and other document preparation tasks rather than use the default behavior).

The default `root.tex` file (recall that `mkroot` created it in the `document` subdirectory earlier) requires two modifications for our specific case here. We use the AMS (*American Mathematical Society*) LATEX packages `amssymb` and `amsmath` (probably most of our usage could be replaced with equivalent Isabelle symbols, but we already know AMS). So insert the the following lines after the `\usepackage{isabelle,isabellesym}` line in `root.tex`:

```
\usepackage{amssymb}
\usepackage{amsmath}
\usepackage{xspace}
```

Finally, uncomment the optional bibliography lines at the end of the `root.tex` file:

```
% optional bibliography
\bibliographystyle{abbrv}
\bibliography{root}
```

You could also modify `\title`, `\author` and other LATEX fields if desired. Recall that `mkroot` populated those fields earlier.

[9] See §2.1 of [2].

[10] https://github.com/AncientZygote/izzie/

The `Test/document` directory should now contain:

```
root.bib  root.tex
```

We are ready to run `isabelle build -D Test` now (from our terminal open above the `Test` directory level) and create a pdf document from our theory file:

```
dalton@dalton-Precision-3541:$ isabelle build -D Test
Running TestSess ...
Document at /home/dalton/IsabelleStuff/Test/output/document.pdf
Finished TestSess (0:00:22 elapsed time, 0:00:43 cpu time, factor
1.91)
0:00:27 elapsed time, 0:00:43 cpu time, factor 1.55
```

The `Test` directory should now contain:

```
document  output  ROOT  SqrtTutor1.thy
```

The `output` directory should now contain:

```
document  document.pdf
```

`document.pdf` should be a seven page pdf document with title, author, hyperlinked table of contents, three chapters and References (did not bother to include that in the TOC). The `document` subfolder (`Test/output/document`) should contain:

```
Cancellation.tex         isabelletags.sty  root.bbl  root.tex
comment.sty              Multiset.tex      root.bib  root.toc
Euclidean_Algorithm.tex  pdfsetup.sty      root.blg  session_graph.pdf
Factorial_Ring.tex       Primes.tex        root.log  session.tex
isabelle.sty             railsetup.sty     root.out  SqrtTutor1.tex
isabellesym.sty          root.aux          root.pdf
```

That concludes this brief tutorial on LaTeX printing an Isabelle theory file.

References

[1] T. Nipkow, L. C. Paulson, and M. Wenzel. *Isabelle/HOL: A Proof Assistant for Higher-Order Logic*, volume 2283. 2002.

[2] M. Wenzel. *The Isabelle System Manual*. https://isabelle.in.tum.de/doc/system.pdf.

[3] M. Wenzel. *Isabelle/jEdit*. https://isabelle.in.tum.de/doc/jedit.pdf.