Environment for structured mathematical proofs

Mathematical proofs are hard to write. Either one writes too many details, and no-one will want to read the proof. Or one writes too little, and details in the proof will be wrong. And if a bug is found, how does one correct it? Republishes the whole proof? Can bugs in proofs be fixed by others (as a kind of pull request for mathematical proof steps)? Can we track dependencies between proofs? Etc. Etc.

To support better mathematical proof writing, I would like to have an environment (consisting of a suitable data format, a storage backend, as well as tools for editing, managing, analysing) for writing (human-readable) mathematical proofs. In its simplest form, a proof would be a hierarchical document with rough proof steps at the top level, and more and more refined proofs steps below that.

The software project would be to design (the basics of?) such an environment.

Features (ideally):

- A data format for hierarchical proofs (based on XML, YAML, set of files, …?)
- A backend for storing them (a git repository might already do the trick, possibly)
- Support for editing proofs (in LaTeX, preferably)
- Support for viewing proofs (in the web browser)
- Support for exporting proofs (as noninteractive document, e.g., PDF)
- Infrastructure for feedback / corrections / linking to other proofs etc.
- Analysis (e.g., dependency analysis, what breaks if a proof step is wrong, …)
- Refactoring (changing the syntax of a symbol, for example)
- Theorem prover support (for the most detailed level of proof steps)

Of course, this is a list of features for a long-term project. They are to give an idea what such an environment would ideally support. Within the scope of the software project, we would have to narrow down the set of features feasible in 600 hours.

If the tool works nicely, I might use it for teaching in the future. Licensing must be open source. Extending the topic into a thesis could be possible if it looks promising.
Contact ("client"): Dominique Unruh, Chair of Security & Theoretical Computer Science, dominique.unruh@ut.ee