Exercises

Chapter 8

Sean Li [1]

1. Redacted

Problem

(8.1) Let

$$\begin{aligned}\Gamma \equiv\ & \mathbb{Z} : *_s, \mathbb{N}^+ : *_s \\ & \triangleright\ p\ (m, n, u) \coloneqq \texttt{sorry} : \exists x, y : \mathbb{Z}.(m\ x + n\ y = 1) \\ & \triangleright\ \text{coprime}(m, n) \coloneqq \texttt{sorry} : *_p \\ & \triangleright\ q\ (m, n) \coloneqq \texttt{sorry} : \text{coprime}(m, n) \to \text{coprime}(n, m) \\ & \equiv n : \mathbb{N}^+, m : \mathbb{N}^+, u : \text{coprime}(m, n)\end{aligned}$$

Prove $\exists x, y : \mathbb{Z}.(n\ x + m\ y = 1)$ in Γ.

Solution.

Proof.

1. $q\ (m, n) : \text{coprime}(m, n) \to \text{coprime}(n, m)$
2. $q\ (m, n)\ u : \text{coprime}(n, m)$
3. $p\ (n, m, (q\ (m, n)\ u)) : \exists x, y : \mathbb{Z}.(n\ x + m\ y = 1)$

■

Problem

(8.2) Consider the following formal proof in analysis.

Proof.

1. $V : *_s$
2. $\quad u : V \subseteq \mathbb{R}$
3. $\quad\quad \text{bounded-from-above}(V, u) \coloneqq \exists y : R\,.\forall x : \mathbb{R}, (x \in V \Rightarrow x \leq y) : *_p$
4. $\quad\quad s : \mathbb{R}$
5. $\quad\quad\quad \text{upper-bound}(V, u, s) \coloneqq \forall x \in \mathbb{R}.(x \in V \Rightarrow x \leq s) : *_p$
   $\quad\quad\quad \text{least-upper-bound}(V, u, s) \coloneqq \text{upper-bound}(V, u, s) \wedge$
6. $\quad\quad\quad\quad \forall x : \mathbb{R}.(x < s \Rightarrow \neg\ \text{upper-bound}(V, u, x)) : *_p$
7. $\quad\quad v : V \neq \emptyset$
8. $\quad\quad\quad w : \text{bounded-from-above}(V, u)$
9. $\quad\quad\quad\quad p_4\ (V, u, w\ v) \coloneqq \texttt{sorry} : \exists^1\ s : \mathbb{R}.\ \text{least-upper-bound}(V, u, s)$
10. $S \coloneqq \left\{x : \mathbb{R} \mid \exists n : \mathbb{R}.\left(n \in \mathbb{N} \wedge x = \frac{n}{n+1}\right)\right\}$
11. $p_6 \coloneqq \texttt{sorry} : S \subseteq \mathbb{R}$
12. $p_7 \coloneqq \texttt{sorry} : \text{bounded-from-above}(S, p_6)$
13. $p_8 \coloneqq \texttt{sorry} : \text{least-upper-bound}(S, p_7, 1)$

■

Translate the proof into a more usual format. Note $\exists^1$ denotes unique existence, that is,

$$\exists^1\ n : \alpha.\ P\ (n) \coloneqq \exists n : \alpha.(P\ (n) \wedge \neg(\exists k : \alpha.(P\ (k) \wedge k \neq n)))$$

Which lines are formalized definitions? Which of them are formalized mathematical statements?

Which constants have been introduced before the text and which are introduced within?

Underline all instantiations of parameter lists and explain accurately what has been instantiated for what, and why that is correct.

Solution. What we want to prove is that 1 is the least upper bound of the set $\left\{x : \mathbb{R} \mid \exists n \in \mathbb{R}, \left(n \in \mathbb{N} \wedge x = \frac{n}{n+1}\right)\right\}$. (For shorter notation we use $S \equiv \left\{\frac{n}{n+1} : n \in \mathbb{N}\right\}$)

Proof. We first give formal definitions of a set being "bounded above".

Definition A set [1] $V \subseteq \mathbb{R}$ [2] being **bounded from above** [3] means that there exists $y \in \mathbb{R}$ such that for all $x \in \mathbb{R}$, x being an element of V implies that $x \leq y$.

For $s \in \mathbb{R}$ [4] to **be the upper bound of V** [5], it means that any real x being an element of V implies that $x \leq s$.

For $s \in \mathbb{R}$ to be the **least upper bound of V** [6], it means that s is a upper bound of V and any real number $x \in \mathbb{R}$ such that $x < s$ is not a upper bound of V.

Corollary 1. Any non-empty set $V \subseteq \mathbb{R}$ bounded from above has one and only one least upper bound.

Consider the set $S := \left\{ \frac{n}{n+1} : n \in \mathbb{N} \right\}$ [10]. Because division is closed under $\mathbb{R}$ when $n + 1 \neq 0$, $S \subseteq \mathbb{R}$ [11]. By *...proof omitted...*, S is bounded from above [12], and by *...proof omitted...* and the fact that S is bounded from above, 1 is the least upper bound for S [13]. ■

Lines (3), (5), (6), and (10) are definitions; those introduce new notions and constants, and (9), (11), (12), and (13) all statements; those construct the proof for the goal and serve as intermediate steps in the main proof.

The sets V and S, proof $u : V \subseteq \mathbb{R}$, the element $s \in \mathbb{R}$ are all defined in the proof. The sets $\mathbb{R}$ and $\mathbb{N}$, the proposition constructor $\subseteq$, the set constructor notation, real operations, and the set $\emptyset$ are all defined out of the proof.

We use blue for constants defined within the proof, and red for proofs outside.

1. $V : *_s$
2. $\quad u : V \subseteq \mathbb{R}$
3. $\quad\quad \text{bounded-from-above}(V, u) := \exists y : R\,.\forall x : \mathbb{R}, (x \in V \Rightarrow x \leq y) : *_p$
4. $\quad\quad s : \mathbb{R}$
5. $\quad\quad\quad \text{upper-bound}(V, u, s) := \forall x \in \mathbb{R}.(x \in V \Rightarrow x \leq s) : *_p$
6. $\quad\quad\quad \text{least-upper-bound}(V, u, s) := \text{upper-bound}\underline{(V, u, s)^1} \wedge \forall x : \mathbb{R}.\left(x < s \Rightarrow \neg\ \text{upper-bound}\ \underline{(V, u, x)^2}\right) : *_p$
7. $\quad\quad v : V \neq \emptyset$
8. $\quad\quad\quad w : \text{bounded-from-above}\underline{(V, u)^3}$
9. $\quad\quad\quad p_4\ (V, u, w\ v) := \texttt{sorry} : \exists^1\ s : \mathbb{R}.\ \text{least-upper-bound}\underline{(V, u, s)^4}$
10. $S := \{x : \mathbb{R} \mid \exists n : \mathbb{R}.(n \in \mathbb{N} \wedge x = n\,/(n+1))\}$
11. $p_6 := \texttt{sorry} : S \subseteq \mathbb{R}$

12. p_7 := `sorry` : bounded-from-above$\underline{(S, p_6)}^5$
13. p_8 := `sorry` : least-upper-bound$\underline{(S, p_7, 1)}^6$

In instantiation 1 on line 5, (V, u, s) states the proposition that s is an upper bound of V in order to proof that s is the least upper bound of V.

In instantiation 2 on line 6, (V, u, x) states that the proposition of x being an upper bound of V, which eventual leads to contradiction. This proves that no such x exists.

In instantiation 3 on line 8, (V, u) construct a proposition of V being bounded from above.

In instantiation 4 on line 9, (V, u, s) constructed a proposition of s being the least upper bound, which was introduced as the one and only one such element of $\mathbb{R}$ that satisfies this.

In instantiation 5 on line 12, (S, p_6) constructed a proposition that S was bounded from above, and is proven by p_7.

In instantiation 6 on line 13, $(S, p_7, 1)$ constructed a proposition that S has 1 as the least upper bound, and is proven by p_8.

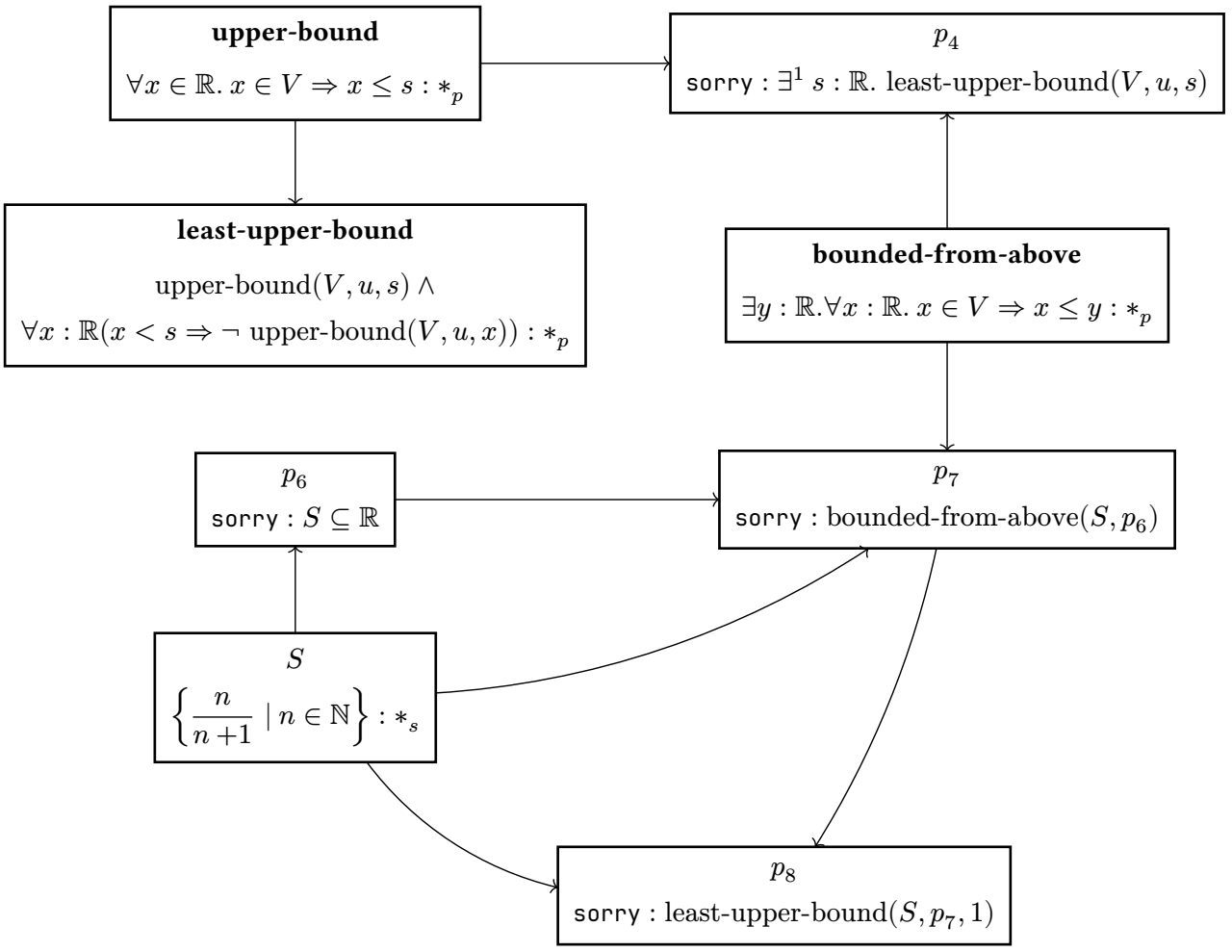
All of this is is correct because the types match: by the PAT paradigm it means that each evidence provided suffices to construct each next step of the proof.

Problem

(8.3) Consider the formal proof in 8.2. State the partial order representing the dependencies between the definitions given in this text.

Solution. Denote the set of definitions as S and dependency as $\leq$.

The Hasse Diagram of $(S, \leq)$ is



Problem

(8.4) Consider the following formal text in algebra.

1. $S : *_s$
2. $\quad \mathtt{op} : S \to S \to S$
3. $\quad\quad \text{semigroup}(S, \mathtt{op}) := \forall x, y, z : S \,.(\mathtt{op}\ x\ (\mathtt{op}\ y\ z) = \mathtt{op}\ (\mathtt{op}\ x\ y)\ z) : *_p$
4. $\quad\quad u : \text{semigroup}(S, \mathtt{op})$
5. $\quad\quad\quad e : S$
6. $\quad\quad\quad\quad \underline{\text{unit}(S, \mathtt{op}, u, e) := \forall x : S \,.(\mathtt{op}\ x\ e = x \wedge \mathtt{op}\ e\ x = x) : *_p}$
7. $\quad\quad\quad \text{monoid}(S, \mathtt{op}, u) := \exists e : S \,.\ \text{unit}(S, \mathtt{op}, u, e) : *_p$
8. $\quad\quad\quad e_1, e_2 : S$
9. $\quad\quad\quad\quad \underline{p_4\ (S, \mathtt{op}, u, e_1, e_2) := \mathtt{sorry} : (\text{unit}(S, \mathtt{op}, u, e_1) \wedge \text{unit}(S, \mathtt{op}, u, e_2)) \Rightarrow e_1 = e_2}$

Translate this into a more usual format.

Underline all variables that are bound to a binding variable introduced in the text.

Rewrite definition of semigroup and unit using $\Gamma \rhd a\ (\ldots) := M : N$ format.

Solution.

Definition Let S be a set [1] and $\times$ a binary operation closed over S [2].

The tuple $\langle S, \times \rangle$ forms a **semigroup** [3] if $\times$ is associative over S. That is, for any arbitrary elements $x, y, z \in S$

$$x \times (y \times z) = (x \times y) \times z$$

Let u [4] be the semigroup $\langle S, \times \rangle$. The element $e \in S$ [5] is called the **unit** [6] of u if for any element $x \in S$, we have

$$x \times e = x \text{ and } e \times x = x$$

A semigroup is called a **monoid** [7] if it has an unit.

Let $e_1, e_2 \in S$ [8]. If both of them are units of u, then $e_1 = e_2$, proof by `sorry` [9].

---

1. $S : *_s$
2. $\quad \mathtt{op} : \underline{S} \to \underline{S} \to \underline{S}$
3. $\quad\quad \text{semigroup}(\underline{S}, \underline{\mathtt{op}}) := \forall x, y, z : \underline{S} \,.(\underline{\mathtt{op}}\ x\ (\underline{\mathtt{op}}\ y\ z) = \underline{\mathtt{op}}(\underline{\mathtt{op}}\ x\ y)\ z) : *_p$
4. $\quad\quad u : \underline{\text{semigroup}}(\underline{S}, \underline{\mathtt{op}})$

5. $e : \underline{S}$
6. $\quad \underline{\text{unit}}\left(\underline{S}, \underline{\texttt{op}}, \underline{u}, \underline{e}\right) := \forall x : \underline{S}\ .\left(\underline{\texttt{op}}\ x\ \underline{e} = x \wedge \underline{\texttt{op}}\ e\ x = x\right) : *_p$
7. $\text{monoid}\left(\underline{S}, \underline{\texttt{op}}, \underline{u}\right) := \exists \underline{e} : \underline{S}\ .\underline{\text{unit}}\left(\underline{S}, \underline{\texttt{op}}, \underline{u}, \underline{e}\right) : *_p$
8. $e_1, e_2 : \underline{S}$
9. $\quad p_4\ \left(\underline{S}, \underline{\texttt{op}}, \underline{u}, \underline{e_1}, \underline{e_2}\right) :=$
   $\quad\quad \texttt{sorry} : \left(\underline{\text{unit}}\left(\underline{S}, \underline{\texttt{op}}, \underline{u}, \underline{e_1}\right) \wedge \underline{\text{unit}}\left(S, \underline{\texttt{op}}, \underline{u}, \underline{e_2}\right)\right) \Rightarrow \underline{e_1} = \underline{e_2}$

The definitions could be rewritten as follows:

$$S : *_s, \texttt{op} : S \to S \to S \triangleright$$
$$\quad \text{semigroup}(S, \texttt{op}) := \forall x, y, z : S\ .(\texttt{op}\ x\ (\texttt{op}\ y\ z)) = \texttt{op}\ (\texttt{op}\ x\ y)\ z$$
$$S : *_s, \texttt{op} : S \to S \to S, u : \text{semigroup}(S, \texttt{op}), e : S \triangleright$$
$$\quad \text{unit}(S, \texttt{op}, u, e) := \forall x : S\ .(\texttt{op}\ x\ e = x \wedge \texttt{op}\ e\ x = x)$$

Problem

(8.5) Identify the definitions in the following text and rewrite the text in a formal format.

Definition The real number r is **rational** if there exist integer numbers p and nonzero q such that $r = \frac{p}{q}$.

A real number that is not rational is called **irrational**. The set of all rational numbers is called $\mathbb{Q}$.

Every natural number is rational. The number 0.75 is rational, but $\sqrt{2}$ is irrational.

Solution.

1. $r : \mathbb{R}$
2. $\quad \text{rational}(r) := \exists p, q : \mathbb{Z}.\left(q \neq 0 \wedge r = \dfrac{p}{q}\right) : *_p$
3. $\quad \text{irrational}(r) := \neg\ \text{rational}(r) : *_p$
4. $\mathbb{Q} := \{x : \mathbb{R} \mid \text{rational}(x)\}$
5. $\text{all-nat-rational} := \texttt{sorry} : \forall n : \mathbb{N}.\ \text{rational}(n)$
6. $\text{p75-rational} := \texttt{sorry} : \text{rational}(0.75)$
7. $\text{sqrt2-irrational} := \texttt{sorry} : \text{irrational}\left(\sqrt{2}\right)$

Problem

(8.6) Consider the following mathematical text from number theory:

Definition If k, l, and m are integers, m being positive, then one says that k is **congruent** to l modulo m if m divides $k - l$.

We write $k \equiv l \pmod{m}$ to indicate that k is congruent to l modulo m.

Hence $-3 \equiv 17 (\mathrm{mod}\, 5)$, but not $-3 \equiv -17 (\mathrm{mod}\, 5)$.

If $k \equiv l \pmod{m}$, then also $l \equiv k \pmod{m}$.

$k \equiv l \pmod{m}$ iff there is an integer u s.t. $k = l + m\, u$.

Formalize the definitions, indicate the scope of all variables and constants introduced in the text.

Identify all instantiations in the formal text and check that the type conditions are respected.

Solution. Different variables have been colored the same, with the binders underlined. All instantiations have been underlined.

1. $\underline{k}, \underline{l}, \underline{m} : \mathbb{Z}$
2. $\quad \underline{h} : m > 0$
3. $\quad\quad$ congr-mod$(k, l, m, h) := m \mid k - l : *_p$
4. $\underline{u} :=$ `sorry` $: 5 > 0$
5. $p_1 :=$ `sorry` $:$ congr-mod$(\underbrace{-3, 17, 5, u}_{})$
6. $p_2 :=$ `sorry` $: \neg$ congr-mod$(\underbrace{-3, -17, 5, u}_{})$
7. $\underline{k}, \underline{l}, \underline{m} : \mathbb{Z}$
8. $\quad \underline{h} : m > 0$
9. $\quad\quad \underline{\text{congr-sym}}(k, l, m, h) :=$ congr-mod$(\underbrace{k, l, m, h}_{}) \Rightarrow$ congr-mod$(\underbrace{l, k, m, h}_{}) : *_p$
10. $\quad\quad \underline{\text{congr-exist}}(k, l, m, h) :=$ congr-mod$(\underbrace{k, l, m, h}_{}) \Leftrightarrow \exists u : \mathbb{Z}.(k = l + m\, u) : *_p$
11. $\quad\quad h_{\text{trans}} :=$ `sorry` $:$ congr-sym$(\underbrace{k, l, m, h}_{})$
12. $\quad\quad h_{\text{exists}} :=$ `sorry` $:$ congr-exist$(\underbrace{k, l, m, h}_{})$

—

Completed Jan 13 2:04 am.