Coq 证明助手小课堂

刘涵之 (MisakaCenter)

2021 年 3 月 14 日

1 群论、皮亚诺算术

1.1 群论

1.1.1 群的定义

`Variable` A: `Type`.

`Variable` e: A.

`Variable` mul: $A \to A \to A$.

`Variable` inv: $A \to A$.

`Notation` "x + y" := $(mul\ x\ y)$.

`Notation` "- x" := $(inv\ x\ )$.

`Notation` "0" := e.

`Hypothesis` $assoc$: $\forall\ (x\ y\ z{:}\ A),\ (x + y) + z = x + (y + z)$.

`Hypothesis` $left\_unit$: $\forall\ (x{:}\ A),\ 0 + x = x$.

`Hypothesis` $left\_inv$: $\forall\ (x{:}\ A),\ (\text{-}\ x) + x = 0$.

1.1.2 群的性质拓展

`Theorem` $right\_inv$: $\forall\ (x{:}\ A),\ x + (\text{-}\ x) = 0$.

`Theorem` $right\_unit$: $\forall\ (x{:}\ A),\ x + 0 = x$.

1.1.3 两个小练习

`Theorem` *double_inv*: $\forall$ (x: A), - - $x = x$.

`Theorem` *funny*: $\forall$ x y z, (x + y) + (-y + z) = x + z.

1.2 皮亚诺算术

1.2.1 自然数定义

```
Inductive nat :=
| O
| S (n: nat)
.
```

```
Fixpoint plus (n m: nat): nat :=
match n with
| O ⇒ m
| S x ⇒ S (plus x m)
end.
```

`Notation` "x + y" := (*plus* x y).

1.2.2 加法的性质

`Theorem` *plus_right_unit*: $\forall$ x: *nat*, x + O = x.

`Lemma` *plus_1*: $\forall$ x:*nat*, S x = x + S O.

`Theorem` *plus_comm*: $\forall$ (x y: *nat*), x + y = y + x.

1.2.3 两个小练习

`Theorem` *plus_S*: $\forall$ x y: *nat* , x + S y = S (x + y).

`Theorem` *plus_assoc*: $\forall$ (x y z: *nat*), (x + y) + z = x + (y + z).

2 可供参考的资料

[1] Coq 证明助手，https://coq.inria.fr/

[2] Software Foundations，https://softwarefoundations.cis.upenn.edu/

[3] 软件基础（中译版），https://coq-zh.github.io/SF-zh/

[4] 本次课程资料：https://github.com/MisakaCenter/Notes/blob/main/algebra