A minor variation on "On a proof of Kaplansky's Theorem"

Theorem: In a ring with identity, an element without a left inverse but with at least one right inverse has infinitely many right inverses.

□

We assume b to be a ring element without left inverses and of which we assume a to be a right inverse; that is, we have —with multiplication denoted by juxtaposition and with x ranging over the ring— :

(1) $(\forall x :: xb \neq 1)$, and

(2) $ba = 1$.

The theorem states that the set of b's right inverses is infinite. Proving that a set is infinite amounts to proving that the set contains an infinite sequence all whose elements are different. Calling the sequence $s_i\ (0 \leq i)$ we can —naively— define the sequence by choosing s_0 and by inventing a function f such that

$$s_{i+1} = f \cdot s_i \ , \text{ for } i : 0 \leq i \ .$$

The elements of s must be right inverses of b ; since the only right inverse we know about is a we have no choice and we must take

$$s_0 = a \ , \quad \text{and}$$

we must see to it that f satisfies

(3) $(\forall x :: \ bx = 1 \ \Rightarrow \ b\,(f \cdot x) = 1)$.

That all elements of s are different can be proved by simple mathematical induction (over s's range), provided that f satisfies:

(4) $(\forall x :: \ f \cdot x \neq a)$, and

(5) $(\forall x, y :: \ x \neq y \ \Rightarrow \ f \cdot x \neq f \cdot y)$.

Formulae (2), (3), and (4) form the functional specification of function f . Of these three, (4) is the least specific: it only states that f is injective. The other two connect f with properties of the ring. Requirement (3) is the simplest one; it shows that the definition of f must have the following shape:

$$f \cdot x = \text{"something"} + a \ ,$$

where "something" differs from 0 ; moreover, because of (4) , it must depend upon x . In view of (0) , we have little choice and we conclude that the following proposal deserves further investigation. As a matter of fact, it satisfies all requirements:

$$(6) \qquad (\forall x :: \ f{\cdot}x \ = \ xb - 1 + a) \quad .$$

The calculations needed to show that (5) implies (2)∧(3)∧(4) are essentially the same as in [0][1] , which is why we omit them here. In its mathematical contents the above proof is the same as Dijkstra's proof, but my variation embodies a slightly better modularisation. In particular, (2) , (3) , and (4) are properties of function f that have nothing to do with s being a sequence; furthermore, the introduction of the c_k's is unnecessary.

The above reminds me of the exercise I carried out in [1] . This is not so surprising, because that exercise was also about the infinity of a given set, albeit in a different algebraic structure. Indeed, the macroscopic structures of the proof in [1] and the above proof are the same. This observation —and the desire to obtain some experience with the use of LaTeX— were the main incentives to write this little note. This elaboration of rh170 was written after the ETAC had read rh170 , and upon Wim Feijen's suggestion that I be more explicit about the heuristics leading to the definition of function f . So be it.

references

[0] E.W. Dijkstra
On a proof of Kaplansky's Theorem
EWD1124, Austin, 1992.

[1] R.R. Hoogerwoord
A little exercise in combinator logic
rh133, Eindhoven, 1990.

Eindhoven, 4 june 1992

Rob R. Hoogerwoord
department of mathematics and computing science
Eindhoven University of Technology

[1] more precisely: lemma 0 in [0] amounts to $(5) \Rightarrow (2)$, lemma 1 amounts to $(5) \Rightarrow (4)$, and lemma 2 amounts to $(5) \Rightarrow (3)$.

postbus 513
5600 MB Eindhoven