January 24 2014

1. Uniqueness
2. Division Algorithm

Uniqueness

To prove that an object x is unique,

① Suppose x and y satisfy the conditions and $x \neq y$.
Reach a contradiction.

② Suppose x and y satisfy these conditions, prove $x = y$.

Example: $\mathbb{R}$, Additive identity $\exists$ unique $x \in \mathbb{R}$ such that $\forall y \in \mathbb{R}$, $y + x = y$

Existance: Let $x=0$, then for any $y \in \mathbb{R}$, $y+0=y$.

Uniqueness: Suppose $x_1, x_2 \in \mathbb{R}$ are both additive identities.

ctrl-C

So $x_1 + x_2 = x_1$ ($y = x_1$, $x = x_2$ in defn) and

$x_2 + x_1 = x_2$ ($y = x_2$, $y = x_1$, in defn)

Since $\mathbb{R}$ is commutative under addition,

$x_1 + x_2 = x_2 + x_1$ So $x_1 = x_2$.

Another proof: Suppose $x_1, x_2 \in \mathbb{R}$ are additive identities and $x_1 \neq x_2$.

ctrl-V

Since $x_1 = x_2$ and $x_1 \neq x_2$, contradiction.

Division Algorithm

$$\begin{array}{r} 392 \\ 8\,\overline{)\,3141} \\ \underline{24} \\ 74 \\ \underline{72} \\ 21 \\ \underline{16} \\ 5 \end{array}$$

quotient q

dividend a

divisor b

remainder r

$$3141 = 8\cdot 392 + 5$$

$$\underset{\in\mathbb{Z}}{a} = q\underset{\in\mathbb{N}}{b} + r$$

$$\boxed{0 \leq r < b}$$

~~13 divided by 3 equals 2 with rem 7.~~ False

Example: $a = -13$ $\quad b = 3$

$$-13 = 3(-5) + (2)$$

Division Algorithm: Let $a \in \mathbb{Z}$, $b \in \mathbb{N}$. Then there exists unique $q, r \in \mathbb{Z}$ such that $a = qb + r$ and $0 \leq r < b$.

Proof: Existence proof is done in A3.

Uniqueness: Suppose both q_1, r_1 and q_2, r_2 satisfy the conclusion of the div. alg. So $a = q_1 b + r_1$ and $a = q_2 b + r_2$ where $0 \leq r_1 < b$ and $0 \leq r_2 < b$.

Subtract the two equations to get $q_1 b + r_1 - q_2 b - r_2 = 0$.

Then $b(q_1 - q_2) = r_2 - r_1$. Since $q_1 - q_2 \in \mathbb{Z}$, $b \mid (r_2 - r_1)$

Since $0 \leq r_1 \leq b$ and $0 \leq r_2 \leq b$, $-(b-1) \leq r_2 - r_1 \leq b-1$

Since the only integer in $[-(b-1), b-1]$ that is divisible by b is 0, $r_1 - r_2 = 0$. So $r_1 = r_2$. Then

$$b(q_1 - q_2) = 0$$

Since $b \neq 0$, $q_1 - q_2 = 0$, so $q_1 = q_2$.

Example: Let A be an invertible matrix. Then A^{-1} is unique.

$(AA^{-1} = A^{-1}A = I)$

Suppose B, C are both inverses of A.

Then $B = BI = B(AC) = (BA)C = IC = C$

since C is an inverse associative B is an inverse