Division Lemma

Division Lemma

Division Lemma

The Division Lemma (Euclid)

Let $d \in \mathbb{N}$. Then for each $x \in \mathbb{Z}$, there exist unique numbers $q \in \mathbb{Z}$ and $r \in \{0, \ldots, d-1\}$ such that $x = qd + r$.

quotient divisor remainder

Outline of Proof.

1. Prove existence of q and r when $x \in \omega$ by induction. $(\forall x \in \omega)\, P(x)$
2. Prove existence of q and r when $x \in \mathbb{Z}$. $(\forall x \in \mathbb{Z})\, P(x)$
3. Prove uniqueness of q and r.

- $(\forall d \in \mathbb{N})(\forall x \in \mathbb{Z})\underbrace{(\exists!\, q \in \mathbb{Z})(\exists!\, r \in \{0, \cdots, d-1\})(x = qd + r)}_{P(x)}$
- $P(x)$ is a "unique existence" sentence.

Strategy for uniqueness proof (see Lec 7 on uniqueness)

$$(\forall q_1, q_2 \in \mathbb{Z})(\forall r_1, r_2 \in \{0, \dots, d-1\})\Big[(x = q_1 d + r_1) \wedge (x = q_2 d + r_2) \Longrightarrow (q_1 = q_2) \wedge (r_1 = r_2)\Big]$$

Part 1: Proof of Existence of q and r when $x \in \omega$

Let $P(x)$ be the sentence

There exist numbers $q \in \mathbb{Z}$ and $r \in \{0, \ldots, d-1\}$ such that $x = qd + r$.

(WTS: $(\forall x \in \omega)\, P(x)$ by induction)

BASE CASE: $P(0)$ is true because $0 = 0 \cdot d + 0$.

INDUCTIVE STEP: Let $x \in \omega$ such that $P(x)$ is true. So we can pick $q_0 \in \mathbb{Z}$ and $r_0 \in \{0, \cdots, d-1\}$ such that $x = q_0 d + r_0$. Then $x+1 = q_0 d + r_0 + 1$. Now either $r_0 \in \{0, \cdots, d-2\}$ or $r_0 = d-1$.

Case 1. Suppose $r_0 \in \{0, \cdots, d-2\}$. Then $r_0 + 1 \in \{0, \cdots, d-1\}$. Let $q = q_0$ and $r = r_0 + 1$. Then $q \in \mathbb{Z}$, $r \in \{0, \cdots, d-1\}$, and $x+1 = qd + r$.

Case 2. Suppose $r_0 = d-1$. Then $x+1 = q_0 d + r_0 + 1 = q_0 d + d - 1 + 1 = q_0 d + d = (q_0+1)d$. Let $q = q_0 + 1$ and $r = 0$. Then $q \in \mathbb{Z}$, $r \in \{0, \cdots, d-1\}$, and $x+1 = qd + r$.

Thus in either case, $P(x+1)$ is true.

CONCLUSION: Therefore, by induction, for each $x \in \omega$, $P(x)$ is true.

Part 2: Proof of Existence of q and r when $x \in \mathbb{Z}$

Comment: In class, I mistakenly considered $x+1$, which was not needed.

Consider any $x \in \mathbb{Z}$. Then either $x \geqslant 0$ or $x \leqslant -1$.

Case 1. Suppose $x \geqslant 0$. Then $x \in \boldsymbol{\omega}$, so $P(x)$ is true by Part 1.

Case 2. Suppose $x \leqslant -1$. Then $-x \in \omega$, so $P(-x)$ is true by Part 1.

So we can pick $q_0 \in \mathbb{Z}$ and $r_0 \in \{0, \dots, d-1\}$ such that $-x = q_0 d + r_0$.

Then $x = -q_0 d - r_0$ $\boxed{\cancel{\text{and } x+1 = -q_0 d - r_0 + 1}}$. Now $r_0 = 0$ or $r_0 \in \{1, \dots, d-1\}$

Subcase a Suppose $r_0 = 0$. Then $x \cancel{+1} = -q_0 d \cancel{+1}$. Let $q = -q_0$ and $r = \cancel{1}\,0$.

Then $q \in \mathbb{Z}$, $r \in \{0, \dots, d-1\}$, and $x \cancel{+1} = qd + r$.

Subcase b Suppose $r_0 \in \{1, \dots, d-1\}$. Then $x \cancel{+1} = -q_0 d - r_0 \cancel{+1} = -q_0 d - d + d - r_0 \cancel{+1}$

$= (-q_0 - 1)d + (\cancel{1+} d - r_0)$.

Since $1 \leq r_0 \leq d-1$, $1-d \leq -r_0 \leq -1$, so

$1\ \cancel{2} \leq \cancel{1+} d - r_0 \leq d - 1$

Let $q = -q_0 - 1$ and $r = d - r_0$. Then

$q \in \mathbb{Z}$, $r \in \{0, \cdots, d-1\}$, and $x = qd + r$.

Thus in either subcase, $P(x)$ is true.

Thus in either case, $P(x)$ is true. In other words, for each $x \in \mathbb{Z}$, $P(x)$ is true.

Part 3: Proof of Uniqueness of q and r

Consider any $x \in \mathbb{Z}$. Suppose $q_1, q_2 \in \mathbb{Z}$, $r_1, r_2 \in \{0, \ldots, d-1\}$, $x = q_1 d + r_1$, and $x = q_2 d + r_2$. We wish to show that $q_1 = q_2$ and $r_1 = r_2$. Now either $r_1 \leq r_2$ or $r_2 \leq r_1$.

We will only consider $r_1 \leq r_2$ because the other case is similar. Note that

$$0 = x - x = (q_1 d + r_1) - (q_2 d + r_2)$$
$$= (q_1 - q_2) d - (r_2 - r_1)$$

So $(q_1 - q_2) d = r_2 - r_1$. Observe that $0 \leq r_2 - r_1 \leq r_2 \leq d-1$. So it follows that $q_1 - q_2 \geq 0$ because $d \geq 1$ and $r_2 - r_1 \geq 0$.

Claim. $q_1 - q_2 = 0$.

Pf. Suppose otherwise, that is, assume $q_1 - q_2 \geq 1$. Then $(q_1 - q_2) d \geq d$, so $r_2 - r_1 \geq d$. This is a contradiction to $r_2 - r_1 \leq d-1$. $\square$

By the claim, $q_1 = q_2$. Then $0 = (q_1 - q_2)d = r_2 - r_1$, so $r_1 = r_2$.

This complete the proof of uniqueness. $\square$

<u>Recap</u> To prove the division lemma:

$$(\forall d \in \mathbb{N})(\forall x \in \mathbb{Z})(\exists! \, q \in \mathbb{Z})(\exists! \, r \in \{0, \dots, d-1\})(x = qd + r)$$

<u>Strategy for proof</u> Let $d \in \mathbb{N}$.

① $$(\forall x \in \omega)\underbrace{(\exists q \in \mathbb{Z})(\exists r \in \{0, \cdots, d-1\})(x = qd + r)}_{= P(x)}$$

② $$(\forall x \in \mathbb{Z}) \, P(x)$$

$\longrightarrow$ ③ $$(\forall x \in \mathbb{Z})(\forall q_1, q_2 \in \mathbb{Z})(\forall r_1, r_2 \in \{0, \cdots, d-1\})$$
$$\left[(x = q_1 d + r_1) \wedge (x = q_2 d + r_2) \implies (q_1 = q_2) \wedge (r_1 = r_2) \right]$$

Scratch work

$$\begin{array}{ccccccc} x & & q & & d & & r \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ 14 & = & 2 & \cdot & 5 & + & 4 \end{array}$$

$$15 = 2 \cdot 5 + \underbrace{4 + 1}$$

$$\uparrow$$

$$\begin{aligned} x+1 &= 2 \cdot 5 + 5 \\ &= (2+1)5 + 0 \end{aligned}$$

$$\begin{array}{ccccccc} x & & q & & d & & r \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ -12 & = & -3 & \cdot & 5 & + & 3 \end{array}$$

$$\begin{array}{ccccccc} -x & & q_0 & & d & & r_0 \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ 12 & = & 2 & \cdot & 5 & + & 2 \end{array}$$

$$-12 = -2 \cdot 5 - 2$$

$$-12 + 1 = -2 \cdot 5 - 2 + 1$$

$$-11 = -2 \cdot 5 - 2 + 1$$

$x+1$

$$-11 = -3 \cdot 5 + 4$$

Scratch work

$$-11 = -3 \cdot 5 + 4$$

$$= (-2-1) \cdot 5 + 4$$

$$= -2 \cdot 5 - 5 + 4$$

$$-11 = -2 \cdot 5 - 2 + 1$$

$$= \underbrace{-2 \cdot 5 - 5}_{} + \underbrace{5 - 2 + 1}_{}$$

$$= (-2-1)5 + 4$$

$$\in \{0, \dots, 4\}$$