Well-ordered Proof

Definition a set S is partially ordered if there exists a binary predicate $R: S \times S \to \{T, F\}$ satisfying

a. Reflective $R(x, x) = T$
b. Asymmetric $\left(R(x, y) \text{AND } R(y, x)\right)$ IMPLIES $(x = y)$
c. Transitive $\left(R(x, y) \text{AND } R(y, z)\right)$ IMPLIES $R(x, z)$

R is a partial order of S

Example Some examples of partial order:

$\leq: \mathbb{R} \times \mathbb{R}$
Divides: $\mathbb{Z}^+ \times \mathbb{Z}^+$
$\subseteq: S\ (\text{any set}) \times \mathcal{P}(S)$
$=: \mathbb{R} \times \mathbb{R}$

Some examples of not partial order:

$<: \mathbb{R} \to \mathbb{R}$ (not reflective)
$\leq: \mathbb{C} \to \mathbb{C}\ \left(\forall x \in \mathbb{C}. \forall y \in \mathbb{C}. x \leq y \text{ IFF } |x| \leq |y|\right), \leq (-1,1)$ AND $\leq (1, -1)\ \ -1 \neq 1$, not asymmetric

Definition S is totally ordered if there exists a partial order R on S such that $\forall x, y \in S. R(x, y)$ OR $R(y, x)$

Example $\leq: \mathbb{R} \times \mathbb{R}$

Not total order: Divides: $\mathbb{Z}^+ \times \mathbb{Z}^+, \subseteq: \mathcal{P}(S) \times \mathcal{P}(S)$

Definition a paritial order R for S is a well ordering of S, if every non-empty subset of S has a smallest element.

$\forall T \in \mathcal{P}(s). \exists m \in T. \forall x \in T. R(m, x)$

Example $\leq: \mathbb{N} \times \mathbb{N}$ is a well-ordering , $\leq: \mathbb{Z} \times \mathbb{Z}$ is not $(\forall x \in \mathbb{Z}. \exists y \in \mathbb{Z}. y \leq x)$

Let an ordering $<^*$: $\mathbb{Z} \coloneqq |x| < |y|$ OR $|x| = |y|$AND $x < y$. i.e. $0 <^* -1 <^* 1 <^* -2 <^* 2 \ldots$ is a well-ordering.

Let an ordering $\ll: \mathbb{Q}^+ \coloneqq$ comparing max(numerator, denumerator), then the acutal value, i.e. $\frac{1}{1} \ll \frac{1}{2} \ll \frac{2}{1} \ll \frac{1}{3} \ll \frac{2}{3} \ll \frac{3}{2} \ll \frac{3}{1}$ is a well ordering.

Well-ordering Proof

To prove $\forall e \in S. P(e)$, where $\ll$ is a well ordering of S

L1 Suppose $\exists e \in S.$ NOT $P(e)$ is false (construct a contradiction)
L2 Let $C = \{\, e \in S \mid P(e) = F \,\}$ be the set of counter examples
L3 $C \neq \emptyset$ by L1, L2
L4 Let e be the smallest element of C, e exists since S is well-ordered and $\emptyset \neq C \subseteq S$
  Let $e' \in S$
  …
  L5 $e' \in C$
  L6 $e' \neq e$
  L7 $e' \ll e$
Contradiction since e is not the smallest element of C

$\forall e \in S. P(e)$ by contradiction

Theorem Every element $\frac{m}{n} \in \mathbb{Q}^+$ can be expressed in reduced form $c = \frac{m'}{n'}, \gcd(m', n') = 1$

Proof Suppose $\exists \frac{m}{n} \in \mathbb{Q}^+$ that can't be expressed in reduced form.

Let $C = \left\{ m \in \mathbb{Z}^+ \,\middle|\, \exists n \in \mathbb{Z}^+ \text{ such that } \frac{m}{n} \text{ can't be expressed in reduced form} \right\}$

By assumption $C \neq \emptyset$

Since $\mathbb{Z}^+$ is well-ordered, C has the smallest element, take such m_0

By definition of C, take $n_0 \in \mathbb{Z}^+, \frac{m_0}{n_0}$ can't be expressed in reduced form, in particular

$\gcd(m_0, n_0) > 1$

Take $n_0' = \frac{n_0}{\gcd(m_0,n_0)} \in \mathbb{Z}^+, m_0' = \frac{m_0}{\gcd(m_0,n_0)} \in \mathbb{Z}^+, n_0' < n_0, m_0' < m_0$

Since $\frac{m_0'}{n_0'} = \frac{m_0}{n_0}, m_0' \in C$.

Because $m_0' < m_0, m_0' \in C, m_0'$ is not the smallest element in C.

Every element $\frac{m}{n} \in \mathbb{Q}^+$ can be expressed in reduced form $c = \frac{m'}{n'}, \gcd(m', n') = 1$ by contradiction