Divisibility

João Paixão and Lucas Rufino

October 24, 2020

1 Definitions

1.1 Preorder

Definition 1.1 (Reflexivity)**.** $A \mid A$

Definition 1.2 (Transitivity)**.** $A \mid B$ and $B \mid C \implies A \mid C$

Definition 1.3 (Isomorphic)**.** $A = B \iff A \mid B$ and $B \mid A$

Lemma 1.1. $A = B \iff (A \mid B \impliedby TRUE \implies B \mid A)$

1.2 Yoneda

Definition 1.4 (Yoneda $\mid$)**.** $A \mid B \iff \forall X(X \mid A \implies X \mid B)$

Lemma 1.2 (Yoneda 1 $=$)**.** $A = B \iff \forall X(X \mid A \iff X \mid B)$

Lemma 1.3 (Yoneda 2 $=$)**.** $A = B \iff \forall X(A \mid X \iff B \mid X)$

1.3 Initial and Terminal Object $(1$ and $0)$

Definition 1.5 (Initial)**.** $1 \mid A$

Definition 1.6 (Terminal)**.** $A \mid 0$

1.4 Meets $(A \operatorname{gcd} B)$

Definition 1.7 (Meet)**.** $A \mid B \operatorname{gcd} C \iff A \mid B$ and $A \mid C$

Lemma 1.4 (Zero Element)**.** $A \operatorname{gcd} 0 = A$

Proof.

$$
\begin{aligned}
& X \mid A \operatorname{gcd} 0 \\
\iff & \quad \{ \text{ Meet } \} \\
& X \mid A \text{ and } X \mid 0 \\
\iff & \quad \{ \text{ Terminal } \}
\end{aligned}
$$

$$
\begin{aligned}
& X \mid A \text{ and } TRUE \\
\iff & \quad \{ \text{ A and TRUE = A } \} \\
& X \mid A
\end{aligned}
$$

□

Lemma 1.5 (Absolute Element). $A \operatorname{gcd} 1 = 1$

Proof.

$$
\begin{aligned}
& 1 \mid A \operatorname{gcd} 1 \\
\iff & \quad \{ \text{ Initial } \} \\
& TRUE \\
\iff & \quad \{ \text{ Reflexivity } \} \\
& A \operatorname{gcd} 1 \mid A \operatorname{gcd} 1 \\
\iff & \quad \{ \text{ Meet } \} \\
& A \operatorname{gcd} 1 \mid A \text{ and } A \operatorname{gcd} 1 \mid 1 \\
\implies & \quad \{ \text{ A and B } \implies \text{ B } \} \\
& A \operatorname{gcd} 1 \mid 1
\end{aligned}
$$

□

Lemma 1.6 (Associativity). $A \operatorname{gcd}(B \operatorname{gcd} C) = (A \operatorname{gcd} B) \operatorname{gcd} C$

Proof.

$$
\begin{aligned}
& X \mid A \operatorname{gcd}(B \operatorname{gcd} C) \\
= & \quad \{ \text{ Meet } \} \\
& X \mid A \text{ and } X \mid B \operatorname{gcd} C \\
= & \quad \{ \text{ Meet } \} \\
& X \mid A \text{ and } (X \mid B \text{ and } X \mid C) \\
= & \quad \{ \text{ Associativity of And } \} \\
& (X \mid A \text{ and } X \mid B) \text{ and } X \mid C \\
= & \quad \{ \text{ Meet } \} \\
& X \mid A \operatorname{gcd} B \text{ and } X \mid C \\
= & \quad \{ \text{ Meet } \} \\
& X \mid (A \operatorname{gcd} B) \operatorname{gcd} C
\end{aligned}
$$

□

Lemma 1.7 (Commutativity). $A \operatorname{gcd} B = B \operatorname{gcd} A$

Proof.

$$
\begin{aligned}
& X \mid A \gcd B \\
= & \quad \{ \text{ Meet } \} \\
& X \mid A \text{ and } X \mid B \\
= & \quad \{ \text{ Commutativity of And } \} \\
& X \mid B \text{ and } X \mid A \\
= & \quad \{ \text{ Meet } \} \\
& X \mid B \gcd A
\end{aligned}
$$

□

1.5 Joins (A lcm B)

Definition 1.8 (Join)**.** $A \text{ lcm } B \mid C \iff A \mid C \text{ and } B \mid C$

Lemma 1.8 (Zero Element)**.** $A \text{ lcm } 1 = A$

Proof.

$$
\begin{aligned}
& A \text{ lcm } 1 \mid X \\
\iff & \quad \{ \text{ Join } \} \\
& A \mid X \text{ and } 1 \mid X \\
\iff & \quad \{ \text{ Initial } \} \\
& A \mid X \text{ and } TRUE \\
\iff & \quad \{ \text{ A and TRUE = A } \} \\
& A \mid X
\end{aligned}
$$

□

Lemma 1.9 (Absolute Element)**.** $0 \text{ lcm } A = 0$

Proof.

$$
\begin{aligned}
& 0 \text{ lcm } A \mid 0 \\
\iff & \quad \{ \text{ Terminal } \} \\
& TRUE \\
\iff & \quad \{ \text{ Reflexivity } \} \\
& 0 \text{ lcm } A \mid 0 \text{ lcm } A \\
\iff & \quad \{ \text{ Join } \} \\
& 0 \mid 0 \text{ lcm } A \text{ and } A \mid 0 \text{ lcm } A \\
\implies & \quad \{ \text{ A and B } \implies \text{ A } \} \\
& 0 \mid 0 \text{ lcm } A
\end{aligned}
$$

□

Lemma 1.10 (Associativity)**.** $A \text{ lcm } (B \text{ lcm } C) = (A \text{ lcm } B) \text{ lcm } C$

Proof.

$$\begin{array}{ll} & A \text{ lcm } (B \text{ lcm } C) \mid X \\ \Longleftrightarrow & \quad \{\text{ Join }\} \\ & A \mid X \text{ and } B \text{ lcm } C \mid X \\ \Longleftrightarrow & \quad \{\text{ Join }\} \\ & A \mid X \text{ and } (B \mid X \text{ and } C \mid X) \\ \Longleftrightarrow & \quad \{\text{ Associativity of And }\} \\ & (A \mid X \text{ and } B \mid X) \text{ and } C \mid X \\ \Longleftrightarrow & \quad \{\text{ Join }\} \\ & A \text{ lcm } B \mid X \text{ and } C \mid X \\ \Longleftrightarrow & \quad \{\text{ Join }\} \\ & (A \text{ lcm } B) \text{ lcm } C \mid X \end{array}$$

□

Lemma 1.11 (Commutativity)**.** $A \text{ lcm } B = B \text{ lcm } A$

Proof.

$$\begin{array}{ll} & A \text{ lcm } B \mid X \\ = & \quad \{\text{ Join }\} \\ & A \mid X \text{ and } B \mid X \\ = & \quad \{\text{ Commutativity of And }\} \\ & B \mid X \text{ and } A \mid X \\ = & \quad \{\text{ Join }\} \\ & B \text{ lcm } A \mid X \end{array}$$

□

Lemma 1.12 (Golden Rule)**.** $A \mid A \operatorname{gcd} B \iff B \text{ lcm } A \mid B$

Proof.

$$\begin{array}{ll} & A \mid A \operatorname{gcd} B \\ \Longleftrightarrow & \quad \{\text{ Meet }\} \\ & A \mid A \text{ and } A \mid B \\ \Longleftrightarrow & \quad \{\text{ Reflexivity }\} \\ & TRUE \text{ and } A \mid B \\ \Longleftrightarrow & \quad \{\text{ Reflexivity }\} \\ & B \mid B \text{ and } A \mid B \\ \Longleftrightarrow & \quad \{\text{ Join }\} \end{array}$$

$$B \text{ lcm } A \mid B$$

$\square$

1.6 Adjoints ($*$ and $/$)

Definition 1.9 (Adjoint)**.** $A * B \mid C \iff A \mid C/B$

Definition 1.10 (Associativity of $*$)**.** $A * (B * C) = (A * B) * C$

Definition 1.11 (Commutativity of $*$)**.** $A * B = B * A$

Lemma 1.13 ($*$ distributes over Joins)**.** $(A \text{ lcm } B) * C = (A * C) \text{ lcm } (B * C)$

Proof.

$$\begin{array}{ll}
 & (A \text{ lcm } B) * C \mid X \\
\iff & \quad \{ \text{ Adjoint } \} \\
 & A \text{ lcm } B \mid X/C \\
\iff & \quad \{ \text{ Join } \} \\
 & A \mid X/C \text{ and } B \mid X/C \\
\iff & \quad \{ \text{ Adjoint } \} \\
 & A * C \mid X \text{ and } B * C \mid X \\
\iff & \quad \{ \text{ Join } \} \\
 & (A * C) \text{ lcm } (B * C) \mid X
\end{array}$$

$\square$

Lemma 1.14 ($/$ distributes over Meets)**.** $(A \operatorname{gcd} B)/C = (A/C) \operatorname{gcd} (B/C)$

Proof.

$$\begin{array}{ll}
 & X \mid (A \operatorname{gcd} B)/C \\
\iff & \quad \{ \text{ Adjoint } \} \\
 & X * C \mid A \operatorname{gcd} B \\
\iff & \quad \{ \text{ Meet } \} \\
 & X * C \mid A \text{ and } X * C \mid B \\
\iff & \quad \{ \text{ Adjoint } \} \\
 & X \mid A/C \text{ and } X \mid B/C \\
\iff & \quad \{ \text{ Meet } \} \\
 & X \mid (A/C) \operatorname{gcd} (B/C)
\end{array}$$

$\square$

Lemma 1.15 (Preservation of infima)**.** $1 * A = 1$

Proof.

$$
\begin{array}{ll}
 & 1 * A \mid X \\
\iff & \quad \{ \text{ Adjoint } \} \\
 & 1 \mid X/A \\
\iff & \quad \{ \text{ Initial } \} \\
 & TRUE \\
\iff & \quad \{ \text{ Initial } \} \\
 & 1 \mid X
\end{array}
$$

□

Lemma 1.16 (Preservation of suprema)**.** $0/A = 0$

Proof.

$$
\begin{array}{ll}
 & X \mid 0/A \\
\iff & \quad \{ \text{ Adjoint } \} \\
 & X * A \mid 0 \\
\iff & \quad \{ \text{ Terminal } \} \\
 & TRUE \\
\iff & \quad \{ \text{ Terminal } \} \\
 & X \mid 0
\end{array}
$$

□

Lemma 1.17 (Left cancellation law)**.** $(A/B) * B \mid A$

Proof.

$$
\begin{array}{ll}
 & (A/B) * B \mid A \\
\iff & \quad \{ \text{ Adjoint } \} \\
 & A/B \mid A/B \\
\iff & \quad \{ \text{ Reflexivity } \} \\
 & TRUE
\end{array}
$$

□

Lemma 1.18 (Right Cancelation law)**.** $A \mid (A * B)/B$

Proof.

$$
\begin{array}{ll}
 & A \mid (A * B)/B \\
\iff & \quad \{ \text{ Adjoint } \} \\
 & A * B \mid A * B \\
\iff & \quad \{ \text{ Reflexivity } \}
\end{array}
$$

$$TRUE$$

$\square$

Lemma 1.19 (Monotonicity of $*$). $A \mid B \implies A * C \mid B * C$

Proof.

$$
\begin{aligned}
& A \mid B \\
\iff & \quad \{ \text{ A and TRUE = A } \} \\
& A \mid B \text{ and } TRUE \\
\iff & \quad \{ \text{ Right Cancellation Law } \} \\
& A \mid B \text{ and } B \mid (B * C)/C \\
\implies & \quad \{ \text{ Transitivity of } \mid \} \\
& A \mid (B * C)/C \\
\iff & \quad \{ \text{ Adjoint } \} \\
& A * C \mid B * C
\end{aligned}
$$

$\square$

Lemma 1.20 (Monotonicity of $/$). $A \mid B \implies A/C \mid B/C$

Proof.

$$
\begin{aligned}
& A \mid B \\
\iff & \quad \{ \text{ TRUE and A = A } \} \\
& TRUE \text{ and } A \mid B \\
\iff & \quad \{ \text{ Left Cancellation Law } \} \\
& (A/C) * C \mid A \text{ and } A \mid B \\
\implies & \quad \{ \text{ Transitivity of } \mid \} \\
& (A/C) * C \mid B \\
\iff & \quad \{ \text{ Adjoint } \} \\
& A/C \mid B/C
\end{aligned}
$$

$\square$

Lemma 1.21 (Weak-inverse $*$). $A * B = ((A * B)/B) * B$

Proof.

$$
\begin{aligned}
& ((A * B)/B) * B \mid A * B \\
\iff & \quad \{ \text{ Left Cancellation Law } \} \\
& TRUE \\
\iff & \quad \{ \text{ Right Cancellation Law } \}
\end{aligned}
$$

$$
\begin{array}{rl}
 & A \mid (A * B)/B \\
\Longrightarrow & \quad \{ \text{ Monotonicity of } * \text{ } \} \\
 & A * B \mid ((A * B)/B) * B
\end{array}
$$

□

Lemma 1.22 (Weak-inverse /). $A/B = ((A/B) * B)/B$

Proof.

$$
\begin{array}{rl}
 & A/B \mid ((A/B) * B)/B \\
\Longleftrightarrow & \quad \{ \text{ Right Cancellation Law } \} \\
 & TRUE \\
\Longleftrightarrow & \quad \{ \text{ Left Cancellation Law } \} \\
 & (A/B) * B \mid A \\
\Longrightarrow & \quad \{ \text{ Monotonicity of / } \} \\
 & ((A/B) * B)/B \mid A/B
\end{array}
$$

□

Lemma 1.23 (/ distributes over $*$). $A/(B * C) = (A/B)/C$

Proof.

$$
\begin{array}{rl}
 & X \mid (A/B)/C \\
\Longleftrightarrow & \quad \{ \text{ Adjoint } \} \\
 & X * C \mid A/B \\
\Longleftrightarrow & \quad \{ \text{ Adjoint } \} \\
 & (X * C) * B \mid A \\
\Longleftrightarrow & \quad \{ \text{ Associativity of } * \text{ } \} \\
 & X * (C * B) \mid A \\
\Longleftrightarrow & \quad \{ \text{ Adjoint } \} \\
 & X \mid A/(C * B)
\end{array}
$$

□

Lemma 1.24 (Duality). $A \gcd B \mid (A * B)/(B \text{ lcm } A)$

Proof.

$$
\begin{array}{rl}
 & X \mid A \gcd B \\
\Longleftrightarrow & \quad \{ \text{ Meet } \} \\
 & X \mid A \text{ and } X \mid B \\
\Longrightarrow & \quad \{ \text{ Monotonicity of }^{*} \text{ } \}
\end{array}
$$

$$
\begin{array}{ll}
& X * B \mid A * B \text{ and } X * A \mid B * A \\
\iff & \quad \{ \text{ Commutativity of } * \ \} \\
& B * X \mid A * B \text{ and } A * X \mid A * B \\
\iff & \quad \{ \text{ Adjoint } \} \\
& B \mid (A * B)/X \text{ and } A \mid (A * B)/X \\
\iff & \quad \{ \text{ Join } \} \\
& B \text{ lcm } A \mid (A * B)/X \\
\iff & \quad \{ \text{ Adjoint } \} \\
& (B \text{ lcm } A) * X \mid A * B \\
\iff & \quad \{ \text{ Commutativity of } * \ \} \\
& X * (B \text{ lcm } A) \mid A * B \\
\iff & \quad \{ \text{ Adjoint } \} \\
& X \mid (A * B)/(B \text{ lcm } A)
\end{array}
$$

□

2 Exercises

1. (Weakening) $A \mid A \text{ lcm } B$
2. (Projection) $A \operatorname{gcd} B \mid A$
3. (Idempotency) $A \text{ lcm } A = A$
4. (Meet | Join) $A \operatorname{gcd} B \mid A \text{ lcm } B$
5. (Monotonicity of lcm) $A \mid B$ and $C \mid D \implies A \text{ lcm } C \mid B \text{ lcm } D$
6. $A * A/A = A$
7. (Self-Distributivity) $A \operatorname{gcd}(B \operatorname{gcd} C) = (A \operatorname{gcd} B) \operatorname{gcd}(A \operatorname{gcd} C)$
8. (Absorption) $A \operatorname{gcd}(A \text{ lcm } B) = A$