Part IA Discrete Maths Notes

- d divides n

  $$d \mid n \Rightarrow n = k \cdot d$$

- a is congruent to b modulo m

  $$a \equiv b(mod m) \Rightarrow m \mid (a - b)$$

  $$a \equiv b \ (mod \ m) \Leftrightarrow m \cdot a \equiv n \cdot b \ (mod \ m \cdot n)$$

- The freshman's dream, for prime p

  $$(m + n)^p \equiv m^p + n^p \ (mod \ p)$$

- The dropout lemma, for prime p

  $$(m + 1)^p \equiv m^p + 1 \ (mod \ p)$$

- The multiple dropout lemma, for prime p. Proved with induction and the dropout lemma

  $$(m + i)^p \equiv m^p + i \ (mod \ p)$$

- Fermat's Little Theorem, for prime p

  $$\begin{aligned} i^p &\equiv i \ (mod \ p) \\ i^{p-1} &\equiv 1 \ (mod \ p) \qquad \text{whenever } i \text{ is not a multiple of } p \end{aligned}$$

- Monoid

  Structure containing a set, an identity element, and an associative binary operation

- Commutativity

  $$m \circ n = n \circ m$$

- Euclid's Algorithm

  $$\begin{aligned} m \equiv \ & m' \ (mod \ n) \Rightarrow (CD(m, n) = CD(m', n)) \\ & \Rightarrow \forall \ d \in \mathbb{Z}^+ \ \ d \mid m \wedge d \mid n \Leftrightarrow d \mid m' \wedge d \mid n \\ & (\Rightarrow) \text{ Assume } d \mid m \wedge d \mid n \end{aligned}$$

  By $m \equiv m' \ (mod \ n)$

  $$\begin{aligned} & m' = k_0 \cdot n + m \text{ for some } k_0 \\ & \Rightarrow d \mid m' \wedge d \mid n \end{aligned}$$

- Cases

  $$gcd(m, n) = \begin{cases} n & \text{if } n \mid m \\ gcd(n, rem(m, n)) & \text{otherwise} \end{cases}$$

  - Commutative: $gcd(m,n) = gcd(n,m)$
  - Associative: $gcd(l, gcd(m,n)) = gcd(gcd(l,m), n)$
  - Linearity: $gcd(l \cdot m, l \cdot n) = l \cdot gcd(m,n)$

- Euclid's Theorem For all positive integers k,m, and n

  $$k \mid (m \cdot n) \wedge gcd(k,m) = 1 \Rightarrow k \mid n$$

- Linear Combinations

  $$k_1 \cdot m + k_2 \cdot n = gcd(m,n)$$

  found using Euclid's extended algorithm

- Inverses

  $[a]_n$ has an inverse iff $gcd(a,n) = 1$

  $$gcd(a,n) = 1 \Rightarrow a \cdot k_1 + n \cdot k_2 = 1$$

  put modulo n

  $$[a \cdot k_1 + n \cdot k_2]_n = [1]_n$$
  $$[a \cdot k_1]_n = [1]_n$$

  - Used to solve congruences, e.g. $7 \cdot z \equiv 4 \ (mod\ 13)$, multiply by $[7]_{13}^{-1}$

Fundamental Theorem of Arithmetic

1. Prime factorisation (strong induction)

   2 prime
   n: either prime or of form $a \cdot b$ with $1 < a < n$ and $1 < b < n$
   Therefore product of primes

2. Uniqueness (induction of number of prime factors, r)

   $r = 1$:
   prime, suppose prime can be expressed as $n = q_1 q_2 \dots q_s$ a contradiction
   therefore unique
   $r = k$:
   $n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_k$ by Euclid's theorem p_1 divides both sides so equals q_i
   it's trivial and harmless to swap this in the ordering so that it is q_1
   Cancelling gives
   $p_2 \dots p_k = q_2 \dots q_k$
   of length $k-1$ which holds

- Ordered pair

  $$< a, b >= \{\{a\}, \{a, b\}\}$$

- Disjoint set

  $$A \uplus B = (\{1\} \times A) \cup (\{2\} \times B)$$

- Cantor-Bernstein-Schroeder Theorem

  The existence of an injection from set A to B implies

  $$A \lesssim B \text{ or } \#A \leq \#B$$

  From the axiom of choice, the existence of a subjection from B to A, implies

  $$A \lesssim B \text{ or } \#A \leq \#B$$

  For all sets A and B

  $$(A \lesssim B \wedge B \lesssim A) \Rightarrow A \cong B$$

- Reflexive - $(a, a) \in R$
- Symmetric - $(a, b) \in R \Rightarrow (b.a) \in R$
- Anti-Symmetric - $(a, b) \in R \wedge (b, a) \in R \Rightarrow a = b$
- Transitive - $(a, b) \in R \wedge (b, c) \in R \Rightarrow (a, c) \in R$
- Total - $\forall\, a, b \in A (a, b) \in R \vee (b, a) \in R$

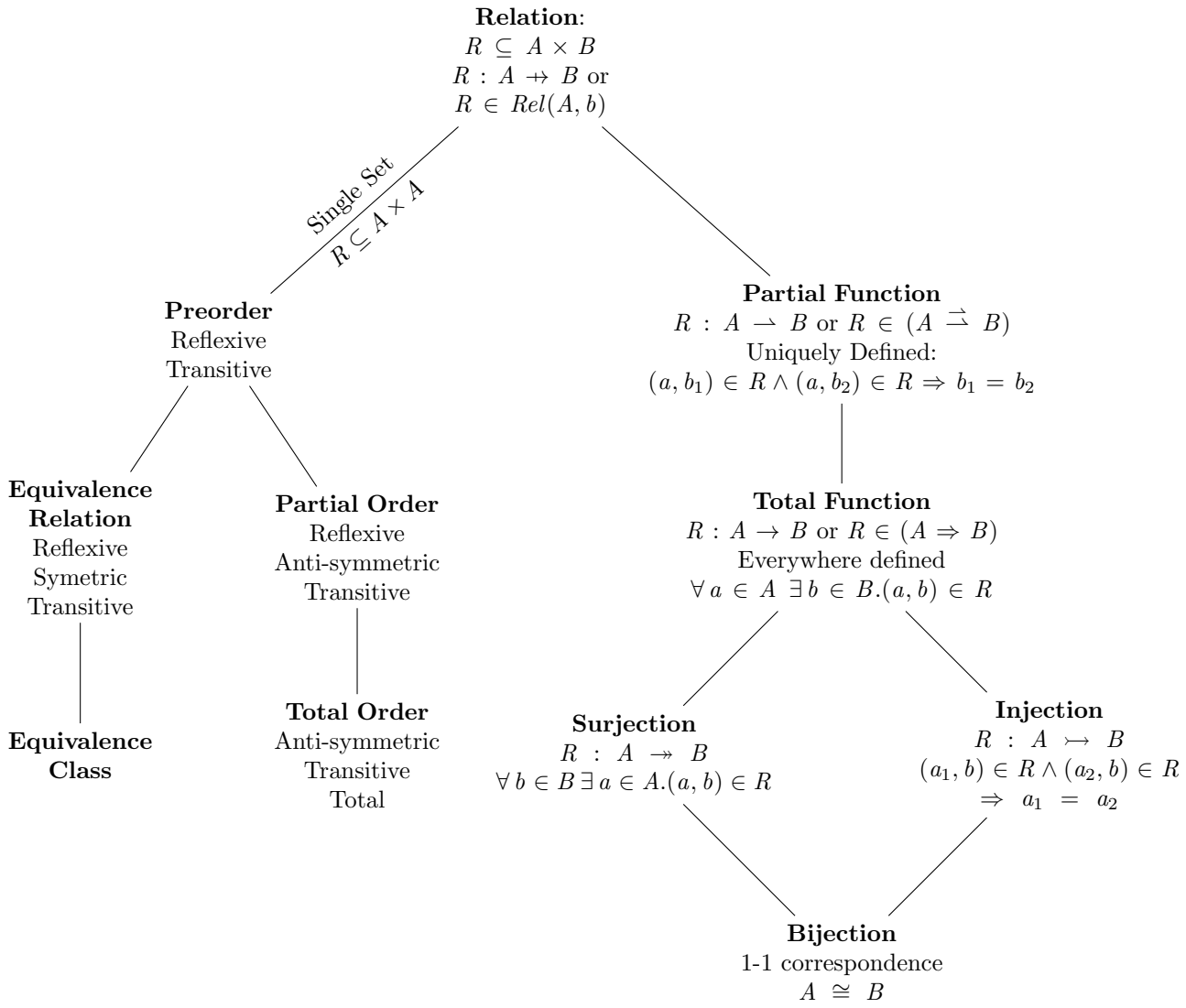

Figure 1: Relations