Lecture 4

Def: An integer p is said to be *prime* if $p \neq 0$, $p \neq \pm 1$ and the only divisor of p are ± 1 and $\pm p$.

An integer that is not prime is called *composite*.

Euclid's Lemma: If p is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof: Suppose p is prime, $p \mid ab$, and $p \nmid b$. Since $p \nmid b$ and p is prime, $\gcd(p,b) = 1$. Otherwise, we have $\gcd(p,b) \neq 1$ with $\gcd(p,b) \mid p$ and $\gcd(p,b) \mid b$.

But this is not possible because $\gcd(p,b)$ would be p and $p \nmid b$.

By Prop. 7, $p \mid a$.

Euclid's lemma shows a very important property of primes. A property that can be used to define a prime number.

Theorem 10: Let $p \in \mathbb{Z} \setminus \{0, \pm 1\}$. p is prime if and only if p has this property:

if $p | ab$, then $p | a$ or $p | b$.

Another def of primes

Proof:

($\Rightarrow$) Euclid's lemma.

($\Leftarrow$) We want to prove that the only divisors of p are $\{\pm 1, \pm p\}$.

Suppose p satisfies the property above. Let a be a divisor of p. Then

$p = am$ for some $m \in \mathbb{Z}$. From this $p | am$, then $p | a$ or $p | m$.

If $p | a$, then $a = \pm p$.

If $p | m$, $m = pl$ for some $l \in \mathbb{Z}$. Then $p = am = apl \Rightarrow al = 1 \Rightarrow a = \pm 1$. $\blacksquare$

Corollary 11: If p is prime and $p | a_1 a_2 \cdots a_n$, then p divides at least one a_i.

Proof: Exercise.

Why are primes important?

Prime numbers are the building blocks for all integers

The Fundamental Theorem of Arithmetic

Theorem: Every integer $n \in \mathbb{Z} \setminus \{0, \pm 1\}$ can be factored uniquely into the product of primes.

Explicitly ⇝ There are distinct primes $p_1, p_2, \dots, p_r$ and positive integers $\alpha_1, \alpha_2, \dots, \alpha_r$ such that $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ and $\alpha_i \geqslant 0 \;\; \forall i$.

The factorization is unique in the following sense: If $n = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$ for distinct primes $q_1, q_2, \dots, q_s$ and positive integers $\beta_1, \beta_2, \dots, \beta_s$, then $r = s$ and if we arrange the two sets of primes in increasing order, then $p_i = \pm q_i$ and $\alpha_i = \beta_i$ for all $1 \leq i \leq r$.

Proof: Read Thm 1.7 and Thm 1.8 from Hungerford's.

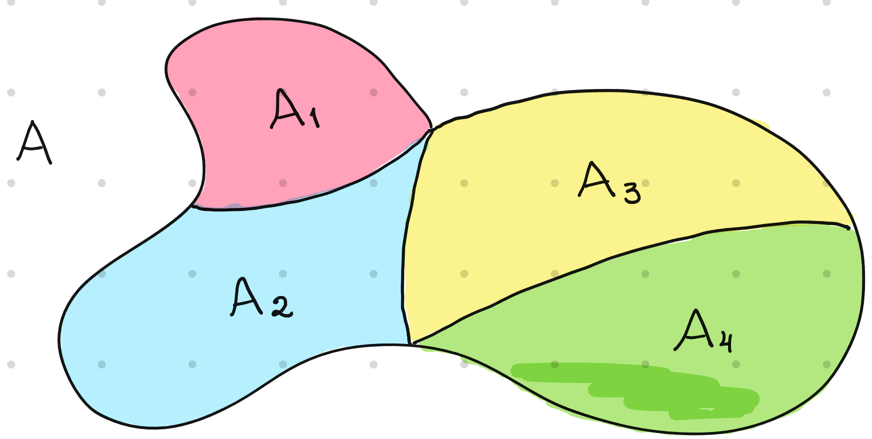
Digression - Equivalence Relations

IDEA: Want to generalize the concept of equality.

Def: Let A be a nonempty set. A partition of A is a collection $A_1, A_2, A_3, \ldots$ of subsets of A such that

(1) $A_i \cap A_j = \phi$ for all i, j with $i \neq j$. A_i are mutually disjoint

(2) $A = \bigcup A_i$. A is equal to the union of the subsets



Ex:

- $\{\ldots,-4,-2,0,2,4,\ldots\}$, $\{\ldots,-3,-1,1,3,\ldots\}$ is a partion of $\mathbb{Z}$.
- The collection formed by $\{a\}$ for all $a \in \mathbb{Z}$ is a partition of $\mathbb{Z}$.
- $(-\infty,0)$, $[0,\infty)$ is a partition of $\mathbb{R}$
- $(-\infty,3)$, $\{3\}$, $[3,\infty)$ is not a partition of $\mathbb{R}$, since $\{3\} \cap [3,\infty) = \{3\}$.

Def: Let A be a set. A relation on A is a subset $R \subseteq A \times A$.

If $(a,b) \in R$, we say a is related to b.

$$A \times B := \{(a,b) \mid a \in A,\ b \in B\}$$

$A = \{1,2\}$ $B = \{3,4\}$

$A \times B = \{(1,3),(1,4),(2,3),(2,4)\}$

Notation: aRb — $(a,b) \in R$ $\qquad$ $a\not R b$ — $(a,b) \notin R$

⚠ Order matters! aRb is different from bRa

Ex: Equality Relation

Define the relation $=$ as the subset $\{(a,a) \mid a \in A\} \subseteq A \times A$

$a=b$ means $(a,b) \in =$ and $a \neq b$ means $(a,b) \notin =$

Ex: Define $f := \{(x, x^2) \mid x \in \mathbb{R}\} \subseteq \mathbb{R} \times \mathbb{R}$.

If $(a,b) \in f$, then $b = a^2$ and we denote it by $f(a) = a^2$.

function

Every real function is a relation.

Ex: Relation induced by a partition

Consider a set A with a partition $\mathcal{P} = \{A_i \mid i \in I\}$. Define the relation

$$a R b \iff a \text{ and } b \text{ are in the same subset}$$

$$R = \{(a,b) \in A \times A \mid a, b \in A_i \text{ for some } i \in I\}$$