DEF $a \mid b$ if $(\exists x)(ax=b)$

$0 \mid 0$

$\mathrm{Div}(a) = \{b \mid b \mid a\}$

$\mathrm{Div}(a,b) = \mathrm{Div}(a) \cap \mathrm{Div}(b)$

$\mathrm{Div}(1) = \{\pm 1\}$

$\mathrm{Div}(0) = \mathbb{Z}$

$a \mid b$
$\Downarrow$
$\pm a \mid \pm b$

DEF $\underline{d}$ is $\underline{\underline{a}}$ gr.c.d. of $\underline{a}$ and $\underline{b}$ if

(1) $d \in \mathrm{Div}(a,b)$ — d is a common divisor

(2) $(\forall e \in \mathrm{Div}(a,b))(e \mid d)$

if d is a gr.c.d. then $\gcd(a,b) = |d|$

$\underline{\underline{\text{Ex}}}$. -6 is a gr.c.d. of 18 and 30

$\mathrm{Div}(18,30) = \{\pm 1, \pm 2, \pm 3, \pm 6\} =$
$= \mathrm{Div}(6)$

$\mathrm{Div}(0,0) = \mathrm{Div}(0) \cap \mathrm{Div}(0) = \mathbb{Z} \cap \mathbb{Z} = \mathbb{Z}$

all of $\mathbb{Z}$ has a common multiple: $\underline{\underline{0}}$

$\therefore \quad \gcd(0,0) = 0$

<u>THM</u> $(\forall a,b)(\exists \gcd(a,b))$

<u>DO</u> d is a gr.c.d. of $\underline{a}$ and $\underline{b}$ if and only if

$$\mathrm{Div}(a,b) = \mathrm{Div}(d)$$

DO

HW?

<u>LEMMA</u> ("Euclid's gcd lemma")

$\mathrm{Div}(a,b) = \mathrm{Div}(a-b,b)$

$\mathrm{Div}(a,b) = \mathrm{Div}(b,a)$

$\mathrm{Div}(a,b) = \mathrm{Div}(\pm b, \pm a)$

$\mathrm{Div}(a,0) = \mathrm{Div}(a)$

? $\gcd(30,78)$

$$\begin{aligned}\mathrm{Div}(30,78) &= \mathrm{Div}(78,30) \overset{E}{=} \mathrm{Div}(48,30) \overset{E}{=} \mathrm{Div}(18,30)\\ &= \mathrm{Div}(30,18) \overset{E}{=} \mathrm{Div}(12,18) = \mathrm{Div}(18,12) \overset{E}{=} \mathrm{Div}(6,12)\\ &= \mathrm{Div}(12,6) \overset{E}{=} \mathrm{Div}(6,6) \overset{E}{=} \mathrm{Div}(0,6) = \mathrm{Div}(6,0) = \mathrm{Div}(6)\end{aligned}$$

E indicates the use of "Euclid's gcd lemma"

$\therefore$ $\gcd(30,78) = 6$

EUCLID'S ALGORITHM

Pf by induction using Euclid's alg.

permutation of a set Ω:

DEF: bijection $f : \Omega \to \Omega$

$|\Omega| = n$

$\#$ permutations $= n! = n(n-1)\cdots 2\cdot 1$

$0! = 1$

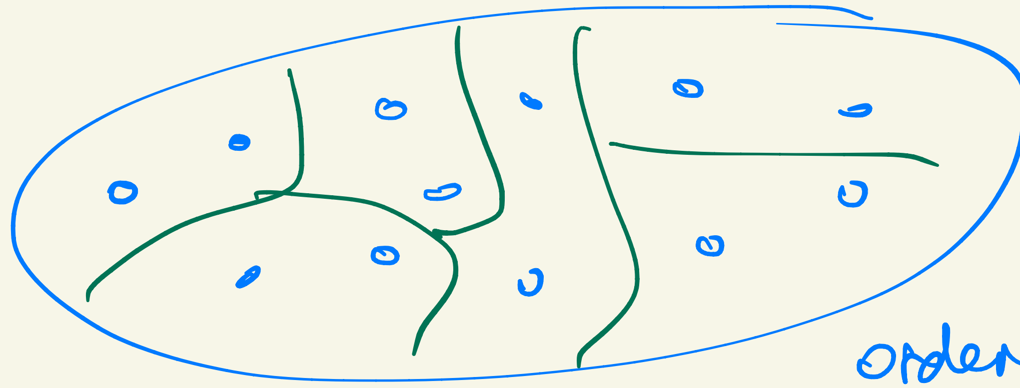
recurrence $\quad n! = n\cdot(n-1)! \quad (n\geq 1)$

"variations": picking k out of n objects <u>in order</u>

$\#$ ways to do this: $n(n-1)\cdots(n-k+1)$

$\#$ k-<u>subsets</u> of an <u>n-set</u> : set of n elements

(dealing k cards out of a deck of n cards) set of ordered hands: Ω



ordered k-tuples of distinct elements from an n-set

$$|\Omega| = n(n-1)\cdots(n-k+1)$$

$(3,1,2) \sim (1,3,2)$ equiv. rel.

equiv. classes $\longleftrightarrow$ unordered k-tuples

size of each eq. class: $k!$

uniform partition: all equiv. classes have same size

unif. partition of a set of size N
each eq. class has size K
$\Longrightarrow$ # eq. classes is N/K

$\therefore$ # k-subsets of an n-set is

$$\boxed{\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!}}$$

$k \geq 0$

$n \geq 0$

\binom{n}{k}

$$\binom{n}{0} = 1$$

$$\binom{n}{n} = 1$$

if $n < k$ then

$$\binom{n}{k} = \underline{\underline{0}}$$

$$\binom{10}{12} = \frac{10 \cdot 9 \cdot 8 \cdots 3 \cdot 2 \cdot 1 \cdot 0 \cdot (-1)}{12!}$$

$$\binom{x}{k} \stackrel{\text{def}}{=} \frac{x(x-1)\cdots(x-k+1)}{k!} \quad \leftarrow \text{polynomial of degree } \underline{\underline{k}}$$

$k \geq 0$, k integer but $x \in \mathbb{R}$ $x \in \mathbb{C}$

Newton's binomial coefficients

$\binom{n}{k} = \binom{n}{n-k}$ combinatorial proof:

bijective proof:

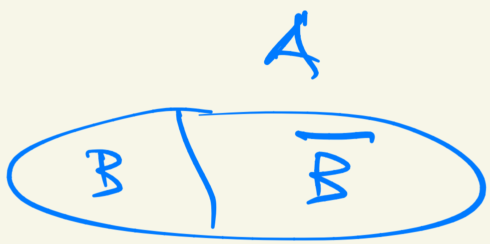
$|A| = n$

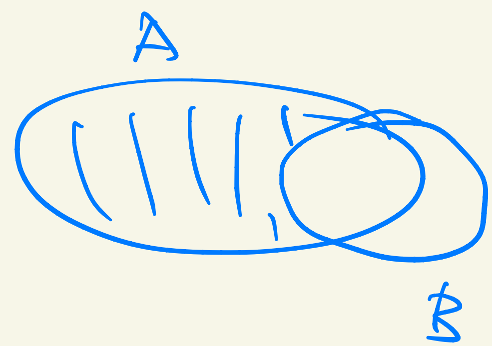
$\underline{B} \subseteq A$, $|B| = k$

$B \longmapsto \overline{B}$ <u>complement</u> of B in A

$= \underline{A \setminus B}$

$\boxed{\texttt{\textbackslash setminus} \quad \text{LaTeX}}$





<u>DO</u>

$\overline{A \cup B} = \overline{A} \cap \overline{B}$

$A, B \subseteq \Omega$

$\overline{A \cap B} = \overline{A} \cup \overline{B}$

DeMorgan's Law

$\overline{\overline{A}} = A$

$$f : A \longrightarrow B$$

$$x \in A$$

$$x \longmapsto f(x) \qquad \text{"mapsto"}$$

$$\boxed{\text{LaTeX} \quad \backslash\text{mapsto}}$$

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!}$$

$$0 \le k \le n$$

$$\binom{n}{2} = \frac{n(n-1)}{2} = \frac{n!}{2!\,(n-2)!}$$

$$\binom{0}{0}$$

$$\binom{1}{0} \quad \binom{1}{1}$$

$$\binom{2}{0} \quad \binom{2}{1} \quad \binom{2}{2}$$

$$\binom{3}{0} \quad \binom{3}{1} \quad \binom{3}{2} \quad \binom{3}{3}$$

PASCAL'S TRIANGLE

1

1 1

1 2 1

1 3 3 1

1 4 6 4 1

1 5 10 10 5 1

PASCAL'S IDENTITY

$$\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$$

HW/DO Give combinatorial proof

$\forall x,y$ $\left.\begin{array}{l} d \mid a \\ d \mid b \end{array}\right\} \Longrightarrow d \mid \underbrace{x \cdot a + y \cdot b}$

linear combination of $\underline{a}$, $\underline{b}$ with integer coefficients

BEZOUT'S LEMMA

If $\underline{d}$ is a gr.c.d. of $\underline{a}$ and $\underline{b}$ then

$(\exists x,y)(d = ax + by)$