List of Theorems for Mathematics for Informatics

Contents

1 The set of natural numbers is well-ordered.

Theorem 1. *$\mathbb{N}$ is well-ordered.*

Proof. Let A be a subset of $\mathbb{N}$ with no minimum (we need to prove that $A = \emptyset$).
$0 \notin A$, because 0 is the minimum of $\mathbb{N}$.
Set $B = \mathbb{N} \setminus A$, then $B \neq \emptyset$ and $0 \in B$. Let $m \in B$ s.t. $m < x \ \ \forall x \in A$.
Then $m+1 \in B$. Indeed assume by contradiction that $m+1 \in A$, then $m+1 \leq x \quad \forall x \in A$, then $m+1$ would be the minimum of A, but A has no minimum by assumption.
Then by the fourth Peano's axiom $B = \mathbb{N}$ and $A = \emptyset$, therefore $\mathbb{N}$ satisfies the hypothesis of the definition of well ordered set.

□

2 Theorem of existence of the quotient and the remainder in the Euclidean division between integers (aka Division Algorithm).

Theorem 2. $\forall \, n,m \in \mathbb{Z}, \ \ m \neq 0, \quad \exists! \; q \in \mathbb{Z}, \quad \exists! r \in \mathbb{N}, \; 0 \leq r < |m|, \ \ s.t.:$

$$n = mq + r$$

q is called quotient and $r = rem(n,m)$ is called remainder.

Proof. (existence)

- Assume $n \geq 0, \ \ m > 0$. By induction on n:

$$\mathbb{P}(n) = \{\exists! \; q, \; \exists! \; r \ \ 0 \leq r < |m| \text{ s.t. } n = mq + r\}$$

  $\mathbb{P}(0)$ is true, just take $q = r = 0$. Assume that $\exists \tilde{n} \geq 0$ s.t. $\mathbb{P}(\tilde{n})$ is true for $0 \leq n < \tilde{n}$.
  If $\tilde{n} < m$ we set $q = 0$ and $r = \tilde{n}$, done.
  Else if $\tilde{n} \geq m$ we consider the number $\tilde{n} - m$, which is non-negative and less than $\tilde{n}$, then by induction hypothesis:

$$\Longrightarrow \; \exists! \; \tilde{q}, \; \tilde{r} \ \text{ s.t. } \ \tilde{n} - m = m\tilde{q} + \tilde{r} \; \Longrightarrow \; \tilde{n} = m(\tilde{q}+1) + \tilde{r}$$

  Done.

- Assume $n < 0$, $m > 0$.

$$\exists! \; \tilde{q}, \tilde{r} \ \text{ s.t. } \ (-n) = m\tilde{q} + \tilde{r}$$

  If $\tilde{r} = 0$ then $n = (-\tilde{q})m$, done. Else if $\tilde{r} > 0$:

$$\Longrightarrow \; n = -m\tilde{q} - \tilde{r} + m - m = (-\tilde{q} - 1)m + (m - \tilde{r})$$

  Pick $q = (-\tilde{q} - 1)$, since $-\tilde{q} - 1 \in \mathbb{Z}$; and $r = m - \tilde{r}$, since $0 \leq m - \tilde{r} < m$, done.

- Assume $m < 0$

  $$n = (-m)q + r = (-q)m + r$$

  We already proved that $\exists! q, r$ s.t. $n = q|m| + r$. Pick $-q$, done.

(uniqueness)
Assume by contradiction that:

$$\exists\, q, q' \in \mathbb{Z} \;\; and \;\; \exists\, r, r' \in [0, |m|) \quad s.t. \quad n = mq + r = mq' + r'$$

- If $r = r' \implies m(q - q') = 0 \implies q = q'$
- If $r' > r$ then $r' - r = m(q - q') \implies 0 \leq m(q - q') < m \overset{q,q' \; integers}{\implies} q = q'$. Contradiction, $r' - r$ must be zero but we assumed $r' > r$. So $r' > r$ is impossible.
- If $r' < r$ same thing, also impossible.

Therefore q and r are indeed unique. □

3 Existence and Uniqueness of the Greatest Common Divisor.

Theorem 3. *Let $n, m \in \mathbb{Z}$, not both zero. Then $\gcd(n, m)$ exists finite and is unique.*
As a byproduct of the proof:

$$\exists\, x, y \in \mathbb{Z} \;\; s.t. \;\; \gcd(n, m) = xn + ym$$

Proof. (uniqueness)
Assume that M and M' are both greatest common divisors of n and m. By the definition of gcd:

- $(M|n \;\; and \;\; M|m) \implies M|M'$
- $(M'|n \;\; and \;\; M'|m) \implies M'|M$

Then, since gcd > 0, $M = M'$. Therefore, the $\gcd(n, m)$ is unique.

(existence)

Let $S = \{s \in \mathbb{Z}, \; s > 0 \;\; s.t. \;\; s = xn + ym, \;\; x, y \in \mathbb{Z}\}$. There is at least the element $n^2 + m^2$, since they are not both zero. Therefore, $S \neq \emptyset$.

$$S \neq \emptyset \;\; S \subseteq \mathbb{N} \implies \exists\, d = min(S)$$

Since $d \in S, \;\; \exists\, \bar{x}, \bar{y} \in \mathbb{Z} \;\; s.t. \;\; d = \bar{x}n + \bar{y}m$. It is our candidate for gcd.

We need to prove that $d|n$ and $d|m$.

By Euclidean division, $\exists! q, r \quad s.t. \quad n = qd + r$. If $r = 0$, done. Else:

$$r = n - qd = n - q(\tilde{x}n + \tilde{y}m) = n(1 + q\tilde{x}) - \tilde{y}qm$$

In particular, $n(1 + q\tilde{x}) - \tilde{y}qm \in S$. Then:

$$d = \min(S) \implies r \geq d$$

Contradiction, since we assumed that $r < d$. Then $r = 0$ and $n = qd$, therefore $d|n$ is true. Same thing for $d|m$.

Now we need to prove that $\forall c$ s.t. $c|n$ and $c|m$ we have $c|d$. Take a common divisor c of n, m. Then:

$$\exists n, k \in \mathbb{Z} \text{ s.t. } m = ch \text{ and } n = ck$$

$$d = \tilde{x}n + \tilde{y}m = \tilde{x}ch + \tilde{y}kc = (\tilde{x}h + \tilde{y}k)c \implies c|d$$

Then $d = \tilde{x}n + \tilde{y}m$ fits the definition of $\gcd(n, m)$. □

4 Existence and Uniqueness of the Least Common Multiple.

Theorem 4. *Let $n, m \in \mathbb{N}$, not both zero. Then $\text{lcm}(n, m)$ exists finite and is unique, and:*

$$\text{lcm}(n, m) = \frac{n * m}{\gcd(n, m)}$$

Proof. (uniqueness)
Assume that M and M' are both $\text{lcm}(n, m)$. By the definition of lcm:

- $(n|M \;\; and \;\; m|M) \implies M'|M$
- $(n|M' \;\; and \;\; m|M') \implies M|M'$

Then, since $\text{lcm}(n, m) \geq 0$, $M = M'$.

(existence)

By definition, $M = \text{lcm}(n, m)$ if:

1. $n|M$ and $m|M$
2. $\forall \; c \;\; s.t. \;\; n|c \;\; and \;\; m|c \;\; then \;\; M|c$

(1.)
Notice that:

$$\exists \; m', n' \;\; s.t. \;\; m = m' \gcd(n, m) \;\; and \;\; n = n' \gcd(n, m)$$

Take our candidate for $\text{lcm}(n, m)$ M as:

$$M = \frac{nm}{\gcd(n, m)} = \frac{n'm' \gcd(n, m) \gcd(n, m)}{\gcd(n, m)} = n'm' \gcd(n, m) = nm' = n'm$$

$$(M = nm' = n'm) \overset{\text{by def}}{\Longrightarrow} (n|M \;\; and \;\; m|M)$$

We proved that M is a multiple of both n and m.

(2.)

Take any $c \in \mathbb{Z}$ s.t. $n|c$ and $m|c$ (means that $\exists\, k \in \mathbb{Z}$ s.t. $c = mk$ and $\exists\, h \in \mathbb{Z}$ s.t. $c = nh$). By transitivity:

$$\gcd(n,m)|c, \text{ which means } \exists\, c' \in \mathbb{Z} \;\; s.t. \;\; c = c' \gcd(n,m)$$

We want to prove that $n'm'|c'$.

$$c = nh = hn' \gcd(n,m) \implies c' = hn' \implies n'|c'$$

$$\text{analoguely, } \; m'|c'$$

By definition of gcd:

$$\exists\, x,y \in \mathbb{Z} \;\; s.t. \;\; \gcd(n,m) = xn + ym = xn' \gcd(n,m) + ym' \gcd(n,m)$$

$$\implies xn' + ym' = 1 \implies \gcd(n',m') = 1 \implies n',m' \text{ are coprime}$$

Since $n'|c'$, $m'|c'$ and n',m' are coprime $\implies n'm'|c'$. Then:

$$n'm'|c' \implies n'm' \gcd(n,m)|c' \gcd(n,m) \implies n'm|c$$

$$\implies \frac{nm}{\gcd(n,m)}|c \implies M|c$$

Then M fits the definition of $\mathrm{lcm}(n,m)$. $\square$

5 Fundamental Theorem of Arithmetic.

Theorem 5. *Any natural number $n \geq 2$ can be written as a product of prime natural numbers, and this combination is unique up to rearrangement.*

This means that:

$$if \quad n = p_1 * p_2 * ... * p_s = q_1 * ... * q_k \ \ with \ \ p_i, q_j \ \ prime \ > 0 \ \ then:$$

$$s = k \ \ and \ there \ is \ a \ bijection \ \ \phi : \{1,...,s\} \to \{1,...,k\} \ \ s.t. \ \ \forall\, i, \ \exists\, j \ \ s.t. \ \ p_i = q_{\phi(j)}$$

Proof. (existence) By induction on n.

$$\mathbb{P}(n) = \text{"}\exists \ \ p_1, ..., p_m \ \text{ primes} > 0 \ \text{ s.t. } \ n = \prod_{i=1}^{m} p_i \text{ "}$$

$\mathbb{P}(2)$: true since 2 is prime.

Assume that $\exists\, \bar{k}$ s.t. $\mathbb{P}(k)$ is true $\forall\, k, \ 2 \leq k < \bar{k}$, prove that $\mathbb{P}(\bar{k})$ is true:

If $\bar{k}$ is prime, $\mathbb{P}(\bar{k})$ is true, done.

If $\bar{k}$ is not prime, $\exists\, d, h \ \geq 2$ s.t. $\bar{k} = dh$.

Since $d, h < \bar{k}$, by induction hypothesis $\exists\, q_1, ..., q_k$ and $\exists\, p_1, ..., p_r$ s.t. $d = q_1 * ... * q_k, \ \ h = p_1 * ... * p_r$ and $\bar{k} = q_1 * ... * q_k * p_1 * ... * p_r$, which is a product of prime numbers.

(uniqueness)

Assume that

$$n = \prod_{j=1}^{r} p_j = \prod_{i=1}^{s} q_s \quad \text{with} \quad r, s \geq 1 \quad \text{and} \quad p_j, q_i \ \text{ primes}$$

We assume that $r \leq s$. We prove uniqueness by induction on r:

$$r = 1 : n = p_1 \implies p_1 \ \ prime \implies \begin{cases} s = 1 \ \ \text{(otherwise } \ n \ \text{ would not be prime)} \\ q_1 = p_1 \end{cases}$$

Assume uniqueness holds true for any $r, \ \ 1 \leq r \leq \bar{r}$. Prove that it holds for $\bar{r}$:

$$p_{\bar{r}} \left| \prod_{j=1}^{s} q_j \right. \overset{q_j \ prime}{\Longrightarrow} \exists\, 1 \leq a \leq s \ \ s.t. \ \ p_r = q_a$$

Then:

$$p_1 * ... * \cancel{p_{\bar{r}}} = q_1 * ... * \cancel{q_a} * ... * q_s$$
$$\prod_{i=1}^{\bar{r}-1} p_i = \prod_{j=1}^{a-1} q_j * \prod_{j=a+1}^{s} q_j$$

And this is true by induction hypothesis. Therefore, it is unique $\forall\, r \in \mathbb{N}$.

$\square$

6 The Chinese Theorem of the remainder.

Theorem 6. *Given 4 integers a,b,n,m; the system of congruences:*

$$(*)\begin{cases} x \equiv a \bmod n \\ x \equiv b \bmod m \end{cases}$$

Admits solutions if and only if $\gcd(m,n)|(b-a)$.
If c is a solution, then every element of $[c]_{\mathrm{lcm}(n,m)}$ *is a solution, and there is no other solution.*

Proof. (constructive proof)
(existence)
We need to prove:

$$\text{existence} \iff \gcd(m,n)|(b-a)$$

$(\implies)$
We assume that a solution exists and prove that $\gcd(m,n)|(b-a)$.
By hypothesis, $\exists\, c \in \mathbb{Z}$ solution of $(*)$, i.e.:

$$\exists\, h,k \text{ s.t. } c = a + hn = b + km$$

Then $b-a = hn - km = (hx - kw)\gcd(n,m), \quad x,w \in \mathbb{Z}$.

$$\implies \gcd(n,m)|(b-a)$$

$(\impliedby)$
We assume that $\gcd(m,n)|(b-a)$ and prove that solution exists.
By hypothesis, $\exists\, k \;\; s.t. \;\; b-a = k\gcd(m,n) = k(m\beta + n\alpha)$. Then:

$$b - a = \alpha kn + \beta km$$

$$c = b - \beta km = a + \alpha kn$$

c is a solution, since $(b-\beta km) \bmod m = b$ and $(a+\alpha kn) \bmod n = a$
(uniqueness)
Let $M = \mathrm{lcm}(n,m)$. We want to prove that if c is a solution, then $\forall\, q \in \mathbb{Z}$, $c + qM$ is also a solution.
Assume that c and c' are two solutions.

$$\begin{aligned} c &= a + hn = b + km \\ c' &= a + h'n = b + k'm \end{aligned} \qquad \text{for some } k,k',h,h' \in \mathbb{Z}$$

$$c - c' = \begin{cases} (h-h')n \implies n|(c-c') \\ (k-k')m \implies m|(c-c') \end{cases}$$

By the definition of lcm, this implies:

$$\implies M|(c-c') \iff c-c' = \gamma M \iff c = c' + \gamma M$$

Then c and c' are in the same equivalence class, and no other solution exists.

$\square$

7 Fermat's Little Theorem

Theorem 7. *Let n be a prime (positive) number, let $a \in \mathbb{Z}$ s.t. $\gcd(a,n) = 1$. Then:*

$$a^{n-1} \equiv 1 \bmod n$$

Proof. Firstly, we need to prove that if p is prime, $\forall a \in \mathbb{N} \quad a^n \equiv a \bmod n$. By induction:

$a = 0$: true, since $0 \equiv 0 \bmod n$ is true. Assume that it's true for $\bar{n} \in \mathbb{N}$, prove for $\bar{n}+1$:

$$(a+1)^n = \sum_{k=0}^{n} \binom{n}{k} a^k = \sum_{k=1}^{n-1} \binom{n}{k} a^k + a^n + 1$$

Since $n \,\Big|\, \binom{n}{k}$ if n prime and $1 \leq k < n$:

$$\operatorname{rem}\left(\sum_{k=1}^{n} \binom{n}{k} a^k, n\right) = 0$$

By induction hypothesis:

$$\operatorname{rem}(a^n, n) = a$$

Then:

$$\sum_{k=1}^{n-1} \binom{n}{k} a^k + a^n + 1 \equiv a+1 \bmod n \implies (a+1)^n \equiv a+1 \bmod n$$

Therefore $a^n \equiv a \bmod n$ with n prime is true $\forall a \in N$.

Then we prove $a^{n-1} \equiv 1 \bmod n$:

$a = 0$: not concerned.

$a = 1$: true.

$a > 1$:

$$\gcd(a,n) = 1 \implies a \text{ cancellable mod } n \implies$$
$$a^n \equiv a \bmod n \implies a^{n-1} \equiv 1 \bmod n$$

$a < 0$:

Set $b = -a$, then:

$$\gcd(b,n) = \gcd(a,n) = 1 \implies b \text{ cancellable mod } n$$

Then:

$$b^n \equiv b \bmod n \implies b^{n-1} \equiv 1 \bmod n$$

$\square$

8 Euler-Fermat's Theorem

Theorem 8. *Let $n \in \mathbb{N}, n \geq 2$, $a \in \mathbb{Z}$ s.t.* $\gcd(n,a) = 1$. *Then:*

$$a^{\varphi(n)} \equiv 1 \bmod n$$

Proof. Let us define the function $L_a : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^*$ as:

$$L_a(x) = ax \bmod n$$

L_a is indeed well defined. Note that if a and x are invertible $\bmod n$ (they are), also their product is.

I claim that L_a is a bijection. Indeed, take $[x]_n, [y]_n \in (\mathbb{Z}/n\mathbb{Z})^*$ s.t. $L_a(x) = L_a(y)$. Then:

$$a^{-1}ax \equiv a^{-1}ay \bmod n \implies x \equiv y \bmod n \implies [x]_n = [y]_n \implies L_a \text{ injective}$$

Take some $[z]_n \in (\mathbb{Z}/n\mathbb{Z})^*$. We want to prove that:

$$\exists\, x \in (\mathbb{Z}/n\mathbb{Z})^* \ \ s.t. \ \ ax \equiv z \bmod n$$

Take $x \equiv a^{-1}z$, done.

L_a is a bijection between elements of $(\mathbb{Z}/n\mathbb{Z})^*$, therefore it is just a reshuffling of elements of the set. $\iff \exists$ bijection I from $\{1, ..., \varphi(n)\}$ to itself s.t. if b_i is the i^{th} element of $(\mathbb{Z}/n\mathbb{Z})^*$ then $L_a(b_i) = b_{I(i)}$.

$$\prod_{j=1}^{\varphi(n)} L_a(b_j) = L_a(b1) * L_a(b_2) * ... * L_a(b_{\varphi(n)}) =$$

$$= ab_1 * ab_2 * ... * ab_{\varphi(n)}$$

$$= b_{I(1)} * b_{I(2)} * ... * b_{I(\varphi(n))}$$

Then we have:

$$a^{\varphi(n)}(b_1 * ... * b_{\varphi(n)}) \equiv b_1 * ... * b_{\varphi(n)} \bmod n$$

$$b \in (\mathbb{Z}/n\mathbb{Z})^* \implies b \ \ cancellable \bmod n$$

Then:

$$a^{\varphi(n)} \equiv 1 \bmod n$$

□

9 Equivalence of the notions of Path-connectedness and Walk-connectedness in simple graphs

Theorem 9. *Let $G = (V,E)$ be a graph, let $v,w \in V$.*
v and w are path-connected if and only if they are walk-connected.

Proof. ($\Longrightarrow$)

True since a path is also a walk.

($\Longleftarrow$)

Take $P = \{p : \text{walks containing } v \text{ and } w\}$. We know by hypothesis that $P \neq \emptyset$.

Take $A = \{k \in \mathbb{N} : \ k = \text{len}(p), \ p \in P\}$.

$$A \subseteq \mathbb{N}, \, A \neq \emptyset \implies A \text{ is well-ordered}$$

$$\implies \exists \, m = min(A) \implies \exists \, p_0 \in P \; s.t. \; len(p) = m$$

We need to prove that p_0 is a path.

By contradiction, assume that $p_o = \{v_0 = v, ..., v_m = w\}$ is not a path. This means that there exist $i, j \quad i < j$ s.t. $v_i = v_j$. Now define $\bar{p} = \{v_0, .., v_i = v_j, v_{j+1}, .., v_m\}, \ \bar{p} \in P$.

$$\text{len}(\bar{p}) < (\text{len}(p) = m)$$

Contradiction, p_0 is not the minimum walk. This means that such i and j do not exist, thus p_0 is a path. □

10 A graph *G=(V,E)* is 2-connected if and only if, for every two vertices *v,w* in *G*, *v* different from *w*, there exists a cycle in *G* containing *v* and *w*.

Theorem 10. *Let G=(V,E) be a graph, #V ≥ 3. Then:*
G is 2-connected if and only if $\forall \, v,w \in V, v \neq w \quad \exists$ a cycle in G containing both v and w.

Proof. ($\Longleftarrow$)

Assume that $\forall \, v,w \in V, v \neq w \ \exists \, C$ cycle containing v and w.

$$C = (v, u_1, ..., u_k, w, u_r, ..., u_s, v)$$

If any node is removed ($\neq v,w$), v and w are still connected, therefore G is 2-connected.

($\Longrightarrow$)

Assume that G is 2-connected.

We define $\text{dist}(v,w) = \min\{\text{len}(p) : p \text{ path connecting } v,w\}$, if such set is empty, we set $\text{dist}(v,w) = +\infty$. By induction on $k = \text{dist}(v,w)$:

Let $k = 1$. Take v, w s.t. $\text{dist}(v, w) = 1$.

$$\text{dist}(v, w) = 1 \iff \text{node } \eta = \{v, w\} \in E$$

Consider $G - \eta$. I claim that $G - \eta$ is connected. Indeed, assume by contradiction that $G - \eta$ is disconnected, then it has at least 2 connected components A_1 and A_2. One of them contains v, the other one contains w. Assume that the component containing v has at least one other node u (we can do this assumption because we know that $\#V \geq 3$).
Consider $G - v$. Since it is connected by hypothesis, i can connect u and w, but since u does not belong to the connected component containing w, then i cannot connect u and w. So there is a contradiction, therefore $G - \eta$ must be connected.

$$G - \eta \text{ connected } \implies \exists\, p = (v, y_1, ..., y_s, w) \text{ path in } G - \eta \text{ connecting } v \text{ and } w$$

Then $C = (v, y_1, ..., y_s, w, v)$ is a cycle in G containing v and w. Therefore it is true for $k = 1$.
Assume that $\exists\, k \geq 1$ s.t. $\forall\, v, w \in V : \text{dist}(v, w) = k$ i can find a cycle containing them.
Now prove that $\forall\, v, w \in V : dist(v, w) = k + 1$ i can find a cycle containing them.

$$\text{dist}(v, w) = k + 1 \implies \exists\, p = (v, \alpha_1, ..., \alpha_k, w)$$

By induction hypothesis $\exists\, C$ cycle containing v and α_k:

$$C = (v, u_1, \ldots, u_r, \alpha_k, u_{r+2}, \ldots, u_s, v)$$

Call:

$$p_1 = (v, u_1, \ldots, u_r, \alpha_k) \quad p_2 = (\alpha_k, u_{r+2}, \ldots, u_s, v)$$

$G - \alpha_k$ is connected by hypothesis $\implies \exists\, \bar{p}$ connecting v and w.
Call this path $\bar{p} = (v = \beta_0, ..., \beta_t, w)$.
Let q be the largest index s.t. $0 \leq q \leq t$ and $\beta_q \in C$. (there is at least $v = \beta_0$ in C)
Assume $\beta_q \in p_1$, then i construct the following walk:

$$(\text{elements of } p_1 \text{ until } \beta_q, \beta_q + 1, ..., \beta_t, w, \text{ the whole } p_2)$$

This is a cycle containing v and w.
Assume $\beta_q \notin p_1$, then $\beta_q \in p_2$, repeat the same construction.
Therefore we have the thesis. $\square$

11 Theorem of characterization of trees.

Theorem 11. *Let T=(E,V) be a graph. The following are equivalent:*

1. *T is a tree*
2. $\forall\, v, v' \in V,\quad \exists!$ *path connecting v and* v'
3. *T is connected and* $\forall\, e \in E$*,* $T - e$ *is disconnected*
4. *T has no cycles and* $\forall\, e \in \binom{V}{2}$*,* $e \notin E$*,* $T + e$ *has a cycle*

Proof. ($1. \implies 2.$) Assume T is a tree.

Choose $v \neq v' \in V$. Let $p = (v_0 = v, v_1, \ldots, v_r = v')$. p is a path connecting v and v'. This path exists since T is a tree, therefore is connected.
By contradiction, assume that there exists $\bar{p}$ path in T s.t.:

$$\bar{p} = (u_0 = v, u_1, \ldots, u_s = v'),\; p \neq \bar{p}$$

Let $\bar{j} \in \{1, .., s-1\}$ the smallest index s.t. $u_{\bar{j}} \neq v_{\bar{j}}$.
Let $\bar{k} \in \{\bar{j}+1, ..., s\}$ the smallest index greater than $\bar{j}$ s.t. $u_{\bar{k}} = v_{\bar{k}}$
Then there is a cycle:

$$C = (u_{\bar{j}-1}, u_{\bar{j}}, ..., u_{\bar{k}} = v_{\bar{k}}, v_{\bar{k}-1}, ..., v_{\bar{j}}, u_{\bar{j}-1})$$

Contradiction with the assumption that T is a tree. Therefore, such path $\bar{p}$ does not exists and we have the thesis.

($2. \implies 3.$)

T is connected by hypothesis. Choose any $e = \{v_1, v_2\} \in E$. Remove e, then by hypothesis there is no way to connect v_1 and v_2, this implies that $T - e$ is disconnected.

($3. \implies 4.$)

Assume by contradiction that $C = (v_0, v_1, \ldots, v_r, v_0)$ is a cycle in T.

Remove the edge $e = \{v_0, v_1\}$.

Choose $w, w' \in V(T)$. By connectedness, there is path $p = (w_0 = w, \ldots, w_q = w')$ connecting w and w' in T.

- If e is not an edge of the path, nothing to prove: T still contains a path with w and w' and we have a contradiction.
- If e is an edge on the path, $\exists\, j \in \{1, \ldots, q-1\}:\; v_0 = w_j, v_1 = w_{j+1}$.

Take the path $(w = w_0, \ldots, w_j = v_0, v_r, v_{r-1}, \ldots, v_1 = w_{j+1}, w_{j+2}, \ldots, w_q = w')$. Then $T - e$ is connected. Contradiction with the hypothesis that $T - e$ is disconnected. Then T has no cycles.

Now we need to prove that $\forall e \in \binom{V}{2}, e \notin E$, $T+e$ has a cycle. Let $v_a, v_b \in V$ s.t. $e = \{v_a, v_b\} \notin E$. By definition, T is connected, i.e. $\exists p = (v_a, v_1, \ldots, v_i = v_b)$ path. Then $(v_a, v_1, \ldots, v_i = v_b, v_a)$ is a cycle in $T+e$ and we have the thesis.

(4. $\implies$ 1.)

T has no cycles by hypothesis. We need to prove that T is connected.

Take $v, v' \in V$ such that $e = \{v, v'\} \notin E$ (since if we take two vertices connected by an edge, then the edge is the path and we have nothing to prove) and consider $T+e$. $T+e$ contains a cycle by hypothesis and I claim that e is contained in the cycle, this means that there is a cycle $C = (v, v', w_1, \ldots, w_k, v)$ in $T+e$. But this means that there is a path between v and v' in T, therefore T is a tree. □

12 Theorem of characterization of finite trees (with Euler formula).

Theorem 12. *Let T=(V,E) be a finite graph. Then the following are equivalent:*

1. *T is a tree*

5. *$|V| - 1 = |E|$ (Euler's formula) and T is connected.*

   ($|V| - 1 = |E| \iff |V| - 1 = \frac{1}{2}\sum_{i=1}^{n} \deg(v_i)$)

Proof. (1. $\implies$ 5.)

Assume T is a tree.

By induction on $n = |V|$.

$n = 1, 2$ Euler's formula is trivial, holds true.

Assume that $\exists k \geq 2$ s.t. $\forall$ trees with $|V| = k$ Euler's formula is true. Let T be a tree with $|V| = k+1$. Prove that Euler's formula is true for T.

Since a tree with $|V| > 1$ has at least 2 leaves, $\exists\, v_a \in V(T)$ which is a leaf. $T - v_a$ is a tree with k verteces. By induction hypothesis $|V(T - v_a)| = |E(T - v_a)| + 1$. Then:

$$|V(T - v_a)| = |E(T - v_a)| + 1 \implies |V(T)| - 1 = |E(T)|$$

By induction hypothesis we have the thesis.

(5. $\implies$ 1.)

Assume that T is a connected graph with $|V| - 1 = |E|$.

By induction on $|V| = k$. For $k = 1, 2$, T satisfying 5. is a tree.

Assume that $\exists\, k \geq 2$ s.t. every connected finite graph satisfying Euler's formula is also a tree and consider a connected graph T with $|V(T)| = k+1$ satisfying Euler's formula.

First, I prove that T has at least 1 leaf. Indeed:

$$T \text{ has no leaves } \implies \forall i \ \ \deg(v_i) \geq 2 \implies \sum_{i=0}^{k+1} \deg(v_i) \geq 2(k+1)$$

Contradiction, because by hypothesis T must satisfy Euler's formula. Therefore, $\exists\, v_a \in V(T)$ leaf. Consider now $T - v_a$. It has k vertices and is connected.

$$|V(T-v_a)| = k \qquad |E(T-v_a)| = |E(T)| - 1 = k-1$$

$$\implies T - v_a \quad satisfies\ \ Euler's\ \ formula$$

By induction hypothesis, it is a tree.
Since v_a is a leaf, also T is a tree. By induction hypothesis, 5. $\implies$ .1. □

13 Every connected finite graph has a spanning tree.

Theorem 13. *Let G=(V,E) be a connected finite graph, then it has a spanning tree.*

Proof.

$$C = \{G' \text{ subgraph of } G : G' \text{ connected, } V(G) = V(G')\}$$

$$G \in C \implies C \neq \emptyset$$

Take A as:

$$A = \{n \in \mathbb{N} : n = |E(G')|,\ G' \in C\}, \quad A \neq \emptyset \text{ since } C \neq \emptyset$$

$$A \subseteq \mathbb{N},\ A \neq \emptyset \implies A \text{ well ordered } \implies$$

$$\implies \exists\, m = \min(A) \implies \exists\, T \in C\ \ s.t.\ \ |E(T)| = m$$

We use the characterization of trees 1. $\iff$ 3., which is:

$$T \text{ is a tree } \iff T \text{ is connected and } \forall\, e \in E(T)\ \ T - e \text{ is disconnected}$$

Assume by contradiction that T is not a tree. Then:

$$\exists\, \bar{e} \text{ s.t. } T - \bar{e} \text{ is connected}$$

But then:

$$(T - \bar{e}) \in C \quad and \quad |E(T - \bar{e})| < |E(T)| = m$$

is a contradiction. Then T is a tree. □