$\boxed{12.3. (c)}$ Prove, with a derivation, that the following formula is a tautology.

$(P \Rightarrow Q) \Rightarrow ((P \wedge R) \Rightarrow (Q \wedge R))$

{Assume}

(1) $\boxed{P \Rightarrow Q}$

{Assume}

(2) $\boxed{P \wedge R}$

{$\wedge$-elim. on (2)}

(3) P

{$\wedge$-elim. on (2)}

(4) R

{$\Rightarrow$-elim. on (1) and (3)}

(5) Q

{$\wedge$-intro on (4) and (5)}

(6) $Q \wedge R$

{$\Rightarrow$-intro on (2) and (6)}

(7) $(P \wedge R) \Rightarrow (Q \wedge R)$

{$\Rightarrow$-intro on (1) and (7)}

(8) $(P \Rightarrow Q) \Rightarrow ((P \wedge R) \Rightarrow (Q \wedge R))$

$\boxed{15.6.\ (6)}$ $\exists x[P(x) \vee Q(x)] \Rightarrow (\exists x[P(x)] \vee \exists x[Q(x)])$

(Prove the tautology using derivations)

{Assume}

(1) $\boxed{\exists x[P(x) \vee Q(x)]}$

{Assume}

(2) $\boxed{\neg \exists x[P(x)]}$

{negation on (2)}

(3) $\exists x[P(x)] \Rightarrow F$

{De Morgan on (2)}

(4) $\forall x[\neg P(x)]$

{$\exists x$ - elim. on (1)}

(5) Pick a with $P(a) \vee Q(a)$

{$\forall$-elim. on (4) and (5)}

(6) $\neg P(a)$

{implication on (5)}

(7) $\neg P(a) \Rightarrow Q(a)$

{$\Rightarrow$ -elim. on (7) and (6)}

(8) $Q(a)$

{$\exists x$-intro}

(9) $\exists x[Q(x)]$

{$\Rightarrow$-intro on (2) and (9)}

(10) $\neg \exists x[P(x)] \Rightarrow \exists x[Q(x)]$

{implication on (10)}

(11) $\exists x[P(x)] \vee \exists x[Q(x)]$

{$\Rightarrow$ -intro on (1) and (11)}

(12) $\exists x[P(x) \vee Q(x)] \Rightarrow (\exists x[P(x)] \vee \exists x[Q(x)])$

15.9 Prove the following tautology via logical derivations.

$$(\forall x[x \in \mathbb{N} : P(x)] \Rightarrow \exists y[y \in \mathbb{N} : Q(y)]) \Rightarrow \exists z[z \in \mathbb{N} : P(z) \Rightarrow Q(z)]$$

Here is first a solution in which we also actually use Leibnitz and calculations (steps marked with "*" on the left)

1

{Assume}

(1) $\forall x[x \in \mathbb{N} : P(x)] \Rightarrow \exists y[y \in \mathbb{N} : Q(y)]$

{Assume}

(2) $\forall z[z \in \mathbb{N} : \neg(P(z) \Rightarrow Q(z))]$

{implication + De Morgan on (2)}

* (3) $\forall z[z \in \mathbb{N} : P(z) \wedge \neg Q(z)]$

{term splitting on (3)}

(4) $\forall z[z \in \mathbb{N} : P(z)] \wedge \forall z[z \in \mathbb{N} : \neg Q(z)]$

{$\wedge$-elim. on (4)}

(5) $\forall z[z \in \mathbb{N} : P(z)]$

{$\Rightarrow$-elim. on (1) and (5)}

(6) $\exists y[y \in \mathbb{N} : Q(y)]$

{$\wedge$-elim. on (4)}

(7) $\forall z[z \in \mathbb{N} : \neg Q(z)]$

{de Morgan on (7)}

(8) $\neg \exists z[z \in \mathbb{N} : Q(z)]$

{$\wedge$-intro on (6) and (8), contradiction}

(9) F

{$\Rightarrow$-intro on (2) and (9), negation, de Morgan}

(10) $\exists z[z \in \mathbb{N} : P(z) \Rightarrow Q(z)]$

{$\Rightarrow$-intro on (1) and (10)}

(11) $(\forall x[x \in \mathbb{N} : P(x)] \Rightarrow \exists y[y \in \mathbb{N} : Q(y)]) \Rightarrow$
$\exists z[z \in \mathbb{N} : P(z) \Rightarrow Q(z)]$

(15.9 still - another solution)

If we do not use calculations, in particular not Leibnitz, then we can do a proof by derivations using case distinction.

i.e. using the tautology $((P \vee Q) \wedge (P \Rightarrow R) \wedge (Q \Rightarrow R)) \Rightarrow R$

②

{Assume}

(1) $\boxed{\forall x [x \in \mathbb{N} : P(x)] \Rightarrow \exists y [y \in \mathbb{N} : Q(y)]}$

{impl. on (1)}

(2) $\neg \forall x [x \in \mathbb{N} : P(x)] \vee \exists y [y \in \mathbb{N} : Q(y)]$

{Assume}

(3) $\boxed{\neg \forall x [x \in \mathbb{N} : P(x)}$

{de Morgan on (3)}

(4) $\exists x [x \in \mathbb{N} : \neg P(x)]$

{$\exists$* - elim. on (4)}

(5) Pick a with $\neg P(a)$, $a \in \mathbb{N}$

{$\wedge$-$\vee$- weakening on (5)}

(6) $\neg P(a) \vee Q(a)$

{impl. on (6)}

(7) $P(a) \Rightarrow Q(a)$

{$\exists$* - intro on (7)}

(8) $\exists z [z \in \mathbb{N} : P(z) \Rightarrow Q(z)$

{$\Rightarrow$ -intro on (3) and (8)}

(9) $\neg \forall x [x \in \mathbb{N} : P(x)] \Rightarrow \exists z [z \in \mathbb{N} : P(z) \Rightarrow Q(z)]$

{Assume}

(10) $\boxed{\exists y [y \in \mathbb{N} : Q(y)]}$

{$\exists$* - elim. on (10)}

(11) Pick b with $Q(b)$, $b \in \mathbb{N}$

{$\wedge$-$\vee$- weakening on (11)}

⊙*

(12) $\neg P(b) \vee Q(b)$

{implication on (12)}

(13) $P(b) \Rightarrow Q(b)$

{$\exists x$-intro on (13)}

(14) $\exists z[z \in \mathbb{N} : P(z) \Rightarrow Q(z)]$

{$\Rightarrow$-intro on (10) and (14)}

(15) $\exists y[y \in \mathbb{N} : Q(y)] \Rightarrow \exists z[z \in \mathbb{N} : P(z) \Rightarrow Q(z)]$

{case distinction on (2), (9), (15),
$\Rightarrow$-elimination with the subsitution
$\neg\forall x[x \in \mathbb{N} : P(x)]$ for P
$\exists y[y \in \mathbb{N} : Q(y)]$ for Q and
$\exists z[z \in \mathbb{N} : P(z) \Rightarrow Q(z)]$ for R}

(16) $\exists z[z \in \mathbb{N} : P(z) \Rightarrow Q(z)]$

{$\Rightarrow$-intro on (1) and (16)}

(17) $\left(\forall x[x \in \mathbb{N} : P(x)] \Rightarrow \exists y[y \in \mathbb{N} : Q(y)]\right) \Rightarrow$
$\exists z[z \in \mathbb{N} : P(z) \Rightarrow Q(z)]$

and we have the full proof only with derivations.

16.12 Prove or give a counter example

(a) $A \times B = B \times A$

This statement does not hold for any A, B - sets.

For example, take $A = \{0\}$, $B = \{1\}$. Then

$$A \times B = \{(0,1)\} \neq \{(1,0)\} = B \times A.$$

(b) $A \subseteq B \Rightarrow A \times C \subseteq B \times C$

This statement is true for any sets A, B, C. Here is a proof:

Assume $A \subseteq B$. Let $(a,c) \in A \times C$.

Then $a \in A$ and from $A \subseteq B$, we have $a \in B$.

Also, from $(a,c) \in A \times C$, we have $c \in C$.

Hence $(a,c) \in B \times C$.

We have proven that under the assumption $A \subseteq B$, it holds that $A \times C \subseteq B \times C$.

Hence $A \subseteq B \Rightarrow A \times C \subseteq B \times C$ holds.

(c) $A \times B = C \times D \Rightarrow A = C$

This statement does <u>not</u> hold in general. Here is a counter-example. Take

$$B = D = \emptyset, \quad A = \{0\}, \quad C = \{1\}.$$

Then $A \times B = \emptyset = C \times D$. But, obviously, $A \neq C$.

$\boxed{18.8}$ (b) Let $f: A \to B$ be an injection and $S, T \subseteq A$. Then we will prove that $f(S \setminus T) = f(S) \setminus f(T)$

Here is the proof:

From task 18.3. (c) we have that for any mapping $f: A \to B$ (hence not necessarily an injection) and $S, T \subseteq A$,

$$f(S) \setminus f(T) \subseteq f(S \setminus T):$$

We still need to show the opposite inclusion.

So, let $y \in f(S \setminus T)$. Then there exists an $x \in S \setminus T$ such that $y = f(x)$. From $x \in S \setminus T$ we have that $x \in S$ and $x \notin T$, hence $x \in S$.

Now from $x \in S$ and $y = f(x)$, we get $y \in f(S)$.

We still need to show that $y \notin f(T)$.

Assume, towards a contradiction, that $y \in f(T)$.

Then there is a $t \in T$ with $y = f(t)$.

Hence (since also $y = f(x)$) we have

$$f(x) = f(t).$$

Since f is an injection, this yields that $x = t$.

But we already know that $x \notin T$ and $t \in T$, which together with $x = t$ yields $x \notin T$ and $x \in T$, a contradiction!

Hence our assumption was wrong, i.e., $y \notin f(T)$.

We have shown that $y \in f(S)$, $y \notin f(T)$, i.e., $y \in f(S) \setminus f(T)$ and this completes the proof.

18.10

Let V be a finite set. A bijection $f: V \to V$ is called a permutation.

①

(a) Give all permutations of $\{1, 2, 3\}$.

So, we need all bijections $f: \{1,2,3\} \to \{1,2,3\}$

Since we have maps of finite sets, it is handy to use the following notation: $f = \begin{pmatrix} 1 & 2 & 3 \\ f(1) & f(2) & f(3) \end{pmatrix}$

So we have:

$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ $f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ $f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ $f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

(b) which permutations are inverses of each other?

$f_1^{-1} = f_1, \; f_2^{-1} = f_2, \; f_4^{-1} = f_4, \; f_6^{-1} = f_6$

and $f_3^{-1} = f_5, \; f_5^{-1} = f_3$

(c) If V has n element, how many mappings are there from V t V? How many permutations on V?

Mappings there are n^n. In general, by B^A we denote the set of all mappings from A to B, i.e. $B^A = \{f \mid f: A \to B\}$. If $|A| = n$, $|B| = m$, then $|B^A| = m^n$ which justifies the notation also.

Why? Take an element in A (or V), say $a \in A$. There are $|B|$ possibilities for $f(a)$. Each choice is good. So, if we have $A = V$ with $|V| = n$, and $B = V$ with $|V| = n$, then

There are n^n mappings.

any choice for an element $a \in V$ can be combined with any choice for an element $b \in V$, $b \neq a$.

When is comes to permutations, the choice is restricted and the total number (on V) is $n! = n \cdot (n-1) \cdots 2 \cdot 1$

Why?

We pick first an element $a_1 \in V$. There are n possibilities for $f(a_1)$. Then we take another element $a_2 \in V, a_2 \neq a_1$.

Since $f(a_1)$ is already fixed, possible values for $f(a_2)$ are all elements in $V \setminus \{f(a_1)\}$ and there are $n-1$ such.

Once, we have picked $f(a_2)$, we take $a_3 \in V, a_3 \notin \{a_1, a_2\}$ and are left with $n-2$ possibilities, namely all elements in $V \setminus \{f(a_1), f(a_2)\}$, and so on.

When $f(a_1), \dots, f(a_{n-1})$ are fixed, there remains a unique element for $f(a_n)$.

Hence, the total number of permutations is

$$n \cdot (n-1) \cdot (n-2) \cdots 1$$

the unique poss. for $f(a_n)$.

poss. for $f(a_3)$

poss. for $f(a_2)$

possibilities for $f(a_1)$

and this is $n!$.

$\boxed{19.13}$ Let $L = \{x, y, z\}$ be the set of letters.

The formula set M is given by the following inductive definition: (1)

__Basis__ : - Every $l \in L$ is element of M

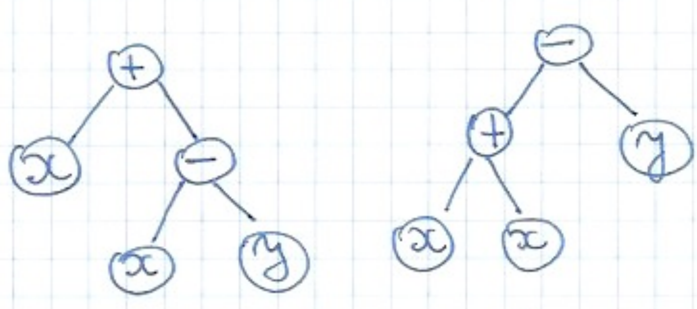
__Step__ : - (Case 1) if $e_1 \in M$ and $e_2 \in M$, then $e_1 + e_2 \in M$

- (Case 2) if $e_1 \in M$ and $e_2 \in M$, then $e_1 - e_2 \in M$.

(a) Is there for every formula in M only one construction tree possible?

(b) Prove by structural induction that in every formula of M the number of "+" and "−" symbols __together__ are one less then the number of letters in the formula.

(a) The answer is no. For example
$x + x - y$ is a formula and it can be constructed by the following two different construction trees



The reason is that our formulae do not include parenthesis, i.e. there is no unique "top" symbol (+ or −) in a formula.

(b) To be fully precise, we first define (inductively also) the set of all finite words over the alphabet $\hat{L} = \{x, y, z, +, -\}$. ②

notation $\hat{L}^*$

The definition is as follows

<u>Base</u> : $\varepsilon \in \hat{L}^*$

<u>Step</u> : If $w \in \hat{L}^*$ and $a \in \hat{L}$, then $aw \in \hat{L}^*$.

Then we define precisely two functions

$$\#_{+-} : \hat{L}^* \to \mathbb{N} \quad \text{and} \quad \#_{\ell} : \hat{L}^* \to \mathbb{N}$$

that count the number of "+" and "−" signs together, and the number of letters $l \in L$, respectively, in a finite word over $\hat{L}$. The definition is inductive as well. We have

$$\#_{+-}(\varepsilon) = 0 \;, \quad \#_{+-}(aw) = \begin{cases} \#_{+-}(w) \;, & a \notin \{+,-\} \\ \#_{+-}(w)+1, & a \in \{+,-\} \end{cases}$$

for $a \in \hat{L}$, $w \in \hat{L}^*$.

and

$$\#_{\ell}(\varepsilon) = 0 \;, \quad \#_{\ell}(aw) = \begin{cases} \#_{\ell}(w), & l \notin L \\ \#_{\ell}(w)+1, & l \in L \end{cases}$$

again for $a \in \hat{L}$, $w \in \hat{L}^*$.

Now, it is important to notice that

$M \subseteq \hat{L}^*$, and our task is to prove

that $\forall e\,[e \in M : \#_{+-}(e) = \#_{\ell}(e) - 1]$

This we show by structural induction (on the structure of formulas in M).

We have

Base: $e = \ell \in L$.

Then $\#_{+-}(e) = 0$ and $\#_\ell(e) = 1$ and the property holds, since $\#_{+-}(e) = 0 = 1-1 = \#_\ell(e) - 1$.

Induction hypothesis: Assume that the property holds for e_1, e_2, that is $\#_{+-}(e_1) = \#_\ell(e_1) - 1$
$\#_{+-}(e_2) = \#_\ell(e_2) - 1$.

Induction step:

(Case 1) We consider $e = e_1 + e_2$.

Then $(*)$ $\#_{+-}(e) = \#_{+-}(e_1) + \#_{+-}(e_2) + 1$

and $(**)$ $\#_\ell(e) = \#_\ell(e_1) + \#_\ell(e_2)$.

So,
$$\begin{aligned}\#_{+-}(e) &= \#_{+-}(e_1) + \#_{+-}(e_2) + 1 \\ &\overset{(IH)}{=} \#_\ell(e_1) - 1 + \#_\ell(e_2) - 1 + 1 \\ &= \#_\ell(e) - 1\end{aligned}$$

(Case 2) - completely analogous, $e = e_1 - e_2$.

Then
$$\begin{aligned}\#_{+-}(e) &= \#_{+-}(e_1) + \#_{+-}(e_2) + 1 \\ &\overset{IH}{=} \#_\ell(e_1) - 1 + \#_\ell(e_2) - 1 + 1 \\ &= \#_\ell(e) - 1\end{aligned}$$

To be fully precise (over pedantic) we need to also prove $(*)$ and $(**)$. These are properties of $\#_{+-}$, $\#_\ell$ and will be proven by induction $\longrightarrow$ structural induction of L^*

and can also be done by natural induction on the length of words in $\hat{\Sigma}^*$.

[we stick to the structural induction]

Both are instances of the following property

⦿ for all $v, w \in \hat{\Sigma}^*$, we have

$$\#_{+-}(vw) = \#_{+-}(v) + \#_{+-}(w)$$

and $$\#_e(vw) = \#_e(v) + \#_e(w).$$

where vw denotes the concatenation of v and w.

Proof: By induction on the structure (equivalently, length of v)

Base: $v = \varepsilon$. Then $vw = w$ and

$$\#_{+-}(vw) = 0 + \#_{+-}(w) = \#_{+-}(v) + \#_{+-}(w).$$

$$\#_e(vw) = \#_e(w) = 0 + \#_e(w) = \#_e(v) + \#_e(w).$$

Inductive hypothesis: Assume the property holds for u, that is

$$\#_{+-}(uw) = \#_{+-}(u) + \#_{+-}(w)$$

$$\#_e(uw) = \#_e(u) + \#_e(w).$$

Inductive step: Let $v = au$ for $a \in \hat{\Sigma}$ (and from the IH the property holds for u)

Then $vw = (au)w = a(uw)$ and

$$\#_{+-}(vw) = \begin{cases} 1 + \#_{+-}(uw) & \text{, if } a \in \{+,-\} \\ \#_{+-}(uw) & \text{, if } a \notin \{+,-\} \text{ i.e. } a \in \{x,y,z\} \end{cases}$$

$$\overset{IH}{=} \begin{cases} 1 + \#_{+-}(u) + \#_{+-}(w) & \text{, if } a \in \{+,-\} \\ \#_{+-}(u) + \#_{+-}(w) & \text{, if } a \in \{x,y,z\} \end{cases}$$

and since

$$\#_{+-}(v) = \begin{cases} 1 + \#_{+-}(u), & \text{if } a \in \{+,-\} \\ \#_{+-}(u), & \text{if } a \in \{x,y,z\} \end{cases}$$

we get that $\#_{+-}(vw) = \#_{+-}(v) + \#_{+-}(w)$.

Analogously, one proves that

$$\#_e(uw) = \#_e(u) + \#_e(w).$$

Finally, for completeness, we include the inductive definition (structural induction / induction on the length of u) of uv:

<u>Base</u>: If $u = \varepsilon$, then $uv = v$

<u>Step</u>: If $u = au'$, then $uv = a(u'v)$.

With this we have a fully precise treatment of this problem. I have written it like this to provide you with more examples of inductive definitions and proofs.

This is not exactly necessary (or expected) from this task, so here (see next page) is the shorter solution in which we hide all details about $\#_{+-}$, $\#_e$ and uv.

19.13 – shorter solution (not so detailed)

(b) Let $\#_{+-}(e)$ denote the number of + and – (together) symbols in a formula e of M.

Let $\#_\ell(e)$ denote the number of letters in a formula e of M.

We prove that $\#_{+-}(e) = \#_\ell(e) - 1$ by structural induction on e in M.

Base: $e = \ell \in L$.

Then $\#_{+-}(e) = 0$, $\#_\ell(e) = 1$ and it holds

$$\#_{+-}(e) = 0 = 1 - 1 = \#_\ell(e) - 1.$$

Step: (Case 1) Let $e = e_1 + e_2$, and assume that the property holds for e_1, e_2 (any formula simpler than e)

Then
$$\begin{aligned}\#_{+-}(e) &= \#_{+-}(e_1) + 1 + \#_{+-}(e_2)\\ &\overset{IH}{=} \#_\ell(e_1) - 1 + 1 + \#_\ell(e_2) - 1\\ &= \#_\ell(e_1 + e_2) - 1 = \#_\ell(e) - 1\end{aligned}$$

(Case 2) Let $e = e_1 - e_2$, and again by the IH. the property holds for e_1 and e_2.

Then (analogously)
$$\begin{aligned}\#_{+-}(e) &= \#_{+-}(e_1) + 1 + \#_{+-}(e_2)\\ &\overset{IH}{=} \#_\ell(e_1) - 1 + 1 + \#_\ell(e_2) - 1\\ &= \#_\ell(e_1 - e_2) - 1 = \#_\ell(e) - 1.\end{aligned}$$

and this completes the proof.