

CPSC-354 Report

Nikolai Semerdjiev
Chapman University

October 16, 2025

Abstract

Contents

1	Introduction	2
2	Week by Week	2
2.1	Week 1	2
2.1.1	Notes and Exploration	2
2.1.2	Homework	2
2.1.3	Questions	2
2.2	Week 2	2
2.2.1	Homework	2
2.2.2	Questions	5
2.3	Week 3	6
2.3.1	Homework	6
2.3.2	Questions	7
2.4	Week 4	7
2.4.1	Homework	7
2.4.2	Questions	8
2.5	Week 5	9
2.5.1	Homework	9
2.5.2	Questions	10
2.6	Week 6	10
2.6.1	Homework	10
2.6.2	Questions	11
2.7	Week 7	11
2.7.1	Homework	11
2.7.2	Questions	16
2.8	Week 8	16
2.8.1	Homework	16
2.8.2	Questions	18
3	Essay	18
4	Evidence of Participation	18
5	Conclusion	18

1 Introduction

2 Week by Week

2.1 Week 1

2.1.1 Notes and Exploration

In Week 1, we began with the MIU (or MU) puzzle from Hofstadter's *Gödel, Escher, Bach*. This puzzle introduces the idea of formal systems and rules of inference. It is a good starting point to think about what it means to derive a string from an axiom under a fixed set of rules.

The MU Puzzle

RULES:

1. (Append-U) If a string ends with I, you may append U:
 $xI \rightarrow xIU$.
2. (Double) From Mx you may produce Mxx :
 $Mx \rightarrow Mxx$.
3. (III \rightarrow U) Replace any occurrence of III with U:
 $xIIIy \rightarrow xUy$.
4. (Delete UU) Delete any occurrence of UU:
 $xUUY \rightarrow xy$.

2.1.2 Homework

Problem: Can you derive MU from MI?

Solution: No, it is impossible to derive MU from MI. At first, playing around with the rules, I noticed that the goal was to create the correct number of I's so that they could be converted to a single U. This means we would need $N_I \bmod 3 = 0$, where N_I counts the I's.

Now, consider how each rule affects N_I :

- **(Append-U)** Appends a U, leaves N_I unchanged.
- **(Double)** $Mx \rightarrow Mxx$ doubles N_I ; in modular arithmetic, $N_I \mapsto 2N_I \pmod{3}$.
- **(III \rightarrow U)** Removes three I's, leaving $N_I \bmod 3$ unchanged.
- **(Delete UU)** Only touches U's, leaves N_I unchanged.

Starting from MI, we have $N_I = 1 \equiv 1 \pmod{3}$. Doubling cycles between 1 and 2 modulo 3, never producing 0. Thus, it is impossible to reach $N_I \equiv 0 \pmod{3}$.

Since MU has $N_I = 0$, it cannot be derived from MI.

2.1.3 Questions

What is the reasoning behind being able to convert MIII into MU (using the rule $III \rightarrow U$) but not being able to go the other way (from MU to MIII)?

2.2 Week 2

2.2.1 Homework

Problem: Consider the following ARSs. Draw a picture for each one. Are the ARSs terminating? Are they confluent? Do they have unique normal forms?

1. $A = \{\}, \quad R = \{\}$
2. $A = \{a\}, \quad R = \{\}$
3. $A = \{a\}, \quad R = \{(a, a)\}$
4. $A = \{a, b, c\}, \quad R = \{(a, b), (a, c)\}$
5. $A = \{a, b\}, \quad R = \{(a, a), (a, b)\}$
6. $A = \{a, b, c\}, \quad R = \{(a, b), (b, b), (a, c)\}$
7. $A = \{a, b, c\}, \quad R = \{(a, b), (b, b), (a, c), (c, c)\}$

Solution: For each ARS, I drew a graph (see figures) and analyzed:

- **Termination:** whether there are infinite chains. - **Confluence:** whether every divergence can rejoin.
- **Unique normal forms:** whether each element has a unique NF.

I will include one diagram for each ARS along with a short explanation of my analysis.

ARS 1: $A = \{\}, R = \{\}$ There is no infinite chain, no diverging paths exist as there is no path at all, and nothing exists to violate uniqueness. Therefore \checkmark terminating, \checkmark confluent, and \checkmark has unique normal form.

ARS 2: $A = \{a\}, R = \{\}$



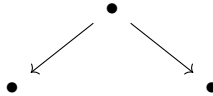
No rewrite steps: no infinite chain, no diverging paths exist or no path at all so it is vacuously satisfied and a is the only reachable normal form from a . Therefore \checkmark terminating, \checkmark confluent, and \checkmark has unique normal form.

ARS 3: $A = \{a\}, R = \{(a, a)\}$



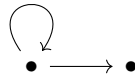
There is an infinite chain, $a \rightarrow^* a$. Since $a \rightarrow^* y$ and $a \rightarrow^* z$, therefore $y = z = a$, joining at a , and there are no normal forms as there is only one term, a , which has infinite outgoing rewrite steps. Therefore \times terminating, \checkmark confluent, and \times unique normal form.

ARS 4: $A = \{a, b, c\}, R = \{(a, b), (a, c)\}$



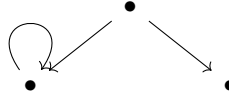
There is no infinite chain, two diverging paths that do not get joined, and two different normal forms from a . Therefore \checkmark terminating, \times confluent, and \times unique normal form.

ARS 5: $A = \{a, b\}, R = \{(a, a), (a, b)\}$



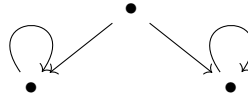
Even with one infinite chain it does not terminate, $a \rightarrow a$ and $a \rightarrow b$ and they join at b , b is the only normal form since a has an infinite chain therefore \times terminating, \checkmark confluent, has a \checkmark unique normal form.

ARS 6: $A = \{a, b, c\}$, $R = \{(a, b), (b, b), (a, c)\}$



Infinite chain at b (since $b \rightarrow b \rightarrow b \dots$). From a the system diverges to b and c with no connecting path to join them. The only normal form is c , but not every element reduces to a unique normal form, so the system is \times terminating, \times confluent, and \times has unique normal form.

ARS 7: $A = \{a, b, c\}$, $R = \{(a, b), (a, c), (b, b), (c, c)\}$



There are two infinite chains ($b \rightarrow b \rightarrow \dots$ and $c \rightarrow c \rightarrow \dots$). From a the system diverges to b and c , but since b only reaches b and c only reaches c , the peak at a does not join. Every element has outgoing rewrite steps, so there are no normal forms. Therefore \times terminating, \times confluent, and \times has unique normal form.

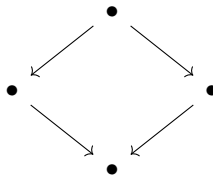
All Eight Combinations

The homework also asked to find examples of ARSs for each of the eight possible combinations of confluence, termination, and unique normal forms. The table below summarizes the results.

Confluent	Terminating	Unique Normal Forms	Example (A, R)
True	True	True	$A = \{a, b, c, d\}$, $R = \{(a, b), (a, c), (b, d), (c, d)\}$
True	True	False	N/A
True	False	True	$A = \{a, b, c, d\}$, $R = \{(a, a), (a, b), (a, c), (b, d), (c, d)\}$
True	False	False	$A = \{a, b, c, d\}$, $R = \{(a, b), (a, c), (b, d), (c, d), (d, d)\}$
False	True	True	N/A
False	True	False	$A = \{a, b, c, d\}$, $R = \{(a, b), (a, c), (b, d)\}$
False	False	True	$A = \{a, b, c\}$, $R = \{(a, b), (a, c), (b, d), (c, d), (d, d)\}$
False	False	False	$A = \{a, b, c\}$, $R = \{(a, a), (a, b), (a, c)\}$

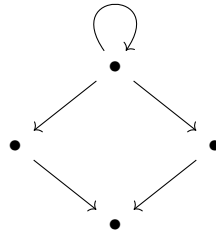
Example Graphs

Graph 1

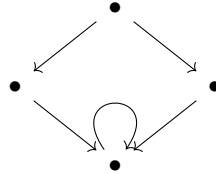


Graph 2 This combination is impossible as termination gives a normal form for each element AND confluence guarantees any two reduction paths from the same element to join therefore all reductions end at some normal form.

Graph 3

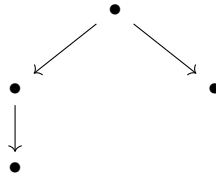


Graph 4

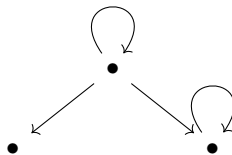


Graph 5 This case is impossible. Every system that is terminating and where every element has a unique normal form must also be confluent. Indeed, if $a \rightarrow^* y$ and $a \rightarrow^* z$, then both y and z reduce to some normal forms. Since the normal form is unique, y and z must reduce to the same normal form, which means the system is confluent.

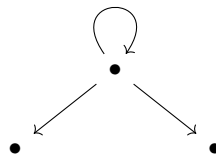
Graph 6



Graph 7



Graph 8



2.2.2 Questions

How can thinking about ARSs help us better understand the way programming languages define and control the process of evaluating programs?

2.3 Week 3

2.3.1 Homework

Exercise 5: Consider the rewrite rules

$$ab \rightarrow ba, \quad ba \rightarrow ab, \quad aa \rightarrow \varepsilon, \quad b \rightarrow \varepsilon$$

Reduce some example strings such as **abba** and **bababa**. **Answer:**

$$\text{abba} \rightarrow \text{abab} \rightarrow \text{aba} \rightarrow \text{aa} \rightarrow \varepsilon.$$

$$\text{bababa} \rightarrow \text{bbaaba} \rightarrow \text{bbba} \rightarrow \text{bba} \rightarrow \text{ba} \rightarrow \text{a}.$$

*No rule applies to a single **a**; this is the farthest you can go.*

Why is the ARS not terminating? **Answer:** There is always a way to terminate if you use the deletion rules (3) and (4), but using only the swap rules (1) and (2) yields an infinite loop (e.g., $\text{ab} \leftrightarrow \text{ba} \leftrightarrow \text{ab} \leftrightarrow \dots$), so the ARS is *not terminating* overall.

Find two strings that are not equivalent. How many non-equivalent strings can you find? **Answer:** Two strings not equivalent: $\text{baba} \not\leftrightarrow^* \text{ababa}$. There are infinitely many non-equivalent pairs: strings split by the parity of the number of *a*'s (even vs. odd), so you can keep making pairs with different *a*-parity.

How many equivalence classes does \leftrightarrow^* have? Can you describe them in a nice way? What are the normal forms? **Answer:** There are 2 equivalence classes under \leftrightarrow^* : (1) strings with an *even* number of *a*'s, which reduce to the normal form ε ; (2) strings with an *odd* number of *a*'s, which reduce to the normal form *a*. Set of normal forms: $\{\varepsilon, a\}$.

Can you modify the ARS so that it becomes terminating without changing its equivalence classes? **Answer:** Yes. Drop $ab \rightarrow ba$ and keep $ba \rightarrow ab$, together with $aa \rightarrow \varepsilon$ and $b \rightarrow \varepsilon$. This orientation is terminating while preserving the same equivalence classes and normal forms (still $\{\varepsilon, a\}$).

Write down a question or two about strings that can be answered using the ARS. Think about whether this amounts to giving a semantics to the ARS. **Answer:** Given any string $x \in \{a, b\}^*$, does x reduce to ε or to *a*? Equivalently: is the number of *a*'s in x even or odd? This gives a semantics mapping each string to ε (even) or *a* (odd).

Exercise 5b: Consider the rewrite rules

$$ab \rightarrow ba, \quad ba \rightarrow ab, \quad aa \rightarrow a, \quad b \rightarrow \varepsilon$$

Reduce some example strings such as **abba** and **bababa**. **Answer:**

$$\text{abba} \rightarrow \text{aba} \rightarrow \text{aa} \rightarrow a.$$

$$\text{bababa} \rightarrow \text{ababa} \rightarrow \text{aaba} \rightarrow \text{aaa} \rightarrow \text{aa} \rightarrow a.$$

*No rule applies to a single **a**; this is the farthest you can go.*

Why is the ARS not terminating? **Answer:** This example still has an infinite chain if you don't use rules (3) or (4): the swaps $ab \leftrightarrow ba$ can loop forever.

Find two strings that are not equivalent. How many non-equivalent strings can you find? **Answer:** Two non-equivalent strings: $bbb \not\leftrightarrow^* babab$. There are infinitely many non-equivalent pairs.

How many equivalence classes does \leftrightarrow^* have? Can you describe them in a nice way? What are the normal forms? **Answer:** There are 2 equivalence classes for \leftrightarrow^* . If a string has *no* a 's, its normal form is ε . If a string has *at least one* a , its normal form is a . Set of normal forms: $\{\varepsilon, a\}$.

Can you modify the ARS so that it becomes terminating without changing its equivalence classes? **Answer:** Drop $ab \rightarrow ba$ and keep $ba \rightarrow ab$, along with $aa \rightarrow a$ and $b \rightarrow \varepsilon$. This orientation terminates while preserving the same equivalence classes and normal forms.

Write down a question or two about strings that can be answered using the ARS. Think about whether this amounts to giving a semantics to the ARS. **Answer:** Given any string $x \in \{a, b\}^*$, does x contain at least one a ? Equivalently: does x reduce to a (some a present) or to ε (no a 's)?

2.3.2 Questions

How does changing the rewrite rule from $aa \rightarrow \varepsilon$ to $aa \rightarrow a$ resemble differences in evaluation strategies when creating a programming language?

2.4 Week 4

2.4.1 Homework

```
while b != 0:
    temp = b
    b = a % b
    a = temp
return a
```

The algorithm always terminates provided that.

1. The inputs satisfy $a \geq 0$ and $b \geq 0$.
2. If $b = 0$ initially, the loop terminates immediately.
3. For $b > 0$, the remainder operation is defined by the division algorithm:

$$a = qb + r, \quad 0 \leq r < b,$$

where $r = a \bmod b$.

Define the measure function

$$\phi(a, b) = b.$$

Consider one loop iteration:

$$(a, b) \mapsto (b, a \bmod b).$$

By the division algorithm,

$$0 \leq a \bmod b < b.$$

Therefore,

$$\phi(a, b) = b > a \bmod b = \phi(b, a \bmod b).$$

Hence ϕ strictly decreases with each iteration.

Since $\phi(a, b)$ is a nonnegative integer, it cannot decrease infinitely. After finitely many steps, we must reach $b = 0$, at which point the loop terminates.

```
function merge_sort(arr, left, right):
    if left >= right:
        return
    mid = floor((left + right) / 2)
    merge_sort(arr, left, mid)
    merge_sort(arr, mid+1, right)
    merge(arr, left, mid, right)
```

The function

$$\phi(\text{left}, \text{right}) = \text{right} - \text{left} + 1$$

is a measure function for `merge_sort` (with integer indices and `mid` = $\lfloor (\text{left} + \text{right})/2 \rfloor$).

Assume $\text{left}, \text{right} \in \mathbb{Z}$ and the procedure is only called with $\text{left} \leq \text{right}$. The branching factor is finite (at most two recursive calls).

Let $n = \phi(\text{left}, \text{right}) = \text{right} - \text{left} + 1$.

- *Base case.* If $\text{left} \geq \text{right}$ then $n \leq 1$ and the function returns without making recursive calls. No decrease condition needs to be checked.
- *Recursive case.* Suppose $\text{left} < \text{right}$, hence $n \geq 2$. Set `mid` = $\left\lfloor \frac{\text{left} + \text{right}}{2} \right\rfloor$. Then $\text{left} \leq \text{mid} < \text{right}$, so both subproblems are well-formed:

$$(\text{left}, \text{mid}) \quad \text{and} \quad (\text{mid} + 1, \text{right}).$$

Their measures are

$$\phi(\text{left}, \text{mid}) = \text{mid} - \text{left} + 1 \quad \text{and} \quad \phi(\text{mid} + 1, \text{right}) = \text{right} - \text{mid}.$$

Using `mid` = $\left\lfloor \frac{\text{left} + \text{right}}{2} \right\rfloor$ and $n = \text{right} - \text{left} + 1$, we get the bounds

$$\phi(\text{left}, \text{mid}) \leq \left\lceil \frac{n}{2} \right\rceil \quad \text{and} \quad \phi(\text{mid} + 1, \text{right}) \leq \left\lfloor \frac{n}{2} \right\rfloor.$$

Since $n \geq 2$, both $\left\lceil \frac{n}{2} \right\rceil < n$ and $\left\lfloor \frac{n}{2} \right\rfloor < n$ hold. Therefore

$$\phi(\text{left}, \text{mid}) < \phi(\text{left}, \text{right}) \quad \text{and} \quad \phi(\text{mid} + 1, \text{right}) < \phi(\text{left}, \text{right}).$$

Hence the measure strictly decreases along every recursive edge.

Because ϕ maps states to \mathbb{N} and strictly decreases with each recursive call, no infinite descent is possible. Together with finite branching, this implies termination.

2.4.2 Questions

How do different evaluation strategies in programming languages (such as call-by-value vs. call-by-name) influence whether a program is guaranteed to terminate, and in what ways can techniques like measure functions help us reason about termination across these strategies?

2.5 Week 5

2.5.1 Homework

Goal: $(\lambda f. \lambda x. f(fx)) (\lambda f. \lambda x. f(f(fx)))$.

–**renaming.** To avoid variable capture, rename bound variables so the two arguments use distinct names:

$$A \equiv \lambda f. \lambda x. f(fx) \quad \text{and} \quad B \equiv \lambda g. \lambda y. g(g(y)).$$

The term is AB .

–**reduction (outer application).**

$$AB \rightarrow_{\beta} \lambda x. B(Bx) \quad (\text{substitute } f := B \text{ in } f(fx)).$$

–**reduction of Bx .**

$$Bx = (\lambda g. \lambda y. g(g(y))) x \rightarrow_{\beta} \lambda y. x(xy).$$

Name this $B_x \equiv \lambda y. x^3(y)$, where x^k denotes k -fold self-composition.

–**reduction of $B(B_x)$.**

$$B(B_x) = (\lambda g. \lambda y. g(g(y))) (\lambda y. x^3(y)) \rightarrow_{\beta} \lambda y. B_x(B_x(y)).$$

Since $B_x y = x^3(y)$, we compute

$$B_x(B_x y) = B_x(x^3(y)) = x^3(x^3(y)) = x^6(y),$$

and then

$$B_x(B_x(B_x y)) = B_x(x^6(y)) = x^3(x^6(y)) = x^9(y).$$

Hence

$$B(B_x) \rightarrow \lambda y. x^9(y).$$

Assemble the result.

$$\lambda x. B(Bx) \rightarrow \lambda x. \lambda y. x^9(y).$$

Renaming $x \mapsto f$ and $y \mapsto a$ gives the canonical Church-numeral form

$$\boxed{\lambda f. \lambda a. f^9(a)}.$$

Thus

$$(\lambda f. \lambda x. f(fx)) (\lambda f. \lambda x. f(f(fx))) = \lambda f. \lambda x. f^9(x).$$

Remark (mathematical interpretation). In Church encodings, natural numbers are functions that iterate an endofunction:

$$n \equiv \lambda f. \lambda x. f^n(x).$$

Here, $\lambda f. \lambda x. f(fx)$ is the numeral 2 (“apply f twice”) and $\lambda f. \lambda x. f(f(fx))$ is the numeral 3 (“apply f thrice”). Applying one numeral to another composes iterations and realizes *exponentiation by iteration*:

$$(2\ 3) = \lambda x. 3^2(x) = \lambda f. \lambda x. f^9(x),$$

so the result corresponds to the number $9 = 3^2$. Conceptually, this is *function iteration*: “do thrice, then do thrice again” = “do nine times.” Before computers, Church’s lambda calculus provided a purely symbolic foundation where numbers are actions (iterations) on functions; your reduction is exactly the arithmetic law that composing “apply-thrice” with itself yields “apply-nine-times.”

2.5.2 Questions

Since Church numerals let us represent arithmetic entirely through function application, what does that suggest about the nature of mathematics—are operations like addition, multiplication, and exponentiation really ‘just’ repeated patterns of substitution and iteration?

2.6 Week 6

2.6.1 Homework

Evaluating fact 3 with fix, let, and let rec

Rules

$$\text{fix } F \rightarrow F(\text{fix } F) \quad (\text{def of fix})$$

$$\text{let } x = e_1 \text{ in } e_2 \rightarrow (\lambda x. e_2) e_1 \quad (\text{def of let})$$

$$\text{let rec } f = e_1 \text{ in } e_2 \rightarrow \text{let } f = \text{fix } (\lambda f. e_1) \text{ in } e_2 \quad (\text{def of let rec})$$

Abbreviation $F \equiv \lambda f. \lambda n. \text{if } n = 0 \text{ then } 1 \text{ else } n * f(n - 1).$

Target term

$$\text{let rec fact} = \lambda n. \text{if } n = 0 \text{ then } 1 \text{ else } n * \text{fact}(n - 1) \text{ in fact } 3.$$

Derivation (each step labeled)

$$\begin{aligned} & \text{let rec fact} = \lambda n. \text{if } n = 0 \text{ then } 1 \text{ else } n * \text{fact}(n - 1) \text{ in fact } 3 \\ & \xrightarrow{\text{def of let rec}} \text{let fact} = \text{fix } (\lambda \text{fact}. \lambda n. \text{if } n = 0 \text{ then } 1 \text{ else } n * \text{fact}(n - 1)) \text{ in fact } 3 \\ & \xrightarrow{\text{def of let}} (\lambda \text{fact}. \text{fact } 3) \text{fix } (\lambda \text{fact}. \lambda n. \text{if } n = 0 \text{ then } 1 \text{ else } n * \text{fact}(n - 1)) \\ & \xrightarrow{\beta} (\text{fix } (\lambda \text{fact}. \lambda n. \text{if } n = 0 \text{ then } 1 \text{ else } n * \text{fact}(n - 1))) 3 \\ & = (\text{fix } F) 3 \\ & \xrightarrow{\text{def of fix}} (F(\text{fix } F)) 3 \\ & \xrightarrow{\beta} (\lambda n. \text{if } n = 0 \text{ then } 1 \text{ else } n * (\text{fix } F)(n - 1)) 3 \\ & \xrightarrow{\beta} \text{if } 3 = 0 \text{ then } 1 \text{ else } 3 * (\text{fix } F) 2 \\ & \xrightarrow{\text{def of if}} 3 * (\text{fix } F) 2 \end{aligned}$$

Expand $(\text{fix } F) 2$:

$$\begin{aligned} (\text{fix } F) 2 & \xrightarrow{\text{def of fix}} (F(\text{fix } F)) 2 \xrightarrow{\beta} (\lambda n. \text{if } n = 0 \text{ then } 1 \text{ else } n * (\text{fix } F)(n - 1)) 2 \\ & \xrightarrow{\beta} \text{if } 2 = 0 \text{ then } 1 \text{ else } 2 * (\text{fix } F) 1 \xrightarrow{\text{def of if}} 2 * (\text{fix } F) 1. \end{aligned}$$

Expand $(\text{fix } F) 1$:

$$\begin{aligned} (\text{fix } F) 1 & \xrightarrow{\text{def of fix}} (F(\text{fix } F)) 1 \xrightarrow{\beta} (\lambda n. \text{if } n = 0 \text{ then } 1 \text{ else } n * (\text{fix } F)(n - 1)) 1 \\ & \xrightarrow{\beta} \text{if } 1 = 0 \text{ then } 1 \text{ else } 1 * (\text{fix } F) 0 \xrightarrow{\text{def of if}} 1 * (\text{fix } F) 0. \end{aligned}$$

Base case $(\text{fix } F) 0$:

$$\begin{aligned}
(\text{fix } F) 0 &\xrightarrow{\text{def of fix}} (F (\text{fix } F)) 0 \xrightarrow{\beta} (\lambda n. \text{if } n = 0 \text{ then } 1 \text{ else } n * (\text{fix } F) (n - 1)) 0 \\
&\xrightarrow{\beta} \text{if } 0 = 0 \text{ then } 1 \text{ else } 0 * (\text{fix } F) (-1) \xrightarrow{\text{def of if}} 1.
\end{aligned}$$

Back-substitute the arithmetic:

$$(\text{fix } F) 0 = 1, \quad (\text{fix } F) 1 = 1, \quad (\text{fix } F) 2 = 2, \quad (\text{fix } F) 3 = \boxed{6}.$$

2.6.2 Questions

If the `fix` operator allows a function to “refer to itself” without any explicit naming or looping construct, what does that reveal about recursion as a *mathematical* idea rather than merely a *programming* one?

Does this suggest that self-reference—and therefore recursion—emerges purely from the rules of substitution and function application, rather than from syntactic features like `while` or `for` loops?

2.7 Week 7

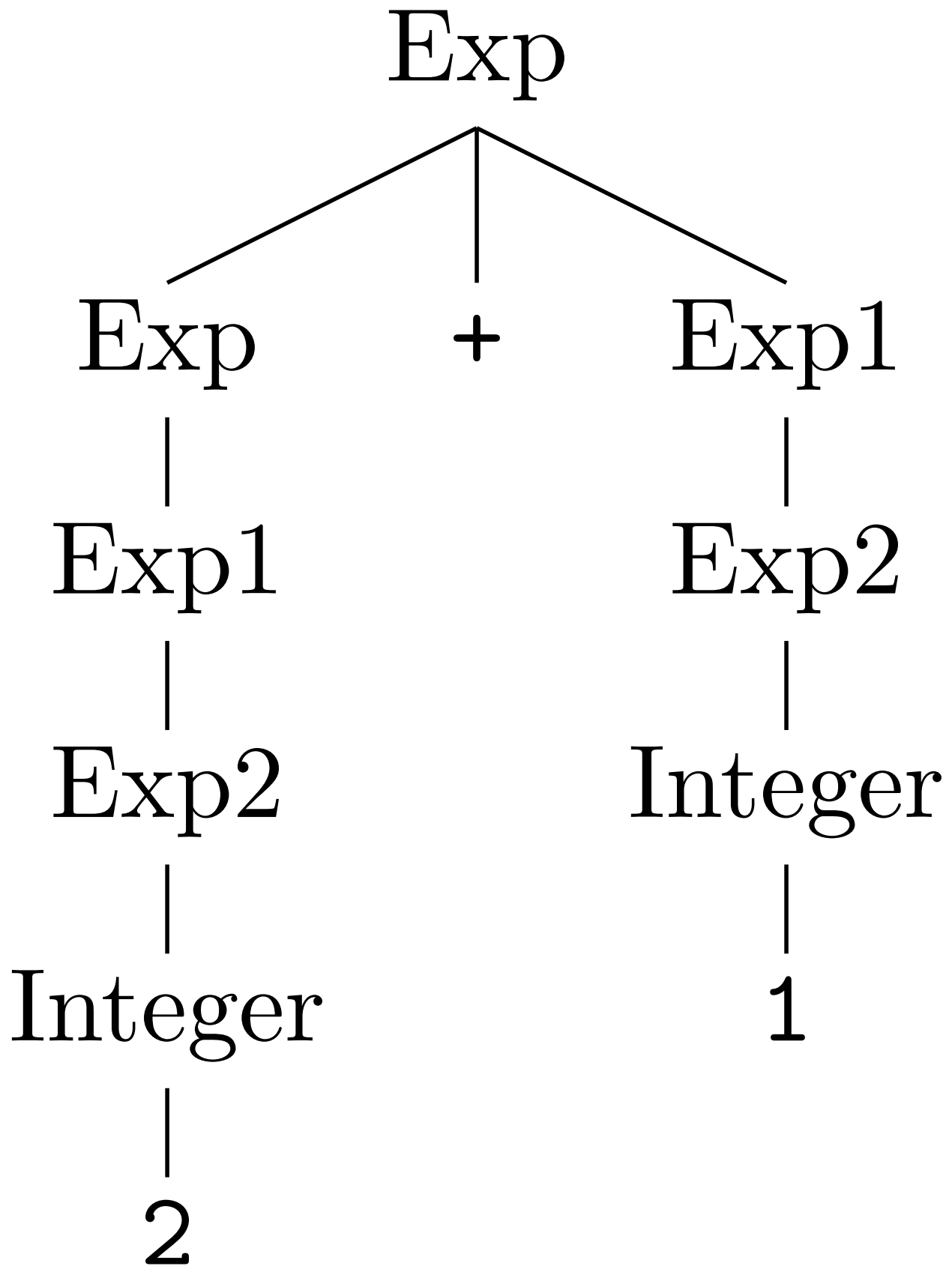
2.7.1 Homework

Parse Trees for the Given Grammar

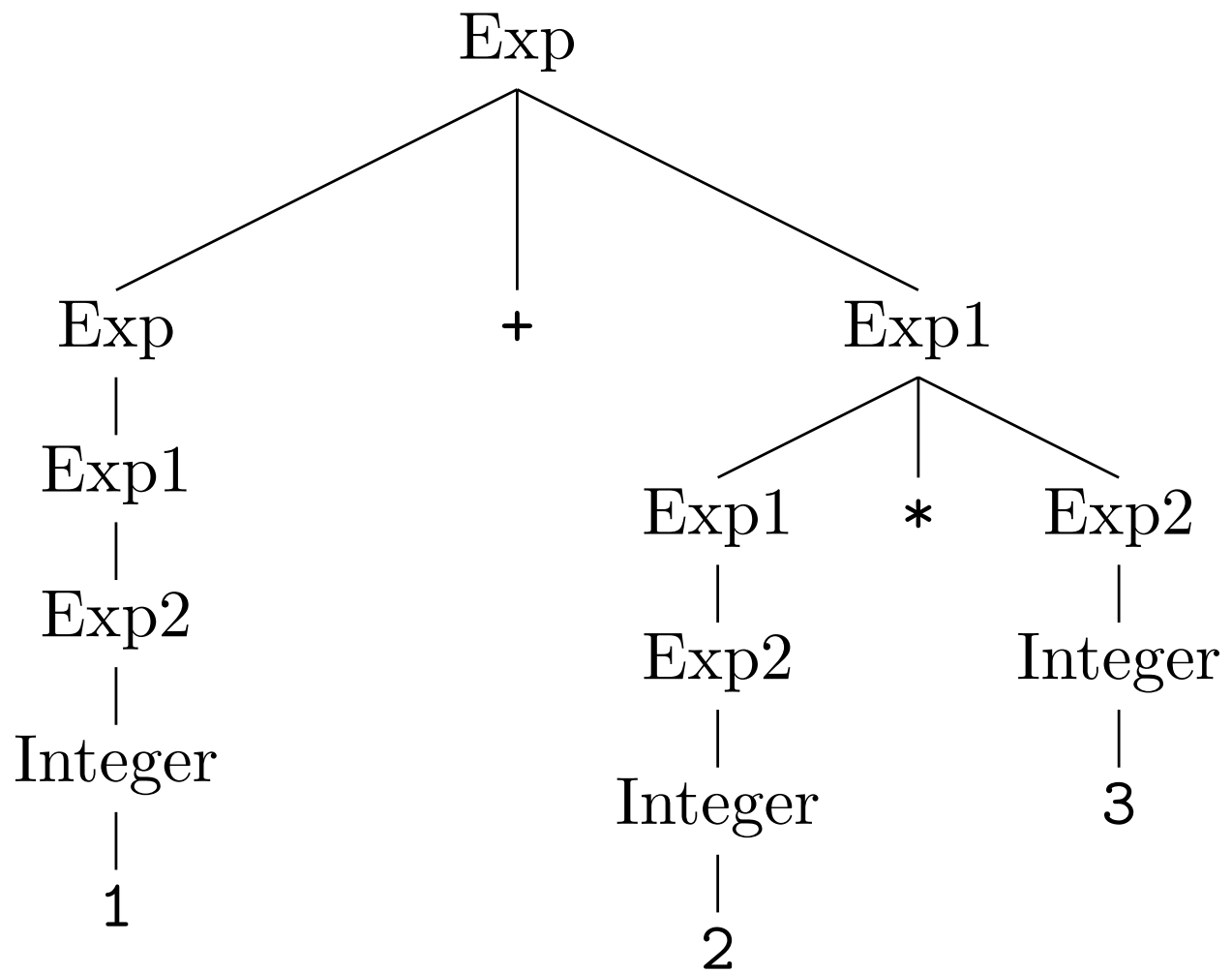
Grammar

$$\begin{aligned}
\text{Exp} &\rightarrow \text{Exp} + \text{Exp1} \mid \text{Exp1} \\
\text{Exp1} &\rightarrow \text{Exp1} * \text{Exp2} \mid \text{Exp2} \\
\text{Exp2} &\rightarrow \text{Integer} \mid (\text{Exp})
\end{aligned}$$

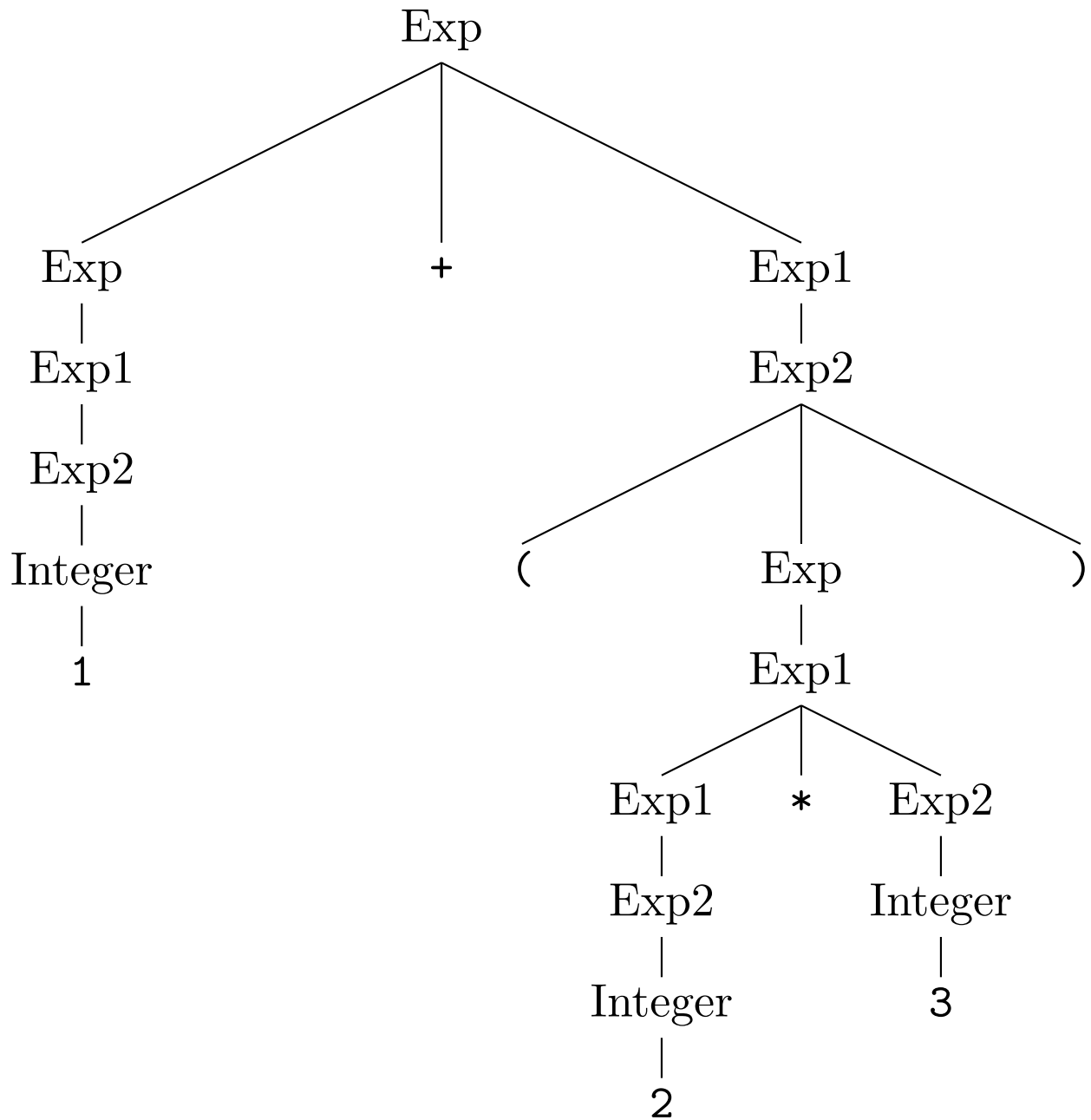
1) 2+1



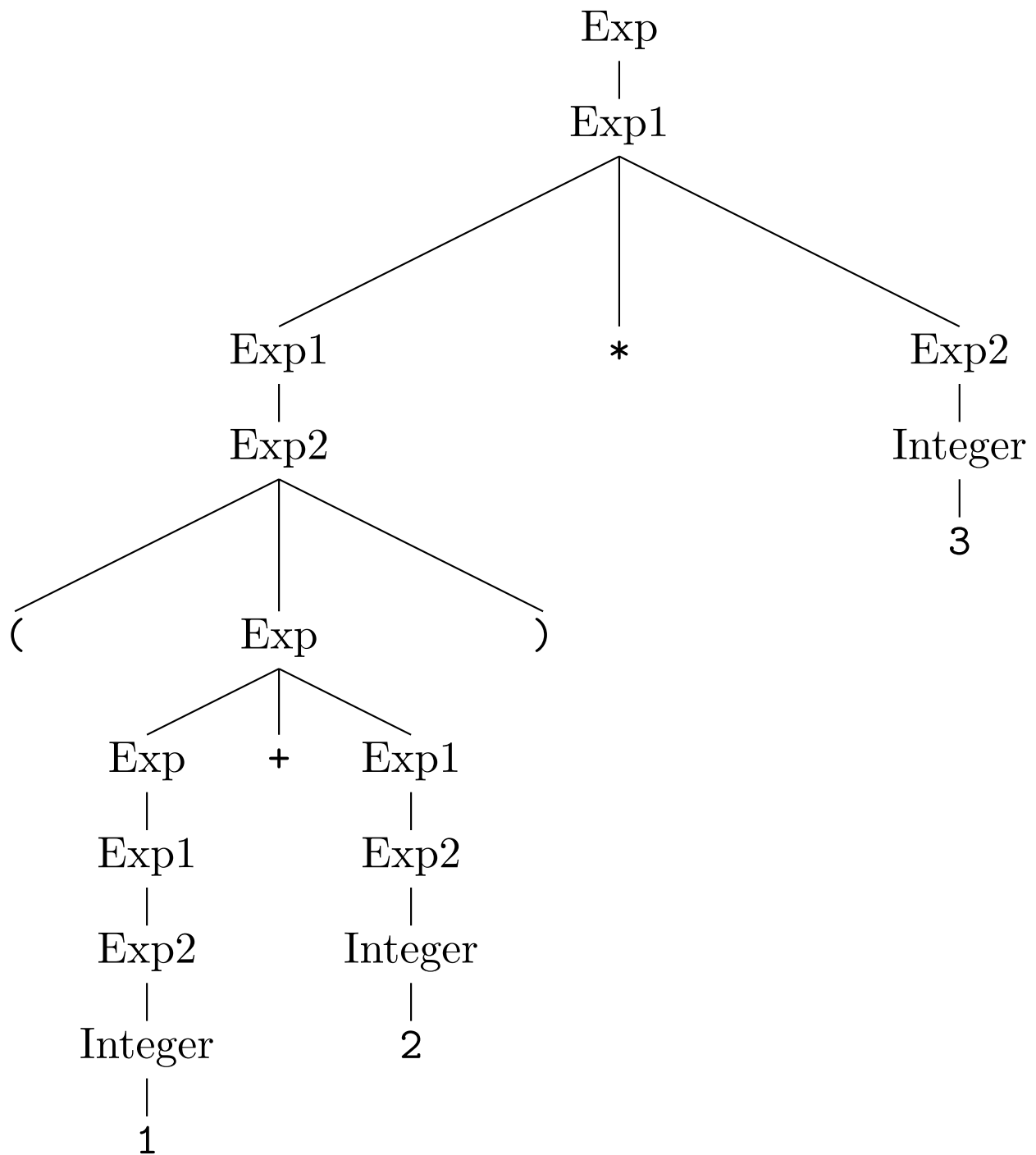
2) 1+2*3



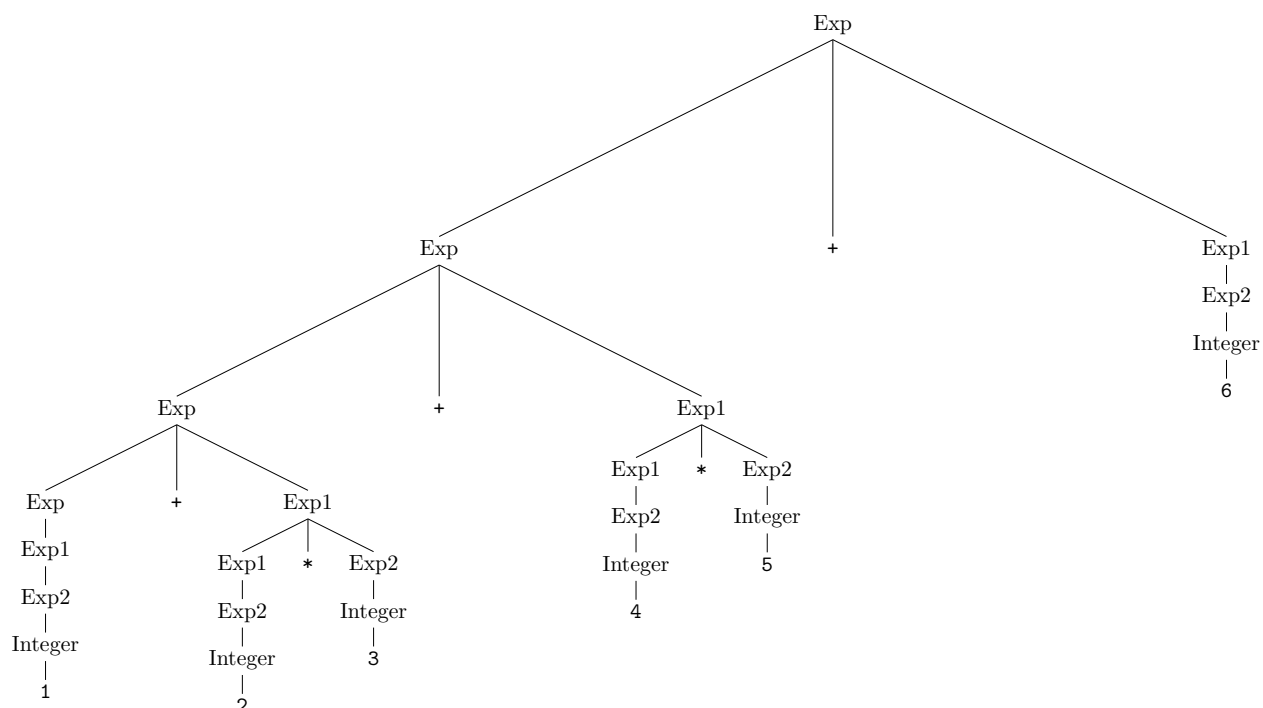
3) $1+(2*3)$



4) $(1+2)*3$



5) $1+2*3+4*5+6$



2.7.2 Questions

When a grammar allows multiple ways to parse the same expression, such as different groupings of additions and multiplications, how can we modify or design the grammar so that the parse tree always reflects the correct operator precedence and associativity?

2.8 Week 8

2.8.1 Homework

Level 5/8: *Adding zero*

Question. Prove, for natural numbers a, b, c ,

$$a + (b + 0) + (c + 0) = a + b + c.$$

Using the identity $x + 0 = x$ (often named `add_zero`) twice:

$$\begin{aligned} a + (b + 0) + (c + 0) &= a + b + (c + 0) && \text{(by } b + 0 = b\text{)} \\ &= a + b + c && \text{(by } c + 0 = c\text{)}. \end{aligned}$$

Lean script.

```
-- Objects: a b c :
rw [add_zero] -- a + (b + 0) + (c + 0) ==> a + b + (c + 0)
rw [add_zero] -- a + b + (c + 0) ==> a + b + c
rfl          -- both sides now identical
```

Level 6/8: *Precision rewriting*

Question. Prove, for natural numbers a, b, c ,

$$a + (b + 0) + (c + 0) = a + b + c,$$

but emphasize *targeted* rewriting (i.e., rewriting only the needed subterm each step).

Same identities as above, but apply them precisely to the subterm containing 0:

$$\begin{aligned} a + (b + 0) + (c + 0) &= a + b + (c + 0) && \text{rewrite only the inner } (b + 0) \\ &= a + b + c && \text{now rewrite the remaining } (c + 0). \end{aligned}$$

Lean script (one precise rewrite at a time).

```
-- Objects: a b c :
rw [add_zero]    -- rewrite (b + 0) -> b
rw [add_zero]    -- rewrite (c + 0) -> c
rfl
```

(If the goal were more complicated, one could direct a rewrite to a specific occurrence using a location, e.g. `'rw [add_zero] at h'` or `'simp [add_zero] with side conditions.`)

Level 7/8: *add_succ*

Theorem (stated).

$$\forall n : \mathbb{N}, \quad n.\text{succ} = n + 1.$$

Useful lemmas.

$$\begin{aligned} 1 &= \text{succ}(0) && \text{(named one_eq_succ_zero),} \\ n + \text{succ}(k) &= \text{succ}(n + k) && \text{(named add_succ),} \\ n + 0 &= n && \text{(named add_zero).} \end{aligned}$$

$$\begin{aligned} n.\text{succ} &= n + 0.\text{succ} && \text{(since succ}(x) = x + 1, \text{ we move via } 1 = \text{succ}(0)) \\ &= \text{succ}(n + 0) && \text{by add_succ} \\ &= \text{succ}(n) && \text{by add_zero} \\ &= n + 1 && \text{unwinding } 1 = \text{succ}(0). \end{aligned}$$

Concretely (mirroring your screenshot), we first rewrite the 1 as `succ(0)`, then use `add_succ`, then `add_zero`, and finish with reflexivity.

Lean script (exact sequence from the level).

```
-- Goal: n.succ = n + 1
rw [one_eq_succ_zero] -- turn 1 into succ 0 on the RHS
rw [add_succ]         -- n + succ 0 -> (n + 0).succ
rw [add_zero]         -- (n + 0).succ -> n.succ
rfl                   -- both sides are n.succ
```

Notes.

- Levels 5 and 6 highlight the same identity $x + 0 = x$ but train you to control *where* a rewrite happens.
- Level 7 chains small lemmas to reach a familiar arithmetic fact: $n + 1 = \text{succ}(n)$.

Question 8 — Natural–Language Proof (Level 8: $2 + 2 = 4$)

Goal. Prove that $2 + 2 = 4$ in Peano arithmetic.

Background/Definitions. Let 0 be the base natural number and let $\text{succ}(n)$ (sometimes written $n.\text{succ}$) denote the successor of n . Define the numerals

$$1 = \text{succ}(0), \quad 2 = \text{succ}(1), \quad 3 = \text{succ}(2), \quad 4 = \text{succ}(3).$$

Addition is defined by the standard recursion rules:

$$(\text{add_zero}) \quad n + 0 = n, \quad (\text{add_succ}) \quad n + \text{succ}(k) = \text{succ}(n + k).$$

Proof. We compute $2 + 2$ using only the recursion rules for $+$ and the numeral definitions.

$2 + 2 = \text{succ}(1) + \text{succ}(1)$	(by the definition of 2)
$= \text{succ}(\text{succ}(1) + 1)$	(by <i>add_succ</i> with $n = \text{succ}(1)$, $k = 1$)
$= \text{succ}(\text{succ}(1) + \text{succ}(0))$	(since $1 = \text{succ}(0)$)
$= \text{succ}(\text{succ}(\text{succ}(1) + 0))$	(by <i>add_succ</i> with $n = \text{succ}(1)$, $k = 0$)
$= \text{succ}(\text{succ}(\text{succ}(1)))$	(by <i>add_zero</i> : $\text{succ}(1) + 0 = \text{succ}(1)$)
$= \text{succ}(\text{succ}(\text{succ}(1)))$	
$= \text{succ}(\text{succ}(\text{succ}(\text{succ}(0))))$	(since $1 = \text{succ}(0)$)
$= \text{succ}(\text{succ}(\text{succ}(\text{succ}(0))))$	
$= 4$	(by the definition of 4).

Therefore, $2 + 2 = 4$. □

(Optional) Lean step correspondence. The proof above mirrors the scripted steps:

```
rw [four_eq_succ_three] rw [three_eq_succ_two] rw [two_eq_succ_one] rw [one_eq_succ_zero] rw [add_succ]
```

2.8.2 Questions

In Peano arithmetic, every arithmetic fact—such as $2 + 2 = 4$ —is proven step by step from simple definitions like 0 and $\text{succ}(n)$. What does this tell us about how much of mathematics can be built from just a few basic rules, and why might this level of formality be both powerful and limiting when compared to the way we usually do arithmetic?

3 Essay

4 Evidence of Participation

5 Conclusion

References

[BLA] Author, [Title](#), Publisher, Year.