1. Recall the three main proof rules: Differential Invariant, Differential Cut, Differential Weakening

The Cut rule “cuts” $A \rightarrow B$ into $A \rightarrow C \land C \rightarrow B$ (if such a $C$ exists). So, if one can prove that $C$ holds, from $A$, then it’s safe to assume it in order to prove $B$ (also, originally, from $A$). The same intuition can be used in the differential context. As long as you prove that a given property already holds throughout the ODE’s execution, then it’s safe to assume it by putting it in the domain.

$$
\text{DC} \quad \frac{F \vdash [x' = \theta \& H]C}{F \vdash [x' = \theta \& H \land C]F}
$$

The differential weakening rule is trivial (the invariant is enforced by design) and essentially used to close the proof after a DC. The general proof technique in this case is to diff-cut in enough properties so that they end up implying the final condition.

$$
\text{DW} \quad \frac{H \vdash F}{F \vdash [x' = \theta \& H]F}
$$

The differential invariant rule is essentially used to lift a property about the differential terms to a property about their derivatives. In conjunction with the $D$ operator, the property is rewritten using the $\theta$ (right-hand side of the differential equation), which we can deal with as a first-order logic formula.

$$
\text{DI} \quad \frac{H \vdash [x' := \theta]F'}{F \vdash [x' = \theta \& H]F'}
$$

2. The $D$ operator on first-order real-arithmetic: what intuitions to keep in mind

To prove that a differentiable real function: $f : \mathbb{R}_+ \rightarrow \mathbb{R}; t \mapsto f(t)$ has a constant sign ($f(t) \leq 0$, say), it is sufficient to prove that $f(0) \leq 0$ and its derivative w.r.t. to the variable $t$ is also non-positive: $f'(t) \leq 0$

$$
f(0) \leq 0 \land f'(t) \leq 0 \rightarrow f(t) \leq 0, \forall t \geq 0
$$

Following the same reasoning, given two functions $f$ and $g$, one has:

$$
f(0) \leq 0 \land g(0) \leq 0 \land f'(t) \leq 0 \land g'(t) \leq 0 \rightarrow f(t) \leq 0 \land g(t) \leq 0, \forall t \geq 0
$$

which also implies that $f(t) \leq 0$ or $g(t) \leq 0$, $\forall t \geq 0$. This should give an intuition about why we need to switch from $\lor$ to $\land$ for the $D$ operator to be sound. Observe that all of these transformations are sufficient conditions. This means, that the differential invariant rule is sound but, alone, is not complete directly.
3. **Case Study: 3D Lotka-Volterra**

The following predator/prey model describes the behavior of the biomasses $x$, $y$ and $z$ of three distinct species. We want to prove that none of the three involved species will disappear: that is we reach an equilibrium cycle.

**Program Variables.**

```
R x.
R y.
R z.
End.
```

**Problem.**

```
x != 0 & y != 0 & z != 0
->
{\{x' = x*(y-z),
y' = y*(z-x),
z' = z*(x-y)
\}
}(x != 0 & y != 0 & z != 0)
```

(a) Apply a DI first (with the postcondition as differential invariant). Observe that
the proof does not close because the condition asks about separate properties for
$x$, $y$ and $z$.

(b) Apply a DC with $xyz \neq 0$ (which is equivalent to the post-condition, but links
explicitly the involved variables).

(c) Close the proof by a DI and DW.

**Quiz**

1. Can you prove that $y > 0 \land x < 0 \rightarrow [x' = x, y' = y]x \neq y$? Explain why or why not.

2. Can you prove $x < x_o \rightarrow [a := \frac{x^2}{2(x-x_o)}; \{x' = v, v' = a, v \geq 0\}]x \leq x_o$ using DI instead
   of ODE (solving the differential equation)? Write down your DI.

3. Try proving the .key files in the recitation zip file.