



Polytech Paris-Sud  
Formation initiale 4<sup>e</sup> année  
Spécialité informatique  
Année 2016-2017

# Vérification et validation

## Cours 2

### Spécification formelle orientée objet

Delphine Longuet

[delphine.longuet@lri.fr](mailto:delphine.longuet@lri.fr)

<http://www.lri.fr/~longuet/Enseignements/16-17/Et4-VV>

# Exemple fil rouge : station service

Une station service TATOL a des postes de distribution de deux types :

- automatiques (par carte bancaire) ouverts 24h/24
- manuels (utilisables seulement si la station est ouverte)

Chaque poste est identifié par un numéro.

Chaque poste peut délivrer 3 sortes de carburant. À chaque instant, il en délivre au plus une sorte.

Chaque poste est muni de 3 compteurs :

- la quantité de carburant servie
- le prix au litre (qui ne change pas pendant la journée)
- le prix total à payer

Les compteurs affichent 0 s'il n'y a pas de distribution en cours.

# Exemple fil rouge : station service

La station dispose de 3 citernes (une par type de carburant) avec :

- le niveau courant de carburant
- un niveau d'alerte pour prévenir le gérant qu'elle va être vide
- un niveau minimal qui, une fois atteint, ne permet plus de délivrer du carburant

Les niveaux d'alerte et minimaux sont les mêmes pour toutes les citernes.

Le système doit garder une trace de tous les achats effectués depuis la dernière ouverture de la station.

Un opérateur ouvre la station quand il arrive et la ferme quand il part.

Quand une livraison de carburant a lieu, l'opérateur met à jour le niveau de la citerne. Une livraison fait toujours repasser les niveaux au-dessus du niveau d'alarme.

# Exemple fil rouge : station service

Pour utiliser un **poste automatique** :

1. Un client insère sa carte bancaire et tape son code
2. Le système authentifie la carte auprès du service bancaire
3. En cas de succès, le client choisit un type de carburant et se sert d'un certain nombre de litres
4. Le système enregistre l'achat, envoie un ordre de débit au service bancaire et remet à zéro les compteurs du poste

Pour utiliser un **poste manuel** :

1. Le client choisit son carburant et se sert
2. Les caractéristiques de l'achat sont envoyées à l'opérateur
3. Lorsque le client a payé en indiquant son numéro de pompe, le pompiste enregistre l'achat et remet à zéro les compteurs du poste

Les postes restent bloqués tant que les compteurs n'ont pas été remis à 0.

# Diagramme de classes

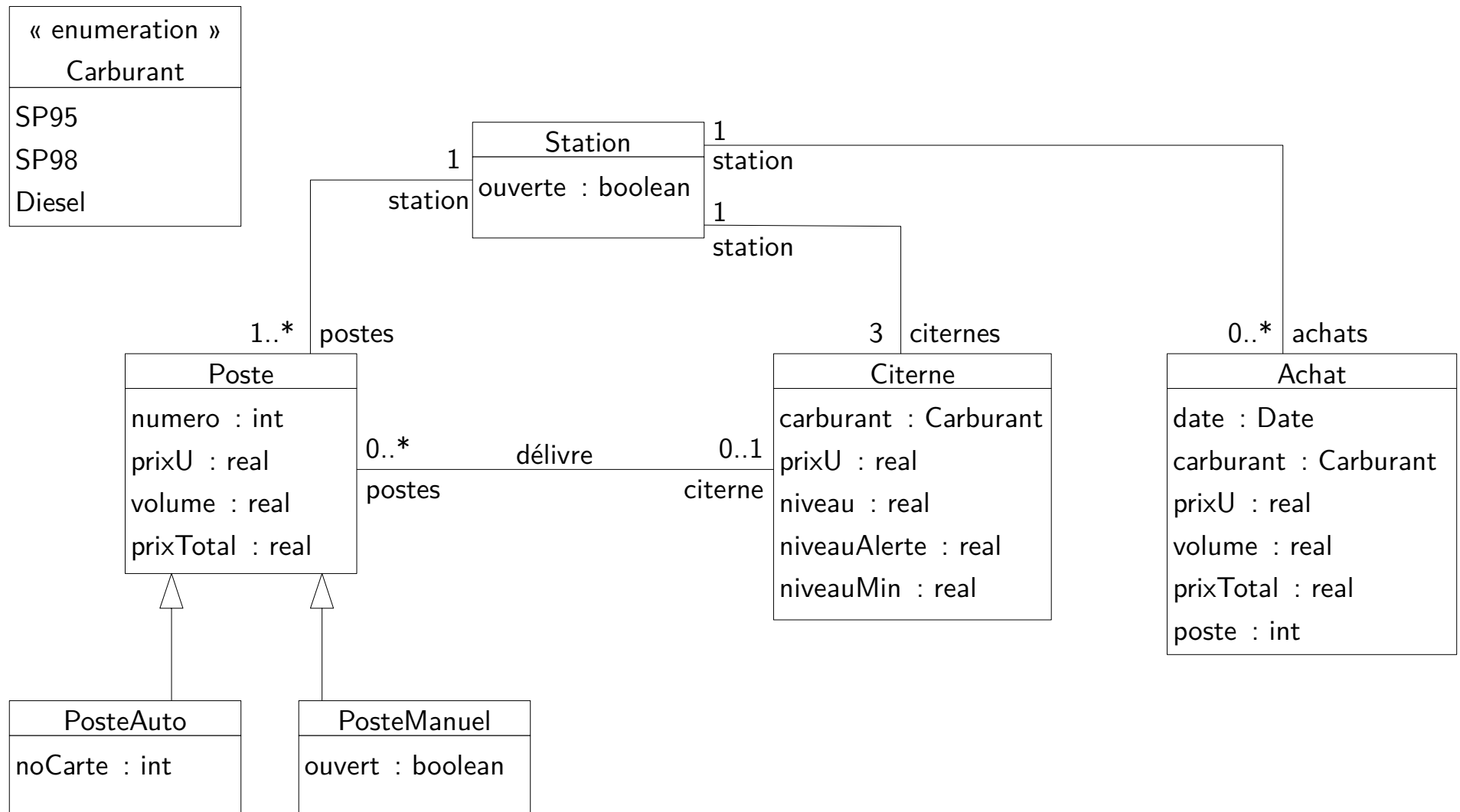
Représentation de la **structure statique interne** du système :

- les classes d'intérêt
- les relations entre classes
- les attributs (et les opérations)

En phase d'analyse :

- **type de données simple** (bool, int, real, string) ou primitif (Date)
- **pas d'opérations** en dehors de celles des cas d'utilisation, qui ne sont pas rattachées à une classe à ce niveau d'abstraction
- pas de visibilité autre que **public**

# Diagramme de classes de Tatol (analyse)



# Limites du diagramme de classes

Diagramme de classes : **structure du système** en termes d'**objets** et de **relations** entre ces objets

**Ne permet pas de représenter :**

- **Valeurs autorisées** des attributs
- **Conditions** sur les associations
- **Relations** entre les attributs ou entre les associations

**Expression des contraintes liées au diagramme :**

- **Notes** dans le diagramme
- **Texte** accompagnant le diagramme
- **OCL** : langage de contraintes formel associé à UML
- Dans ce cours : **logique mathématique orientée objet**

# Contraintes, invariants

## Propriétés :

- Portant sur les éléments du modèle
- Doivent être vérifiées à tout instant
- En général, restriction sur les diagrammes d'objets possibles à partir du diagramme de classes
- Héritage des contraintes de la super-classe vers les sous-classes

## Contraintes présentes dans le diagramme :

- Type des attributs
- Multiplicités des associations



# Contraintes sur les attributs

$\text{prixTTC} = \text{prixHT} \times (1 + \text{taxe})$   
 $0 \leq \text{taxe} \leq 1$

*sous forme de note*

## Produit

id : int            {unique}  
prixHT : real       {prixHT ≥ 0}  
taxe : real  
/prixTTC : real

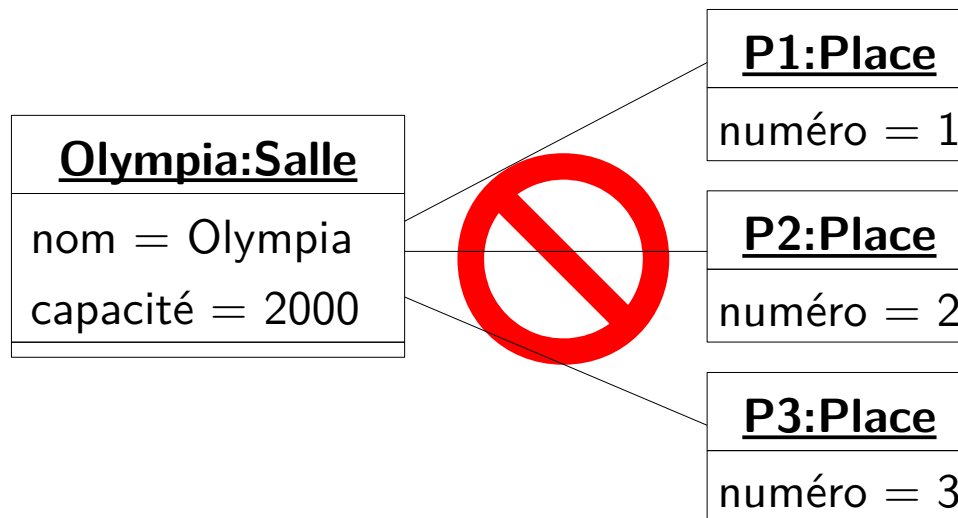
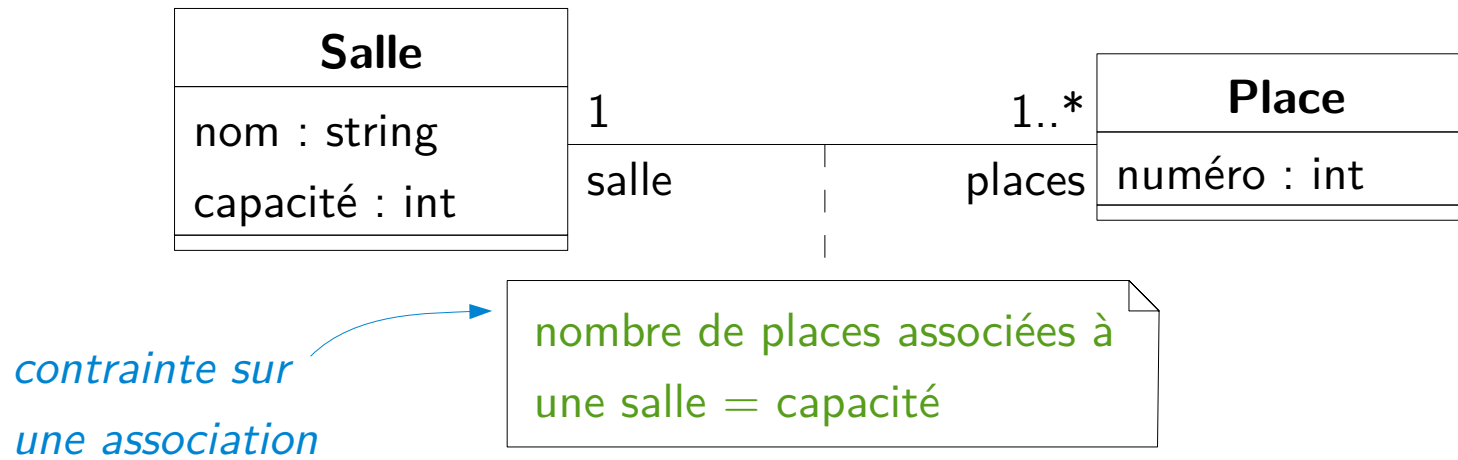
*dans le diagramme*

Contraintes sur la classe Produit :

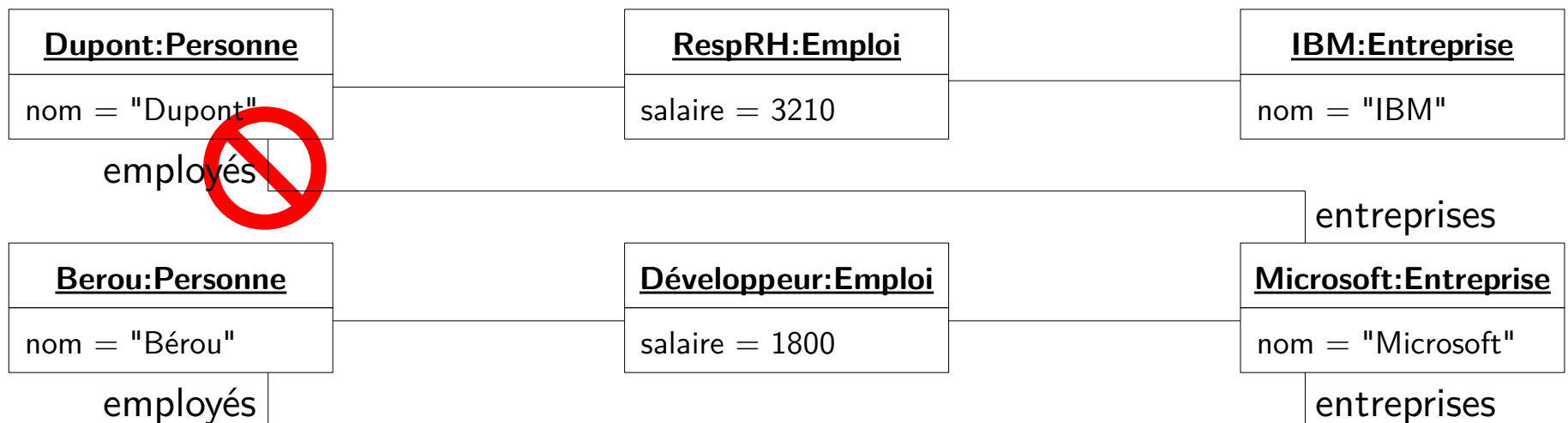
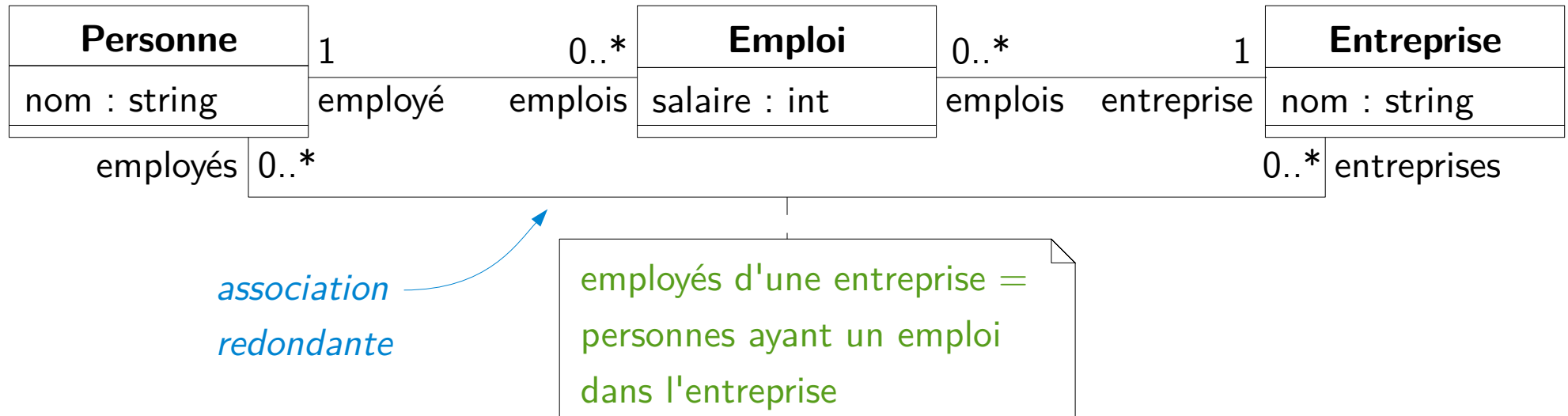
- L'identifiant est unique
- Le prix hors taxe est toujours positif ou nul
- La taxe est comprise entre 0 et 1
- Le prix TTC est égal au prixHT augmenté de la valeur de la taxe appliquée au prixHT

*dans un document annexe*

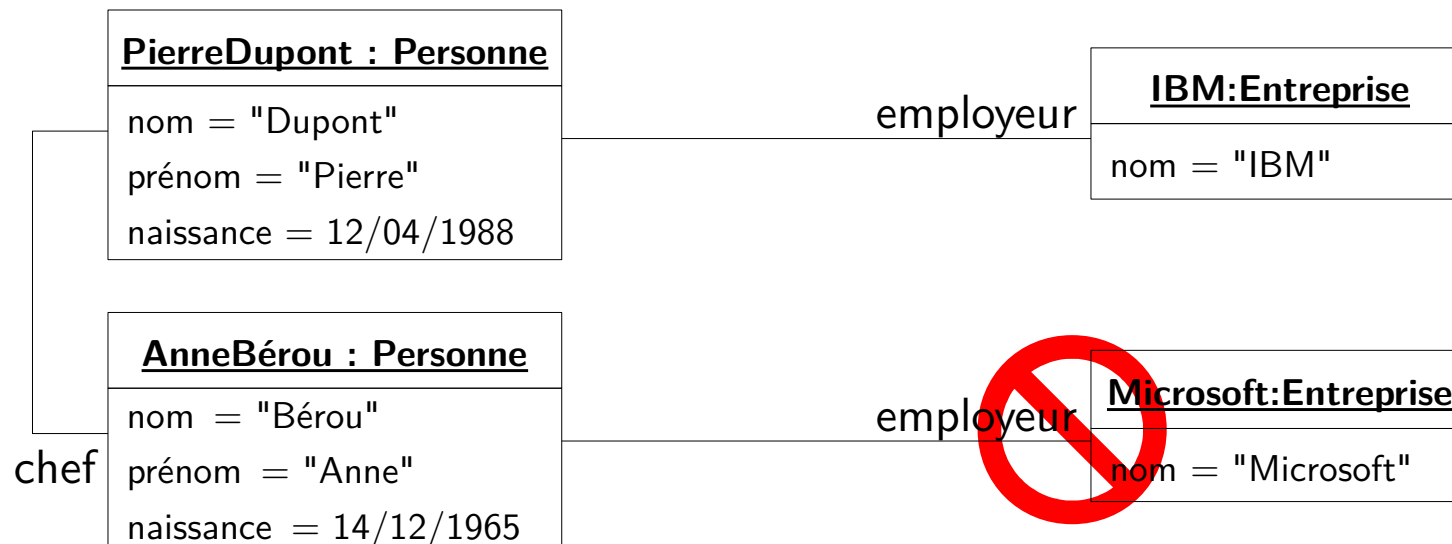
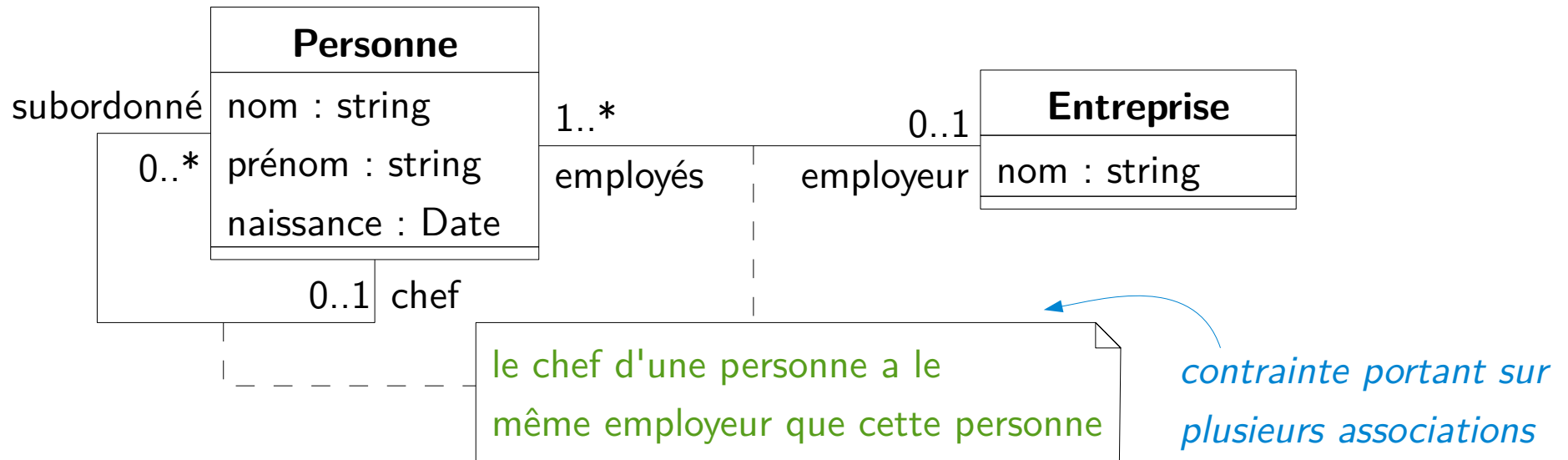
# Contraintes sur les associations



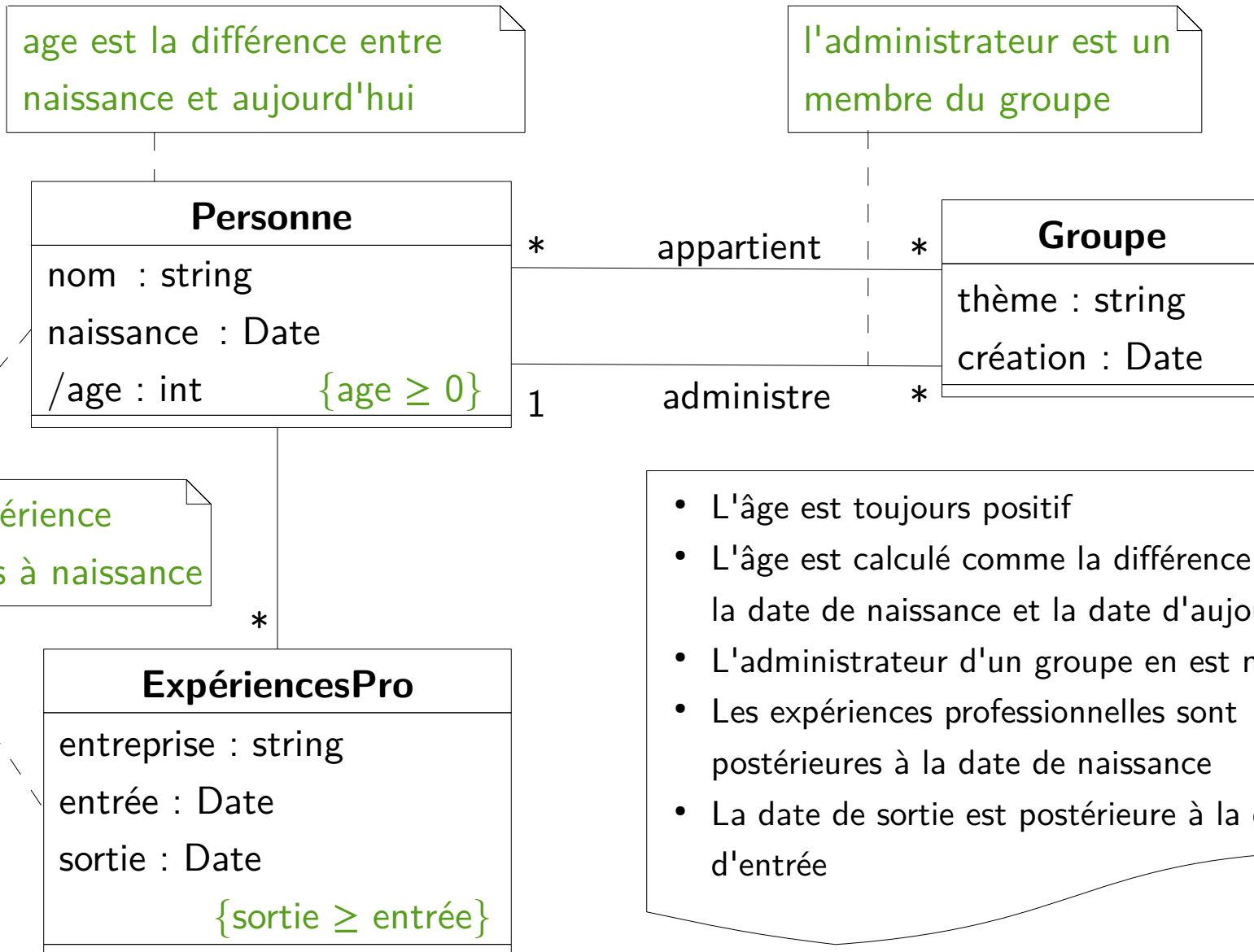
# Contraintes sur les associations



# Contraintes sur les associations



# Contraintes, invariants



- L'âge est toujours positif
- L'âge est calculé comme la différence entre la date de naissance et la date d'aujourd'hui
- L'administrateur d'un groupe en est membre
- Les expériences professionnelles sont postérieures à la date de naissance
- La date de sortie est postérieure à la date d'entrée

# Expression des contraintes

Langage de contraintes : logique mathématique orientée objet

Base : logique mathématique et théorie des ensembles

$\forall c \in A, \exists \dots$

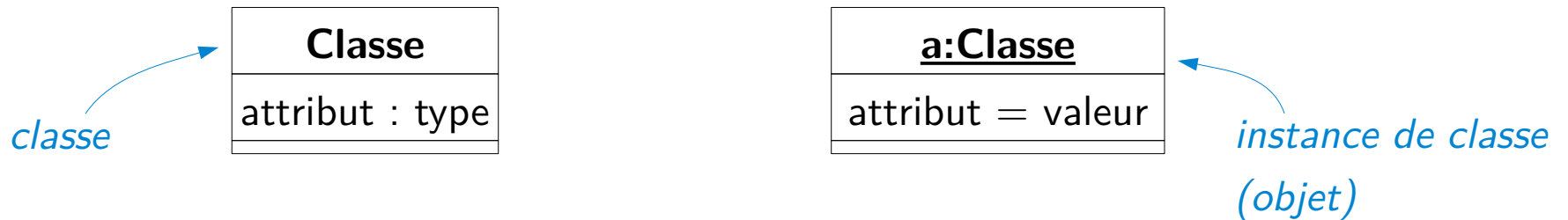
$\{ c \in C \mid \dots \}$

$c > 0 \Rightarrow \dots$

Ajout : termes dénotant

- des valeurs : `utilisateur.nom`
- des objets : `personne.employeur`
- des ensembles de valeurs : `client.vehicules.couleur`
- des ensembles d'objets : `cinema.salles`

# Navigation dans le diagramme de classes

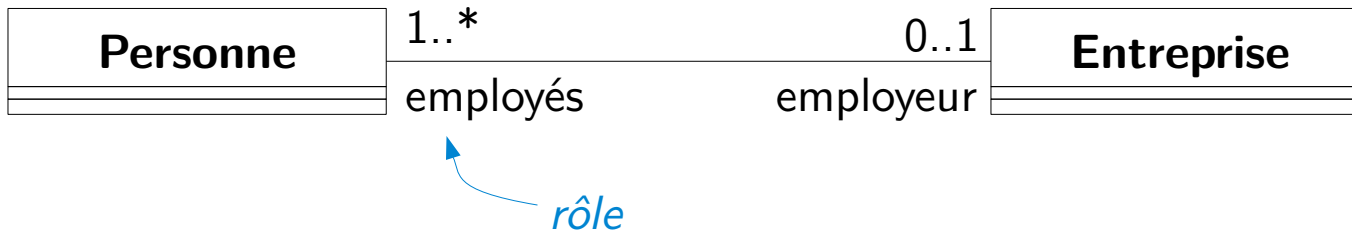


**a.attribut** : valeur de l'attribut de **a**

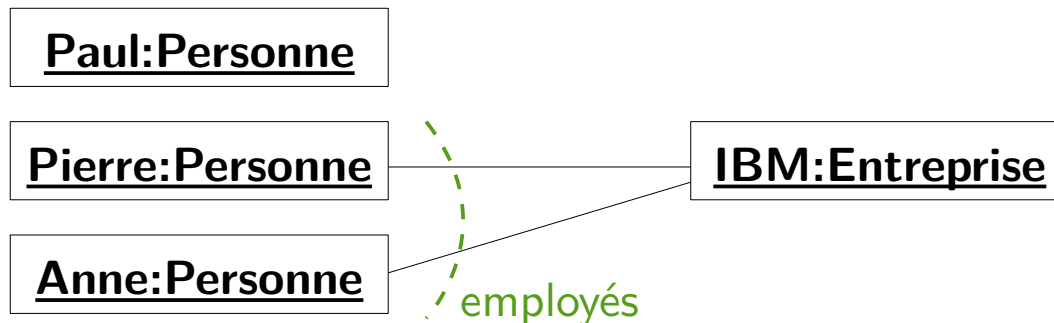
<u>pile:Produit</u>
id = 7846210
prixHT = 2,03
taxe = 0,20
prixTTC = 2,49

$\text{pile.prixHT} \geq 0$   
 $0 \leq \text{pile.taxe} \leq 1$   
 $\text{pile.prixTTC} = \text{pile.prixHT} \times (1 + \text{pile.taxe})$

# Navigation dans le diagramme de classes



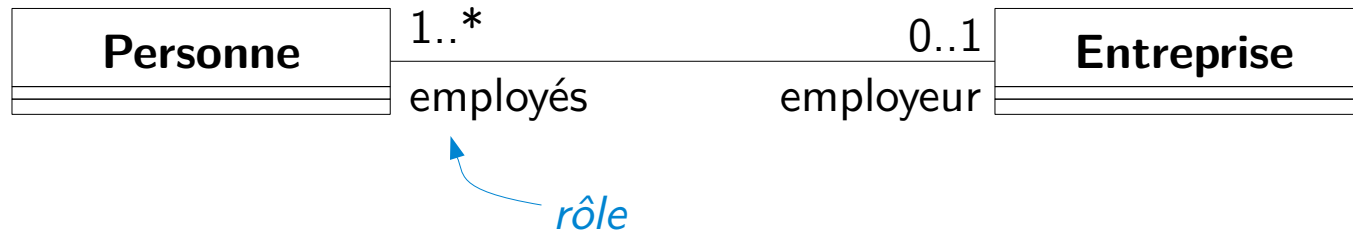
**a.role** : ensemble d'objets liés à **a** par l'association de terminaison **role**



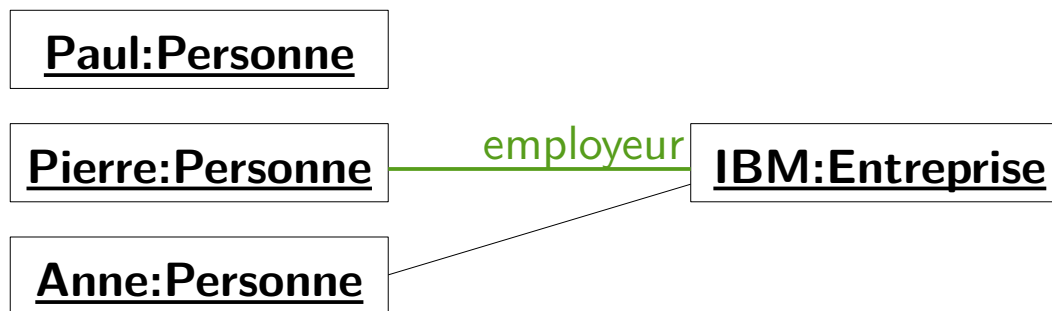
`IBM.employés = {Pierre, Anne}`



# Navigation dans le diagramme de classes



**a.role** : ensemble d'objets liés à **a** par l'association de terminaison **role**

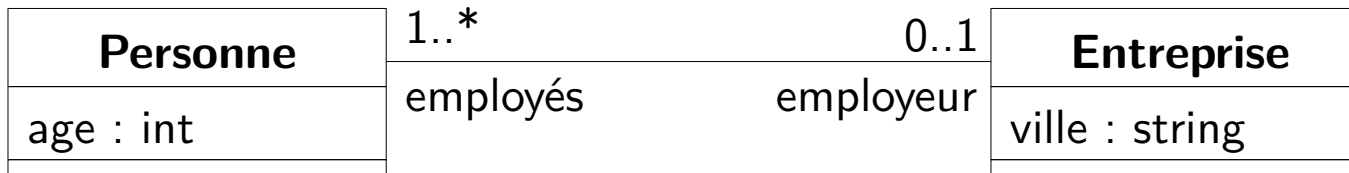


$IBM.employés = \{Pierre, Anne\}$   
 $Pierre.employeur = IBM$   
 $Paul.employeur = \emptyset$

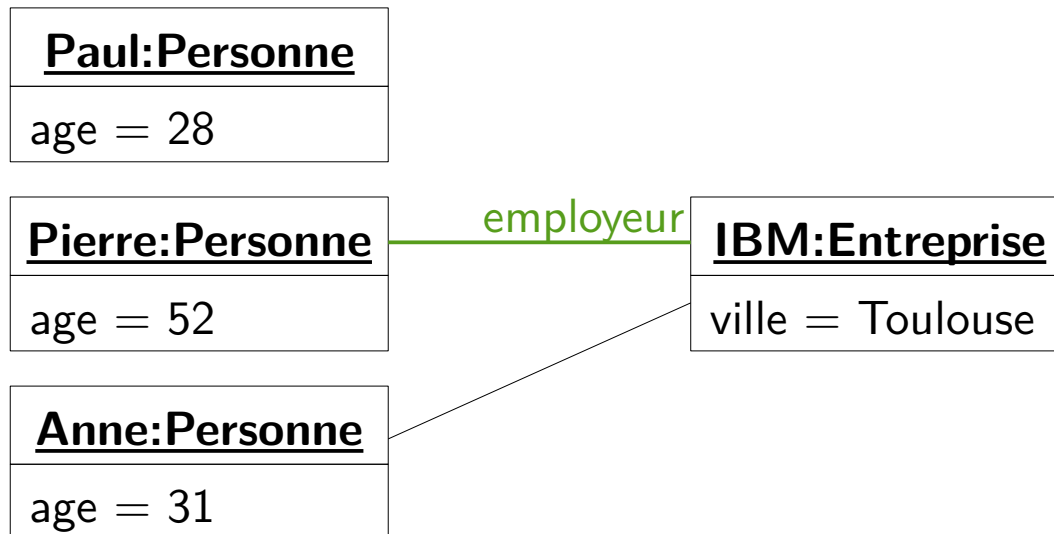
Multiplicité 0..1 ou 1 : **a.role** est un singleton, noté sans accolade par convention

Si **a** n'est lié à aucun objet par l'association, **a.role** =  $\emptyset$

# Navigation dans le diagramme de classes



**a.role.attribut** : ensemble des valeurs de l'attribut pour les objets liés à **a** par l'association de terminaison **role**



Pierre.employeur.ville = Toulouse  
IBM.employés.age = {52,31}  
Paul.employeur.ville

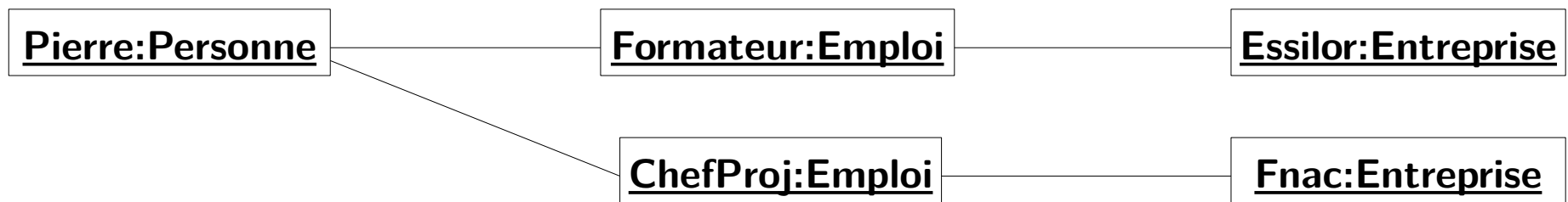
Si **a** n'est lié à aucun objet par **role**, **a.role.attribut** n'est pas défini

# Navigation dans le diagramme de classes



**a.role1.role2** : ensemble des ensembles d'objets liés par **role2** à chaque objet lié à **a** par **role1**

Par convention, ensemble « aplati » :  $\{ \{a,b\}, \{c\}, \{d\} \} \rightarrow \{a,b,c,d\}$



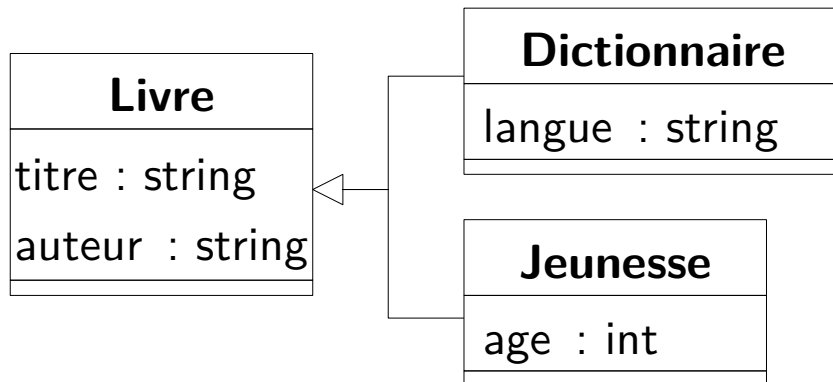
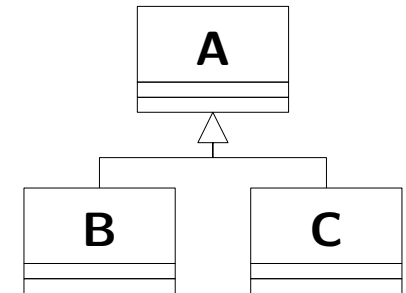
`Pierre.emplois.entreprise = {Essilor,Fnac}`

# Ensembles d'objets

**Classe** = ensemble de ses instances

**Hiérarchie** :  $B \cup C \subseteq A$ , avec  $B \cap C = \emptyset$

Certains objets de  $A$  peuvent n'être des objets ni de  $B$  ni de  $C$



Hurlevent  $\in$  Livre

MaxLili  $\in$  Livre

Larousse  $\in$  Livre

Larousse  $\in$  Dictionnaire

Hurlevent  $\notin$  Jeunesse

<u>Hurlevent:Livre</u>
titre = "Hurlevent"
auteur = "Brontë"

<u>Larousse:Dictionnaire</u>
titre = "Petit Larousse"
auteur = "Collectif"
langue = "français"

<u>MaxLili:Jeunesse</u>
titre = "Max et Lili"
auteur = "Saint Mars"
age = 6

# Expression des invariants

**Invariant** : Contrainte portant sur tous les objets d'une classe

Forme générale d'un invariant :

$$\forall a \in \text{Classe}, P(a)$$

Produit
id : int
prixHT : real
taxe : real
prixTTC : real

Le prix hors taxe d'un produit est toujours positif

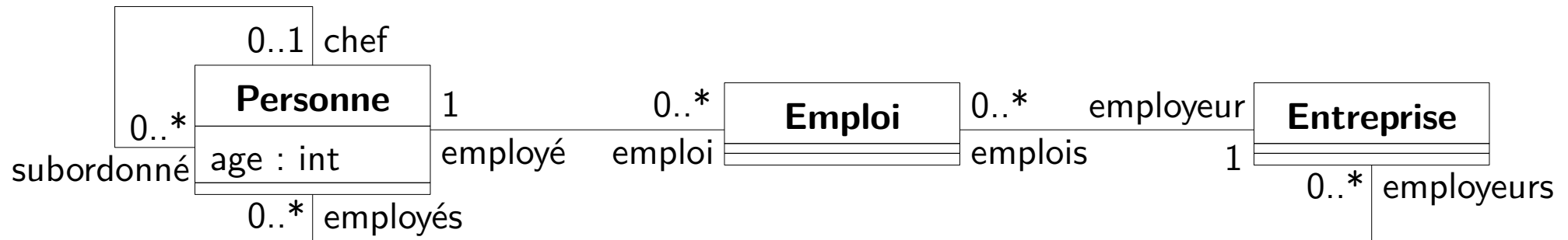
$$\forall p \in \text{Produit}, p.\text{prixHT} \geq 0$$

Le prix TTC d'un produit est égal à son prixHT augmenté de la valeur de la taxe appliquée au prixHT

$$\forall p \in \text{Produit}, p.\text{prixTTC} = p.\text{prixHT} \times (1 + p.\text{taxe})$$

En particulier, dans une hiérarchie, **héritage des invariants** par les sous-classes

# Expression des invariants



Les employés de l'entreprise sont les personnes ayant un emploi dans l'entreprise

$$\forall e \in \text{Entreprise}, e.\text{emplois.employé} = e.\text{employés}$$

Le chef d'une personne a le même employeur que cette personne

$$\forall p \in \text{Personne}, p.\text{chef} \neq \emptyset \Rightarrow p.\text{employeurs} \cap p.\text{chef.employeurs} \neq \emptyset$$

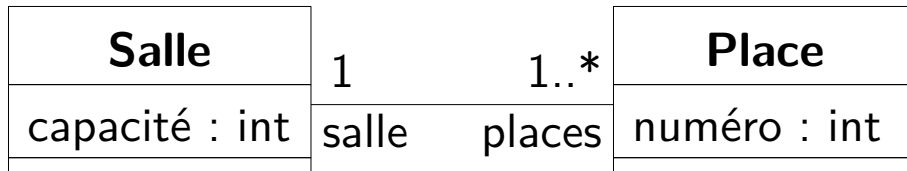
Tous les employés d'une entreprise ont plus de 16 ans

$$\forall e \in \text{Entreprise}, \forall a \in e.\text{employés.age}, a \geq 16$$

Une entreprise n'a jamais plus de 10 employés de moins de 18 ans

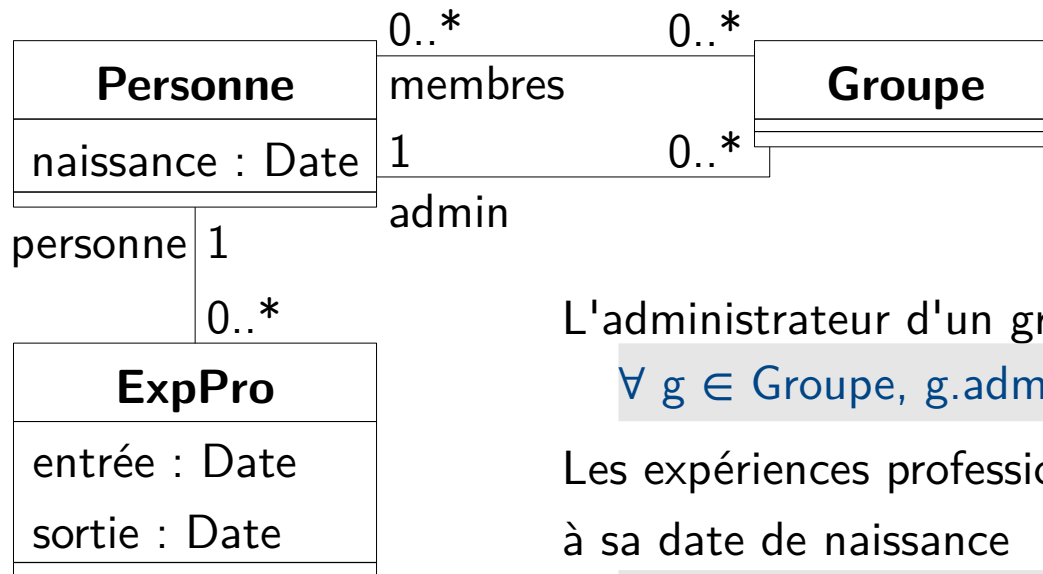
$$\forall e \in \text{Entreprise}, |\{p \in e.\text{employés} \mid p.\text{age} < 18\}| \leq 10$$

# Expression des invariants



Le nombre de places de la salle égale sa capacité

$\forall s \in \text{Salle}, |s.\text{places}| = s.\text{capacité}$



L'administrateur d'un groupe en est un membre

$\forall g \in \text{Groupe}, g.\text{admin} \in g.\text{membres}$

Les expériences professionnelles d'une personne sont postérieures à sa date de naissance

$\forall e \in \text{ExpPro}, e.\text{entrée} \geq e.\text{personne.naissance}$

L'identifiant d'un produit est unique

$\forall p1, p2 \in \text{Produit}, p1 \neq p2 \Rightarrow p1.\text{id} \neq p2.\text{id}$