Logique du 1er ordre égalitaire
ac prédicat d'arité 2 : "égalité" → déduire les conséquences logiques

# Réécritures et formes normales. Exemples.

Q 20

Motivation : à partir d'un système d'égalités, pouvoir définir d'autres égalités, plus faciles à manier (ou plus générales).

Ex : Théorie des groupes.

| | Egalités |
|---|---|
| "composition" $\circ$ (binaire) | $(x \circ y) \circ z = x \circ (y \circ z)$ |
| "inverse" $i$ (unaire) | $e \circ x \simeq x$ |
| "neutre" $e$ (0-aire) | $i(x) \circ x \simeq e$. |

↳ permet de déduire $e \simeq i(x) \circ x$.

## I Formalisation de la théorie équationnelle.

### A) Généralités sur les langages.

BAA p34

**Déf 1** : Une signature $\Sigma$ est un ensemble de symboles de fonctions, chacune possédant une arité $n$ (nombre d'arguments). On note $\Sigma^{(n)}$ : fonctions d'arité $n$. $\Sigma^{(0)}$ : symboles de constantes.

BAA p35

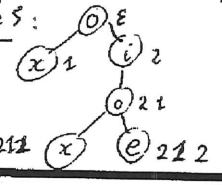
**Déf 2** : Soit $\Sigma$ une signature et $X$ un ensemble de variables telles que $\Sigma \cap X = \emptyset$. On définit inductivement les termes $T$ (ou $T(\Sigma, X)$) par :
$X \subseteq T$ et $\forall n \geq 0, \forall f \in \Sigma^{(n)}, \forall t_1, \dots, t_n \in T, \ f(t_1, \dots, t_n) \in T$.

**Exemple 3** : Théorie des groupes. $\Sigma = \{\circ, i, e\}$.
$\circ \in \Sigma^{(2)}$, $i \in \Sigma^{(1)}$, $e \in \Sigma^{(0)}$. Soit $x \in X$. Alors
$\circ(x, i(\circ(x, e)))$ est un terme. On pourra noter $x \circ (i(x \circ e))$.

**Déf 4** : On peut illustrer un terme par un arbre. On définit inductivement l'ensemble des positions d'un terme $s$ : $Pos(s)$, ensemble de suites de nombres positifs :
- si $x \in X$, et $x = s$, $Pos(s) := \{\varepsilon\}$, soit la suite vide.
- si $s = f(s_1, \dots, s_n)$, $Pos(s) := \{\varepsilon\} \cup \bigcup_{i=1}^{n} \{ip \mid p \in Pos(s_i)\}$.

La taille $|s|$ d'un terme $s$ est le cardinal de $Pos(s)$. Le sous-terme de $s$ à la position $p$ se définit par induction :
$s|_\varepsilon := s$ et $f(s_1, \dots, s_n)|_{ip} := s_i|_p$

**Exemple 5** :




pour $s = \circ(x, i(\circ(x, e)))$.
$Pos(s) = \{\varepsilon, 1, 2, 21, 211, 212\}$.
$|s| = 6$ $\quad s|_{21} = \circ(x, e)$.

**Déf 6** : Une substitution sur $T(\Sigma, X)$ est une application $\sigma : V \to T$ telle que $\sigma(x) \neq x$ pour seulement un nombre fini de $x$. On l'étend par induction aux termes. Son domaine est $D(\sigma) = \{x \in V ; \sigma(x) \neq x\}$. Un terme $t$ est une instance d'un terme $s$ ssi il existe $\sigma$ tq $\sigma(s) = t$.

**Exemple 7** : Sur la théorie des groupes, si $\sigma : x \mapsto (y \circ y)$, alors
$\sigma(x \circ i(x \circ e)) = (y \circ y) \circ (i((y \circ y) \circ e))$.

### B) Théorie équationnelle.

BAA p39

**Déf 8** : Soit $\Sigma$ une signature, $V$ variables (infini dénombrable). Une identité est une paire $(s, t) \in T \times T$. On note $s \simeq t$. Si $E$ est un ensemble d'identités, on définit la relation de réduction $\to_E \subseteq T \times T$ par :
$s \to_E t$ si $\exists (l, r) \in E$, $p \in Pos(s)$, $\sigma \in Sub$, tq $s|_p = \sigma(l)$ et $t = s[\sigma(r)]_p$.

**Exemple 9** : $G := \{x \circ e \simeq x \ ; \ x \circ i(x) \simeq e\}$.
$x \circ i(x \circ e) \to_G x \circ i(x) \to_G e$. (cf annexe 1).

BAA p41

**Th 10** : Soit $E$ un ensemble d'identités. La relation $\overset{*}{\leftrightarrow}_E$ (fermeture réflexive, transitive et symétrique de $\to_E$) est la plus petite relation d'équivalence sur $T$ qui contient $E$ et qui soit :
- clos par substitution : $s \overset{*}{\leftrightarrow}_E t$ ssi $\forall \sigma$, $\sigma(s) \overset{*}{\leftrightarrow}_E \sigma(t)$
- clos par $\Sigma$-opérations : si $s = t_1, \dots, t_n \equiv t_n$, $\forall f \in \Sigma^{(n)}$, alors $f(s_1, \dots, s_n) \equiv f(t_1, \dots, t_n)$.

**Exemple 11** : Avec les trois égalités de l'introduction sur la théorie des groupes (associativité, neutre à droite et inverse à gauche), $\overset{*}{\leftrightarrow}_E$ contiendra l'inverse et le neutre à gauche, l'unicité de l'inverse...

BAA p50

**Déf 12** : Soit $\Sigma$ une signature et $E$ un ensemble de $\Sigma$-identités. Soit $M$ constitué d'un domaine $A$ et d'un morphisme qui à tout $f$ de $\Sigma^{(n)}$ associe une fonction $f^M : A^n \to A$. $M$ est appelé modèle (noté $M \models E$) si chaque identité de $E$ tient dans $M$.

BAA p50

**Déf 13** : La relation $s \simeq t$ est conséquence sémantique de $E$ ($E \models s \simeq t$) ssi elle tient dans tout modèle de $E$. La relation $\approx_E$ définie par $\approx_E := \{(s, t) \in T \times T \mid E \models s \simeq t\}$ est appelée théorie équationnelle induite par $E$.

**Exemple 14** : Modèles de la théorie des groupes : $\mathfrak{S}_n$, $M_n(\mathbb{R})$, $\mathbb{U}$, $\mathbb{Q}$, $\mathbb{F}_p$...

Coro 15 : La théorie équationnelle est close par morphisme ; pour tout morphisme $\phi$ sur $T$, $s \approx_E t$ implique $\phi(s) \approx_E \phi(t)$.

BAA p55 — Th 16 (de Birkhoff) : Soit $E$ un ensemble d'identités. Alors $\overset{*}{\leftrightarrow}_E$ coïncide avec $\approx_E$.

## II Systèmes de réduction et de réécriture.

AA → — Def 17 : Un système de réduction abstrait est un couple $(A, \to)$, où la flèche $\to$, appelée réduction, est une relation binaire sur $A$.

Exemple 18 : La relation de réduction $\to_E$ est une réduction !

BAA p3 — Def 19 : On considère $(A, \to)$, $x \in A$ est réductible si $\exists y \in A$ tq $x \to y$.
$x$ est sous forme normale s'il n'est pas réductible.
$y$ est une forme normale de $x$ si $x \overset{*}{\to} y$ et $y$ est une forme normale.
$x$ et $y$ sont joignables si $\exists z \in A$, $x \overset{*}{\to} z \overset{*}{\leftarrow} y$. On note $x \downarrow y$.

TER p60 — Exemple 20 : On définit les entiers naturels par 0 (constante) et le successeur S (unaire), et la fonction Min (binaire). Les relations de réduction sont : $\{Min(Sx, Sy) \to S(Min(x,y)),\ Min(x,0) \to 0,\ Min(0,x) \to 0\}$.
$SSS(0)$ est une forme normale. $b$ est la forme normale de $Min(S^3(0), S^4(0))$. De plus, $Min(Min(S^3(0),0), S^2(0))$ et $Min(S(0),0)$ sont joignables.

AA >9 — Def 21 : Une réduction $\to$ est dite :
- Church-Rosser si $x \overset{*}{\leftrightarrow} y \Rightarrow x \downarrow y$. (cf annexe 2)
- confluente si $y_1 \overset{*}{\leftarrow} x \overset{*}{\to} y_2 \Rightarrow y_1 \downarrow y_2$. (cf annexe 3).
- terminante si il n'y a pas de chaîne infinie $a_0 \to a_1 \to \dots$
- normalisante si chaque élément a une forme normale.
- convergente si elle est confluente et terminante.

AA >11 — Th 22 : Une réduction confluente est Church-Rosser, et réciproquement.

Coro 23 : Si $\to$ est confluente et $x \overset{*}{\leftrightarrow} y$ alors :
1) $x \overset{*}{\to} y$ si $y$ est une forme normale.
2) si $x$ et $y$ sont en forme normale, alors $x = y$.

Coro 24 : Si $\to$ est confluente, chaque élément a au plus une forme normale. (cf exemple 15)

Coro 25 : Si $\to$ est normalisant et confluent, chaque élément a une unique forme normale.

Exemple 26 : Toujours sur les entiers, on définit l'addition + (binaire) et les relations de réduction : $\{+(S(x), y) \to S(x+y)\ ,\ +(0,x) \to x\}$.
Normalisant + confluent $\Rightarrow \exists!$ forme normale.

Def 27 : Une règle de réécriture est une identité $s \to t$ telle que $s$ ne soit pas une variable, et toutes les variables de $t$ sont dans $s$. On peut écrire $s \to t$. Un système de réécriture $(\Sigma, R)$ est un ensemble de règles de réécriture.
Un système de réécriture est un cas particulier de système de réduction.

Exemple 28 : La logique combinatoire, avec 3 fonctions unaires : S, K, I.
Règles de réduction : $\{((S \cdot x) \cdot y) \cdot z) \to (x \cdot z) \cdot (y \cdot z)\ ,\ I \cdot x \to x\ ,\ (K \cdot x) \cdot y \to x\}$
Si on pose $B = S(KS)K$, avec la convention "les parenthèses sont les plus à gauche possible", on a : $B\,x\,y\,z \to x(yz)$.
On aimerait savoir si le système de réécriture est confluent !

BAA p15 — Principe 29 d'induction bien fondée : Soit $(A, \to)$ un système de réduction terminant, et $P$ une propriété sur les éléments de $A$ :
$$\frac{\forall x \in A,\ (\forall y \in A,\ x \overset{+}{\to} y \Rightarrow P(y)) \Rightarrow P(x)}{\forall x \in A,\ P(x).}$$

BAA p18 — Exemple 30 : L'ordre lexicographique sur deux systèmes de réduction terminants $(A, >_A)$ et $(B, >_B)$ défini par : $(A \times B,\ >_{A \times B})$ avec $(x,y) >_{A \times B} (x',y')$ si $(x >_A x') \vee (x = x' \wedge (y >_B y'))$.
$P(x) :=$ "il n'y a pas de chaîne infinie commençant par $x$ sur $A \times B$", montre que $A \times B$ est terminant.

BAA p28 — Def 31 : Une relation $\to$ est localement confluente si :
$y_1 \leftarrow x \to y_2 \Rightarrow y_1 \downarrow y_2$. (cf annexe 4).

Rem 32 : Ceci n'implique pas la confluence ! (cf annexe 5).

BAA p29 — Lemme 33 (de Neumann) : Une relation terminante est confluente si et seulement si elle est localement confluente.

## III Terminaison et confluence de systèmes de réécriture.

### A) Etude de la confluence.

Dans un premier temps : étant données deux termes $s$ et $t$ on voudrait savoir s'il existe $\sigma$ une substitution telle que $\sigma s \underset{E}{\simeq} \sigma t$ !

**Déf 34 :** La substitution $\sigma$ est plus générale que la substitution $\sigma'$ s'il existe une substitution $\delta$ telle que $\sigma' = \delta\sigma$. On écrit $\sigma \leq \sigma'$.

**Lemme 35 :** $\leq$ est un pré-ordre sur les substitutions (réflexivité et transitivité).

BAA p 72

**Déf 36 :** Un problème d'unification est un ensemble fini d'équations $S = \{s_1 =^? t_1, \dots, s_n =^? t_n\}$. Un unificateur de $S$ est une substitution telle que $\forall i,\ \sigma s_i = \sigma t_i$. $\sigma$ est un unificateur le plus général si pour tout $\sigma'$ unificateur, $\sigma \leq \sigma'$.

**Ex 37 :** $\Sigma = \{f:2, g:1, e:0\}$, alors $s = f(f(e,y), g(x))$ et $t = f(z, y)$ sont unifiables ; l'unificateur le plus général est $\sigma = [\,{}^{z}/_{f(e,y)},\ {}^{y}/_{g(x)}\,]$.

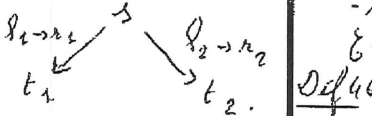
BARR p 135

**Th 38 :** Le problème suivant est indécidable.

entrée : un SR, nommé $R$. sortie : oui si $R$ est confluent.

Plusieurs cas peuvent se présenter si on a :

On a les règles $l_i \to r_i \in R$, des positions $p_i$ et des substitutions $\sigma_i$ telles que $s|_{p_i} = \sigma_i l_i$ et $t_i = s[\sigma_i r_i]_p$.




1er cas : $p_1$ et $p_2$ sont dans des sous-arbres séparés (annexe 6). On a la confluence locale.

2ème cas : $p_1$ est un préfixe de $p_2$ (cf annexe 7).

Cas 2.1 : la règle de réécriture $l_1 \to r_1$ ne change pas le sous-arbre $l_2$ : on a la confluence locale (cf annexe 8).

BARR p 139

Cas 2.2 : les deux domaines de réécriture s'intersectent...

**Déf 39 :** En reprenant les notations précédentes : si $\mathrm{Var}(l_1, r_1) \cap \mathrm{Var}(l_1, r_2) = \emptyset$, soit $p$ tel que $l_1|_p$ ne soit pas une variable, et soit $\theta$ un unificateur le plus général de $l_1|_p =^? l_2$. Cela détermine une paire critique $(\theta r_2, (\theta l_1)[\theta r_2]_p)$.

**Th 40 (des paires critiques) :** Un SR est localement confluent ssi toutes ses paires critiques sont joignables.

**Cor 41 :** La confluence d'un SR fini et terminant est décidable.

## B) Etude de la terminaison.

**Th 42 :** Le problème TERM suivant :

entrée : un SR fini. sortie : oui s'il est terminant, est indécidable.

BAA p 93 — DVT

Quelques éléments de théorie des ensembles :

**Déf 43 :** $\leq$ est un beau-pré-ordre (ou pré-bel-ordre) sur un ensemble $D$ si pour toute suite infinie $(s_i)_{i \in \mathbb{N}} \in D^{\mathbb{N}}$, il existe $i < j$ tels que $s_i \trianglelefteq s_j$.

**Prop 44 :** Soit $\leq$ un pré-bel-ordre. On a équivalence entre :

- $\leq$ est un pré-bel-ordre.
- $\forall (s_i)_{i \in \mathbb{N}} \in D^{\mathbb{N}}$, $\exists \phi : \mathbb{N} \to \mathbb{N}$ strictement croissante, telle que $\forall i \in \mathbb{N},\ s_{\phi(i)} \trianglelefteq s_{\phi(i+1)}$.

**Th 45 :** de Higman : soit $\leq$ un pré-bel-ordre sur $D$. On définit $\trianglelefteq$ sur $D^*$ :

- $\varepsilon \trianglelefteq \varepsilon$
- $s \trianglelefteq t$ et $b \in D$, alors $s \trianglelefteq bt$.
- si $a \leq b$ et $s \trianglelefteq t$ alors $as \trianglelefteq bt$.

$\trianglelefteq$ est un pré-bel-ordre.

**Déf 46 :** Un ordre de réduction sur $T(\Sigma)$ est un ordre bien fondé, clos par substitutions et $\Sigma$-opérations. Un ordre de simplification $<$ est un ordre sur les termes, clos par substitution, par $\Sigma$-opérations, et : $\forall f \in \Sigma^{(n)},\ \forall i \leq n,\ x_i < f(x_1, \dots, x_n)$.

**Th 47 :** Un SR est terminant ssi il existe un ordre de réduction $>$ satisfaisant $l > r$ pour tout $l \to r \in R$.

BAA p 103

**Déf 48 :** $\Sigma$ signature, muni d'un pré-bel-ordre $\leq$. L'ordre de plongement $\trianglelefteq$ :

- si $s \trianglelefteq x_i$ alors $s \trianglelefteq t(x_1, \dots, x_i, \dots, x_n)$.
- si $s \leq t$, $a_1, \dots, a_m, b_1, \dots, b_n$ des termes avec $m \leq n$, et une suite croissante $j_1, \dots, j_m$ tq $a_i \trianglelefteq b_{j_i}$, alors $s(a_1, \dots, a_m) \trianglelefteq t(b_1, \dots, b_n)$.

**Th 49 :** Soit $<$ un ordre de simplification sur $T(\Sigma)$.

Si $\Sigma$ est fini, alors $<$ est bien fondée.

DVT

Annexe 1 :

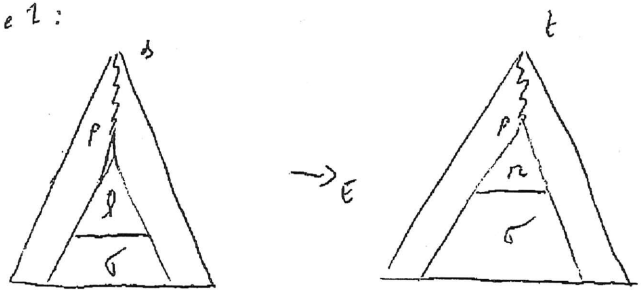
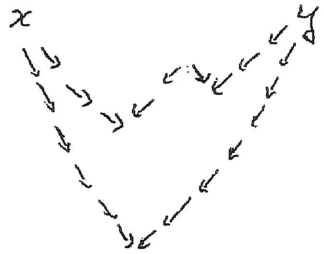
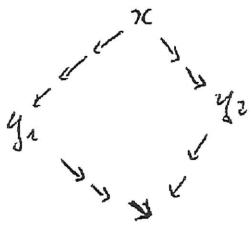



Illustration de $s \to_\varepsilon t$.

Annexe 2 :

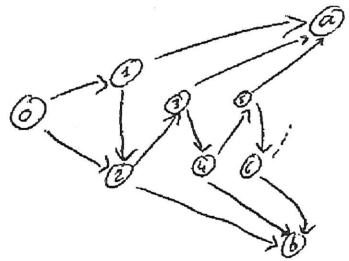



Annexe 3 :

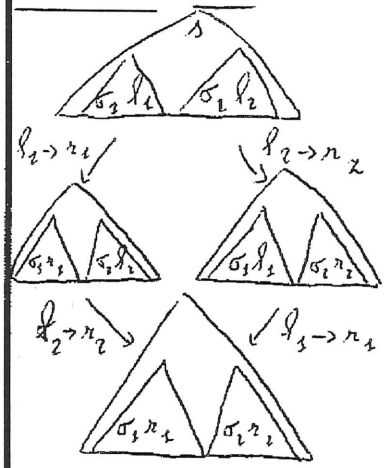



Annexe 4 :

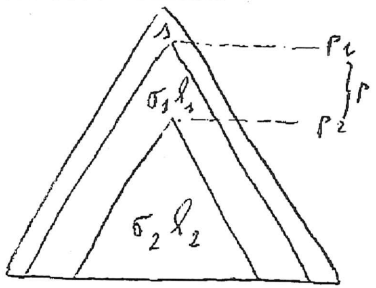

Annexe 5


Annexe 6 : cas 1 :




Annexe 7 : cas 2 :




Annexe 8 : Cas 2.1.