Maîtrise de Mathématiques

Logique et Complexité, TD6

Natacha Portier

Jeudi 27 mars 2003

Exercice 1 : Éliminez les quanteurs dans la formule suivante, pour le corps des nombres complexes dans le langage des corps, puis pour le corps des nombres réels dans le langage des corps ordonnés :

$$\forall u \exists v \quad xv^{29} + yv^4 + u^{2002} = 0$$

Définitions : Un corps ordonné est un corps dont on distingue une partie, appelée le cône des éléments positifs ou nuls, qui doit satisfaire aux conditions suivantes : -1 n'est pas positif ; pour tout x, de x ou de $-x$ l'un des deux est positif ; la somme de deux éléments positifs est positive ; le produit de deux éléments positifs est positif.

La relation "$x - y$ est positif" définit une relation R. On peut montrer que : 1 est positif ; la caractéristique du corps est nulle ; tout carré est positif ; si x est positif non nul alors $-x$ ne l'est pas (d'où la définition de négatif et de valeur absolue) ; le produit de deux négatifs est positif et le produit d'un négatif et d'un positif est négatif ; R est un ordre total compatible avec l'addition et la multiplication : si $x \leq y$ alors $x + z \leq y + z$ et si de plus $z \geq 0$ alors $xz \leq yz$, alors que si $z \leq 0$ on a $xz \geq yz$; l'ordre est dense et sans extrémités et admet l'inégalité triangulaire.

Réciproquement, un corps muni d'un ordre compatible avec l'addition et la multiplication admet un cône positif ayant les bonnes propriétés. Un corps ordonné sera dorénavant une structure $(K; =; \leq; 0; 1; +; -; \times)$.

Un corps ordonné est réel clos s'il satisfait le théorème de la valeur intermédiaire pour les polynômes : un polynôme s'annule entre deux points où il prend des valeurs de signes opposés.

Nous allons montrer que la théorie des corps réels clos, qui est une théorie du premier ordre (exercice : donner les axiomes) est complète et admet l'élimination des quanteurs.

Question 2,1 : encadrement des zéros Montrer ce qui suit. Si $P(x)$ est un polynôme unitaire à coefficients dans le corps ordonné K et si m est le maximum des valeurs absolues des coefficients alors les zéros de P dans K sont compris entre $-m-1$ et $m+1$.

Question 2,2 : continuité Montrer ce qui suit. Dans un corps ordonné si $P(a) > 0$ il existe $\epsilon > 0$ tel que $P(x)$ reste positif sur le segment $[a-\epsilon; a+\epsilon]$.

Question 2,3 : monotonie locale Montrer ce qui suit. Dans un corps ordonné si $P'(a) > 0$ il existe $\epsilon > 0$ tel que $P(x) > P(a)$ si $a < x \leq a+\epsilon$ et $P(x) < P(a)$ si $a - \epsilon \leq x$.

Question 2,4 : Montrer ce qui suit dans le cas des corps réels clos. Dans un corps ordonné, si P est un polynôme non constant dont le dérivé P' reste positif ou nul sur le segment $[a; b]$ $(a < b)$ alors $P(a) < P(b)$.

Question 2,5 : existence de la clôture réelle Montrer que tout corps ordonné se plonge dans un corps réel clos. Indication : ajouter les éléments manquants les uns après les autres, comme pour construire la clôture algébrique.

Question 2,6 : unicité Si k est un sous-corps de K on appelle clôture algébrique relative de k dans K l'ensemble (qui est un corps) des éléments de K qui sont algébriques sur k.

Soient k_1 et k_2 des corps ordonnés isomorphes plongés dans des corps K_1 et K_2 réels clos. Soient L_1 et L_2 les clôtures algébriques relatives de k_1 dans K_1 et de k_2 dans K_2. Alors tout isomorphisme entre k_1 et k_2 s'étend, et de manière unique, en un isomorphisme de corps ordonnés entre L_1 et L_2.

Question 2,7 : Montrer que la théorie des corps réels clos est complète et admet l'élimination des quanteurs.

Définitions : Soient $\mathcal{L}$ un langage, $\mathfrak{M}$ et $\mathfrak{N}$ deux structures sur $\mathcal{L}$, p un entier et σ une application d'un sous-ensemble de M dans un sous-ensemble de N. L'application σ est un 0-isomorphisme si c'est un morphisme. C'est un $(p+1)$-isomorphisme si pour tout $a \in M$ (resp. $b \in N$) il existe un p-isomorphisme prolongeant σ et défini en a (resp. dont l'image contienne b).

Question 3,1 : Quel est le rapport entre un ∞-isomorphisme, un p-isomorphisme pour p fixé et un p-isomorphisme pour tout p ?

Question 3,2 : Soit $\bar{a} \in M$, $\bar{b} \in N$ des n-uples. Supposons qu'il existe un p-isomorphisme qui envoie $\bar{a}$ sur $\bar{b}$. Montrer qu'alors pour toute formule ϕ de rang de quantification au plus p on a $\mathfrak{M} \models \phi(\bar{a})$ ssi $\mathfrak{N} \models \phi(\bar{b})$.

Question 3,3 : Dans cette question, $\mathcal{L}$ est le langage contenant un prédicat binaire R en plus de l'égalité, $\mathfrak{M}$ et $\mathfrak{N}$ sont des structures où l'interprétation de R est une relation d'équivalence, M est l'union des C_n pour tout n entier où C_n est une classe d'équivalence de cardinal exactement n, et $\mathfrak{N}$ est une extension de $\mathfrak{M}$ avec un nombre quelconque de classes d'équivalence infinies. Montrer que cette extension est élémentaire.