

---

# Solució de l'examen final de Lògica

F. M. E.

15/01/2008

---

## Problemes Resolts

**Problema 1.** Sigui  $(X, \leq)$  totalment ordenat. Demostreu que són equivalents:

1.  $(X, \leq)$  és ben ordenat.
2. A  $(X, \leq)$  val el principi d'inducció següent: Si  $S$  és un subconjunt de  $X$  tal que

$$\text{per a cada } x \text{ de } X \text{ si } \{y \in X \mid y < x\} \subseteq S \text{ llavors } x \in S, \quad (1)$$

llavors  $S = X$ .

(indicació: Feu-ho per reducció a l'absurd. Per demostrar la implicació  $2 \Rightarrow 1$ , donat  $T \subseteq X$  considereu el conjunt  $\{x \in X \mid x < y \text{ per a tot } y \in T\}$ ).

### Solució:

$1 \Rightarrow 2$  Sigui  $S$  és un subconjunt de  $X$  satisfent (1). Hem de demostrar que  $S = X$ . Si no fos així, prenem  $a$  el mínim de  $X \setminus S$ , que existeix per 1. Per ser  $a$  mínim,  $\{y \in X \mid y < a\}$  no té elements de  $X \setminus S$  i per tant està contingut a  $S$ . Com que  $S$  satisfà (1) resulta que  $a \in S$ , contradicció.

$2 \Rightarrow 1$  Recíprocament, sigui  $T$  un subconjunt no buit de  $X$ . Hem de veure que  $T$  té mínim. Si no fos així, considerem  $S := \{x \in X \mid x < y \text{ per a tot } y \in T\}$ . Anem a demostrar que  $S$  satisfà (1). Sigui  $x$  un element qualsevol de  $X$ , distingirem segons  $x \in S$  o no. Si  $x$  és de  $S$  ja ho tenim, mentre que si  $x$  no és de  $S$ , hi ha algun  $y \in T$  amb  $y \leq x$ . Com que  $T$  no té mínim resulta que hi ha algun  $z \in T$  amb  $z < y \leq x$  i per tant  $z \in \{y \in X \mid y < x\} \not\subseteq S$ . Com que  $S$  satisfà (1), per la hipòtesi 2 resulta que  $S = X$ . Però això implica que  $T$  és buit, contradicció.

**Problema 2.** Considerem la signatura que només conté un símbol de relació binària  $+$ .

1. Si  $G$  és un grup i  $r$  un enter positiu, demostreu que el conjunt  $rG = \{rg \mid g \in G\}$  és definible ( $rg$  denota la suma  $\overbrace{g + \cdots + g}^r$  de  $g$  amb si mateix  $r$  cops).
2. Quins són els conjunts definibles de  $\mathbb{Z}/3\mathbb{Z}$  (el grup cíclic de 3 elements)?
3. I els de  $\mathbb{Z}/p\mathbb{Z}$ , on  $p$  és primer?
4. I els de  $\mathbb{Z}/p^2\mathbb{Z}$ ?
5. I els de  $\mathbb{Z}/p^n\mathbb{Z}$ ?

(Indicació: els automorfismes del grup cíclic de  $m$  elements  $\mathbb{Z}/m\mathbb{Z}$  són de la forma  $\bar{x} \mapsto r\bar{x}$  amb  $r$  primer amb  $m$ . Al grup cíclic  $G = \mathbb{Z}/p^n\mathbb{Z}$  de  $p^n$  elements, useu els conjunts de la forma  $p^k G$  per a construir els ‘àtoms’).

**Solució:**

1. La fórmula  $\exists y(x = \overbrace{y + \cdots + y}^n)$ , on  $\overbrace{y + \cdots + y}^n$  és el terme que representa sumar  $y$   $n$  cops amb si mateix, defineix el conjunt  $nG$ .
2. A  $G = \mathbb{Z}/3\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}\}$  podem definir els dos subconjunts  $\{\bar{0}\}$  i  $\{\bar{1}, \bar{2}\}$  mitjançant les fórmules (amb variable lliure  $x$ )  $\forall y(x + y = y)$  i  $\neg \forall y(x + y = y)$  respectivament. Si veiem que dos punts qualssevol del segon estan a la mateixa òrbita per automorfisme (hi ha un automorfisme de l’estructura que envia l’un a l’altre) aquest dos conjunts no es poden trencar en trossos definibles més petits i per tant tot conjunt definible serà reunió d’alguns d’aquests. Però l’automorfisme  $\bar{x} \mapsto \bar{2}\bar{x}$  envia  $\bar{1}$  a  $\bar{2}$ . Tindrem doncs  $2^2$  conjunts definibles:  $\emptyset$ ,  $\{\bar{0}\}$ ,  $\{\bar{1}, \bar{2}\}$  i  $\{\bar{0}, \bar{1}, \bar{2}\}$ .
3. Ara és idèntic al cas anterior, però amb  $p$  primer qualssevol. Les mateixes fórmules d’abans defineixen els conjunts  $\{\bar{0}\}$  i  $\{\bar{1}, \dots, \overline{p-1}\}$ . També en aquest cas tots els punts del segon conjunt estan a la mateixa òrbita per automorfisme: si  $0 \leq r < p$ ,  $h_r : \bar{x} \mapsto r\bar{x}$  envia  $\bar{1}$  a  $\bar{r}$ ; per tant  $f_s \circ f_r^{-1}$  envia  $\bar{r}$  a  $\bar{s}$  quan  $0 \leq r, s < p$ .
4. Considerem els conjunts  $A_2 = p^2G$ ,  $A_1 = pG - p^2G$ ,  $A_0 = G - pG$ . Aquests tres conjunts són definibles ja que són diferència de definibles (apartat 1). Veiem que  $A_2 = \{\bar{0}\}$ ,  $A_1 = \{\bar{p}, \bar{2p}, \dots, \overline{(p-1)p}\}$  i  $A_0 = \{\bar{r} \mid 0 < r < p^2, r \text{ primer amb } p\}$ , on les classes denoten restes mòdul  $p^2$ . L’afirmació és clara en el cas de  $A_2$ . Òbviament  $\{\bar{p}, \bar{2p}, \dots, \overline{(p-1)p}\} \subseteq A_1$ . Recíprocament si  $\bar{k} \in A_1$  llavors  $\bar{k} = p\bar{r}$  per un cert  $0 \leq r < p^2$ , però això implica que  $p$  divideix  $k$ .  $k \neq 0$  ja que  $\bar{k} \notin pG$ . De la mateixa manera es fa per  $A_0$ . Ara veiem que tots els elements de  $A_1$  estan a la mateixa

òrbita: l'automorfisme  $f_s \circ f_r^{-1}$  envia  $\overline{rp}$  a  $\overline{sp}$  si  $0 < r, s < p$ . El mateix passa amb  $A_0$ :  $f_s \circ f_r^{-1}$  envia  $\overline{r}$  a  $\overline{s}$  si  $0 < r, s < p^2$  i els dos són primers amb  $p$ . Així tenim  $2^3$  conjunts definibles, corresponents a prendre totes les possibles unions d'alguns  $A_i$ .

5. Considerem ara  $A_i = p^i G - p^{i+1} G$  per  $i = 0, \dots, n-1$  i  $A_n = p^n G$ . Aquests conjunts són definibles per l'apartat 1. Si veiem que dos punts qualssevol del mateix  $A_i$  estan a la mateixa òrbita ja haurem acabat: els conjunts definibles s'obtenen fent unions, de totes les maneres possibles d'alguns dels  $A_0, A_1, \dots, A_n$ . Per tant hi haurà  $2^{n+1}$  conjunts definibles. Per a  $A_n$  és clar, doncs només conté el neutre. Mostrem que  $A_i = \{ \overline{p^i r} \mid 0 < r < p^{n-i}, r \text{ primer amb } p \}$ . Si  $0 < r < p^{n-i}$  i  $r$  és primer amb  $p$ , òbviament  $\overline{p^i r} \in p^i G$  i  $\overline{p^i r} \notin p^{i+1} G$  ja que si hi fos tindriem  $\overline{p^i r} = \overline{p^{i+1} s}$  i això implica que  $p$  divideix  $r$ . Si  $g \in p^i G - p^{i+1} G$ ,  $g = \overline{p^i t}$  per un cert  $t$ . Si dividim  $t$  per  $p^{n-i}$  obtenim  $t = r + qp^{n-i}$  i per tant  $g = \overline{p^i r}$ . Com que  $g \notin p^{i+1} G$ ,  $r$  ha de ser primer amb  $p$ . Un cop fet això és fàcil verificar que tots els punts a  $A_i$  estan a la mateixa òrbita: l'automorfisme  $f_s \circ f_r^{-1}$  envia  $\overline{rp^i}$  a  $\overline{sp^i}$  si  $0 < r, s$  són primers amb  $p$ .

**Problema 3.** Suposem que  $\Sigma$  és un conjunt de fórmules i  $\varphi, \psi$  són fórmules.

1. Demostreu que si  $x$  és una variable que no és lliure ni a  $\Sigma$  ni a  $\psi$ , llavors:

$$\Sigma, \varphi \models \psi \quad \text{si i només si} \quad \Sigma, \exists x \varphi \models \psi$$

2. Demostreu que si  $c$  és una constant que no apareix ni a  $\Sigma$  ni a  $\varphi$ , llavors:

$$\Sigma \models \varphi_c^x \quad \text{si i només si} \quad \Sigma \models \forall x \varphi$$

**Solució:**

1. La implicació de dreta a esquerra és fàcil usant que  $\varphi \models \exists x \varphi$ . Suposem que  $\Sigma, \exists x \varphi \models \psi$ . Si  $M \models \Sigma[\sigma]$  i  $M \models \varphi[\sigma]$  llavors també  $M \models \exists x \varphi[\sigma]$  i per tant  $(\Sigma, \exists x \varphi \models \psi) M \models \psi[\sigma]$ . Hem usat  $M \models \Sigma[\sigma]$  per denotar que  $M \models \theta[\sigma]$  per a tota  $\theta \in \Sigma$ .

Recíprocament suposem  $\Sigma, \varphi \models \psi$  i siguin  $M$  una estructura i  $\sigma : V \rightarrow D_M$  una assignació de variables tal que  $M \models \Sigma[\sigma]$  i  $M \models \exists x \varphi[\sigma]$ . Hem de veure que  $M \models \psi[\sigma]$ . Com que  $M \models \exists x \varphi[\sigma]$ , per definició existeix  $a \in D_M$  tal que  $M \models \varphi[\sigma_a^x]$ . Com que  $x$  no és variable lliure a cap de les fórmules de  $\Sigma$ , pel lema de coincidència, tenim que  $M \models \Sigma[\sigma_a^x]$ . Com que  $\Sigma, \varphi \models \psi$ , llavors  $M \models \psi[\sigma_a^x]$ . Com que  $x$  tampoc és lliure a  $\psi$ , pel lema de coincidència,  $M \models \psi[\sigma]$ .

2. La implicació de dreta a esquerra és immediata usant que  $\forall x\varphi \models \varphi_c^x$  i la transitivitat de la conseqüència lògica.

Recíprocament suposem  $\Sigma \models \varphi_c^x$  i siguin  $M$  una estructura i  $\sigma : V \rightarrow D_M$  una assignació de variables tal que  $M \models \Sigma[\sigma]$ . Hem de veure que  $M \models \forall x\varphi[\sigma]$ . Donat un element  $a \in D_M$  qualsevol hem de veure que  $M \models \varphi[\sigma_a^x]$ . Considerem  $N$  l'estructura que és igual a  $M$  llevat que li canviem la interpretació de la constant  $c$ : fem  $c^N := a$ . Com que la constant  $c$  no apareix a  $\Sigma$  i  $M \models \Sigma[\sigma]$ , resulta que  $N \models \Sigma[\sigma]$ . Com que  $\Sigma \models \varphi_c^x$  tenim que  $N \models \varphi_c^x[\sigma]$ . Pel lema de substitució  $N \models \varphi[\sigma_{c^N}^x]$ , és a dir  $N \models \varphi[\sigma_a^x]$ . Com que  $c$  no apareix a  $\varphi$  podem concloure  $M \models \varphi[\sigma_a^x]$ .

**Problema 4.** Es aquest exercici denotarem els conjunts amb minúscules i les classes amb majúscules. Recordem que una aplicació  $F$  és una classe de parells ordenats tals que si  $(x, y) \in F$  i  $(x, z) \in F$  llavors  $y = z$ . Podeu usar que hi ha una fórmula predicativa (amb variable lliures  $x, y, z$ ) que expressa  $x = (y, z)$ .

1. Escribeu una fórmula amb variable lliures  $F, X$  que expressi que el domini de  $F$  és  $X$ .
2. Escribeu una fórmula amb variable lliures  $F, Y$  que expressi que el recorregut (o imatge) de  $F$  està contingut a  $Y$ .
3. Usant els apartats anteriors demostra que si  $X$  i  $Y$  són classes llavors

$${}^X Y = \{f \mid f \text{ és una aplicació de } X \text{ en } Y\}$$

també és una classe. Indica quins axiomes has usat.

4. Demostra que si  $x$  i  $y$  són conjunts llavors  ${}^x y$  també és conjunt. Quins axiomes has usat?
5. Què podem dir de  ${}^X Y$  quan  $X$  és classe pròpia?

### Solució:

1. Una manera de fer-ho seria:

$$\varphi(X, F) := \forall x \left( x \in X \leftrightarrow \exists y \exists z ({}'z = (x, y)' \wedge z \in F) \right)$$

Aquesta fórmula només que expressa que el domini de  $F$  és igual a  $X$ , però no expressa que  $F$  és una funció.

2. Una manera de fer-ho seria:

$$\psi(Y, F) := \forall y \left( \exists x \exists z ({}'z = (x, y)' \wedge z \in F) \rightarrow y \in Y \right)$$

Aquesta fórmula només que expressa que el recorregut (o imatge) de  $F$  està contingut a  $Y$ , però tampoc expressa que  $F$  és una funció.

3. L'axioma de reemplaçament diu (entre altres coses) que si  $X, Y$  són classes i  $\mu(f, X, Y)$  és una fórmula predicativa (només quantifiquem sobre conjunts) llavors  $\{f \mid \mu(f, X, Y)\}$  és una classe. Tot es redueix escriure una fórmula predicativa  $\mu(f, X, Y)$  que expressi 'f és una funció amb domini igual a  $X$  i recorregut contingut en  $Y$ ' i aplicar-ho. Pels apartats anteriors ja tenim fórmules  $\varphi(X, F)$  i  $\psi(Y, F)$  que expressen que el domini de  $F$  és igual a  $X$  i el recorregut de  $F$  està contingut a  $Y$ . A més aquestes fórmules són predicatives. Estem usant (vist a classe) que  $x = (y, z)$  es pot expressar amb una fórmula predicativa. També hem vist a teoria que hi ha una fórmula predicativa, posem  $\theta(F)$ , que expressa que  $F$  és una funció. Per exemple, podem prendre

$$\theta(F) := \forall z \exists x \exists y \left( z \in F \rightarrow 'z = (x, y)'' \right) \wedge \forall x \forall u \forall v \left( '(x, u) \in F' \wedge '(x, v) \in F' \rightarrow u = v \right),$$

on  $'(x, u) \in F'$  és una abreviatura de la fórmula  $\exists z ('z = (x, u)' \wedge z \in F)$ .

Així, la fórmula  $\mu(f, X, Y)$  és  $\theta(f) \wedge \varphi(X, f) \wedge \psi(Y, f)$ .

4. Observem que  ${}^x y \subseteq P(x \times y)$ , doncs tot element  $f \in {}^x y$  és un conjunt de parells de  $x \times y$  i per tant  $f \in P(x \times y)$ . Per l'aparta anterior sabem que  ${}^x y$  és una classe. Ja vàrem veure que si  $x$  i  $y$  són conjunts,  $x \times y$  és conjunt. Això sortia d'aplicar els axiomes del parell, comprensió, parts i subconjunts (de fet reemplaçament). Ara apliquem subconjunts un altre cop i ja hem acabat.
5. Quan  $X$  és classe pròpia  ${}^X Y$  és buit (i per tant també és conjunt!). La raó és que tota aplicació  $F$  amb domini IGUAL a  $X$  també ha de ser classe pròpia. Això és per l'axioma de reemplaçament (informalment: hi ha tantes parelles a  $F$  com elements té  $X$ ). Considerem la funció  $G : F \rightarrow X$  que a cada parella de  $F$  l'hi extreu la primera coordenada ( $G((x, y)) = x$ ). Si  $F$  fos conjunt, per reemplaçament,  $X$  (la imatge de  $G$ ) també seria conjunt.