

1. Martin-Löf-típuselmélet

Martin-Löf-típuselméletek olyan programozási nyelvek, amelyek tisztán és teljesen típusos, funkcionális nyelvek, típusokon belül megfogalmazhatók a programokkal szemben támasztott elvárások, és ha helyesek, akkor a programok típusellenőrzése során ezek automatizált módon igazolást nyernek.

A Martin-Löf-típuselméletek két alapvető fogalommal dolgoznak: az egyik a *függő függvénytípus*, a másik az *egyenlőség típus*. Ennek következménye, hogy elég kifejezőerővel rendelkeznek ahhoz, hogy a matematikai állításokat és bizonyításokat formalizálni lehessen bennük. Konkrétan, alkalmas típuselméletben, az egész matematika elhelyezhető szőröstül-bőröstül.

Egy minimális extenzionális Martin-Löf-típuselmélettel (MEMLTT) kezdünk, amelyik alkalmas a fő problémák és motivációk bemutatására.

1.1. Megjegyzés (Általánosított Descartes-szorzat a halmazelméletben). Halmazelméleti tanulmányainkból ismert fogalom egy függvényrendszer (vagy függvénycsalád) Descartes-szorzata. Legyen

$$F : I \rightarrow \text{Set}, i \mapsto A_i$$

egy olyan függvény, ami egy I halmaz minden egyes i eleméhez egy A_i halmazt rendel. Ezek szerint $F(i) = A_i$, minden $i \in I$ -re. (Set a halmazok osztálya. Az I -n értelmezett halmazcsaládokat néha Set^I jelöli.) Sokszor az egyszerűség kedvéért ezt csak az

$$(A_i)_{i \in I} \text{ vagy } (A(i))_{i \in I}$$

szimbólummal jelöljük, nem elfelejtve, hogy ez egy függvény, azaz minden j -re $(A_i)_{i \in I}(j) = A_j$. Egy ilyen függvénycsalád *szorzata* függvények egy olyan halmaza, amelyben a függvények i -hez tartozó értékei éppen a család A_i elemében van benne:

$$\prod_{i \in I} A_i \stackrel{\text{def.}}{=} \left\{ f : I \rightarrow \bigcup_{i \in I} A_i \mid f(i) \in A_i \right\}.$$

Ezt hívjuk **függő szorzatnak** vagy **általánosított Descartes-szorzatnak**.

1.2. Megjegyzés (Kiválasztási axióma ZFC-ben). A szorzat elemeit alkotó függvények úgy nevezett kiválasztófüggvények, mert minden egyes i -re f voltaképpen kiválaszt az A_i -ből egy elemet. A legismertebb képviselője a Riemann-integrál elméletében található, amikor egy $[a, b]$ intervallum felosztása esetén az adott részintervallumból kiválasztunk egy elemet és ott számoljuk ki az integrálandó függvény egy értékét a téglányösszeg kiszámításához.

A szorathoz kapcsolódik a formális-axiomatikus halmazelmélet egyik leghírhedtebb axiómája, a **kiválasztási axióma** (a Zermeli-Fraenkel-choice halmazelmélet (ZFC) kódjában a „choice” erre utal.)

1.1. Definíció (Kiválasztási axióma). A halmazelméletben kiválasztási axiómának nevezzük azt az állítást, hogy „nemüres halmazok nemüres családjának szorzata nem üres”:

$$(\forall I \neq \emptyset)(\forall (A_i) \in \text{Set}^I) \left((\forall i \in I)(A_i \neq \emptyset) \rightarrow \left(\prod_{i \in I} A_i \right) \neq \emptyset \right).$$

Jóllehet ez az axióma a matematikában nagyon széles alkalmazásra talált (pl. igazolható a segítségével, hogy minden lineáris térnek van bázisa), megkövetelése a programozásban használatos matematikákban meglehetősen sok programvégrehajtási problémával járna (ezt úgy mondjuk, hogy ez az állítás erősen inkonstruktív). Hogy Bertrand Russell magyarázatával éljünk, ha semmi se lenne a világon a számítógép számára, csak egy pár zokni, akkor sehogy nem lehetne megmondani a számítógépnek, hogy ebből a (tökéletesen ugyanolyan két zokniból álló) párból *válasszon ki* egyet, mert nem lenne támpontja a kiválasztásra.

1.2. Definíció (Minimális extenzionális Martin-Löf típuselmélet (MEMLTT)). Az MEMLTT egy struktúra, amely a következő komponensekből áll:

Szortok

Típusok: Egy halmaz*, Ty.

Termek: Minden $A : Ty$ típushoz egy $Tm(A)$ halmaz*, amely A termeit, az A típusú programokat tartalmazza.

Műveletek

Függő függvénytípus (Π)

Π -formáció: Bármely $A : Ty$ típus és $B : Tm(A) \rightarrow Ty$ típusfüggvény esetén létezik egy $\Pi(A, B) : Ty$ típus.

$$\frac{A : Ty \quad B : Tm(A) \rightarrow Ty}{\Pi(A, B) : Ty}$$

Π -bevezetés (*lambda-absztrakció*): Bármely $A : Ty$, $B : Tm(A) \rightarrow Ty$ és metaelméleti $f : \prod_{x:Tm(A)} Tm(B(x))$ függvény esetén létezik egy $lam(A, B, f) : Tm(\Pi(A, B))$ term.

$$\frac{A : Ty \quad B : Tm(A) \rightarrow Ty \quad f : \prod_{x:Tm(A)} Tm(B(x))}{lam(A, B, f) : Tm(\Pi(A, B))}$$

Π -elimináció (*applikáció*): Bármely $A : Ty$, $B : Tm(A) \rightarrow Ty$, $t : Tm(\Pi(A, B))$ és $a : Tm(A)$ esetén létezik egy $app t a : Tm(B(a))$ term.

$$\frac{t : Tm(\Pi(A, B)) \quad a : Tm(A)}{app t a : Tm(B(a))}$$

Azonosságtípus (Id)

Id-formáció: Bármely $A : Ty$ típus és $x, y : Tm(A)$ termék esetén létezik egy $Id_A(x, y) : Ty$ típus.

$$\frac{A : Ty \quad x, y : Tm(A)}{Id_A(x, y) : Ty}$$

Id-bevezetés (reflexivitás): Ha a metaelméletben x és y megegyezik (p egy bizonyítéka $x = y$ -nak), akkor létezik egy term, amely ezt az azonosságot tanúsítja a típuselméleten belül.

$$\frac{A : Ty \quad x, y : Tm(A) \quad p : (x = y)}{refl(A, x, y, p) : Tm(Id_A(x, y))}$$

Id-elimináció (azonosság-tükrözés): Ha létezik egy term, amely az x és y azonosságát tanúsítja, akkor x és y a metaelméletben is egyenlő.

$$\frac{p : \text{Tm}(\text{Id}_A(x, y))}{x = y}$$

Egyenlőségek

A Π -típusra vonatkozó szabályok

β -szabály: Bármely $f : \prod_{x:\text{Tm}(A)} \text{Tm}(B(x))$ és $a : \text{Tm}(A)$ esetén az applikáció kiértékeli a függvényt.

$$\text{app lam}(A, B, f) a = f(a)$$

η -szabály: Bármely $t : \text{Tm}(\Pi(A, B))$ termre teljesül, hogy azonos az η -expanziójával.

$$\text{lam}(A, B, x \mapsto \text{app } t \ x) = t$$

Az Id-típusra vonatkozó szabályok

β -szabály: Bármely $p : \text{Tm}(\text{Id}_A(x, y))$ azonosság-bizonyítékra teljesül:

$$\text{refl}(\text{equality_reflection}(p)) = p$$

η -szabály: Bármely metaelméleti $q : (x = y)$ bizonyításra teljesül:

$$\text{equality_reflection}(\text{refl}(q)) = q$$

2. Az azonosság-bizonyítások Egyértelműsége (UIP)

Ebben a fejezetben megmutatjuk, hogy az EMLTT axiómáiból következik az azonosság-bizonyítások egyértelműsége (Uniqueness of Identity Proofs, UIP).

2.1. Axióma (UIP a metaelméletben). A bizonyítások irrelevanciáját feltételezzük a metaelméleti proposíciókra.

$$\forall(A : \text{Type}), \forall(x, y : A), \forall(p, q : x = y), \quad p = q.$$

2.1. Tétel (Az η_{Id} levezethető). Minden $A : \text{Ty}$, $x, y : \text{Tm}(A)$ és $t : (x = y)$ metaelméleti bizonyítás esetén:

$$\text{equality_reflection}(A, x, y, \text{refl}(A, x, y, t)) = t$$

Bizonyítás. Legyenek A, x, y és t adottak. A bal és jobb oldal is az $x = y$ proposíció egy-egy bizonyítása a metaelméletben. A metaelméleti UIP axióma alapján bármely két ilyen bizonyítás egyenlő. Ezzel a tétel bizonyított. \square

2.2. Tétel (UIP levezethető a típuselméletben). Minden $A : Ty$, $x, y : Tm(A)$ és $p, q : Tm(Id_A(x, y))$ esetén $p = q$. Ez azt jelenti, hogy minden azonosságtípus h-propozíció (azaz legfeljebb egy terme van).

Bizonyítás. Legyenek A, x, y, p, q adottak. Az Id -típus β -szabálya szerint:

$$p = \text{refl}(A, x, y, \text{equality_reflection}(A, x, y, p))$$

$$q = \text{refl}(A, x, y, \text{equality_reflection}(A, x, y, q))$$

Az $\text{equality_reflection}$ függvények értékei metaelméleti bizonyítások az $x = y$ tényre. A metaelméleti UIP axióma szerint ezek a bizonyítások egyenlőek:

$$\text{equality_reflection}(A, x, y, p) = \text{equality_reflection}(A, x, y, q)$$

Mivel a refl függvény argumentumai egyenlőek, a függvényértékek is egyenlőek lesznek:

$$\text{refl}(A, x, y, \dots) = \text{refl}(A, x, y, \dots)$$

Ebből következik, hogy $p = q$. □

2.3. Tétel (K-szabály levezethetősége). Minden $A : Ty$, $x : Tm(A)$ és $p : Tm(Id_A(x, x))$ esetén:

$$p = \text{refl}(A, x, x, \text{eq_refl}_x)$$

ahol eq_refl_x az $x = x$ triviális bizonyítása.

Bizonyítás. Ez közvetlen következménye az előző tételnek (UIP a típuselméletben). Mivel a $Id_A(x, x)$ típusnak legfeljebb egy eleme lehet, és $\text{refl}(A, x, x, \text{eq_refl}_x)$ egy ilyen elem, ezért minden p elemnek egyenlőnek kell lennie vele. □

3. Függvény-extenzionalitás

A függvény-extenzionalitás azt mondja ki, hogy két függvény akkor és csak akkor egyenlő, ha pontonként ugyanazt az értéket adják. Ez levezethető az EMLTT η -szabályából.

3.1. Tétel (Függvény-extenzionalitás). Bármely $A : Ty$, $B : Tm(A) \rightarrow Ty$ és $f, g : Tm(\Pi(A, B))$ esetén, ha

$$\forall x : Tm(A), \quad \text{app } f \ x = \text{app } g \ x$$

akkor $f = g$.

Bizonyítás. Tegyük fel, hogy f és g pontonként egyenlőek. A Π -típus η -szabálya szerint minden t függvényre $t = \text{lam}(x \mapsto \text{app } t \ x)$. Ezt alkalmazva f -re és g -re:

$$f = \text{lam}(x \mapsto \text{app } f \ x)$$

$$g = \text{lam}(x \mapsto \text{app } g \ x)$$

Mivel a feltétel szerint $\text{app } f \ x = \text{app } g \ x$ minden x -re, a két λ -kifejezés teste megegyezik. Ebből következik, hogy a két absztrakció is egyenlő, tehát $f = g$. □

4. Kombinátorok és azonosságok

Ebben a részben bemutatunk néhány alapvető kombinátort és bizonyítjuk azok tulajdonságait. A $A \rightarrow B$ jelölést a nem-függő függvénytípusra használjuk: $\Pi(A, \text{fun } _ \Rightarrow B)$.

4.1. Lemma (I kombinátor). Minden $A : \text{Ty}$ típushoz létezik egy term $\text{Tm}(A \rightarrow A)$.

Bizonyítás. Az identitásfüggvényt a λ -absztrakcióval definiáljuk: $\text{lam}(x \mapsto x)$. Ez a term a $\text{Tm}(A \rightarrow A)$ típusba tartozik. \square

4.2. Lemma (K kombinátor). Minden $A, B : \text{Ty}$ típushoz létezik egy term $\text{Tm}(A \rightarrow (B \rightarrow A))$.

Bizonyítás. A konstansfüggvényt kétszeres λ -absztrakcióval definiáljuk: $\text{lam}(x \mapsto \text{lam}(y \mapsto x))$. Ez a term a $\text{Tm}(A \rightarrow (B \rightarrow A))$ típusba tartozik. \square

4.3. Lemma. A $\text{lam}(f \mapsto f)$ és a $\text{lam}(f \mapsto \text{lam}(x \mapsto \text{app } f \ x))$ kifejezések ugyanazt a függvényt definiálják a $(A \rightarrow A) \rightarrow (A \rightarrow A)$ típuson.

Bizonyítás. Jelölje az első kifejezést I_1 , a másodikat I_2 . Azt kell belátnunk, hogy $I_1 = I_2$. A függvény-ekstenzionalitás miatt elegendő megmutatni, hogy bármely $f : \text{Tm}(A \rightarrow A)$ argumentumra ugyanazt az értéket adják.

$$\text{app } I_1 \ f = f$$

$$\text{app } I_2 \ f = \text{lam}(x \mapsto \text{app } f \ x)$$

A Π -típus η -szabálya szerint $f = \text{lam}(x \mapsto \text{app } f \ x)$. Tehát $\text{app } I_1 \ f = \text{app } I_2 \ f$ minden f -re, amiből következik, hogy $I_1 = I_2$. \square

5. Az Azonosság Szimmetriája

5.1. Lemma (Az azonosság szimmetriája). Ha $p : \text{Tm}(\text{Id}_A(x, y))$, akkor létezik egy $q : \text{Tm}(\text{Id}_A(y, x))$.

Bizonyítás. Legyen $p : \text{Tm}(\text{Id}_A(x, y))$. Az equality-reflection szabály alapján ebből következik, hogy a metaelméletben $x = y$. Ebből triviálisan következik, hogy $y = x$ is igaz a metaelméletben. A 'refl'konstruktorral ebből létrehozhatunk egy termet a $\text{Tm}(\text{Id}_A(y, x))$ típusban. \square

6. A Refl Injektivitása

6.1. Tétel. A refl konstruktor injektív a bizonyítás argumentumára nézve. Azaz, ha A, x, y rögzítettek, és $t_1, t_2 : (x = y)$ metaelméleti bizonyítások, akkor

$$\text{refl}(A, x, y, t_1) = \text{refl}(A, x, y, t_2) \implies t_1 = t_2$$

Bizonyítás. Tegyük fel, hogy $\text{refl}(A, x, y, t_1) = \text{refl}(A, x, y, t_2)$. Vegyük mindkét oldalra az 'equality-reflection' függvényt:

$$\text{equality_reflection}(\text{refl}(A, x, y, t_1)) = \text{equality_reflection}(\text{refl}(A, x, y, t_2))$$

Az Id-típus η -szabálya szerint $\text{equality_reflection}(\text{refl}(t)) = t$. Ezt alkalmazva a fenti egyenlet mindkét oldalára kapjuk:

$$t_1 = t_2$$

Ezzel a tétel bizonyítást nyert. □

7. Természetes Számok

Az EMLTT kiterjeszthető a természetes számok típusával, amely tartalmazza a nullát, a rákövetkező (szukcesszor) műveletet és az indukciós elvet.

7.1. Definíció (EMLTT Természetes Számokkal). Ez a struktúra kiterjeszti az EMLTT-t a következőkkel:

- **Típus:** Egy Nat' : Ty típus.
- **Nulla:** Egy zero' : $\text{Tm}(\text{Nat})$ term.
- **Rákövetkező:** Egy succ' : $\text{Tm}(\text{Nat}) \rightarrow \text{Tm}(\text{Nat})$ függvény.
- **Indukciós elv ($\text{nat_ind}'$):** Bármely $P : \text{Tm}(\text{Nat}) \rightarrow \text{Ty}$ predikátum, $p_0 : \text{Tm}(P(\text{zero}))$ báziseset, és $p_s : (\forall k : \text{Tm}(\text{Nat}), \text{Tm}(P(k)) \rightarrow \text{Tm}(P(\text{succ}(k))))$ indukciós lépés esetén, minden $n : \text{Tm}(\text{Nat})$ -ra létezik egy term:

$$\text{nat_ind}(P, p_0, p_s, n) : \text{Tm}(P(n))$$

A következő számítási szabályokkal:

- **Nulla eset:** $\text{nat_ind}(P, p_0, p_s, \text{zero}) = p_0$
- **Szukcesszor eset:** $\text{nat_ind}(P, p_0, p_s, \text{succ}(n)) = p_s(n, \text{nat_ind}(P, p_0, p_s, n))$

Szorzat

Definíció. Legyen \mathcal{C} kategória, $A_1, A_2 : \mathcal{C}_o$. Ekkor az $A_1 \times A_2 : \mathcal{C}_o$ *szorzatobjektum* a $\text{pr}_i : \text{Hom}(A_1 \times A_2; A_i)$ ($i = 1; 2$) projekciókkal, ha minden $C : \mathcal{C}_o$ -re és $f_i : \text{Hom}(C; A_i)$ -re ($i = 1; 2$) egyértelműen létezik az az $f_1 \times f_2 : \text{Hom}(C; A_1 \times A_2)$ (*szorzatmorfizmus*), hogy az alábbi diagram kommutál:

$$\begin{array}{ccccc} A_1 & \xleftarrow{\text{pr}_1} & A_1 \times A_2 & \xrightarrow{\text{pr}_2} & A_2 \\ & \nwarrow f_1 & \uparrow f_1 \times f_2 & \nearrow f_2 & \\ & & C & & \end{array}$$

A \mathcal{C} kategória *kartéziusi*, ha benne bármely két objektumnak van szorzata.

Megjegyzés. A morfizmusszorzás definiáló tulajdonságai tehát a

$$\text{pr}_i \circ x = f_i \quad (i = 1; 2)$$

egyenlőségek. Ha valami az x -be helyettesítve igazgá teszi ezeket az egyenlőségeket, akkor az a definíció egyértelműségi kitétele miatt a szorzatmorfizmus. Ezt sokszor használjuk szorzattal való egyenlőség igazolásánál.

Lemma (Konverziós szabályok).

$$\begin{aligned} \beta_i^\times : \quad & \text{pr}_i \circ (f_1 \times f_2) = f_i & (i = 1; 2) \\ \eta^\times : \quad & (\text{pr}_1 \circ g) \times (\text{pr}_2 \circ g) = g \end{aligned}$$

ahol $g : \text{Hom}(C; A_1 \times A_2)$ tetszőleges.

Bizonyítás. A β^\times -k a kommutálás következményei. η^\times pedig a szorzatmorfizmus egyértelműségéből következik. A definícióból ugyanis, tetszőleges $g : \text{Hom}(C; A_1 \times A_2)$ -re az $f_i := \text{pr}_i \circ g$ választással triviálisan következik, hogy $f_i = \text{pr}_i \circ g$:

$$\begin{array}{ccccc} A_1 & \xleftarrow{\text{pr}_1} & A_1 \times A_2 & \xrightarrow{\text{pr}_2} & A_2 \\ & \nwarrow \text{pr}_1 \circ g & \uparrow g & \nearrow \text{pr}_2 \circ g & \\ & & C & & \end{array}$$

de ilyenből csak egy van, ami a $(\text{pr}_1 \circ g) \times (\text{pr}_2 \circ g)$ szorzatmorfizmus, így:

$$(\text{pr}_1 \circ g) \times (\text{pr}_2 \circ g) = g$$

Megjegyzés. η^\times valójában ekvivalens a szorzatmorfizmus egyértelműségével. Tegyük fel ugyanis, hogy a definícióban az egyértelműség *helyett* az $(\text{pr}_1 \circ g) \times (\text{pr}_2 \circ g) = g$ egyenlőséget követeljük meg minden $g : \text{Hom}(C; A_1 \times A_2)$ -re. Legyen g tehát olyan, hogy teljesíti a kommutálási feltételt: $\text{pr}_i \circ g = f_i$. Ekkor

$$f_1 \times f_2 = (\text{pr}_1 \circ g) \times (\text{pr}_2 \circ g) = g,$$

vagyis a szorzatmorfizmus az egyetlen olyan, ami teljesíti β^\times szabályokat.

Lemma (A morfizmusszorzás kongruenciája).

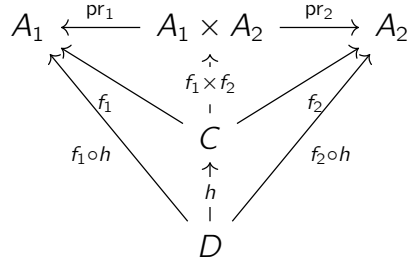
$$(f_1 \times f_2) \circ h = (f_1 \circ h) \times (f_2 \circ h)$$

ahol $h : \text{Hom}(D; C)$ tetszőleges, a definíció jelöléseivel.

Bizonyítás. Azt kell belátni, hogy $(f_1 \times f_2) \circ h$ teljesíti az $(f_1 \circ h) \times (f_2 \circ h)$ morfizmusszorzat definiáló tulajdonságait, azaz a következőket:

$$\text{pr}_i \circ x = f_i \circ h \quad (i = 1; 2).$$

Nyilván



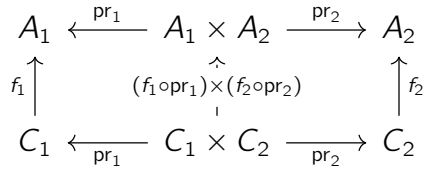
kommutál, tehát

$$\text{pr}_i \circ ((f_1 \times f_2) \circ h) = (\text{pr}_i \circ (f_1 \times f_2)) \circ h = f_i \circ h.$$

Definíció (Torii). Legyen \mathcal{C} kartéziusi kategória, $A_1, A_2, C_1, C_2 : \mathcal{C}_o$, $f_i : \text{Hom}(C_i; A_i)$ ($i = 1; 2$). Ekkor f_1 és f_2 torii-val jelölt szorzata:

$$f_1 \sqcup f_2 \stackrel{\text{def.}}{=} (f_1 \circ \text{pr}_1) \times (f_2 \circ \text{pr}_2).$$

Megjegyzés. Kommutatív diagramban ábrázolva a torii középén van:



Később látni fogjuk, hogy egy karteziánus \mathcal{C} kategória $\mathcal{C} \times \mathcal{C} \rightarrow \mathcal{C}$ bifunktoriális szorzatművelete maga a torii, amit már most is lehet látni a diagramon.

Lemma (Egyenlőségek torii-ra).

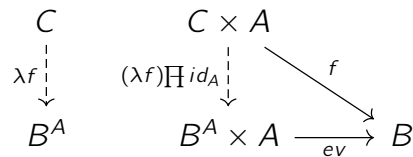
$$\beta_i^\sqcup : \text{pr}_i \circ (f_1 \sqcup f_2) = f_i \circ \text{pr}_i \quad (i = 1; 2)$$

$$(\eta^\sqcup : (\text{pr}_1 \circ g) \times (\text{pr}_2 \circ g) = g)$$

$$\sqcup \circ : (f_1 \sqcup f_2) \circ h = (f_1 \circ \text{pr}_1 \circ h) \times (f_2 \circ \text{pr}_2 \circ h)$$

Exponenciális

Definíció. Legyen \mathcal{C} kartéziusi kategória, $A, B : \mathcal{C}_o$. Ekkor a $B^A : \mathcal{C}_o$ *exponenciális objektum* az $\text{ev} : \text{Hom}(B^A \times A; B)$ evaluációval, ha minden $C : \mathcal{C}_o$ -re és $f : \text{Hom}(C \times A; B)$ -re egyértelműen létezik az a $\lambda f : \text{Hom}(C; B^A)$ (*exponenciális adjungált*), hogy az alábbi diagram kommutál:



Ha a \mathcal{C} kartéziusi kategóriában bármely két objektumunk van exponenciálisa, akkor \mathcal{C} -t *kartéziusian zárt kategóriának* nevezzük.

Megjegyzés. Tehát a hatványmorfizmus vagy exponenciális adjungált definiáló egyenlete:

$$ev \circ (x \boxtimes id_A) = f$$

Ha ez teljesül x helyére téve egy morfizmusra, akkor az az adjungált.

Lemma (Konverziós szabályok).

$$\beta^{\rightarrow} : ev \circ ((\lambda f) \boxtimes id_A) = f$$

$$\eta^{\rightarrow} : \lambda(ev \circ (g \boxtimes id_A)) = g$$

minden $g : \text{Hom}(C; B^A)$ -ra.

Bizonyítás. Az első azonos a kommutatív tulajdonsággal. A másodikhoz azt kell megmutatni, hogy van olyan f , amire teljesül, hogy

$$ev \circ (g \boxtimes id_A) = f$$

márpedig ez az f triviálisan az $ev \circ (g \boxtimes id_A)$. Így az egyértelműségből következik az η szabály.

Megjegyzés. Nyilván itt is igaz az, hogy az egyértelműségi kitétel ekvivalens az η szabállyal. Valóban! Tegyük fel, hogy teljesül $ev \circ (g \boxtimes id_A) = f$. Ekkor

$$\lambda f = \lambda(ev \circ (g \boxtimes id_A)) = g.$$

Az egyik legfontosabb technika az exponenciálisra vonatkozóan a Currying–unCurrying.

Lemma (Természetes izomorfia 1). Ha \mathcal{C} kartéziusian zárt kategória, akkor az alábbi Set-izomorfizmus teljesül:

$$\text{Hom}(C \times A; B) \cong \text{Hom}(C; B^A)$$

Bizonyítás. A definiáló diagram

$$\begin{array}{ccc} C & & C \times A \\ \downarrow \lambda f & & \downarrow g \boxtimes id_A \\ B^A & & B^A \times A \end{array} \quad \begin{array}{ccc} & & \searrow f \\ & & \downarrow ev \\ & & B \end{array} \quad \begin{array}{c} \text{ev} \circ (g \boxtimes id_A) \end{array}$$

alapján, legyen:

$$\Phi : \text{Hom}(C \times A; B) \rightarrow \text{Hom}(C; B^A), \quad \Phi(f) \stackrel{\text{def.}}{=} \lambda f$$

$$\Psi : \text{Hom}(C; B^A) \rightarrow \text{Hom}(C \times A; B), \quad \Psi(g) \stackrel{\text{def.}}{=} ev \circ (g \boxtimes id_A).$$

Set-ben az izomorfizmusok bijekció, ezért azt kell belátni, hogy

$$\Phi(\Psi(g)) = g \quad \text{és} \quad \Psi(\Phi(f)) = f$$

Rendre az η és β szabályok alapján:

$$\Phi(\Psi(g)) = \lambda(ev \circ (g \sqcup id_A)) = g$$

és

$$\Psi(\Phi(f)) = ev \circ ((\lambda f) \sqcup id_A) = f$$

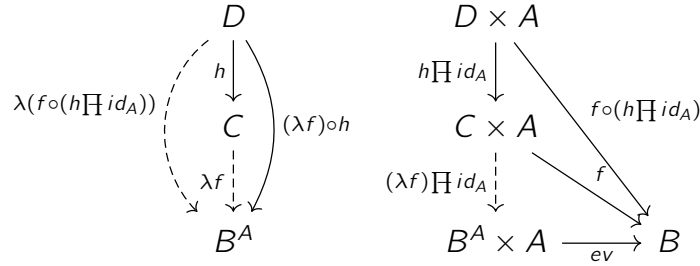
Lemma (Kongruencia).

$$\lambda(f \circ (h \sqcup id_A)) = (\lambda f) \circ h$$

minden $h : \text{Hom}(D; C)$ -re.

Bizonyítás. Elég belátni, hogy $(\lambda f) \circ h$ teljesíti az $\lambda(f \circ (h \sqcup id_A))$ definiáló egyenlőséget, azaz

$$ev \circ (((\lambda f) \circ h) \sqcup id_A) = f \circ (h \sqcup id_A).$$



$$ev \circ (((\lambda f) \circ h) \sqcup id_A) = ev \circ (((\lambda f) \circ h \circ pr_1) \times (id_A \circ pr_2)) =$$

Lemma (Természetes izomorfia 2). Ha \mathcal{C} kartéziusian zárt kategória, akkor az alábbi Set-izomorfizmus természetes \mathcal{C} -ben:

$$\Phi : \text{Hom}(C \times A; B) \rightarrow \text{Hom}(C; B^A); f \mapsto \lambda f$$

Bizonyítás. Rögzítsük A, B -t. A két funktor, ami között Φ vált két reprezentációja \mathcal{C} -nek:

$$F_{\times} : \mathcal{C}^{op} \rightarrow \text{Set}, F_{\times}(C) = \text{Hom}(C \times A; B); F_{\times}(f) = f \circ _$$

$$F_{\uparrow} : \mathcal{C}^{op} \rightarrow \text{Set}, F_{\uparrow}(C) = \text{Hom}(C; B^A); F_{\uparrow}(f) = f \circ _$$

Ezek valóban funktorok, mert $(F(f) \circ F(g))(h) = F(f)(F(g)(h)) = F(f)(g \circ h) = f \circ g \circ h = F(f \circ g)(h)$ és $F(id) = id \circ _ = _$. Ezek egyben izofunktorok, mert invertálhatók, ezért legitim reprezentációnak nevezni őket. F_{\times} és F_{\uparrow} inverze rendre:

$$G_{\times}(\text{Hom}(C \times A; B)) = C; G_{\times}(f') = f'(id), \quad G_{\uparrow}(\text{Hom}(C; B^A)) = C; G_{\uparrow}(f') = f'(id)$$

Yoneda-tételkör

Motiváció – Homset reprezentáció

$$\mathcal{C}_o \ni A \cong B \Leftrightarrow \text{Hom}(_, A) \cong \text{Hom}(_, B) \in \text{Set}$$

„Egy objektumot egyértelműen meghatároz a többi objektumhoz való viszonya”
Ezzel pl. $A^1 \cong A$ igazolható így: minden X -re

$$\text{Hom}(X, A^1) \xrightarrow{\Psi_X} \text{Hom}(X \times 1, A) \xrightarrow{\text{Hom}(\varphi_X, A)} \text{Hom}(X, A)$$

ahol Ψ_X az uncurrying, és

$$X \times 1 \xrightarrow{\varphi_X} X \Rightarrow \text{Hom}(X \times 1, A) \xrightarrow{\text{Hom}(\varphi_X, A)} \text{Hom}(X, A)$$

$\text{Hom}(\varphi_X, A)$ a Yoneda-megfeleltetés. $\text{Hom}(\varphi_X, A) \circ \Psi_X$ szintén izomorfizmus és természetes transzformáció, így a két Homset izomorf.

Funktor

$$\begin{array}{ccc} \text{id} \curvearrowright A & \xrightarrow{g} & F(\text{id}_A) = \text{id}_{F(A)} \curvearrowright F(A) \\ & \searrow f & \downarrow F(f) \\ & f \circ g & F(f \circ g) = F(f) \circ F(g) \end{array}$$

$$\begin{array}{ccc} & \xrightarrow{g} & \\ & \searrow f & \downarrow F^{op}(f) \\ & f \circ g & F^{op}(g) \circ F^{op}(f) = F^{op}(f \circ g) \end{array}$$

Az első a kovariáns funktor, a másik a kontravariáns. Példa funktorokra: a kategóriából az oppozit kategóriába menő $(_)^{op} : X \mapsto X, f \mapsto f^{op}$; $\text{Hom}(_, A)$; $\text{Hom}(_ \times A, B)$. Ez a két utóbbi Set-be menő és kontravariáns, azaz "presheaf" ($\mathcal{C}^{op} \rightarrow \text{Set}$).

Yoneda-lemma

Lemma (Yoneda-lemma 1, Nat-os alak) Legyen \mathcal{C} egy kategória, $A \in \text{Obj}(\mathcal{C})$, és $F : \mathcal{C}^{op} \rightarrow \mathbf{Set}$ egy kontravariáns funktor. Ekkor az alábbi izomorfia fennáll:

$$\text{Nat}(\text{Hom}(_, A), F) \cong F(A)$$

azaz van olyan $\Phi : \text{Nat}(\text{Hom}(_, A), F) \rightarrow F(A)$ és $\Psi : F(A) \rightarrow \text{Nat}(\text{Hom}(_, A), F)$, amelyek egymás inverzei.

Bizonyítás. (Φ) Legyen $\eta \in \text{Nat}(\text{Hom}(_, A), F)$ tetszőleges, kell ehhez egy alkalmas $F(A)$ -beli elem. Tetszőleges $X \in \mathcal{C}_0$ -ra $\eta_X : \text{Hom}(X, A) \rightarrow F(X)$ morfizmus, ezért

$$\Phi(\eta) \stackrel{\text{def.}}{=} \eta_A(\text{id}_A) \in F(A).$$

(Ψ) Legyen $x \in F(A)$. Kell egy alkalmas $\Psi(x) \in \text{Nat}(\text{Hom}(_, A), F)$ természetes transzformáció. Legyen $X \in \mathcal{C}_0$ és $f \in \text{Hom}(X, A)$ tetszőleges. Ekkor:

$$\Psi(x)_X(f) \stackrel{\text{def.}}{=} (F(f))(x) \in F(X)$$

amivel $\Psi(x) : \text{Hom}(X, A) \rightarrow F(X)$ lesz.

Még azt kell igazolni, hogy $\Psi(x)$ **természetes transzformáció**.

Legyen $g : Y \rightarrow X$ morfizmus,

$$\begin{array}{ccccc} X & & \text{Hom}(X, A) & \xrightarrow{\Psi(x)_X} & F(X) \\ g \uparrow & & \text{Hom}(g, A) \downarrow & & \downarrow F(g) \\ Y & & \text{Hom}(Y, A) & \xrightarrow{\Psi(x)_Y} & F(Y) \end{array}$$

Definíciója szerint $\text{Hom}(g, A) : \text{Hom}(X, A) \rightarrow \text{Hom}(Y, A)$, $f \mapsto f \circ g$, így tetszőleges $f \in \text{Hom}(X, A)$ -re:

$$\begin{aligned} (F(g) \circ \Psi(x)_X)(f) &= F(g)(F(f)(x)) = (F(g) \circ F(f))(x) = F(f \circ g)(x) = \\ &= \Psi(x)_Y(f \circ g) = \Psi(x)_Y(\text{Hom}(g, A)(f)) = (\Psi(x)_Y \circ \text{Hom}(g, A))(f). \end{aligned}$$

Kell $\Phi \circ \Psi = \text{id}_{F(A)}$. Legyen $x \in F(A)$.

$$(\Phi \circ \Psi)(x) = \Phi(\Psi(x)) = \Psi(x)_A(\text{id}_A) = F(\text{id}_A)(x) = \text{id}_{F(A)}(x) = x$$

Kell $\Psi \circ \Phi = \text{id}_{\text{Nat}(\text{Hom}(_, A), F)}$. Legyen $\eta \in \text{Nat}(\text{Hom}(_, A), F)$ természetes transzformáció, $X \in \mathcal{C}_0$ és $g \in \text{Hom}(X, A)$.

$$(\Psi \circ \Phi)(\eta)(X)(g) = (\Psi(\Phi(\eta)))(X)(g) = (\Psi(\eta_A(\text{id}_A)))(X)(g) = F(g)(\eta_A(\text{id}_A)) =$$

$$\begin{array}{ccccc} A & & \text{Hom}(A, A) & \xrightarrow{\eta_A} & F(A) \\ g \uparrow & & \text{Hom}(g, A) \downarrow & & \downarrow F(g) \\ X & & \text{Hom}(X, A) & \xrightarrow{\eta_X} & F(X) \end{array}$$

kommutativitása miatt

$$= (\eta_X(\text{Hom}(g, A)(\text{id}_A))) = (\eta_X(\text{id}_A \circ g)) = \eta(X)(g) = \text{id}_{\text{Nat}(\text{Hom}(_, A), F)}(\eta)(X)(g)$$

Lemma (Yoneda-lemma 2, reprezentált funktor alak) \mathcal{C} kategória, $A, B \in \text{Obj}(\mathcal{C})$. Ekkor az alábbi izomorfia fennáll:

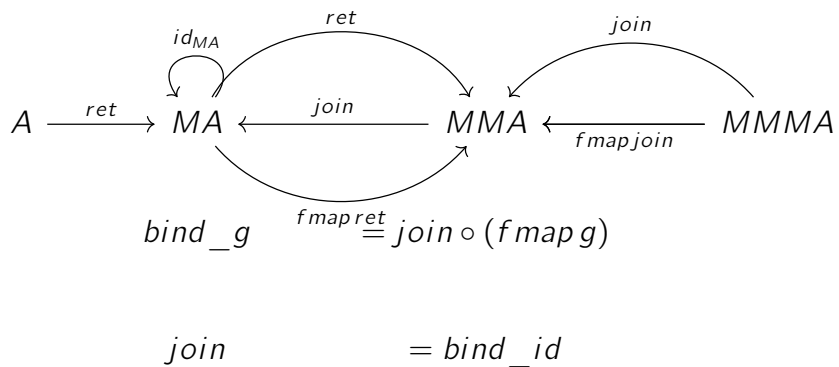
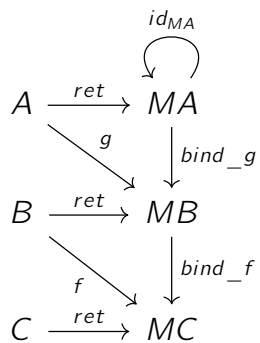
$$\text{Nat}(\text{Hom}(_, A), \text{Hom}(_, B)) \cong \text{Hom}(A, B)$$

Bizonyítás. $F(_) := \text{Hom}(_, B)$.

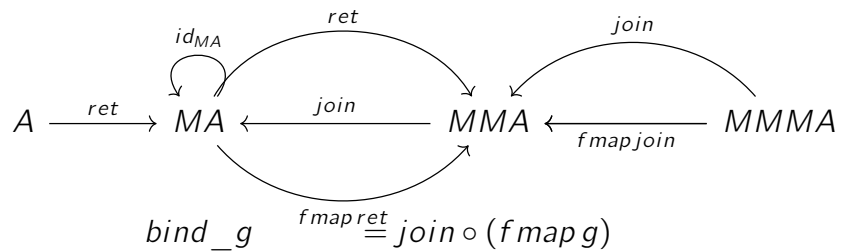
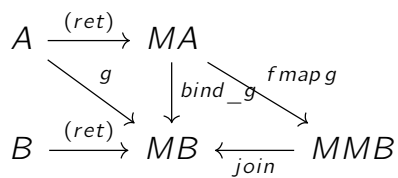
Lemma (Objektumok izomorfijának jellemzése) \mathcal{C} kategória, $A, B \in \text{Obj}(\mathcal{C})$. Ekkor az alábbi ekvivalencia fennáll:

$$\text{Hom}(_, A) \cong \text{Hom}(_, B) \Leftrightarrow A \cong B$$

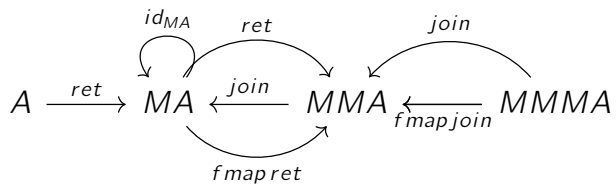
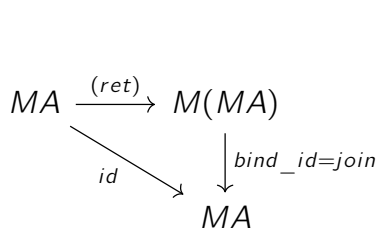
Nomádok



Oda:

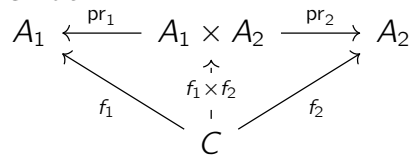


vissza:



Összefoglaló

Szorzat



$$\begin{aligned}
 f_i &= pr_i \circ (f_1 \times f_2) & (i = 1; 2) \\
 g &= (pr_1 \circ g) \times (pr_2 \circ g) & (\forall g : C \rightarrow A_1 \times A_2)
 \end{aligned}$$

Terminális

$$A \xrightarrow{!_A} 1$$

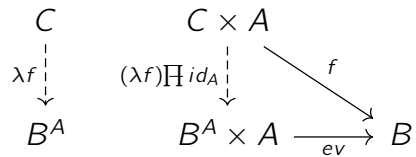
$$g = !_A \quad \forall g : A \rightarrow 1$$

Iniciális

$$0 \xrightarrow{!_A} A$$

$$g = !_A \quad \forall g : 0 \rightarrow A$$

Exponenciális



$$\begin{aligned}
 f &= ev \circ ((\lambda f) \text{H} id_A) \\
 g &= \lambda(ev \circ (g \text{H} id_A)) \quad (\forall g : C \rightarrow B^A)
 \end{aligned}$$