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 szőröstűl-bőröstűl.

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

$$F : I \to Set, i \mapsto A_i$$

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:

$$\prod_{i\in I} A_i \overset{\text{def.}}{=} \left\{ f : I \to \bigcup_{i\in I} A_i \;\middle|\; f(i) \in A_i \right\}.$$

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 képiselője 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 szorzathoz kapcsolódik a formális-axiomatikus halmazelmélet egyik leghírhedtebb axiómája, **a kiválasztási axióma** (a Zermeli-Fraenkel-choice halmazelmélt (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”:

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

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 $\mathrm{Tm}(A)$ halmaz*, amely A termeit, az A típusú programokat tartalmazza.

Műveletek

Függő függvénytípus (Π)

Π-*formáció:* Bármely $A : \mathrm{Ty}$ típus és $B : \mathrm{Tm}(A) \to \mathrm{Ty}$ típusfüggvény esetén létezik egy $\Pi(A, B) : \mathrm{Ty}$ típus.

$$\frac{A : \mathrm{Ty} \qquad B : \mathrm{Tm}(A) \to \mathrm{Ty}}{\Pi(A, B) : \mathrm{Ty}}$$

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

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

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

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

Azonosságtípus (Id)

Id-formáció: Bármely $A : \mathrm{Ty}$ típus és $x, y : \mathrm{Tm}(A)$ termek esetén létezik egy $\mathrm{Id}_A(x, y) : \mathrm{Ty}$ típus.

$$\frac{A : \mathrm{Ty} \qquad x, y : \mathrm{Tm}(A)}{\mathrm{Id}_A(x, y) : \mathrm{Ty}}$$

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.

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

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

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

Egyenlőségek

A Π-típusra vonatkozó szabályok

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

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

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

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

Az Id-típusra vonatkozó szabályok

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

$$\mathrm{refl}(\mathrm{equality\_reflection}(p)) = p$$

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

$$\mathrm{equality\_reflection}(\mathrm{refl}(q)) = q$$

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 propozíciókra.

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

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

$$\mathrm{equality\_reflection}(A, x, y, \mathrm{refl}(A, x, y, t)) = t$$

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

2.2. Tétel (UIP levezethető a típuselméletben)**.** Minden $A : \mathsf{Ty}$, $x, y : \mathsf{Tm}(A)$ és $p, q : \mathsf{Tm}(\mathsf{Id}_A(x, y))$ 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:

$$p = \mathsf{refl}(A, x, y, \mathsf{equality\_reflection}(A, x, y, p))$$

$$q = \mathsf{refl}(A, x, y, \mathsf{equality\_reflection}(A, x, y, q))$$

Az equality-reflection függvények értékei metaelméleti bizonyítások az $x = y$ tényre. A metaelméleti UIP axióma szerint ezek a bizonyítások egyenlőek:

$$\mathsf{equality\_reflection}(A, x, y, p) = \mathsf{equality\_reflection}(A, x, y, q)$$

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

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

Ebből következik, hogy $p = q$. □

2.3. Tétel (K-szabály levezethetősége)**.** Minden $A : \mathsf{Ty}$, $x : \mathsf{Tm}(A)$ és $p : \mathsf{Tm}(\mathsf{Id}_A(x, x))$ esetén:

$$p = \mathsf{refl}(A, x, x, \mathsf{eq\_refl}_x)$$

ahol $\mathsf{eq\_refl}_x$ az $x = x$ triviális bizonyítása.

Bizonyítás. Ez közvetlen következménye az előző tételnek (UIP a típuselméletben). Mivel a $\mathsf{Id}_A(x, x)$ típusnak legfeljebb egy eleme lehet, és $\mathsf{refl}(A, x, x, \mathsf{eq\_refl}_x)$ 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 $A : \mathsf{Ty}$, $B : \mathsf{Tm}(A) \to \mathsf{Ty}$ és $f, g : \mathsf{Tm}(\Pi(A, B))$ esetén, ha

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

akkor $f = g$.

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

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

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

Mivel a feltétel szerint $\mathsf{app}\, f\, x = \mathsf{app}\, g\, x$ 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 $A \to B$ jelölést a nem-függő függvénytípusra használjuk: $\Pi(A, \mathrm{fun}\_ \Rightarrow B)$.

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

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

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

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

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

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

$$\mathrm{app}\, I_1\, f = f$$

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

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

5. Az Azonosság Szimmetriája

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

Bizonyítás. Legyen $p : \mathrm{Tm}(\mathrm{Id}_A(x, y))$. 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 $\mathrm{Tm}(\mathrm{Id}_A(y, x))$ típusban. □

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

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

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

$$\mathrm{equality\_reflection}(\mathrm{refl}(A, x, y, t_1)) = \mathrm{equality\_reflection}(\mathrm{refl}(A, x, y, t_2))$$

Az Id-típus η-szabálya szerint $\mathrm{equality\_reflection}(\mathrm{refl}(t)) = t$. 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‘: Tm(Nat) term.
- **Rákövetkező:** Egy succ‘: $\mathrm{Tm(Nat)} \to \mathrm{Tm(Nat)}$ függvény.
- **Indukciós elv (nat_ind‘):** Bármely $P : \mathrm{Tm(Nat)} \to \mathrm{Ty}$ predikátum, $p_0 : \mathrm{Tm}(P(\mathrm{zero}))$ báziseset, és $p_s : (\forall k : \mathrm{Tm(Nat)}, \mathrm{Tm}(P(k)) \to \mathrm{Tm}(P(\mathrm{succ}(k))))$ indukciós lépés esetén, minden $n : \mathrm{Tm(Nat)}$-ra létezik egy term:

$$\mathrm{nat\_ind}(P, p_0, p_s, n) : \mathrm{Tm}(P(n))$$

A következő számítási szabályokkal:

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

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

$$\begin{tikzcd}
A_1 & A_1 \times A_2 \arrow[l, "\mathrm{pr}_1"'] \arrow[r, "\mathrm{pr}_2"] & A_2 \\
& C \arrow[ul, "f_1"] \arrow[u, dashed, "f_1 \times f_2"] \arrow[ur, "f_2"'] &
\end{tikzcd}$$

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

Megjegyzés. A morfizmusszorzás definiáló tulajdonságai tehát a

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

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

Lemma (Konverziós szabályok).

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

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

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

$$\begin{tikzcd} A_1 & A_1 \times A_2 \arrow[l, "\mathrm{pr}_1"'] \arrow[r, "\mathrm{pr}_2"] & A_2 \\ & C \arrow[ul, "\mathrm{pr}_1 \circ g"] \arrow[u, dashed, "g"] \arrow[ur, "\mathrm{pr}_2 \circ g"'] & \end{tikzcd}$$

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

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

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

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

vagyis a szorzatmorfizmus az egyetlen olyan, ami teljeseíti $\beta^\times$ szabályokat.

Lemma (A morfizmusszorzás kongruenciája).

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

ahol $h : \mathrm{Hom}(D; C)$ 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:

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

Nyilván

$$\begin{tikzcd}
A_1 & A_1 \times A_2 \arrow[l, "\mathrm{pr}_1"'] \arrow[r, "\mathrm{pr}_2"] & A_2 \\
 & C \arrow[u, dashed, "f_1 \times f_2"] \arrow[ul, "f_1"] \arrow[ur, "f_2"'] & \\
 & D \arrow[u, "h"] \arrow[uul, "f_1 \circ h"] \arrow[uur, "f_2 \circ h"'] &
\end{tikzcd}$$

kommutál, tehát

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

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

$$f_1 \mathbin{\text{⛩}} f_2 \overset{\text{def.}}{=} (f_1 \circ \mathrm{pr}_1) \times (f_2 \circ \mathrm{pr}_2).$$

Megjegyzés. Kommutatív diagramban ábrázolva a torii középen van:

$$\begin{tikzcd}
A_1 & A_1 \times A_2 \arrow[l, "\mathrm{pr}_1"'] \arrow[r, "\mathrm{pr}_2"] & A_2 \\
C_1 \arrow[u, "f_1"] & C_1 \times C_2 \arrow[l, "\mathrm{pr}_1"] \arrow[r, "\mathrm{pr}_2"'] \arrow[u, dashed, "(f_1 \circ \mathrm{pr}_1) \times (f_2 \circ \mathrm{pr}_2)"] & C_2 \arrow[u, "f_2"']
\end{tikzcd}$$

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

Lemma (Egyenlőségek torii-ra).

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

Exponenciális

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

$$\begin{tikzcd}
C \arrow[d, dashed, "\lambda f"'] & C \times A \arrow[d, dashed, "(\lambda f) \mathbin{\text{⛩}} id_A"'] \arrow[dr, "f"] & \\
B^A & B^A \times A \arrow[r, "ev"'] & B
\end{tikzcd}$$

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

Megjegyzés. Tehát a hatványmorfizmus vagy exponenciális adjungált definiáló egyenlete:

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

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

Lemma (Konverziós szabályok).

$$\begin{aligned} \beta^{\to} : &\quad ev \circ ((\lambda f) \sqcap id_A) = f \\ \eta^{\to} : &\quad \lambda(ev \circ (g \sqcap id_A)) = g \end{aligned}$$

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

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

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

márpedig ez az f triviálisan az $ev \circ (g \sqcap id_A)$. 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 $ev \circ (g \sqcap id_A) = f$. Ekkor

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

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:

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

Bizonyítás. A definiáló diagram

$$\begin{tikzcd} C \arrow[d, dashed, "\lambda f"'] \arrow[d, bend left, "g"] & C \times A \arrow[d, dashed, "g \sqcap id_A"'] \arrow[dr, "f"] \arrow[dr, bend left, "ev \circ (g \sqcap id_A)"] & \\ B^A & B^A \times A \arrow[r, "ev"'] & B \end{tikzcd}$$

alapján, legyen:

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

$$\Psi : \mathrm{Hom}(C; B^A) \to \mathrm{Hom}(C \times A; B), \quad \Psi(g) \overset{\text{def.}}{=} ev \circ (g \sqcap id_A).$$

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:

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

és

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

Lemma (Kongruencia).

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

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

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

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

$$\begin{tikzcd}
D \arrow[d, "h"] \arrow[dd, dashed, bend right=60, "\lambda(f\circ(h \sqcap id_A))"'] \arrow[dd, bend left=60, "(\lambda f)\circ h"] \\
C \arrow[d, dashed, "\lambda f"'] \\
B^A
\end{tikzcd}
\qquad
\begin{tikzcd}
D \times A \arrow[d, "h \sqcap id_A"'] \arrow[ddr, "f\circ(h \sqcap id_A)"] & \\
C \times A \arrow[d, dashed, "(\lambda f) \sqcap id_A"'] \arrow[dr, "f"] & \\
B^A \times A \arrow[r, "ev"'] & B
\end{tikzcd}$$

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

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

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

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

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

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

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:

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

Yoneda-tételkör

Motiváció – Homset reprezentáció

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

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

$$\mathrm{Hom}(X\,, A^1) \overset{\Psi_X}{\to} \mathrm{Hom}(X \times 1\,, A) \overset{\mathrm{Hom}(\varphi_X, A)}{\to} \mathrm{Hom}(X\,, A)$$

ahol Ψ_X az uncurrying, és

$$X \times 1 \overset{\varphi_X}{\leftarrow} X \qquad \Rightarrow \qquad \mathrm{Hom}(X \times 1\,, A) \overset{\mathrm{Hom}(\varphi_X, A)}{\to} \mathrm{Hom}(X\,, A)$$

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

Funktor

$$\begin{tikzcd} A \arrow[loop left, "id"] \arrow[r, "g"] \arrow[dr, "f\circ g"'] & {} \arrow[d, "f"] \\ & {} \end{tikzcd} \qquad \begin{tikzcd} F(A) \arrow[loop left, "F(id_A)=id_{F(A)}"] \arrow[r, "F(g)"] \arrow[dr, "F(f\circ g)=F(f)\circ F(g)"'] & {} \arrow[d, "F(f)"] \\ & {} \end{tikzcd}$$

$$\begin{tikzcd} {} \arrow[r, "g"] \arrow[dr, "f\circ g"'] & {} \arrow[d, "f"] \\ & {} \end{tikzcd} \qquad \begin{tikzcd} {} & {} \arrow[l, "F^{op}(g)"'] \\ & {} \arrow[u, "F^{op}(f)"'] \arrow[ul, "F^{op}(g)\circ F^{op}(f)=F^{op}(f\circ g)"] \end{tikzcd}$$

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

Yoneda-lemma

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

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

azaz van olyan $\Phi : \mathrm{Nat}(\mathrm{Hom}(\_, A), F) \to F(A)$ és $\Psi : F(A) \to \mathrm{Nat}(\mathrm{Hom}(\_, A), F)$, amelyek egymás inverzei.
Bizonyítás. (Φ) Legyen $\eta \in \mathrm{Nat}(\mathrm{Hom}(\_, A), F)$ tetszőleges, kell ehhez egy alkalmas $F(A)$-beli elem. Tetszőleges $X \in \mathcal{C}_0$-ra $\eta_X : \mathrm{Hom}(X, A) \to F(X)$ morfizmus, ezért

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

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

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

amivel $\Psi(x) : \mathrm{Hom}(X, A) \to F(X)$ lesz.
Még azt kell igazolni, hogy $\Psi(x)$ **természetes transzformáció.**
Legyen $g : Y \to X$ morfizmus,

$$\begin{array}{ccc} X & \quad & \begin{array}{ccc} \mathrm{Hom}(X,A) & \xrightarrow{\Psi(x)_X} & F(X) \\ {\scriptstyle \mathrm{Hom}(g,A)}\big\downarrow & & \big\downarrow{\scriptstyle F(g)} \\ \mathrm{Hom}(Y,A) & \xrightarrow{\Psi(x)_Y} & F(Y) \end{array} \\ {\scriptstyle g}\big\uparrow & & \\ Y & & \end{array}$$

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

$$(F(g) \circ \Psi(x)_X)(f) = F(g)(F(f)(x)) = (F(g) \circ F(f))(x) = F(f \circ g)(x) =$$

$$= \Psi(x)_Y(f \circ g) = \Psi(x)_Y(\mathrm{Hom}(g, A)(f)) = (\Psi(x)_Y \circ \mathrm{Hom}(g, A))(f).$$

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

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

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

$$(\Psi \circ \Phi)(\eta)(X)(g) = (\Psi(\Phi(\eta))(X)(g) = (\Psi(\eta_A(id_A)))(X)(g) = F(g)(\eta_A(id_A)) =$$

$$\begin{array}{ccc} A & \quad & \begin{array}{ccc} \mathrm{Hom}(A,A) & \xrightarrow{\eta_A} & F(A) \\ {\scriptstyle \mathrm{Hom}(g,A)}\big\downarrow & & \big\downarrow{\scriptstyle F(g)} \\ \mathrm{Hom}(X,A) & \xrightarrow[\eta_X]{} & F(X) \end{array} \\ {\scriptstyle g}\big\uparrow & & \\ X & & \end{array}$$

kommutativitása miatt

$$= (\eta_X(\mathrm{Hom}(g, A)(id_A))) = (\eta_X(id_A \circ g)) = \eta(X)(g) = id_{\mathrm{Nat}(\mathrm{Hom}(\_,A),F)}(\eta)(X)(g)$$

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

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

Bizonyítás. $F(\_) := \mathrm{Hom}(\_, B)$.
Lemma (Objektumok izomorfiájának jellemzése) $\mathcal{C}$ kategória, $A, B \in \mathrm{Obj}(\mathcal{C})$. Ekkor az alábbi ekvivalencia fennáll:

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

Nomádok

$$
\begin{tikzcd}
A \arrow[r, "ret"] \arrow[dr, "g"'] & MA \arrow[loop above, "id_{MA}"] \arrow[d, "bind\_g"] \\
B \arrow[r, "ret"] \arrow[dr, "f"'] & MB \arrow[d, "bind\_f"] \\
C \arrow[r, "ret"] & MC
\end{tikzcd}
\qquad
\begin{tikzcd}
A \arrow[r, "ret"] & MA \arrow[loop above, "id_{MA}"] \arrow[r, bend left=50, "ret"] \arrow[r, bend right=50, "fmap\,ret"'] & MMA \arrow[l, "join"'] & MMMA \arrow[l, "fmap\,join"] \arrow[l, bend right=50, "join"']
\end{tikzcd}
$$

$$
\begin{aligned}
bind\_g &= join \circ (fmap\,g) \\
join &= bind\_id
\end{aligned}
$$

Oda:

$$
\begin{tikzcd}
A \arrow[r, "(ret)"] \arrow[dr, "g"'] & MA \arrow[d, "bind\_g"] \arrow[dr, "fmap\,g"] & \\
B \arrow[r, "(ret)"] & MB & MMB \arrow[l, "join"]
\end{tikzcd}
\qquad
\begin{tikzcd}
A \arrow[r, "ret"] & MA \arrow[loop above, "id_{MA}"] \arrow[r, bend left=50, "ret"] \arrow[r, bend right=50, "fmap\,ret"'] & MMA \arrow[l, "join"'] & MMMA \arrow[l, "fmap\,join"] \arrow[l, bend right=50, "join"']
\end{tikzcd}
$$

$$bind\_g = join \circ (fmap\,g)$$

vissza:

$$
\begin{tikzcd}
MA \arrow[r, "(ret)"] \arrow[dr, "id"'] & M(MA) \arrow[d, "bind\_id=join"] \\
& MA
\end{tikzcd}
\qquad
\begin{tikzcd}
A \arrow[r, "ret"] & MA \arrow[loop above, "id_{MA}"] \arrow[r, bend left=50, "ret"] \arrow[r, bend right=50, "fmap\,ret"'] & MMA \arrow[l, "join"'] & MMMA \arrow[l, "fmap\,join"] \arrow[l, bend right=50, "join"']
\end{tikzcd}
$$

Összefoglaló

Szorzat

$$\begin{tikzcd}
A_1 & A_1 \times A_2 \arrow[l, "\mathrm{pr}_1"'] \arrow[r, "\mathrm{pr}_2"] & A_2 \\
& C \arrow[ul, "f_1"] \arrow[u, dashed, "f_1 \times f_2"] \arrow[ur, "f_2"'] &
\end{tikzcd}$$

$$f_i = pr_i \circ (f_1 \times f_2) \qquad (i = 1; 2)$$
$$g = (pr_1 \circ g) \times (pr_2 \circ g) \quad (\forall g : C \to A_1 \times A_2)$$

Terminális

$$\begin{tikzcd}
A \arrow[r, dashed, "!_A"] & 1
\end{tikzcd}$$

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

Iniciális

$$\begin{tikzcd}
0 \arrow[r, dashed, "!_A"] & A
\end{tikzcd}$$

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

Exponenciális

$$\begin{tikzcd}
C \arrow[d, dashed, "\lambda f"'] \\
B^A
\end{tikzcd}
\qquad
\begin{tikzcd}
C \times A \arrow[d, dashed, "(\lambda f) \Pi\, id_A"'] \arrow[dr, "f"] & \\
B^A \times A \arrow[r, "ev"'] & B
\end{tikzcd}$$

$$f = ev \circ ((\lambda f)\ \Pi\ id_A)$$
$$g = \lambda(ev \circ (g\ \Pi\ id_A)) \quad (\forall g : C \to B^A)$$