- ?/? :

  <
  Irányított gráfok, rajzolhatóság, kromatikus szám
  >
  Irányított gráfok

- 8/17 :

  <
gondosan átnézte és rendkívül sok észrevétellel, javaslattal, kiegészítéssel segített.
  >
gondosan átnézte és rendkívül sok észrevétellel, javaslattal, kiegészítéssel segített. Sok hibát a hallgatók találtak meg: köszönet érte mindenkinek. Külön ki kell emelnem Jaksov Anton segítségét, aki számos olyan hibát talált, amit valószínűleg soha nem vettem volna észre.

- 10/17 :

  <
értéke igaz vagy hamis.) Például a síkgeometriában predikátumok: $E(x)$ („x egyenes”),
  >
a *kijelentés*ek, ezek értéke igaz vagy hamis.) Például a síkgeometriában predikátumok: $E(x)$ („x egyenes”),

- 10/−2 :

  <
a *kvantor hatáskörében* van. Ha egy formulában egy változó egy adott előfordulása
  >
a *kvantor hatáskörében* van. Ha egy formulában egy változó egy adott előfordulása

- 11/11 :

  <
változók, így jelölhetjük az egyiket $\mathcal{A}(x, y)$-nal, a másikat pedig $\mathcal{B}(x, y)$-nal. Észrevehet
  >
változók, így jelölhetjük az egyik formulát $\mathcal{A}(x, y)$-nal, a másikat pedig $\mathcal{B}(x, y)$-nal. Észrevehet

- 13/−1 :

  <
predikátumnak, és az axiómák között felsoroljuk a tulajdonságait.
  >
predikátumnak, és az axiómák között felsoroljuk a tulajdonságait. (Például $x = y \iff y = x$ stb.)

- 14/−5 :

<

egyszerűek, jól érthetőek legyenek. Célszerű, ha minél kevesebb axióma van. Másrészt,

>

egyszerűek, jól érthetőek legyenek. Célszerű, ha minél kevesebb axióma van, de

- 21/4 :

<

Ha A és B halmazok, akkor nyilván $A \cap B := \cap\{A, B\}$.

>

Ha A és B halmazok, akkor nyilván $A \cap B = \cap\{A, B\}$.

- 26/17 :

<

reláció. (Vannak, akik egy reláció *grafikon*járól vagy *gráf*járól beszélnek, amikor párok

>

reláció vagy x *az* R *relációban van* y*-nal*. (Vannak, akik egy reláció *grafikon*járól vagy *gráf*járól beszélnek, amikor párok

- 29/−2 :

<

helyett $R(a)$-t írunk. Ez kényelmes, de néha félreértésekre vezethet, ha például a és $\{a\}$

>

helyett $R(a)$-t is írhatunk. Ez kényelmes, de néha félreértésekre vezethet, ha például a és $\{a\}$

- 32/7 :

<

(5) *reflexív*, ha minden $x \in X$ esetén $(x, x) \in R$;

(6) *irreflexív*, ha minden $x \in X$ esetén $(x, x) \notin R$;

>

(5) *irreflexív*, ha minden $x \in X$ esetén $(x, x) \notin R$;

(6) *reflexív*, ha minden $x \in X$ esetén $(x, x) \in R$;

- 32/13 :

<

Vegyük észre, hogy az első négy tulajdonság csak R-től, míg az utolsó négy R-től és

>

Vegyük észre, hogy az első öt (sic!) tulajdonság csak R-től, míg az utolsó három R-től és

- 33/−4 :

  <

  Megfordítva, legyen $\mathcal{O}$ az X egy osztályozása, és legyen $R \cup \{Y \times Y : Y \in \mathcal{O}\}$. Nyilván $(x, y) \in \mathbb{R}$ pontosan akkor teljesül, ha x és y az $\mathcal{O}$ ugyanazon halmazának elemei. Ez

  >

  Megfordítva, legyen $\mathcal{O}$ az X egy osztályozása, és legyen $R = \cup\{Y \times Y : Y \in \mathcal{O}\}$. Nyilván $(x, y) \in R$ pontosan akkor teljesül, ha x és y az $\mathcal{O}$ ugyanazon halmazának elemei. Ez

- 45/−6 :

  <

$\times_i X_i = \{\emptyset\}$. Ha minden $i \in I$-re $X_i = X$, akkor X^I-t írunk $\times_{i \in I} X_i$ helyett. Így

  >

$\times_i X_i = \{\emptyset\}$. Ha minden $i \in I$-re $X_i = X$, akkor X^I-t is írhatunk $\times_{i \in I} X_i$ helyett. Így

- 35/−12 :

  <

x-et. Egy x elemhez tartozó *kezdőszelet*nek a $\{y \in X : y < x\}$ részhalmazt nevezzük. A

  >

x-et. Egy x elemhez tartozó *kezdőszelet*nek az $\{y \in X : y < x\}$ részhalmazt nevezzük. A

- 40/−14 :

  <

ra képez le, azaz $f(X) = Y$, akkor szokás *szürjektív*nek vagy *szuperjektív*nek is nevezni,

  >

ra képez le, azaz $f(X) = \{f_x : x \in X\} = Y$, akkor szokás *szürjektív*nek vagy *szuperjektív*nek is nevezni,

- 46/−6 :

  <

$A * b$-t írunk. A legszokásosabb műveleti jelek + és ·, az utóbbit gyakran ki sem

  >

$A * b$-t is írhatunk. A legszokásosabb műveleti jelek + és ·, az utóbbit gyakran ki sem

- 50/−13 :

  <

hogy 0 egy nullér művelet $\mathbb{N}$-en. (2) azt fejezi ki, hogy $^+$ egy unér művelet $\mathbb{N}$-en. (3)

  >

hogy kijelölünk egy speciális 0 elemet, azaz 0 egy nullér művelet $\mathbb{N}$-nen. (2) azt fejezi ki, hogy $^+$ egy unér művelet $\mathbb{N}$-en. (3)

- 50/−7 :

  <

azt jelenti, hogy $\mathbb{N}$ minden eleme 0-ból rákövetkezéssel elérhető.

  >

azt jelenti, hogy $\mathbb{N}$ minden eleme 0-ból rákövetkezéssel elérhető, más természetes szám nincs.

- 51/4 :

  <

halmazra $0 \in S$, és ha $n \in S$, akkor $n^+ = (m^+)^+ \in S$, így (5) szerint $S = \mathbb{N}$.

  >

halmazra $0 \in S$, és ha $n \in S$, akkor $n^+ = (m^+)^+ \in S$, így (5) szerint $S = \mathbb{N}$, azaz a $^+$ unér művelet értékkészlete $\mathbb{N} \setminus \{0\}$. Ezt a halmazt $\mathbb{N}^+$-szal fogjuk jelölni, a $^+$ bijekció inverzét pedig $^-$-szal, ez a *megelőzés*.

- 51/−8 :

  <

jelentettek. Számára $0 \in N$ a „zero es numerö mondat rövidítése, ahol az „$\in$” az olasz

  >

jelentettek. Számára $0 \in N$ a „zero es numero” mondat rövidítése, ahol az „$\in$” az olasz

- 52/6 :

  <

$\mathbb{N}^+ = \mathbb{N} \setminus \{0\}$ halmazon értelmezett függvényeket is szokás végtelen sorozatnak nevezni.)

  >

$\mathbb{N}^+$ halmazon értelmezett függvényeket is szokás végtelen sorozatnak nevezni.)

- 53/11 :

  <

φ kölcsönösen egyértelmű, és a bizonyítás kész. □

  >

φ kölcsönösen egyértelmű. □

- 55/11 :

  <

sík rajta van egyetlen egyenesen. Megmutatjuk, hogy akárhogy veszünk véges sok pontot,

  >

sík rajta van egyetlen egyenesen. Elég megmutatni, hogy akárhogy veszünk n pontot,

- 62/−8 :

  <

Egy G monoid azon elemeinek halmazát, amelyeknek van inverze, G^*-gal jelöljük (függetlenül attól, hogy mivel jelöljük a műveletet). Bármely G monoidra $(G^*, *)$ csoport.

  >

Egy G monoid azon elemeinek halmazát, amelyeknek van inverze, $G^\times$-ral szokás jelölni (függetlenül attól, hogy mivel jelöljük a műveletet). Bármely G monoidra $(G^\times, *)$ csoport.

- 63/1 :

<

(*additív jelölés*), a semleges elemet *nullelem*nek nevezzük, és n-el vagy 0-val (ha nagyon

>

(*additív jelölés*), a semleges elemet *nullelem*nek nevezzük, és n-nel vagy 0-val (ha nagyon

- 63/11 :

<

mindkettőt érthetjük h/g alatt.

>

mindkettőt érthetjük h/g alatt.

Az egyműveletes algebrai struktúrák kapcsolatát a 8.1. ábra foglalja össze.

- 63/19 :

<

csoport, amelyben az egységelem az üres halmaz, az inverz pedig a komplementer, míg

>

csoport, amelyben az egységelem az üres halmaz, az inverz pedig az elem maga, míg

- 63/−5 :

<

  - **2.2.12. Példák.** $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Z} \setminus \{0\}, \cdot)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$ és $(\mathbb{R} \setminus \{0\}, \cdot)$ Abel-.

>

  - **2.2.12. Példák.** $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Z}^\times, \cdot)$, $(\mathbb{Q}^\times, \cdot)$ és $(\mathbb{R}^\times, \cdot)$ Abel-.

- 66/16 :

<

$n \in \mathbb{N}$, akkor a $[0, n] \subset \mathbb{N}$ vagy $[1, n] \subset \mathbb{N}^+$ halmazon értelmezett függvényeket *véges sorozat*nak nevezzük. Az x véges sorozatot úgy is jelöljük, hogy $x_0, x_1, \ldots, x_n$ (vagy x_i, $i = 0, 1, 2, \ldots, n$), illetve $x_1, x_2, \ldots, x_n$ (vagy x_i, $i = 1, 2, \ldots, n$). Az $x_1, x_2, \ldots, x_n$ véges sorozatot *rendezett* n-esnek is nevezük; ekkor rendszerint $(x_1, x_2, \ldots, x_n)$-nel jel-

>

$n \in \mathbb{N}$, akkor a $[0, n[\subset \mathbb{N}$ vagy $[1, n] \subset \mathbb{N}^+$ halmazon értelmezett függvényeket *véges sorozat*nak nevezzük. Az x véges sorozatot úgy is jelöljük, hogy $x_0, x_1, \ldots, x_{n^-}$ (vagy x_i, $i = 0, 1, 2, \ldots, n^-$), illetve $x_1, x_2, \ldots, x_n$ (vagy x_i, $i = 1, 2, \ldots, n$). Az $x_0, , x_1, \ldots, x_{n^-}$ illetve $x_1, x_2, \ldots, x_n$ véges sorozatot *rendezett* n-esnek is nevezük; ekkor rendszerint $(x_0, x_1, \ldots, x_{n^-})$-szal illetve $(x_1, x_2, \ldots, x_n)$-nel jel-

- 68/1 :
  <

2.3.13. Általános rekurziótétel. *Legyen adott egy X halmaz és egy X-be képező f függvény, amelynek értelmezési tartománya az $\mathbb{N}$ valamely kezdőszeletéből X-be képező függvények halmaza. (Az f adja a rekurziót.) Ekkor egyértelműen létezik egy $g : \mathbb{N} \to X$ függvény, amely „f-zárt", azaz $g(a) = f\big(g|_{]\leftarrow,a[}\big)$ minden $a \in \mathbb{N}$-re. (Ittt $]\leftarrow, a[$ az a-hoz tartozó kezdőszelet, lásd 1.3.50.)*

A tétel szemléletesen fogalmazva azt mondja, hogy ha adott egy függvényünk, amely egy egydimenziós tömb esetén kiszámítja a tömb már feltöltött kezdetéből, hogy a következő helyre mit kell tennünk, akkor ennek segítségével a tömböt akármeddig feltölthetjük.

A tétel és a bizonyítás érvényes marad akkor is, ha $\mathbb{N}$ helyett tetszőleges N jólrendezett halmaz szerepel. Ezt az általánosabb változatot szokás *transzfinit rekurziótétel*nek nevezni.

* **Bizonyítás.** Az egyértelműség bizonyítása $\mathbb{N}$ jólrendezettségén múlik. (Az ilyen bizonyításokat *transzfinit indukció*val történő bizonyításnak nevezzük.) Tegyük fel, hogy g és g^* is eleget tesz a tétel feltételeinek. Legyen $S = \big\{x \in \mathbb{N} : g(x) \neq g^*(x)\big\}$. Ha S nem üres, akkor létezik legkisebb eleme, legyen ez a. Mivel $g|_{]\leftarrow,a[} = g^*|_{]\leftarrow,a[}$, azt kapjuk, hogy

$$g(a) = f\big(g|_{]\leftarrow,a[}\big) = f\big(g^*|_{]\leftarrow,a[}\big) = g^*(a),$$

ami ellentmond annak, hogy $a \in S$.

A g létezésének bizonyítása hasonlít a rekurziótétel megfelelő részének bizonyítására. Nevezzük $\mathbb{N} \times X$ egy A részhalmazát f-zártnak, ha minden $a \in \mathbb{N}$-re és minden

$$h :]\leftarrow, a[\to X$$

függvényre, amelyre $h \subset A$, az is teljesül, hogy $\big(a, f(h)\big) \in A$. Maga $\mathbb{N} \times X$ egy f-zárt halmaz, ilyen halmaz tehát létezik. Legyen g az összes f-zárt halmaz metszete. Mivel nyilván g is f-zárt, csak azt kell megmutatnunk, hogy g az egész $\mathbb{N}$-en értelmezett függvény. Más szóval, azt fogjuk bizonyítani, hogy ha $c \in \mathbb{N}$, akkor van olyan $x \in X$, hogy $(c, x) \in g$, továbbá ha $(c, y) \in g$, akkor $x = y$. A bizonyítás megint indirekt, transzfinit indukcióval történik. Legyen S azon $\mathbb{N}$-beli c elemek halmaza, amelyekre ez nem igaz. Legyen a az S legkisebb eleme. Ekkor $g|_{]\leftarrow,a[}$ egy $]\leftarrow, a[$-n értelmezett függvény, és mivel a g halmaz f-zárt, ha $x = f\big(g|_{]\leftarrow,a[}\big)$, akkor $(a, x) \in g$. Mivel $a \in S$, ez csak úgy lehet, hogy van olyan $y \in X$, hogy $(a, y) \in g$ és $y \neq x$. Megmutatjuk, hogy $g \setminus \big\{(a, y)\big\}$ is f-zárt. Ez azt jelenti, hogy $b \in \mathbb{N}$ és $h :]\leftarrow, b[\to X$, $h \subset g \setminus \big\{(a, y)\big\}$ esetén $\big(b, f(h)\big) \in g \setminus \big\{(a, y)\big\}$. Ez nyilvánvaló akkor is, ha $b = a$, és akkor is, ha $b \neq a$. Viszont ez ellentmond annak, hogy g a legszűkebb f-zárt halmaz. □

2.3.14. Példa: Fibonacci-számok. Példaként megmutatjuk, hogyan definiálhatók a Fibonacci-számok az előző tétel segítségével pontosan. Legyen $X = \mathbb{N}$, és legyen az $n \mapsto n^-$ leképezése $\mathbb{N}^+$-nak $\mathbb{N}$-re az $n \mapsto n^+$ leképezés inverze. Először az $f(\emptyset) = 0$, $f\Big(\big\{(0, k)\big\}\Big) = 1$ bármely $k \in \mathbb{N}$-re definíciókkal előírjuk, hogy az előző tétel szerint adódó

g-re $g(0) = 0$ és $g(1) = 1$ legyen. Most ha $n > 1$, $h :]\leftarrow, n[\to \mathbb{N}$ egy függvény, akkor legyen $f(h) = h(n^-) + h(n^{--})$. (Megjegyezzük, hogy $n = \min\big(\mathbb{N} \setminus \mathrm{dmn}(h)\big)$.)

>

2.3.13. Általános rekurziótétel. *Legyen adott egy X halmaz és egy X-be képező f függvény, amelynek értelmezési tartománya az X-beli (nullától indexelt) véges sorozatok halmaza. (Az f adja a rekurziót.) Ekkor egyértelműen létezik egy $g : N \to X$ függvény, amely „f-zárt", azaz $g(n) = g_n = f(g_0, g_1, \dots, g_{n^-})$ minden $n \in \mathbb{N}$-re.*

A tétel szemléletesen fogalmazva azt mondja, hogy ha adott egy függvényünk, amely egy egydimenziós tömb esetén kiszámítja a tömb már feltöltött kezdetéből, hogy a következő helyre mit kell tennünk, akkor ennek segítségével a tömböt akármeddig feltölthetjük.

A tétel és a bizonyítás érvényes marad akkor is, ha $\mathbb{N}$ helyett tetszőleges N jólrendezett halmaz szerepel. Ezt az általánosabb változatot szokás *transzfinit rekurziótétel*nek nevezni. Ekkor f értelmezési tartománya az összes, N valamely kezdőszeletéből X-be képező függvény halmaza, és azt állítjuk, hogy egyértelműen létezik egy $g : \mathbb{N} \to X$ függvény, amely „f-zárt", azaz $g(n) = f\big(g|_{]\leftarrow,n[}\big)$ minden $n \in N$-re. (Itt $]\leftarrow, n[$ az $n \in N$-hez tartozó kezdőszelet, lásd 1.3.50.)

* **Bizonyítás.** Az egyértelműség bizonyítása $\mathbb{N}$ jólrendezettségén múlik. (Az ilyen bizonyításokat *transzfinit indukció*val történő bizonyításnak nevezzük.) Tegyük fel, hogy g és g^* is eleget tesz a tétel feltételeinek. Legyen $S = \big\{k \in \mathbb{N} : g(k) \neq g^*(k)\big\}$. Ha S nem üres, akkor létezik legkisebb eleme, legyen ez n. Mivel g és g^* megegyeznek az $]\leftarrow, n[$ intervallumon, azt kapjuk, hogy

$$g(n) = f\big(g|_{]\leftarrow,n[}\big) = f\big(g^*|_{]\leftarrow,n[}\big) = g^*(n),$$

ami ellentmond annak, hogy $n \in S$.

A g létezésének bizonyítása hasonlít a rekurziótétel megfelelő részének bizonyítására. Nevezzük $\mathbb{N} \times X$ egy A részhalmazát f-zártnak, ha minden $n \in \mathbb{N}$-re és minden

$$h :]\leftarrow, n[\to X$$

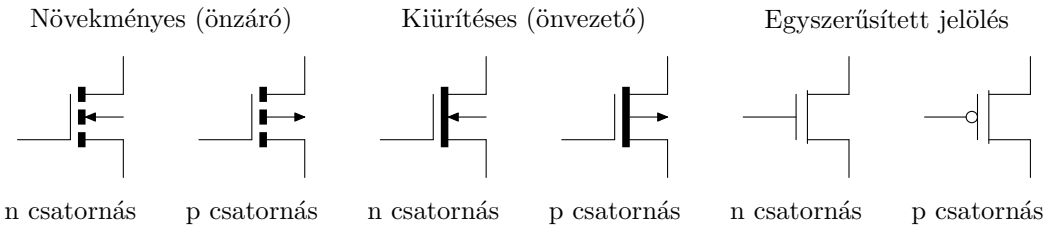
függvényre, amelyre $h \subset A$, az is teljesül, hogy $\big(n, f(h)\big) \in A$. Maga $\mathbb{N} \times X$ egy f-zárt halmaz, ilyen halmaz tehát létezik. Legyen g az összes f-zárt halmaz metszete. Mivel nyilván g is f-zárt, csak azt kell megmutatnunk, hogy g az egész $\mathbb{N}$-en értelmezett függvény. Más szóval, azt fogjuk bizonyítani, hogy ha $k \in \mathbb{N}$, akkor van olyan $x \in X$, hogy $(k, x) \in g$, továbbá ha $(k, y) \in g$, akkor $x = y$. A bizonyítás megint indirekt, transzfinit indukcióval történik. Legyen S azon $\mathbb{N}$-beli k elemek halmaza, amelyekre ez nem igaz. Legyen n az S legkisebb eleme. Ekkor $g|_{]\leftarrow,n[}$ egy $]\leftarrow, n[$-en értelmezett függvény, és mivel a g halmaz f-zárt, ha $x = f\big(g|_{]\leftarrow,n[}\big)$, akkor $(n, x) \in g$. Mivel $n \in S$, ez csak úgy lehet, hogy van olyan $y \in X$, hogy $(n, y) \in g$ és $y \neq x$. Megmutatjuk, hogy $g \setminus \big\{(n, y)\big\}$ is f-zárt. Ez azt jelenti, hogy $m \in \mathbb{N}$ és $h :]\leftarrow, m[\to X$, $h \subset g \setminus \big\{(n, y)\big\}$ esetén $\big(m, f(h)\big) \in g \setminus \big\{(n, y)\big\}$. Ez nyilvánvaló akkor is, ha $m = n$, és akkor is, ha $m \neq n$. Viszont ez ellentmond annak, hogy g a legszűkebb f-zárt halmaz. □

2.3.14. Példa: Fibonacci-számok. Példaként megmutatjuk, hogyan definiálhatók a Fibonacci-számok az előző tétel segítségével pontosan. Legyen $X = \mathbb{N}$. Először az $f(\emptyset) = 0$, $f\Big(\big\{(0,k)\big\}\Big) = 1$ bármely $k \in \mathbb{N}$-re definíciókkal előírjuk, hogy az előző tétel szerint adódó g-re $g(0) = 0$ és $g(1) = 1$ legyen. Most ha $n > 1$, $(h_0, h_1, \dots, h_{n^-})$ egy véges sorozat, akkor legyen $f(h) = h_{n^-} + h_{n^{--}}$. (Megjegyezzük, hogy $n = \min\big(\mathbb{N} \setminus \mathrm{dmn}(h)\big)$.)

- 72/−3 :
  <
lezár. (Az alaplemez kivezetését, a B bázis (base) elektródát mindig az S elektródához
  >
lezár. (Az alaplemez kivezetését, a B bázis (base) elektródát általában az S elektródához

- 73/4 :
  <
zük. Készíthető olyan változat is, amelyben a gyártás során a szigetelő réteg alatt eleve
  >
zük (a bázis a kapcsolásban a forráshoz van kötve). Készíthető olyan változat is, amelyben a gyártás során a szigetelő réteg alatt eleve

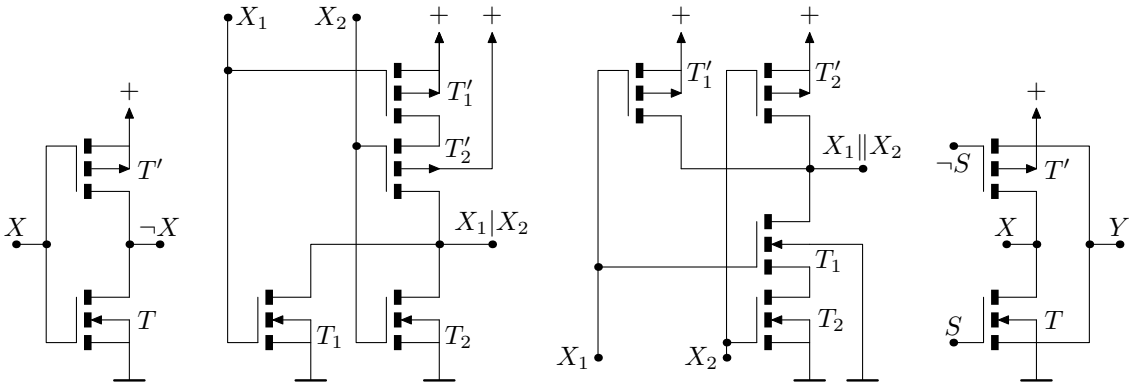
- 73/−4 A 2.2. ábra HELYETT: :
  <
  >



2.2. ábra: MOSFET típusok rajzjele

- 74/10 :
  <
  Hasonlóan működik a középen látható *sem-sem kapu* (*not or*, *NOR*): ha valame-
  >
  Hasonlóan működik a mellette látható *sem-sem kapu* (*not or*, *NOR*): ha valame-

- 74/13 :
  <
feszültségű. A jobb oldalon álló *összeférhetetlen vagy* (*not and*, *NAND*) kapunál, ha
  >
feszültségű. A következő *összeférhetetlen vagy* (*not and*, *NAND*) kapunál, ha



2.3. ábra: Statikus CMOS kapuáramkörök

- 74/−12 :

  <

ben pedig magas feszültségre. Mindkét kapufajta három bemenettel is készülhet (több bemenet növeli a szükséges tápfeszültséget).

  >

ben pedig magas feszültségre. Mindkét kapufajta három, négy, sőt több bemenettel is készülhet. Több bemenet növeli a szükséges tápfeszültséget és a kapcsolási időt, és rontja a kimeneti tulajdonságokat, ezért négynél több bemenetet nemigen használnak. A kapuk után egy nem kaput rakva, *vagy* (*OR*) illetve *és* (*AND*) kapuhoz jutunk. A nem kapu egyúttal erősítőként működve javítja a kimeneti tulajdonságokat is.

- 74/−6 :

  <

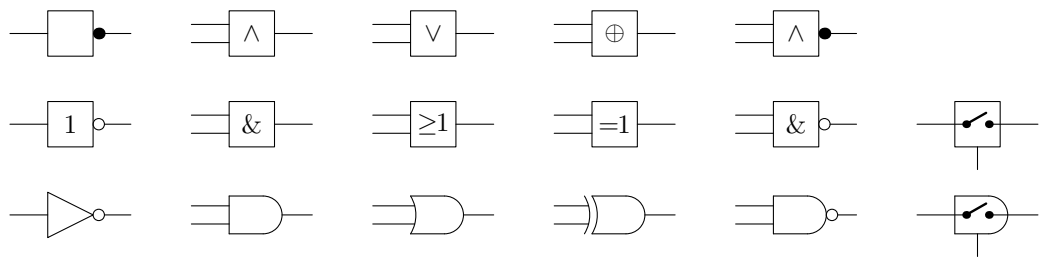
Nagy sebességű áramköröknél bonyolultabb kapcsolásokat használnak.

  >

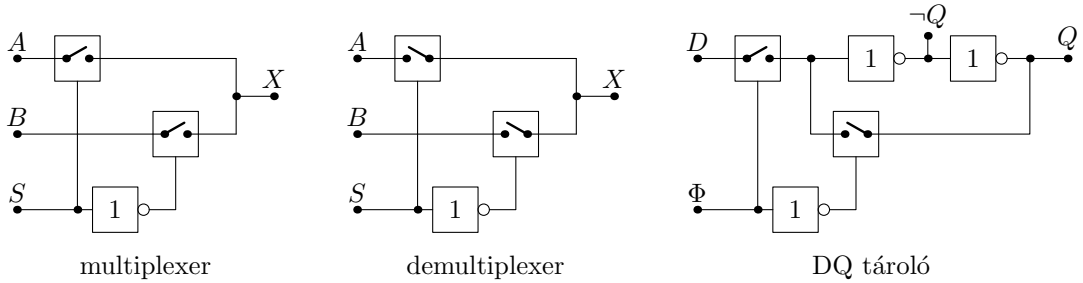
Nagy sebességű áramköröknél bonyolultabb kapcsolásokat használnak.

Végül a 2.3. ábra jobb szélén látható *átvivő kapu* (*transfer gate*) az S bemenet magas szintje esetén összeköti az X bemenetet az Y kimenettel, mert mindkét MOSFET vezet, alacsony szintje esetén pedig elválasztja X-et Y-tól. Mint látjuk, az átvivő kapu működéséhez S negáltjára is szükség van, ezt a bemenetet azonban az egyszerűség kedvéért sem a rajzjelében, sem a kapcsolási rajzokon nem ábrázoljuk, mindig csak az S bemenetet, amelynek magas szintjére az átvivő kapu vezet.

A 2.4. ábra megadja a leggyakoribb kapuk szokásos rajzjeleit. A kimenet invertálását • vagy ∘ jelzi. Ugyanezt a jelzést használják a bemeneteknél is, így sok más kaput is jelölhetünk az invertálás és az (esetleg kettőnél több bemenetű) alapkapuk segítségével.



2.4. ábra: MOSFET típusok rajzjele



2.5. ábra: átvivő kapus kapcsolások

A 2.5. ábra néhány, átvivő kapuval megoldott kapcsolást mutat be. A bal oldalon látható *multiplexer* vagy az A vagy a B bemenő jelet kapcsolja az X kimenetre, attól függően, hogy az S bemenet magas vagy alacsony szintű. Ugyanezt a kapcsolást fordítva is használhatjuk, X-et tekintve bemenetnek, bár ilyenkor jobb az átvivő kapukat megfordítani: így kapjuk a középen látható *demultiplexert*. Ha csak az egyik, mondjuk a B-hez kapcsolódó átvivő kaput fordítjuk meg, akkor az S bemenet magas szintje esetén X a kimenet, A a bemenet, alacsony szintje esetén pedig X a bemenet, B a kimenet. Így ha X egy IC egyik lába, akkor azt kapcsolhatjuk kimenetnek vagy bemenetnek. Végül ha mindkét átvivő kaput ugyanazzal az S-sel vezérelve egyszerre lezárjuk, akkor az X láb el van vágva A-tól és B-től is, így „lebeg”. Ezen két kapcsolás kombinálásával létrehozható *háromállapotú* (*tristate*) lábakat gyakran használnak különböző IC-k (processzor, memória, stb.), ha ugyanis több eszköz dolgozik ugyanarra a „buszra”, akkor az egyik kimenetként kapcsolt lábaival „ad”, néhány bemenetként használt lábaival „vesz”, a többi eszköz lábai „lebegnek”.

Végül igen fontos a 2.5. ábra jobb szélén látható *DQ tároló* (*DQ latch*) egybites tároló elem. Amíg a Φ órajel magas szintű, a D bemeneti adat az átvivő kapun keresztül az inverterre jut, így a $\neg Q$ ponton a negáltja, a Q ponton pedig D jelenik meg (legalább a két inverter késleltetési idejéig D nem változhat, Φ-nek pedig magas szinten kell lennie).

Amint a Φ alacsony szintű lesz, lezár a D-t átvezető átvivő kapu, de kinyit a másik, így a $\neg Q$ és Q ponton a szint nem változik, amíg Φ alacsony szinten marad. A kapcsolás nem érzékeny arra, hogy a két átvivő kapu egyszerre kapcsol-e, hiszen ha esetleg mindkettő nyitva van, ugyanazt a jelet adják az inverter bemenetére, ha pedig a D-hez kapcsolódó már lezárt, de a másik még nem nyitott ki, az első inverter bemeneti kapacitása rövid ideig „tartja" a szintet. A regiszterek és egyéb memória elemek egy processzorban ilyen egybites tárolókból épülhetnek fel. A Q (vagy a $\neg Q$) kimenetekhez közvetlenül kapcsolódhat egy logikai függvényeket megvalósító *kombinációs hálózat*, azaz a processzor többi része, aminek a kimenetei viszont a D bemenetekhez kapcsolódhatnak. A kombinációs hálózat nem lehet olyan gyors, hogy a kimenetei már akkor megváltozzanak, amikor az órajel még magas, viszont az órajel alacsony szintje alatt a kombináció hálózat kimenetének stabilizálódnia kell. Ha ez nem biztosítható, akkor két DQ tárolót kapcsolhatunk egymás után: a második „szolga" tárolót vezérlő órajel csak akkor lesz magas szintű, amikor az első, „mester" tárolót vezérlő órajel már alacsony szintű, és viszont. Az így kapott *mester-szolga tároló* (*MS tároló*, *master-slave latch*, *MS latch*) biztosítja a szolga és a mester közé kapcsolt kombinációs hálózat bemenetének és kimenetének tökéletes időbeli elválasztását.

- 78/9 :
  <
pont végéig, a 3.2. pontból pedig a test, ferdetest, rendezett test 3.2.3. definióját tárgyal-
  >
pont végéig, a 3.2. pontból pedig a test, ferdetest, rendezett test 3.2.3. definícióját tárgyal-

- 79/−18 :
  <
Az összeadás kompatibilis az ekvivalenciával, így az egész számok között értelmezve
  >
Az összeadás kompatibilis a $\sim$ ekvivalenciarelációval, így az egész számok között értelmezve

- 83/2 :
  <
  Bizonyítás. (1) triviális, ha $m = 0$ vagy $n = 0$. Az $n = 1$ eset m szerinti induk-
  >
Az állítás szokásos, kissé pontatlan megfogalmazása: többtagokat úgy szorzunk hogy minden tagot minden taggal szorzunk.

  Bizonyítás. (1) triviális, ha $m = 0$ vagy $n = 0$. Az $n = 1$ eset m szerinti induk-

- 84/−6 :
  <
jobbról nem lehet egyszerűsíteni. Ha a gyűrűben van a nullától különböző egységelem, és x-nek van multiplikatív inverze, akkor x nem lehet sem bal, sem jobb oldali nullosztó, hiszen $xy = 0$-ból illetve $yx = 0$-ból $x^{-1}xy = y = 0$, illetve $yxx^{-1} = y = 0$ következik.

>
jobbról nem lehet egyszerűsíteni. Ha x-nek van multiplikatív inverze, akkor x nem lehet sem bal, sem jobb oldali nullosztó, hiszen $xy = 0$-ból illetve $yx = 0$-ból $y = x^{-1}xy = 0$, illetve $y = yxx^{-1} = 0$ következik.

- 85/3 :

  <
  Rendezett integritási tartományban ha $x > 0$, akkor x-et *pozitív*nak, ha $x < 0$,
  >
  (2) elnevezését az indokolja, hogy (1) fennállása mellett ekvivalens azzal, hogy $x \leq y$, $z \geq 0$ esetén $xz \leq yz$.
  Rendezett integritási tartományban ha $x > 0$, akkor x-et *pozitív*nak, ha $x < 0$,

- 85/−8 :

  <
$1^2 = 1 > 0$. Végül (5)-höz: ha $y > 0$ és $v \leq 0$, akkor $yv \leq 0$. De $y(1/y) = 1 > 0$
  >
$1 = 1^2 > 0$. Végül (5)-höz: ha $y > 0$ és $v \leq 0$, akkor $yv \leq 0$. De $y(1/y) = 1 > 0$

- 88/9 :

  <
kételemű testben $-1 = 1$.
  >
kételemű testben $-1 = 1$.
  A kétműveletes algebrai struktúrák összehasonlítását lásd a ábrán.

- 91/−4 :

  <
$x \bmod 1 = x - \lfloor x \rfloor$ értéket x *törtrészének* nevezzük.
  >
$x \bmod 1 = x - \lfloor x \rfloor$ értéket x *törtrészének* nevezzük.

- 92/11 :

  <
(ez kiköszöböli, hogy ebben az esetben mindig egyirányban történjen a kerekítés); ez a *szabályos kerekítés*. Más *kerekítés* mellett is dönthetünk: $-\infty$ felé való kerekítés esetén
  >
(ez kiküszöböli, hogy ebben az esetben mindig egyirányban történjen a kerekítés); ez a *szabályos kerekítés*. Más *kerekítés* mellett is dönthetünk: $-\infty$ felé (lefelé) való kerekítés esetén

- 92/14 :

<

lebbit; ha $+\infty$ felé kerekítünk, akkor az x-nél nem kisebb pontosan ábrázolható számok

>

lebbit; ha $+\infty$ felé (felfelé) kerekítünk, akkor az x-nél nem kisebb pontosan ábrázolható számok

- 92/16 :

<

metikánál fontosak); végül *csonkítás* esetén az $|x|$-nél kisebb abszolút értékű pontosan

>

metikánál fontosak); végül *csonkítás* (nulla felé kerekítés) esetén az $|x|$-nél nem nagyobb abszolút értékű pontosan

- 92/19 :

<

eredményre, és természetesen általában a műveleteknél is kerekítési hiba lép fel. Ha n

>

eredményre, így általában a műveleteknél kerekítési hiba lép fel. Ha n

- 92/25 :

<

értéke kicsi. A *lebegőpontos számábrázolás* ezt küszüböli ki, a hiba és a szám értéke

>

értéke kicsi. A *lebegőpontos számábrázolás* ezt küszöböli ki, a hiba és a szám értéke

- 105/7 :

<

ként az összes többi előáll (például $\varepsilon_k = \varepsilon_1^k$, $k = 0, 1, \ldots, k-1$), ezeket n-edik *primitív*

>

ként az összes többi előáll (például $\varepsilon_k = \varepsilon_1^k$, $k = 0, 1, \ldots, n-1$), ezeket n-edik *primitív*

- 108/-13 :

<

$a, b, c, d \in \mathbb{R}$, és ez a felírás egyértelmű, mert $a = \Re z$, $b = \Im z$, $c = \Re w$ és $d = \Im w$.

>

$a, b, c, d \in \mathbb{R}$, és ez a felírás egyértelmű, mert $a = \Re(z)$, $b = \Im(z)$, $c = \Re(w)$ és $d = \Im(w)$.

- 109/14 :

<

értéket kapjuk vissza. Nyilván $|0| = 0$, és $p \neq 0$ esetén $|p| > 0$, $|\overline{p}| = |p|$, $|pq| = |p||q|$ (mert mindkét oldal négyzete $p\overline{p}q\overline{q}$). Teljesül a $|p+q| \leq |p|+|q|$ *háromszög-egyenlőtlenség* és

>

értéket kapjuk vissza. Nyilván $|0| = 0$ és $p \neq 0$ esetén $|p| > 0$, $|\overline{p}| = |p|$, $|pq| = |p||q|$ (mert mindkét oldal négyzete ugyanannyi). Teljesül a $|p + q| \leq |p| + |q|$ *háromszög-egyenlőtlenség* és

- 109/−4 :

<

hanem *antikommutatív*. A definícióból könnyen adódik, hogy teljesül a *Jacobi-identitás*:

>

hanem *antikommutatív*. A definícióból könnyen adódik, hogy $i \times j = k$, $j \times k = i$, $k \times i = j$, és teljesül a *Jacobi-identitás*:

- 113/15 :

<

A szorzás nyilván nem kommutatív, hiszen már $\mathbb{H}$-ban sem az. Viszont $\mathbb{R}$-beli ele-

>

A szorzás nem kommutatív, hiszen már $\mathbb{H} \subset \mathbb{O}$-ban sem az. Viszont $\mathbb{R}$-beli ele-

- 114/−16 :

<

(mert mindkét oldal négyzete $(u\overline{u})(v\overline{v})$). Teljesül az $|u + v| \leq |u| + |v|$ *háromszög-*

>

(mert mindkét oldal négyzete ugyanannyi). Teljesül az $|u + v| \leq |u| + |v|$ *háromszög-*

- 121/6 :

<

tásának. A megfeleltetés létezéséből következik az állítás.

>

tásának. A megfeleltetés létezéséből következik az állítás. Figyeljük meg, hogy $n = 0$ is lehetséges.

- 137/−13 :

<

hogy az X végtelen halmazból kiválasztunk egy különböző elemekből álló $x_1, x_2, \ldots$

>

hogy az X végtelen halmazból kiválasztunk egy különböző elemekből álló $x_0, x_1, \ldots$

- 138/4 :

<

létezik $\mathbb{N}$-et X-re képező leképezés.

>

létezik $\mathbb{N}$-et X-re képező leképezés.

Általánosabban, az is igaz, hogy egy X nem üres halmazra $X \precsim Y$ pontosan akkor teljesül, ha létezik Y-t X-re képező leképezés.

- 138/−7 :

  <
  Az $f(m,n)$ függvény „működése” az 5.2. ábrán tanulmányozható.
  >
  Az f függvény „működése” az 5.2. ábrán tanulmányozható.

- 139/7 :

  <
  Bizonyítás. Az X-et helyettesítve $X \setminus Y$-nal, feltehetjük, hogy X és Y diszjunktak.
  >
  Bizonyítás. Az X-et helyettesítve $X \setminus Y$-nal feltehetjük, hogy X és Y diszjunktak.

- 139/16 :

  <
  szerint ekvivalens X-el.
  >
  szerint ekvivalens X-szel.

- 140/−5 :

  <
  Bizonyítás. Mivel $\mathbb{R} \sim \wp(\mathbb{N})$, kapjuk, hogy $\mathbb{C} \sim \wp(\mathbb{N}) \times \wp(\mathbb{N})$. De az $\mathbb{N}$ részhalma-
  >
  Bizonyítás. Mivel $\mathbb{R} \sim \wp(\mathbb{N})$, kapjuk, hogy $\mathbb{R} \times \mathbb{R} \sim \wp(\mathbb{N}) \times \wp(\mathbb{N})$. De az $\mathbb{N}$ részhalma-

- 142/5 :

  <
  és elméleti fizikus 1939-ben bebizonyította, hogy ha ellentmondástalan (ezt reméljük),
  >
  és elméleti fizikus 1939-ben bebizonyította, hogy ha ZFC ellentmondástalan (ezt reméljük),

- 145/10 :

  <
  ahonnan $k = k'$. Ha $m \neq 0$, akkor $m|n$ azzal ekvivalens, hogy $n/m \in \mathbb{N}$.
  >
  ahonnan $k = k'$. Ha $m \neq 0$, akkor $m|n$ azzal ekvivalens, hogy $n/m \in \mathbb{N}$. A $|$ reláció az *oszthatóság*.

- 147/−11 :

  <
  $a \in R$-nek osztója, akkor egység. Az egységeket ezzel a tulajdonsággal tetszőleges $R \neq \{0\}$ integritási tartományban is lehet definiálni, de könnyen adódik, hogy ha van egység, akkor R egységelemes: ha ε egy egység, akkor $\varepsilon|\varepsilon$, így valamely $0 \neq e \in R$-re $\varepsilon = e\varepsilon$.

Innen $a\varepsilon = ae\varepsilon$ minden $a \in R$-re. Mivel $\varepsilon \neq 0$, lehet vele egyszerűsíteni. Az $a \in R$ asszociáltjai az εa alakú elemek, ahol ε egység.

>

$a \in R$-nek osztója, akkor egység. (Az egységeket ezzel a tulajdonsággal tetszőleges $R \neq \{0\}$ integritási tartományban is lehet definiálni, de könnyen adódik, hogy ha van egység, akkor R egységelemes: ha ε egy egység, akkor $\varepsilon|\varepsilon$, így valamely $0 \neq e \in R$-re $\varepsilon = e\varepsilon$. Innen $a\varepsilon = ae\varepsilon$ minden $a \in R$-re. Mivel $\varepsilon \neq 0$, lehet vele egyszerűsíteni.) Az $a \in R$ asszociáltjai az εa alakú elemek, ahol ε egység, így kölcsosen egyértelmű megfeleltetés áll fenn egy nem nulla elem asszociáltjai és az egységek között.

- 147/−3 :

<

tartomány. Egy $0 \neq a \in R$ elemet *felbonthatatlan*nak (vagy *irreducibilis*nek) nevezünk, ha nem egység, és csak triviális módon írható fel szorzatként, tehát $a = bc$, $b, c \in R$

>

tartomány. Egy $a \in R$ elemet *felbonthatatlan*nak (vagy *irreducibilis*nek) nevezünk, ha nem nulla, nem egység, és csak triviális módon írható fel szorzatként, tehát $a = bc$, $b, c \in R$

- 148/1 :

<

egységek és az asszociáltjai. A $0 \neq p \in R$ elemet *prímelem*nek nevezzük, ha nem egység

>

asszociáltjai és az egységek. A $p \in R$ elemet *prímelem*nek nevezzük, ha nem nulla, nem egység

- 148/−21 :

<

integritási tartományban az $a_1, a_2, \ldots, a_n \in R$ elemeknek a $b \in R$ elem *legnagyobb közös*

>

integritási tartományban a $b \in R$ elem az $a_1, a_2, \ldots, a_n \in R$ elemeknek egy *legnagyobb közös*

- 148/−8 :

<

→ **6.1.19. Feladat.** Mutassuk meg, hogy egy integritási tartományban $a|b$ pon-

>

→ **6.1.19. Feladat.** Mutassuk meg, hogy egységelemes integritási tartományban $a|b$ pon-

- 149/−16 :

<

(3) *[Ciklus.] Legyen* $q_{n+1} \leftarrow \lfloor r_n/r_{n+1} \rfloor$, $r_{n+2} \leftarrow r_n \bmod r_{n+1} = r_n - r_{n+1}q_{n+1}$, $x_{n+2} \leftarrow x_n - x_{n+1}q_{n+1}$, $y_{n+2} \leftarrow y_n - y_{n+1}q_{n+1}$, $n \leftarrow n+1$ *és menjünk (2)-re.*

>

(3) *[Ciklus.] Legyen*

$$q_{n+1} \leftarrow \lfloor r_n / r_{n+1} \rfloor,$$

$$r_{n+2} \leftarrow r_n \bmod r_{n+1} = r_n - r_{n+1} q_{n+1},$$

$$x_{n+2} \leftarrow x_n - x_{n+1} q_{n+1},$$

$$y_{n+2} \leftarrow y_n - y_{n+1} q_{n+1},$$

$n \leftarrow n+1$ és menjünk (2)-re.

- 150/−13 :

<

A bővített euklideszi algoritmussal kaphatunk olyan x, y egészeket, hogy $px + my = 1$. Innen $pnx + mny = n$. Mivel p osztója a bal oldalnak, a jobb oldalnak is. □

>

A bővített euklideszi algoritmussal kaphatunk olyan x, y egészeket, hogy $px + my = \pm 1$. Innen $pnx + mny = \pm n$. Mivel p osztója a bal oldalnak, a jobb oldalnak is. □

- 155/1 :

<

6.1.55. Eratoszthenész szitája. Ha egy adott n-ig az összes prímet meg akarjuk

>

6.1.55. Eratoszthenész szitája. Ha egy adott n-ig az összes prímet meg akarjuk

- 161/21 :

<

$k \in \mathbb{Z}$. A kongruencia az $x \equiv 4 \pmod{31}$ kongruenciával ekvivalens; ez a mod 31 ekvivalenciaosztály két mod 62 ekvivalenciaosztály egyesítése, így $x \equiv 4 \pmod{62}$ vagy $x \equiv 35 \pmod{62}$.

>

$k \in \mathbb{Z}$. A kongruencia az $x \equiv 4 \pmod{31}$ kongruenciával ekvivalens; ez a mod 31 ekvivalenciaosztály két mod 62 ekvivalenciaosztály egyesítése, így $x \equiv 4 \pmod{62}$ vagy $x \equiv 35 \pmod{62}$.

- 218/12 A 8.1. ÁBRA HELYETT :

<

>

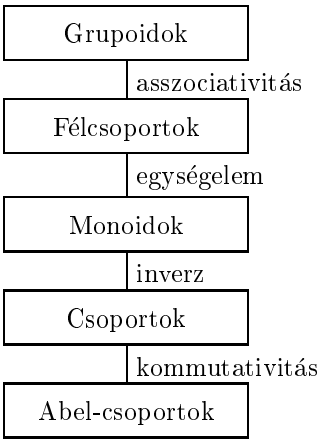
- 221/4 :

<

  - **Példa.** $(\mathbb{R}, +)$ és $\left(\mathbb{R}^*, \cdot\right)$ nem izomorfak, mert az $x + x = 0$ egyenletnek

  >

  - **Példa.** $(\mathbb{R}, +)$ és $\left(\mathbb{R}^\times, \cdot\right)$ nem izomorfak, mert az $x + x = 0$ egyenletnek



8.1. ábra

- 231/19 :

  <

→ **8.1.56. Feladat [2].** Mutassuk meg, hogy $\mathbb{Q}^+$ a szorzással a $\mathbb{Q}\setminus\{0\}$, $\mathbb{R}\setminus\{0\}$, illetve $\mathbb{C}\setminus\{0\}$

  >

→ **8.1.56. Feladat [2].** Mutassuk meg, hogy $\mathbb{Q}^+$ a szorzással a $\mathbb{Q}^\times$, $\mathbb{R}^\times$, illetve $\mathbb{C}^\times$

- 235/−11 :

  <

(3) $(\mathbb{C}\setminus\{0\}/\mathbb{T},\cdot)$ és $(\mathbb{R}^+,\cdot)$;
(4) $(\mathbb{C}\setminus\{0\}/\mathbb{R}^+,\cdot)$ és $(\mathbb{T},\cdot)$;
(5) $(\mathbb{R}/\mathbb{Z},+)$ és $(\mathbb{T},\cdot)$;
(6) $(\mathbb{Q}/\mathbb{Z},+)$ és $(\mathbb{U},\cdot)$;
(7) $(\mathbb{Q}\setminus\{0\}/\mathbb{U}_2,\cdot)$ és $(\mathbb{Q}^+,\cdot)$;
(8) $(\mathbb{R}\setminus\{0\}/\mathbb{U}_2,\cdot)$ és $(\mathbb{R}^+,\cdot)$;

  >

(3) $(\mathbb{C}^\times/\mathbb{T},\cdot)$ és $(\mathbb{R}^+,\cdot)$;
(4) $(\mathbb{C}^\times/\mathbb{R}^+,\cdot)$ és $(\mathbb{T},\cdot)$;
(5) $(\mathbb{R}/\mathbb{Z},+)$ és $(\mathbb{T},\cdot)$;
(6) $(\mathbb{Q}/\mathbb{Z},+)$ és $(\mathbb{U},\cdot)$;
(7) $(\mathbb{Q}^\times/\mathbb{U}_2,\cdot)$ és $(\mathbb{Q}^+,\cdot)$;
(8) $(\mathbb{R}^\times/\mathbb{U}_2,\cdot)$ és $(\mathbb{R}^+,\cdot)$;

- 235/−2 :

<

részcsoportjai $\big(\mathbb{GA}(\mathbb{R}^1),\circ\big)$-nek, de $\mathbb{GL}(\mathbb{R}^1)$ nem normálosztó, míg N normálosztó, és a faktorcsoport izomorf $\mathbb{GL}(\mathbb{R}^1)$-gyel, azaz $(\mathbb{R}\setminus\{0\},\cdot)$-tal.

>

részcsoportjai $\big(\mathbb{GA}(\mathbb{R}^1),\circ\big)$-nek, de $\mathbb{GL}(\mathbb{R}^1)$ nem normálosztó, míg N normálosztó, és a faktorcsoport izomorf $\mathbb{GL}(\mathbb{R}^1)$-gyel, azaz $(\mathbb{R}^\times,\cdot)$-tal.

- 236/3 :

<

(1) $\mathbb{GL}(F^n)/\mathbb{SL}(F^n)$ és $(F^*,\cdot)$;

>

(1) $\mathbb{GL}(F^n)/\mathbb{SL}(F^n)$ és $(F^\times,\cdot)$;

- 237/−1 :

<

8.1.100. Feladat [5]. Mutassuk meg, hogy $(\mathbb{C}\setminus\{0\}/\mathbb{U},\cdot)$ és $(\mathbb{R}^+,\cdot)\times(\mathbb{R}/\mathbb{Q},+)$ izomor-

>

8.1.100. Feladat [5]. Mutassuk meg, hogy $(\mathbb{C}^\times/\mathbb{U},\cdot)$ és $(\mathbb{R}^+,\cdot)\times(\mathbb{R}/\mathbb{Q},+)$ izomor-

- 238/−9 :

<

jelölni, és *n-ed fokú szimmetrikus csoport*nak nevezzük. Nyilvánvalóan S_n rendje $n!$.

>

jelölni, és *n-ed fokú szimmetrikus csoport*nak nevezzük. (Az elnevezés a szimmetrikus polinomokkal való kapcsolatra utal.) Nyilvánvalóan S_n rendje $n!$.

- 240/10 :

<

alkotnak S_n-ben, amit A_n-nel jelölünk és n-ed fokú *alternáló csoport*nak nevezünk. □

>

alkotnak S_n-ben, amit A_n-nel jelölünk és n-ed fokú *alternáló csoport*nak nevezünk. □

Az alternáló csoport elnevezés az alternáló polinomokkal való kapcsolatra utal.

- 241/5 :

<

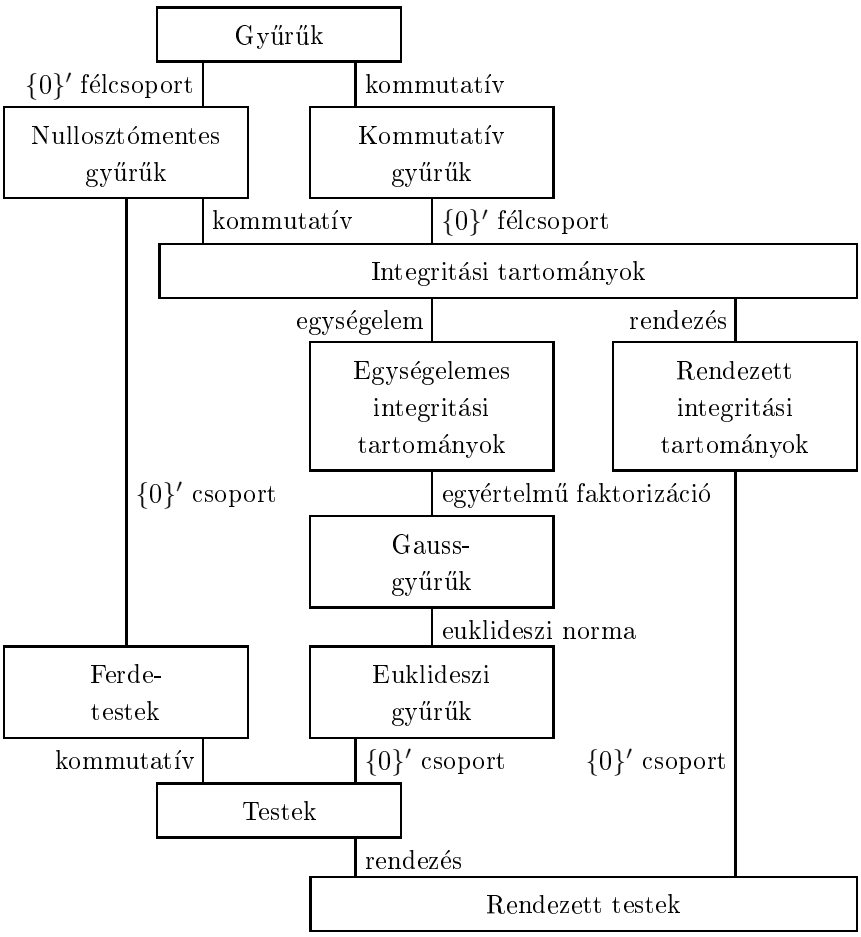
morfak: $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_8$, $\mathbb{Z}_3\setminus\{0\}$, $\mathbb{Z}_5\setminus\{0\}$, $\mathbb{Z}_8\setminus\{0\}$, $\mathbb{Z}_{12}\setminus\{0\}$, S_2, A_3, S_3, D_3, D_4, Q.

>

morfak: $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_8$, $\mathbb{Z}_3^\times$, $\mathbb{Z}_5^\times$, $\mathbb{Z}_8^\times$, $\mathbb{Z}_{12}^\times$, S_2, A_3, S_3, D_3, D_4, Q.

- 242/−14 :
  <
(2) $\mathbb{Z}_7^*$;
  >
(2) $\mathbb{Z}_7^\times$;

- 244/−4 A 8.4. ÁBRA HELYETT :
  <
  >



8.4. ábra

- 256/−17 :

<
φ függvény úgy, hogy
>
φ függvény (*euklideszi norma*) úgy, hogy

- 282/20 :
<
beli gyököket is. (Sok gyűrűben a gyökkeresésre, a faktorizálásra, és az irreducibilitás
>
beli gyököket is. (Sok R gyűrűre a gyökkeresésre, a faktorizálásra, és az irreducibilitás

- 295/−17 :
<
$\cdots+i_n$ és $x^i = x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$. Ezzel a jelöléssel az f polinom $\sum_{|i|\leq m} f_i x^i$ véges összegként
>
$\cdots+i_n$, $i! = i_1!i_2!\cdots i_n!$ és $x^i = x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$. Ezzel a jelöléssel az f polinom $\sum_{|i|\leq m} f_i x^i$ véges összegként

- 295/−1 :
<
$x_2 p_2(x_1, x_2)$ alakban, mert mindkét szorzat konstans tagja nulla.
>
$x_2 p_2(x_1, x_2)$ alakban, mert mindkét szorzat konstans tagja nulla.

* **8.3.132.1. Megjegyzés.** Többhatározatlanú $\mathbb{Z}$ feletti polinomok faktorizálására kívánunk hatékony algoritmust adni, és ehhez szükségünk lesz bizonyos ideálok, a megfelelő faktorgyűrűk és természetes homomorfizmusok vizsgálatára. Ha R gyűrű és I ideál R-ben, $r_1, r_2 \in R$, az $r_1 \equiv r_2 \pmod{I}$ jelölés azt fogja jelenteni, hogy $r_1 - r_2 \in I$.

Tekintsük az R kommutatív egységelemes gyűrű feletti $R[x_1, x_2, \ldots, x_n]$ polinomgyűrűt. Ha $a_1, a_2, \ldots, a_n \in R$, akkor az $f(x_1, x_2, \ldots, x_n) \mapsto f(a_1, a_2, \ldots, a_n)$ leképezése $R[x_1, x_2, \ldots, x_n]$-nek R-be homomorfizmus. Ennek a magja egy I ideál, amely tartalmazza az $x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n$ polinomokat; meg fogjuk mutatni, hogy éppen az ezek által generált ideál. Általánosabban, legyen

$$S = \{x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n\},$$

és tekintsük a komplexusszorzással értelmezett S^α, $\alpha \in \mathbb{N}^+$ halmazt, amely

$$x = (x_1, x_2, \ldots, x_n), \quad a = (a_1, a_2, \ldots, a_n)$$

jelöléssel tömören az $S^\alpha = \left\{(x-a)^i : i \in \mathbb{N}^n,\ |i| = \alpha\right\}$ alakba írható. Az S^α által generált (S^α) ideál az S^α-beli polinomok többszöröseinek összegeiből áll, egy f polinom mellékosztályát pedig reprezentálhatjuk úgy, hogy f-et felírjuk $(x-a)^i$, $i \in \mathbb{N}^n$ alakú polinomok konstansszorosainak összegeként, és elhagyunk minden olyan tagot, amelyre $|i| \geq \alpha$: Az állítás belátásához és a számítás kivitelezéséhez használjuk az $x_i = y_i + a_i$,

$1 \le i \le n$ helyettesítéseket. Egy $f \in R[x_1, x_2, \dots, x_n]$ polinomból a helyettesítéssel egy $g \in R[y_1, y_2, \dots, y_n]$ polinomot kapunk, a $\varphi : f \mapsto g$ leképezés izomorfizmus, amely az S halmazt a $T = \{y_1, y_2, \dots, y_n\}$ halmazba, így az (S^α) ideált a (T^α) ideálba viszi. Ennek elemei az y^i, $i \in \mathbb{N}^n$, $|i| = k$ monomok többszöröseinek összegei. Bármely g polinom mellékosztálya egyetlen α-nál alacsonyabb fokú $\tilde{g}$ polinomot tartalmaz, amit megkaphatunk úgy, hogy g-ből elhagyjuk az összes legalább α-ad fokú tagot. A $\tilde{g}$ polinomot $g \bmod (T^\alpha)$-val fogjuk jelölni. A $g \mapsto \tilde{g} = g \bmod (T^\alpha)$ leképezés a természetes homomorfizmus, amelynek magja (T^α). Speciálisan, $g(y_1, y_2, \dots, y_n) \mapsto g(0, 0, \dots, 0)$ a $g \mapsto g \bmod (T)$ leképezés. A $\varphi^{-1} : \tilde{g} \mapsto \tilde{f}$ leképezéssel, azaz az $y_i = x_i - a_i$, $1 \le i \le n$ helyettesítésekkel megkapjuk az f osztályának reprezentánsát $R[x_1, x_2, \dots, x_n]/(S^\alpha)$-ban. Ezt $f \bmod (S^\alpha)$-val jelöljük; az $f \mapsto \tilde{f} = f \bmod (S^\alpha)$ leképezés a természetes homomorfizmus, amelynek magja (S^α). Speciálisan, $R[x_1, x_2, \dots, x_n]/(S)$ izomorf az R gyűrűvel, a természetes homomorfizmus pedig az $f(x_1, x_2, \dots, x_n) \mapsto f(a_1, a_2, \dots, a_n)$ leképezés.

A következő tételt a fő eredmény, a Hensel-lemma használja.

* **8.3.132.2. Tétel: lineáris diofantoszi egyenlet egyhatározatlanú polinomokra.** *Legyen p prímszám, $\beta \in \mathbb{N}^+$ és $g(x), h(x) \in \mathbb{Z}_{p^\beta}[x]$ polinomok, amelyek főegyütthatója nem osztható p-vel és mod p tekintve relatív prímek. Ekkor minden $f(x) \in \mathbb{Z}_{p^\beta}[x]$ polinomhoz egyértelműen léteznek $\sigma(x), \tau(x) \in \mathbb{Z}_{p^\beta}[x]$ polinomok, amelyekre*

$$\sigma(x)g(x) + \tau(x)h(x) = f(x)$$

és $\deg(\sigma) < \deg(h)$. Ha még $\deg(f) < \deg(g) + \deg(h)$ is teljesül, akkor $\deg(\tau) < \deg(g)$.

Bizonyítás. Először az $f = 1$ esettel foglalkozunk. Indukcióval α szerint megmutatjuk, hogy léteznek olyan $s_\alpha(x), t_\alpha(x) \in \mathbb{Z}_{p^\alpha}[x]$ polinomok, hogy

$$s_\alpha(x)g(x) + t_\alpha(x)h(x) \equiv 1 \pmod{p^\alpha}.$$

Bővített euklidészi algoritmussal kaphatunk olyan $s(x), t(x) \in \mathbb{Z}_p[x]$ polinomokat, amelyekre

$$s(x)g(x) + t(x)h(x) \equiv 1 \pmod{p};$$

ez $s_1 = s$, $t_1 = t$ választással adja az állítást $\alpha = 1$-re. Ha α-ra teljesül az állítás, akkor legyen

$$e_\alpha(x) = \frac{1 - s_\alpha(x)g(x) - t_\alpha(x)h(x)}{p^\alpha},$$

és legyen $s_{\alpha+1}(x) = s_\alpha(x) + p^\alpha e_\alpha(x)s(x)$, $t_{\alpha+1}(x) = t_\alpha(x) + p^\alpha e_\alpha(x)t(x)$. Ekkor

$$\begin{aligned} s_{\alpha+1}(x)g(x) + t_{\alpha+1}(x)h(x) &\equiv s_\alpha(x)g(x) + t_\alpha(x)h(x) + p^\alpha e_\alpha(x)\big(s(x)g(x) + t(x)h(x)\big) \\ &\equiv 1 - p^\alpha e_\alpha(x) + p^\alpha e_\alpha(x)\big(s(x)g(x) + t(x)h(x)\big) \\ &\equiv 1 + p^\alpha e_\alpha(x)\big(s(x)g(x) + t(x)h(x) - 1\big) \equiv 1 \pmod{p^{\alpha+1}}. \end{aligned}$$

Végül osszuk maradékosan az $s_\beta(x)f(x)$ polinomot $h(x)$-szel:

$$s_\beta(x)f(x) = q(x)h(x) + \sigma(x),$$

és legyen

$$\tau(x) = t_\beta(x)f(x) - q(x)g(x).$$

Ekkor

$$\begin{aligned}\sigma(x)g(x) + \tau(x)h(x) &= \big(s_\beta(x)f(x) - q(x)h(x)\big)g(x) + \big(t_\beta(x)f(x) + q(x)g(x)\big)h(x)\\ &= f(x)\big(s_\beta(x)g(x) + t_\beta(x)h(x)\big) \equiv f(x) \pmod{p^\beta}.\end{aligned}$$

(Vegyük észre, hogy a maradékos osztást az α szerinti indukció minden lépésében is elvégezhetjük, ha s_α és t_α fokszámát csökkenteni akarjuk.)

Az egyértelműség bizonyításához tegyük fel, hogy σ_1, τ_1 és σ_2, τ_2 is megoldások. Ekkor

$$\big(\sigma_1(x) - \sigma_2(x)\big)g(x) \equiv \big(\tau_2(x) - \tau_1(x)\big)h(x) \pmod{p^\beta}.$$

Indukcióval megmutatjuk, hogy $\sigma_1(x) \equiv \sigma_2(x) \pmod{p^\alpha}$ és $\tau_2(x) \equiv \tau_1(x) \pmod{p^\alpha}$, $\alpha = 0, 1, \dots, \beta$. Ha ez egy $\alpha < \beta$-ra teljesül, akkor osztva p^α-val,

$$\frac{\sigma_1(x) - \sigma_2(x)}{p^\alpha}g(x) \equiv \frac{\tau_2(x) - \tau_1(x)}{p^\alpha}h(x) \pmod{p^{\beta-\alpha}},$$

tehát mod p is. Mivel $\mathbb{Z}_p[x]$-ben g és h relatív prímek, $h|(\sigma_1 - \sigma_2)/p^\alpha$, de $\deg(\sigma_1 - \sigma_2) < \deg(h)$, így $(\sigma_1 - \sigma_2)/p^\alpha \equiv 0 \pmod{p}$, és hasonlóan $(\tau_2 - \tau_1)/p^\alpha \equiv 0 \pmod{p}$.

Végül, ha $\deg(f) < \deg(g) + \deg(h)$, akkor a fokszámok összehasonlításából következik, hogy $\deg(\tau) < \deg(g)$, mivel $\deg(g)$ főegyütthatója nem nullosztó.

* **8.3.132.3. Tétel: Hensel-lemma többhatározatlanú polinomokra.** *Legyen p prímszám, $\beta \in \mathbb{N}^+$ és $y = (y_1, y_2, \dots, y_n)$ jelöléssel legyen*

$$f(y_1, y_2, \dots, y_n, z) = f(y, z) \in \mathbb{Z}[y, z]$$

egy polinom. Tegyük fel, hogy $f(0, z)$ foka, d, ugyanannyi, mint $f(y, z)$ foka z-ben, és p nem osztja $f(0, z)$ főegyütthatóját. Legyen $S = \{y_1, y_2, \dots, y_n\}$ és legyenek $g_1, h_1 \in \mathbb{Z}[y, z]$ polinomok, amelyekre

(1) *a $\mathbb{Z}[y][z]$-beli (azaz z szerinti) főgyütthatók szorzata ugyanannyi, mint $f \in \mathbb{Z}[y][z]$ főegyütthatója;*

(2) *$f(0, z) \equiv g_1(0, z)h_1(0, z) \pmod{p^\beta}$;*

(3) *$g(z) = g_1(0, z) \bmod p$ és $h(z) = h_1(0, z) \bmod p$ relatív prímek $\mathbb{Z}_p[z]$-ben.*

Ekkor minden $\gamma \in \mathbb{N}^+$-ra léteznek olyan $g_\gamma, h_\gamma \in \mathbb{Z}[y, z]$ polinomok, amelyekre

(4) *$\mathbb{Z}[y][z]$-ben g_γ és g_1 valamint h_γ és h_1 főegyütthatója megegyezik;*

(5) *$g_\gamma(0, z) \equiv g_1(0, z) \pmod{p^\beta}$ és $h_\gamma(0, z) \equiv h_1(0, z) \pmod{p^\beta}$;*

(6) *$f \bmod (S^\gamma, p^\beta) = g_\gamma h_\gamma \bmod (S^\gamma, p^\beta)$.*

Továbbá a g_γ és h_γ polinomok egyértelműek $\bmod (S^\gamma, p^\beta)$.

A bizonyítás konstruktív.

Bizonyítás. A létezést γ szerinti indukcióval bizonyítjuk. Tegyük fel, hogy teljesül γ-ra, és legyen $e_\gamma = f - g_\gamma h_\gamma$. Az e_γ foka $\mathbb{Z}[y][z]$-ben kisebb, mint d, és (6) szerint $e_\gamma \bmod (S^\gamma, p^\beta) = 0$, így e_γ felírható $\sum_{|i|=\gamma} f_i(y,z)y^i$ alakban, ahol f_i foka $\mathbb{Z}[y][z]$-ben kisebb, mint d minden $i \in \mathbb{N}^n$, $|i| = \gamma$-ra. Az előző tétel szerint léteznek olyan egyértelműen meghatározott $\sigma_i(z), \tau_i(z) \in \mathbb{Z}_{p^\beta}[z]$ polinomok, amelyekre

$$\sigma_i(z)g(z) + \tau_i(z)h(z) \equiv f_i(0,z) \pmod{p^\beta},$$

$\deg(\sigma_i) < \deg(h)$, $\deg(\tau_i) < \deg(g)$. Legyen

$$g_{\gamma+1}(y,z) = g_\gamma(y,z) + \sum_{|i|=\gamma} \tau_i(z)y^i, \quad h_{\gamma+1}(y,z) = h_\gamma(y,z) + \sum_{|i|=\gamma} \sigma_i(z)y^i.$$

Ekkor (4) és (5) nyilván teljesülnek, és

$$\begin{aligned}
&f(y,z) - g_{\gamma+1}(y,z)h_{k+1}(y,z) \\
&\quad\equiv f(y,z) - g_\gamma(y,z)h_\gamma(y,z) - g_\gamma(y,z)\sum_{|i|=\gamma}\sigma_i(z)y^i - h_\gamma(y,z)\sum_{|i|=\gamma}\tau_i(z)y^i \\
&\quad\equiv e_\gamma(y,z) - \sum_{|i|=\gamma}\big(\sigma_i(z)g(z) + \tau_i(z)h(z)\big)y^i \\
&\quad\equiv e_\gamma(y,z) - \sum_{|i|=\gamma} f_i(0,z)y^i \equiv 0 \quad \big(\mathrm{mod}(S^{\gamma+1}, p^\beta)\big).
\end{aligned}$$

Az egyértelműség bizonyítása is indukcióval történik; $\gamma = 1$-re teljesül (5) miatt. Tegyük fel, hogy γ-ra teljesül. Mivel (6) teljesül $\gamma+1$-re, $f \equiv g_{\gamma+1}h_{\gamma+1} \ \big(\mathrm{mod}(S^\gamma, p^\beta)\big)$. A g_γ és h_γ egyértelműsége miatt mod (S^γ, p^β) azt kapjuk, hogy

$$g_{\gamma+1}(y,z) - g_\gamma(y,z) = \sum_{|i|=\gamma}\tau_i(y,z)y^i$$

és

$$h_{\gamma+1}(y,z) - h_\gamma(y,z) = \sum_{|i|=\gamma}\sigma_i(y,z)y^i$$

valamely σ_i, τ_i polinomokra. Az $f(y,z) - g_\gamma(y,z)h_\gamma(y,z) = e_\gamma(y,z) = \sum_{|i|=\gamma} f_i(y,z)y^i$ felírásból, mivel

$$\begin{aligned}
0 &\equiv f(y,z) - g_{\gamma+1}(y,z)h_{\gamma+1}(y,z) \\
&\equiv f(y,z) - g_\gamma(y,z)h_\gamma(y,z) - g_\gamma(y,z)\sum_{|i|=\gamma}\sigma_i(y,z)y^i - h_\gamma(x,y)\sum_{|i|=k}\tau_i(y,z)y^i \\
&\equiv e_\gamma(y,z) - \sum_{|i|=\gamma}\big(\sigma_i(0,z)g(z) + \tau_i(0,z)h(z)\big)y^i \\
&\equiv \sum_{|i|=\gamma} f_i(0,z) - \big(\sigma_i(0,z)g(z) + \tau_i(0,z)h(z)\big) \quad \big(\mathrm{mod}(S^{\gamma+1}, p^\beta)\big),
\end{aligned}$$

az előző tételben szereplő egyértelműségből azt kapjuk, hogy $\sigma_i(0,z)$ és $\tau_i(0,z)$ egyértelműen meghatározott, ami azt jelenti, hogy a $g_{\gamma+1}-g_\gamma$ és $h_{\gamma+1}-h_\gamma$ polinomok különbégében az y-ban γ-ad fokú tagok egyértelműen meghatározottak, amiből következik $g_{\gamma+1}$ és $h_{\gamma+1}$ egyértelműsége mod $(S^{\gamma+1},p^\beta)$.

* **8.3.132.4. Egészegyüttható̋s többhatározatlanú polinomok faktorizálása.** A Hensel-lemma előző, többhatározatlanú polinomokra vonatkozó, és az egyhatározatlanú polinomokra vonatkozó változata együtt felhasználható egész együtthatós többhatározatlanú polinomok páronként relatív prím polinomokra való faktorizálására. Először is, akármilyen, akár komplex együtthatós $f(x_1,x_2,\ldots,x_n)=\sum_{i\in\mathbb{N}^n} f_i x^i$ polinomra legyen $B(f)=\sum_{i\in\mathbb{N}^n}|f_i|^2 i!(d-|i|)!$, ahol d a polinom teljes fokszáma. Megmutatható (lásd Knuth [44], 4.6.2–21 feladat), hogy ha $f=gh$, akkor $B(g)B(h)\le B(f)$; ez korlátot ad a lehetséges faktorok együtthatóira.

Csak primitív polinomok faktorizálásával fogunk foglalkozni. Ha az f primitív polinom felírható nem triviális módon gh alakban, ahol $g,h\in\mathbb{Z}[x_1,x_2,\ldots,x_n]$, továbbá g és h relatív prímek, akkor g és h primitív polinomok, és $f\equiv gh\ \big(\mathrm{mod}(S^\gamma,p^\beta)\big)$ minden p prímre és $S=\{x_2-a_2,x_3-a_3,\ldots,x_n-a_n\}$ halmazra, bármely $\gamma,\beta\in\mathbb{N}^+$ kitevőkre. Keressünk olyan a_i, $2\le i\le n$ értékeket és p páratlan prímet, hogy az $x_1=z$, $x_i=y_{i-1}+a_i$ helyettesítések után, az $y=(y_1,y_2,\ldots,y_{n-1})$ jelöléssel a kapott $f^*(y,z)$ polinom teljesítse az előző tétel feltételeit, pontosabban foka z-ben ugyanannyi legyen, mint az eredeti polinom foka x_1-ben, és ha $\tilde{c}\in\mathbb{Z}[y]$ jelöli az $f^*\in\mathbb{Z}[y][z]$ polinom főegyütthatóját, akkor $\tilde{c}(0)$ ne legyen osztható p-vel. Szorozzuk meg $f^*(y,z)$-t $\tilde{c}(y)$-nal, azaz legyen $\tilde{f}(y,z)=\tilde{c}(y)f^*(y,z)$, és alakítsuk szorzattá az $\tilde{f}(0,z)=\tilde{c}(0)f^*(0,z)$ egyhatározatlanú polinomot modulo p. Mindkét tényezőt végigszorozva egy $\mathbb{Z}_p$-beli egységgel, elérhetjük, hogy mindkét tényezőben a főegyüttható $\tilde{c}(0)$-val kongruens modulo p. A főegyütthatókat mindkét tényezőben kicserélve $\tilde{c}(0)$-ra, a kapott $g_1(z)$, $h_1(z)$ polinomokra teljesülnek az egyhatározatlanú polinomokra vonatkozó Hensel-lemma feltételei, így azokat „felemelve” egy mod p^β vett felbontássá, megtalálhatjuk $\tilde{f}(0,z)$ egy $\tilde{g}(0,z)\tilde{h}(0,z)$ szorzattá bontását, amelyre $\tilde{g}(0,z)\equiv g_1(z)\pmod p$ és $\tilde{h}(0,z)\equiv h_1(z)\pmod p$, ha van ilyen. A β kitevőt olyan nagynak kell választani, hogy p^β nagyobb legyen $\tilde{f}(y,z)$ faktorai együtthatóinak abszolút értéke egy korlátjának a kétszeresénél, és célszerű a maradékosztályokat a legkisebb abszolút értékű maradékukkal reprezentálni. A z-ben vett főegyütthatókat kicserélve $\tilde{c}(y)$-ra, a kapott $g_1(y,z)$, $h_1(y,z)$ polinomokra teljesülnek az előző tétel, a Hensel-lemma feltételei $\gamma=1$-re. A Hensel-lemma segítségével „felemelve” ezt a felbontást egy mod (S^γ,p^β) vett felbontássá, ahol γ nagyobb, mint $\tilde{f}$ foka, megtalálhatjuk $\tilde{f}(y,z)$ egy $\tilde{g}(y,z)\tilde{h}(y,z)$ szorzattá bontását, amelyre $\tilde{g}(0,z)\equiv g_1(z)\pmod p$ és $\tilde{h}(0,z)\equiv h_1(z)\pmod p$, ha van ilyen. A maradékosztályokat végig a legkisebb abszolút értékű maradékukkal célszerű reprezentálni, mert ekkor közvetlenül $\tilde{g}(y,z)$ és $\tilde{h}(y,z)$ együtthatóit kapjuk. A $\tilde{g}(y,z)$ és $\tilde{h}(y,z)$ primitív részét véve, $f^*(y,z)$ egy szorzatfelbontását (tehát f egy szorzatfelbontását) kapjuk, és így nyilván minden szorzatfelbontás kiadódik, hiszen mindegyiknek van valamilyen képe mod (S,p).

Az eljárás hátránya, hogy egy „ritka” (kevés nem nulla együtthatót tartalmazó) többhatározatlanú polinom az x_i helyére y_i+a_i-t helyettesítve $(i=2,\ldots,n)$ általában nem marad ritka, ha $a_i\neq 0$. Márpedig sokszor nem tudunk $a_i=0$-t választani, mert

ezzel a választással nem teljesülnek a $\tilde{c}$-ra vonatkozó feltételek. Egy javított eljárást kaphatunk, ha egyszerre csak egy helyettesítést hajtunk végre, mert ekkor nem nő meg olyan nagyon a nem nulla együtthatók száma. Ehhez azonban szükségünk lesz az alábbi tétel által leírt rekurzív eljárásra.

* **8.3.132.5. Polinom diofantoszi egyenletek megoldása többhatározatlanú polinomokra.** *Legyen p prímszám, $\beta \in \mathbb{N}^+$. Tegyük fel, hogy $x = (x_1, x_2, \dots, x_n)$ és $a = (a_1, a_2, \dots, a_n)$ jelöléssel $S = \{x_1 - a_1, \dots, x_n - a_n\}$,*

$$g(z, x_1, \dots, x_n) = g(z, x) \in \mathbb{Z}_{p^\beta}[z, x],$$

$$h(z, x_1, \dots, x_n) = h(z, x) \in \mathbb{Z}_{p^\beta}[z, x],$$

$g(z, a)$ foka ugyanannyi, mint $g(z, x)$ foka z-ben, $h(z, a)$ foka ugyanannyi, mint $h(z, x)$ foka z-ben, $g(z, a)$ és $h(z, a)$ relatív prímek mod p. Ekkor minden $f \in \mathbb{Z}_{p^\beta}[z, x]$ polinomhoz, amelynek foka kisebb, mint γ, léteznek olyan $\sigma(z, x)$ és $\tau(z, x)$ polinomok, hogy

$$\sigma(z, x)g(z, x) + \tau(z, x)h(z, x) \equiv f(z, x) \quad \big(mod\ (S^\gamma, p^\beta)\big).$$

A bizonyítás eljárást ad σ és τ meghatározására.

Bizonyítás. Tudjuk a tételből, hogy $n = 0$-ra teljesül az állítás. Indukcióval, tegyük fel, hogy n-re teljesül, és megmutatjuk, hogy $n + 1$-re is. Helyettesítsünk x_{n+1} helyére $y + a_{n+1}$-et. A kapott polinomokat jelölje rendre $\tilde{f}$, $\tilde{g}$ és $\tilde{h}$. Megmutatjuk α szerinti indukcióval, hogy léteznek $\tilde{\sigma}_\alpha$ és $\tilde{\tau}_\alpha$ polinomok, amelyek foka y-ban kisebb, mint α, és

$$\tilde{\sigma}_\alpha(z, x, y)\tilde{g}(z, x, y) + \tilde{\tau}_\alpha(z, x, y)h(z, x, y) \equiv \tilde{f}(z, x, y) \quad \big(\mathrm{mod}\ (S^\gamma, y^\alpha, p^\beta)\big).$$

Az $\alpha = 1$ esetben azt kell megmutatnunk, hogy léteznek olyan $\tilde{\sigma}_1$ és $\tilde{\tau}_1$ polinomok, hogy

$$\tilde{\sigma}_1(z, x, 0)\tilde{g}(z, x, 0) + \tilde{\tau}_\alpha(z, x, 0)h(z, x, 0) \equiv \tilde{f}(z, x, 0) \quad \big(\mathrm{mod}\ (S^\gamma, p^\beta)\big);$$

ez éppen az n szerinti indukciós feltevésünk. Tegyük fel, hogy α-ra már teljesül az állítás, és legyen

$$e_\alpha(z, x, y) = \tilde{f}(z, x, y) - \tilde{\sigma}_\alpha(z, x, y)\tilde{g}(z, x, y) + \tilde{\tau}_\alpha(z, x, y)h(z, x, y).$$

Mivel ez a polinom mod (S^γ, p^β) egy olyan polinommal ekvivalens, amely osztható y^α-val, ezt $\tilde{f}_\alpha$-val jelölve, alkalmazhatjuk az indukciós feltevést, és olyan s_α és t_α polinomokat kapunk, amelyekre

$$s_\alpha(z, x)\tilde{g}(z, x, 0) + t_\alpha(z, x)\tilde{h}(z, x, 0) \equiv \tilde{f}_\alpha(z, x, 0) \quad \big(\mathrm{mod}\ (S^\gamma, p^\beta)\big).$$

Legyen $\tilde{\sigma}_{\alpha+1}(z,x,y) = \tilde{\sigma}_\alpha(z,x,y) + t_\alpha(z,x)y^\alpha$ és $\tilde{\tau}_{\alpha+1}(z,x,y) = \tilde{\sigma}_\alpha(z,x,y) + t_\alpha(z,x)y^\alpha$. Ekkor

$$\begin{aligned}\tilde{f}(z,x,y) &- \tilde{\sigma}_{\alpha+1}(z,x,y)\tilde{g}(z,x,y) - \tilde{\tau}_{\alpha+1}(z,x,y)\tilde{g}(z,x,y)\\ &\equiv e_\alpha(z,x,y) - t_\alpha(z,x)y^\alpha\tilde{g}(z,x,y) - s_\alpha(z,x)y^\alpha\tilde{h}(z,x,y)\\ &\equiv \tilde{f}_\alpha(z,x,0)y^\alpha - t_\alpha(z,x)y^\alpha\tilde{g}(z,x,0) - s_\alpha(z,x)y^\alpha\tilde{h}(z,x,0)\\ &\equiv 0 \quad \big(\mathrm{mod}\ (S^\gamma, y^{\alpha+1}, p^\beta).\end{aligned}$$

Az $\alpha = \gamma$ esetben megkapjuk az állítást $n+1$-re, ha alkalmazzuk az $y = x_{n+1} - a_{n+1}$ helyettesítést.

* **8.3.132.6. Egészegyütthatós többhatározatlanú polinomok faktorizálása, javított eljárás.** Most is csak primitív polinomok faktorizálásával fogunk foglalkozni. Ha az f primitív polinom felírható gh alakban, ahol $g,h \in \mathbb{Z}[x_1,x_2,\dots,x_n]$, valamint g és h relatív prímek, akkor g és h primitív polinomok, és $f \equiv gh \ \big(\mathrm{mod}\ (S_k^\gamma, S_k', p^\beta)\big)$ minden p prímre és $S_k = \{x_2-a_2, x_3-a_3, \dots, x_k-a_k\}$, $S_k' = \{x_{k+1}-a_{k+1}, \dots, x_n-a_n\}$ halmazra, bármely $\gamma,\beta \in \mathbb{N}^+$ kitevőkre. Keressünk olyan a_i, $2 \le i \le n$ értékeket és p páratlan prímet, hogy az $x_i = a_i$, $2 \le i \le n$ helyettesítések után a kapott polinom foka x_1-ben ugyanannyi legyen, mint az eredeti polinom foka x_1-ben, és ha c jelöli az $f \in \mathbb{Z}[x_2,\dots,x_n][x_1]$ polinom főegyütthatóját (azaz az x_1-ben vett főegyütthatót), akkor $c(a_2,\dots,a_n)$ ne legyen osztható p-vel. Szorozzuk meg f-et c-vel; az

$$f^*(x_1,x_2,\dots,x_n) = c(x_2,\dots,x_n)f(x_1,x_2,\dots,x_n)$$

polinomot fogjuk szorzattá alakítani mod (S^γ, p^β), ahol

$$S = \{x_2-a_2, x_3-a_3, \dots, x_n-a_n\} = S_n = S_k \cup S_k'.$$

Ha a γ kitevőt úgy választjuk, hogy nagyobb legyen, mint f^* foka, a β kitevőt pedig úgy, hogy p^β nagyobb legyen, mint a fellépő g^* és h^* tényezők lehetséges együtthatói abszolút értékeinek kétszerese, az együtthatókat mod p^β a legkisebb abszolút értékű reprezentánssal reprezentálva, megkapjuk a g^* és h^* polinomokat. Primitív részük adja a keresett g és h polinomokat.

Az eljárás lényege, hogy az

$$(1) \qquad f^*(x_1,\dots,x_k,a_{k+1},\dots,a_n) \equiv g_k^*(x_1,\dots,x_k)h_k^*(x_1,\dots,x_k) \ \big(\mathrm{mod}\ (S_k^\gamma, p^\beta)\big)$$

felbontás birtokában valamely k-ra, azt „felemelve" előállítunk egy hasonló felbontást $k+1$-re. A $k=1$ esetben először az egyhatározatlanú $f^*(x_1,a_2,\dots,a_n)$ polinom mod p vett szorzatfelbontását állítjuk elő. Mindkét tényezőt végigszorozva egy $\mathbb{Z}_p$-beli egységgel, elérhetjük, hogy mindkét tényezőben a főegyütthető $c(a_2,\dots,a_n)$-nel kongruens modulo p. A főegyütthatókat mindkét tényezőben kicserélve $c(a_2,\dots,a_n)$-re, a kapott $g_1(x_1)$, $h_1(x_1)$ polinomokra teljesülnek az (egyhatározatlanú polinomokra vonatkozó) Hensel-lemma feltételei $\alpha = 1$-re. A Hensel-lemma segítségével „felemelve" ezt a felbontást egy modulo p^β vett felbontássá, megtalálhatjuk $f^*(x_1,a_2,\dots,a_n)$ egy $g_1^*(x_1)h_1^*(x_1)$ szorzattá

bontását, amelyre $g_1^*(x_1) \equiv g_1(x_1) \pmod p$ és $h_1^*(x_1) \equiv h_1(x_1) \pmod p$, ha van ilyen. Ezzel $k = 1$-re készen vagyunk.

Nézzük az indukciós lépést. Tegyük fel, hogy k-ra van egy (1) szerinti felbontásunk. Az f^*-ból $x_{k+1} = y + a_{k+1}$, $x_{k+2} = a_{k+2}, \dots, x_n = a_n$ helyettesítésekkel kapott $\tilde{f}_k$ polinom egy

$$\tilde{f}_k(x, y, a') \equiv \tilde{g}_{k,j}(x, y)\tilde{h}_{k,j}(x, y) \ \big(\mathrm{mod}\ (S_k^\gamma, y^j, p^\beta)\big) \tag{2}$$

felbontását szeretnénk megkapni, ahol $x = (x_1, \dots, x_k)$ és $a' = (a_{k+2}, \dots, a_n)$. Ez is indukcióval megy: a $j = 1$ esetben az előző lépés eredménye adja a felbontást, egyébként pedig legyen

$$e_{k,j}(x, y) = \tilde{f}(x, y, a') - \tilde{g}_{k,j}(x, y)\tilde{h}_{k,j}(x, y) = c_{k,j}(x, y)y^j.$$

Az előző tétel szerint kaphatunk olyan $\sigma_{k,j}$ és $\tau_{k,j}$ polinomokat, hogy

$$c_{k,j}(x, 0) = \sigma_{k,j}(x)g_k(x) + \tau_{k,j}(x)h_k(x).$$

Legyen $\tilde{g}_{k,j+1}(x, y) = \tilde{g}_{k,j}(x, y) + \tau_{k,j}(x)y^j$, $\tilde{h}_{k,j+1}(x, y) = \tilde{h}_{k,j}(x, y) + \sigma_{k,j}(x)y^j$. Ekkor

$$\begin{aligned}
&\tilde{f}(x, y, a') - \tilde{g}_{k,j+1}(x, y)\tilde{h}_{k,j+1}(x, y) \\
&\quad \equiv \tilde{f}(x, y, a') - \tilde{g}_{k,j}(x, y)\tilde{h}_{k,j}(x, y) - \tilde{g}_{k,j}(x, y)\sigma_{k,j}(x)y^j - \tilde{h}_{k,j}(x, y)\tau_{k,j}(x)y^j \\
&\quad \equiv 0 \ \big(\mathrm{mod}\ (S_k^\gamma, y^{j+1}, p^\beta)\big).
\end{aligned}$$

Végül vegyük észre, hogy a $j = \gamma$ esetben (2)-ből (1) megkapható k helyett $k + 1$-re.

* **8.3.132.7. Megjegyzés.** Az eddig tanult módszerek lehetővé teszik, hogy $\mathbb{Z}$ feletti többhatározatlanú polinomokat páronként relatív prím tényezők szorzatára bontsunk. Ezek persze lehetnek irreducibilis polinomok hatványai; az irreducibilis polinomokat magukat (valahanyadik) gyököt vonva kaphatjuk meg. Ezt hatékonyan úgy tehetjük meg, hogy egy kivételével az összes változó helyébe beírva egy konstanst, valamely p páratlan prím modulusra $\mathbb{Z}_p$ felett meghatározzuk a megfelelő irreducibilis faktor képét. Ennek a képnek a „felemelését” az eddig tanultakhoz hasonlóan, de most Newton-iterációval végezhetjük, amelynek két fajtáját kell kombinálnunk. Ismertetésükhöz szükség lesz a Taylor-formula algebrai változatára.

* **8.3.132.8. Taylor-formula egyhatározatlanú polinomokra.** *Legyen R gyűrű, $f \in R[x]$ polinom. Ekkor az $f(x + y) \in R[x, y]$ polinomra*

$$f(x + y) = f(x) + f'(x)y + g(x, y)y^2$$

valamely $g(x, y) \in R[x, y]$ polinommal.

Bizonyítás. Az $f(x+y)$ polinom nyilván egyértelműen felírható

$$f(x+y) = h(x) + k(x)y + g(x,y)y^2$$

alakban, ahol $h, k \in R[x]$ és $g \in R[x,y]$. Az $y=0$ helyettesítéssel $h = f$. Az y szerint differenciálva,

$$f'(x+y) = k(x) + 2yg(x,y) + l(x,y)y^2,$$

ahol l a g polinom y szerinti deriváltja. Az $y=0$ helyettesítéssel $k = f'$. □

* **8.3.132.9. Ideál-adikus Newton-iteráció.** Tegyük fel, hogy az $F(u) = 0$ algebrai egyenletet akarjuk megoldani, ahol p egy prímszám és $F \in \mathbb{Z}_p[x_1, x_2, \ldots, x_n][u]$. A $\{x_1 - a_1, x_2 - a_2, \ldots x_m - a_m\}$ halmaz, ahol $a_1, a_2, \ldots, a_m \in \mathbb{Z}_p$, az $x_i = y_i + a_i$, $1 \leq i \leq m$ helyettesítésekkel az $S = \{y_1, y_2, \ldots, y_m\}$ halmazba, az F polinom pedig egy $f \in \mathbb{Z}_p[x,y][u]$ polinomba megy át, ahol $y = (y_1, y_2, \ldots, y_m)$ és $x = (x_{m+1}, x_{m+2}, \ldots, x_n)$. Legyen $u \in \mathbb{Z}_p[x,y]$ egy gyöke az $f(u) = 0$ egyenletnek, és írjuk fel u-t

$$u(x,y) = \sum_{|i| \leq \beta} e_i(x) y^i, \quad i \in \mathbb{N}^m$$

alakban. Tegyük fel, hogy $u_1(x) = e_{(0,\ldots,0)}(x)$ ismert; nyilván $f(u_1) \bmod (S) = 0$. Tegyük fel továbbá, hogy $f'(u_1) \bmod (S) \neq 0$, ahol a deriválás u szerint értendő. Megmutatjuk, hogy ha az

$$u_\alpha(x,y) = \sum_{|i| < \alpha} e_i(x) y^i$$

„α-ad rendű ideál-adikus közelítés" ismert, akkor hogyan határozható meg $u_{\alpha+1}(x,y)$. Mivel $f(u_\alpha) \bmod (S^\alpha) = 0$,

$$f(u_\alpha) = \sum_{|i| = \alpha} c_i(x,y) y^i.$$

Mivel

$$u_{\alpha+1} = u_\alpha + \sum_{|i|=\alpha} e_i(x) y^i,$$

és a Taylor-formula szerint

$$f\Big(u_\alpha + \textstyle\sum_{|i|=\alpha} e_i(x)y^i\Big) = f(u_\alpha) + f'(u_\alpha) \displaystyle\sum_{|i|=\alpha} e_i(x) y^i + g\Big(u_\alpha, \textstyle\sum_{|i|=\alpha} e_i(x)y^i\Big)\Big(\displaystyle\sum_{|i|=\alpha} e_i(x) y^i\Big)^2,$$

ahonnan mindkét oldalt $\bmod (S^{\alpha+1})$ tekintve,

$$f(u_{\alpha+1}) \equiv \sum_{|i|=\alpha} c_i(x,0) y^i + \Big(f'(u_\alpha) \bmod (S)\Big)\Big(\sum_{|i|=\alpha} e_i(x) y^i\Big).$$

Mivel $f(u_{\alpha+1}) \bmod (S^{\alpha+1}) = 0$ és $f'(u_\alpha) \bmod (S) = f'(u_1) \bmod (S)$, azt kapjuk, hogy

$$0 \equiv \sum_{|i|=\alpha} c_i(x,0)y^i + \Big(f'(u_1) \bmod (S)\Big)\Big(\sum_{|i|=\alpha} e_i(x)y^i\Big).$$

Innen

$$e_i(x) = \frac{-c_i(x,0)}{f'(u_1) \bmod (S)}$$

minden $|i| = \alpha$-ra $\mathbb{Z}_p[x]$-ben, és az osztásnak maradék nélkülinek kell lenni.

* **8.3.132.10. p-adikus Newton-iteráció.** Tegyük fel, hogy az $f(u) = 0$ algebrai egyenletet akarjuk megoldani, ahol $x = (x_1, x_2, \dots, x_n)$ jelöléssel $f \in \mathbb{Z}[x][u]$. Legyen u egy gyök, p egy prímszám, amiről az egyszerűség kedvéért feltesszük, hogy páratlan, reprezentáljuk a maradékosztályokat a legkisebb abszolút értékű maradékkal, és írjuk fel u-t p-alapú számrendszerben:

$$u(x) = e_0(x) + e_1(x)p + e_2(x)p^2 + \cdots + e_\beta(x)p^\beta,$$

ahol $e_\alpha(x) \in \mathbb{Z}_p[x]$. Tegyük fel, hogy $u_1(x) = e_0(x)$ ismert; nyilván $f(u_1) \equiv 0 \pmod{p}$. Tegyük fel továbbá, hogy $f'(u_1) \bmod p \neq 0$, ahol a deriválás u szerint értendő. Az

$$u_\alpha(x) = e_0(x) + e_1(x)p + e_2(x)p^2 + \cdots + e_{\alpha-1}(x)p^{\alpha-1}$$

„α-ad rendű p-adikus közelítés” ismeretében e_α, és így $u_{\alpha+1}$ meghatározható: $f(u_\alpha) \equiv 0 \pmod{p^\alpha}$ és a Taylor-formula szerint

$$f(u_\alpha + e_\alpha p^\alpha) = f(u_\alpha) + f'(u_\alpha)e_\alpha p^\alpha + g(u_\alpha, e_\alpha p^\alpha)u_\alpha^2 p^{2\alpha},$$

ahonnan

$$\frac{f(u_\alpha + e_\alpha p^\alpha)}{p^\alpha} = \frac{f(u_\alpha)}{p^\alpha} + f'(u_\alpha)e_\alpha + g(u_\alpha, e_\alpha p^\alpha)u_\alpha^2 p^\alpha.$$

Mivel $f(u_{\alpha+1}) = f(u_\alpha + e_\alpha p^\alpha) \equiv 0 \pmod{p^{\alpha+1}}$, azt kapjuk, hogy

$$0 \equiv \frac{f(u_\alpha)}{p^\alpha} + \big(f'(u_\alpha) \bmod p\big)e_\alpha \pmod{p},$$

ahonnan, felhasználva, hogy $f'(u_\alpha) \equiv f'(u_1) \pmod{p}$, kapjuk, hogy

$$e_\alpha = \frac{-f(u_\alpha)/p^\alpha}{f'(u_1) \bmod p}$$

$\mathbb{Z}_p[x]$-ben, és az osztásnak maradék nélkülinek kell lenni.

* **8.3.132.11. Legnagyobb közös osztó számolása többhatározatlanú polinomokra.** A faktorizálásra tanult hatékony eljárások primitív polinomokra alkalmazhatók, a primitív rész képzéséhez pedig az együtthatók legnagyobb közös osztójával végig kell osztani a polinomot. A legnagyobb közös osztó számolására racionális törtfüggvények egyszerűsítéséhez is szükség van; ez az egyik legfontosabb alkalmazás.

A Hensel-lemma segítségével egy, általában még a szubrezultáns algoritmusnál is hatékonyabb eljárást adhatunk $f, g \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$ legnagyobb közös osztójának számolására. Mint a szubrezultáns algoritmusnál láttuk, feltehetjük, hogy f és g primitív polinomok; így persze ez az eljárás is rekurzív lesz. Az alapgondolat, hogy tekintünk egy alkalmas p páratlan prímet és $a_2, \ldots, a_n$ egészeket, az $S = \{x_2 - a_2, \ldots, x_n - a_n\}$ halmazra meghatározzuk a $\mathbb{Z}_p$ feletti $f_1 = f \bmod (S, p)$ és $g_1 = f \bmod (S, p)$ egyhatározatlanú polinomok h_1 legnagyobb közös osztóját, majd az $f_1 = h_1 \cdot (f_1/h_1)$ faktorizálást „felemelve" egy $f = h \cdot (f/h)$ faktorizálássá, ahol $h \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$, reméljük, hogy h a legnagyobb közös osztó. Mivel $h|f$, ha a felemelés sikeres, osztással csak azt kell ellenőriznünk, hogy $h|g$ teljesül-e? Természetesen az (S, p) párt úgy kell megválasztani, hogy f_1 illetve g_1 foka ugyanannyi legyen, mint f illetve g foka x_1-ben. Érdemes még a felemelés előtt legalább két (S, p) párt kipróbálni. Ha a h_1 foka valamelyik esetben nagyobb, mint a másikban, akkor azt a párt elvetjük, és helyette újat választunk. Ha h_1 foka nulla, akkor a legnagyobb közös osztó 1. Ha $\deg(h_1) = \deg(f_1) \leq \deg(g_1)$, akkor $h = f$ lesz a felemelés eredménye, jöhet az osztás. Ha az osztás nem maradék nélküli, akkor újabb (S, p) párral kell próbálkoznunk.

Ez az eljárás elakadhat, ha h_1 és f_1/h_1 nem relatív prímek, mert ekkor a felemelés nem lehetséges. Természetesen megcserélhetjük f és g szerepét, de ha g_1/h_1 és h_1 sem relatív prímek, akkor ez sem segít. (Új (S, p) pár választása sem segít, ha f és g legnagyobb közös osztója nem relatív prím sem f-hez, sem g-hez.) Találhatunk viszont olyan $k, m \in \mathbb{Z}$ egészeket, hogy $kf + mg \bmod (S, p)$ és h_1 hányadosa valamint h_1 relatív prímek. Ezek szorzatát felemelve $kf + mg$ egy szorzatfelbontásává, kapjuk h-t.

- 296/3 :

<

mány. Az $f \in R[x_1, x_2, \ldots, x_n]$ polinomot *szimmetrikus polinom*nak nevezzük, ha a határozatlanok tetszőleges permutációjára ugyanaz marad, azaz ha bármely $\sigma \in S_n$-re

$$f(x_{\sigma_1}, x_{\sigma_2}, \ldots, x_{\sigma_n}) = f(x_1, x_2, \ldots, x_n).$$

>

mány. Az $f \in R[x_1, x_2, \ldots, x_n]$ polinomot *szimmetrikus polinom*nak nevezzük, ha bármely két határozatlan megcserélésekor ugyanaz marad. (Ha ilyenkor a polinom az ellentettjére változik, akkor *alternáló polinom*nak nevezzük.)

- 302/11 :

<

ció egysége a *bit*, és ilyenkor $\log_r p_i$ helyett egyszerűen $\log p_i$-t írunk. Többnyire nem az

>

ció egysége a *bit*, és ilyenkor $\log_r p_i$ helyett egyszerűen $\log p_i$-t írunk; természetes logaritmus esetén az információ egysége a *nat*, tizes alapú logaritmus esetén pedig a *hartley*. Többnyire nem az

- 304/19 :

<

juk.)

>

juk.) Angol nyelvű írott szövegek információtartalmát shannonclaudeelwoodShannon, Claude Elwood (1916–2001)Shannon betűnként 1 bitre becsülte, német nyelvnél 1,3 bitre becsülik.

- 328/9 :

<

jellé, a kvantálási függvény inverzét kell alkalmaznunk.

>

jellé, a kvantálási függvény inverzét kell alkalmaznunk. A villamosmérnökök egyébként a jelteljesítmény és a zajteljesítmény hányadosának mérésére annak tizes alapú logaritmusát, a *Bel*t, vagy inkább a tizedrészét, a *decibel*t (*dB*) használják. Néhány jellemző jel/zaj viszony beszédátvitelnél: 10 dB még érthető; 20 dB használható telefonösszeköttetés; 40 dB rádió minőség; 60 dB igen jó zenei minőség.

- 348/13 :

<

nehéz; egyelőre ezeket főleg az űrtávközlésben használják.)

>

nehéz; egyelőre ezeket főleg az űrtávközlésben használják.) Analóg átvitel esetén a csatornakapacitás az $f \log_r(P/P_z)$ összefüggéssel becsülhető, ahol f a csatorna sávszélessége, P a (teljes, a zajt is tartalmazó) jelteljesítmény, P_z pedig a zajteljesítmény. Ha a csatornakapacitást bit/s-ban azaz *baud*ban akarjuk megkapni, akkor $r = 2$, és $\log(P/P_z)$ a dB-ben mért jel/zaj viszonynak kb. harmada. Például morzejelnél, ha egy pont hossza 20 ms, akkor a frekvencia 25 Hz. Kicsit nagyobb, 40 Hz sávszélességgel számolva, ha 10 dB a szükséges jel/zaj viszony, akkor a távírócsatorna kapacitása $\approx$ 133 bit/s, azaz baud. A telefonátvitel sávszélessége $\approx$ 3 kHz, a Hifi átvitelé $\approx$ 20 kHz csatornánként, a fekete-fehér televízióé 5 MHz, a szinesé 6,5 MHz. Fekete-fehér Tv-nél minimum 35 dB, szinesnél 45 dB jel/zaj viszony szükséges.

- 348/17 :

<

olyan nagy lenne a kódszavak száma. A tétel fontossága mégis felbecsülhetetlen, ugyanis

>

olyan nagy lenne a kódszavak száma. (A bizonyítás alapgondolata, hogy nagyon hosszú kódolandó- és kódszavak esetén elég sok olyan kódolás van, amelynek elég nagy a távolsága, így véletlenszerűen választva kódolást, találhatunk alkalmas kódot.) A tétel fontossága mégis felbecsülhetetlen, ugyanis

- 350/−14 :
  <
  kódszavak halmaza. Ezért a kódszavak halmazát akár a g, akár a H leképezés megadja.
  >
  kódszavak halmaza. Ezért a kódszavak halmazát akár a G, akár a H leképezés megadja.

- 350/−10 :
  <
  mátrixát, H mátrixa oszlopainak lineáris kombinációját kapjuk.
  >
  oszlopmátrixát, H mátrixa oszlopainak lineáris kombinációját kapjuk.

- 353/13 :
  <
  ris kódolást *polinomkódolás*nak nevezzük, $g(x)$ a kód *generátorpolinom*ja, a kódszvak a
  >
  ris kódolást *polinomkódolás*nak nevezzük, $g(x)$ a kód *generátorpolinom*ja, a kódszavak a

- 355/14 :
  <
  sák az ábécét ennek elemei, a K elemszámát jelölje q. Legyen Legyen $0 \neq \alpha \in K$ multip-
  >
  sák az ábécét ennek elemei, a K elemszámát jelölje q. Legyen $0 \neq \alpha \in K$ multip-

- 384/−17 :
  <
  ezek tartalma is egész szám. Van még egy *programmemória*, ennek rekeszei természetes
  >
  ezek tartalma is egész szám. Van még egy *programmemória*, ennek rekeszei természetes

- 386/18 :
  <
  (felüldefiniálható) *szimbolikus címke*szimbolikus címkéket használunk, azaz a címke egy
  >
  (felüldefiniálható) szimbolikus címkéket használunk, azaz a címke egy

- 399/−18 :
  <
  Többet fogunk belátni, két irányban is élesítve az állítást Először megmutatjuk, hogy
  >
  Többet fogunk belátni, két irányban is élesítve az állítást. Először megmutatjuk, hogy

- 411/−11 :
  <
nek bizonyítása azon múlik, hogy sikerült megmutatni, a „kielégíthetőség” problámája
  >
nek bizonyítása azon múlik, hogy sikerült megmutatni, a „kielégíthetőség” problémája

- 414/5 :
  <
: *Feynman Lectures on Computation.* Addison-Wesley, 1996.
  >
: *Feynman Lectures on Computation.* Addison-Wesley, 1996.

- 414/−10 :
  <
  >
Hainzmann J. – Varga S. – Zoltai J.: *Elektronikus áramkörök.* Nemzeti Tankönyvkiadó, Budapest, 2000.

- 414/5 :
  <
Hajós György: *A geometria alapjai.* Nemzeti Tankönyvkiadó, Budapest, 1999.
  >
Hajós Gy.: *A geometria alapjai.* Nemzeti Tankönyvkiadó, Budapest, 1999.

- 415/8 :
  <
  >
Kovács F. F.: *Az informatika VLSI áramkörei.* Pázmány Egyetem Elektronikus Kiadó, 2004.

- 416/−11 :
  <
Székelyhidi László: *Erdős Jenő válogatott előadásai.* Debreceni Egyetem Matematikai Intézet, 2004.
  >
Székelyhidi L.: *Erdős Jenő válogatott előadásai.* Debreceni Egyetem Matematikai Intézet, 2004.