Az algebrai számokról[1]

I. A háttér. Ismeretes a „Nagy Fermat[2] tétel", amely azt állítja, hogy ha $n > 2$ természetes szám, akkor az $x^n + y^n = z^n$ egyenletnek csak triviális megoldása van. Ez a „tétel" nem tétel, csak sejtés. Nagyon sok n-re már bizonyított, és állítólag[3] az is igaz, hogy bármely n esetén csak véges sok lényegesen különböző megoldás lehetséges. A tétel – vagy inkább sejtés – érdekessége abból adódik, hogy Fermat állítása szerint erre a tételre egy csodálatosan egyszerű bizonyítást talált. Ezt a bizonyítást sok kiváló matematikus próbálta már rekonstruálni. A sikertelenségek azt mutatják, hogy Fermat minden bizonnyal tévedett.

Valószínűleg az volt az út, amelyen Fermat elindult, amelyiken mi is el fogunk indulni.

Ha az előbb tekintett n természetes számot nem 2-nél nagyobbnak választjuk, akkor az $n = 1$ esetben egy triviális egyenlethez jutunk; míg $n = 2$ esetén az úgynevezett pitagoraszi számhármasokkal állunk szemben. Itt az $x^2+y^2 = z^2$ egyenlet egész megoldásait keressük. A megoldás szokásos menete a következő:

Elegendő arra az esetre szorítkozni, amikor az x, y, z, számok páronként relatív prímek. Ekkor a kiinduló egyenletet $x^2 = z^2-y^2 = (z+y)(z-y)$ alakban írva az egyértelmű prímtényezős felbontás alapján következtethetünk a megoldásra. (Nem pontosan így történik a vizsgálat, de lényegében igen.)

Mi történik akkor, ha $n > 2$, mi okozza az eltérést? Számokon nem tudjuk az anomáliát megmutatni, de polinomokon igen.

Tegyük fel, hogy az f, g, h, polinomokra teljesül az $f^n + g^n = h^n$ összefüggés, ahol $n > 3$. A bal oldali összeg a komplex számok körében szorzattá bontható:

$$f^n + g^n = (f + g) \cdot (f + \varepsilon g) \cdot (f + \varepsilon^2 g) \cdot \ldots$$

ahol ε egy megfelelő n-edik egységgyök.

Ha azt az esetet nézzük, amikor a szereplő polinomok páronként relatív prímek, akkor a jobb oldali szorzat csak úgy lehet teljes n-edik hatvány, ha minden egyes tényező az. Mivel a jobb oldalon legalább három tényező szerepel, ezért a következő egyenletrendszerhez jutunk:

$$f + g = u^n$$
$$f + \varepsilon g = v^n$$
$$f + \varepsilon^2 g = w^n,$$

ahol u, v, w polinomok. A fenti egyenletek bal oldalán az f és g polinomok kiküszöbölhetők, és ezáltal egy $u_1^n+v_1^n = w_1^n$ alakú egyenlethez jutunk (itt u_1 az u-nak, v_1 a v-nek és w_1 a w-nek számszorosa). Ezek a polinomok az eredetieknél alacsonyabb fokúak; ami ellentmondáshoz vezet, ha feltesszük, hogy a lehető legalacsonyabbfokú megoldást választjuk.

Itt egy csomó kellemetlen dolog lép fel. Mindenesetre sokkal bővebb számkörben kell dolgoznunk és fel kell használnunk az egyértelmű „prímtényezős" felbontást (illetve amit ez a bővebb számkörben jelent).

Ezt az utat fogjuk hát végigjárni (azaz dehogy végigjárni, csak elkezdeni): bővebb számköröket vizsgálunk, és megnézzük igaz-e bennük az egyértelmű prímtényezős felbontás.

II. Az egyértelmű faktorizáció. Ahhoz, hogy egy számkörben „ugyanolyan" aritmetikát tudjunk használni, mint az egész számok körében, arra van szükség, hogy e számkörben elvégezhessük a szükséges műveleteket.

Definíció: *számok egy (nem üres)* **R** *halmazát* **számgyűrű***nek nevezzük, ha bármely két* **R***-beli számmal együtt azok összege, különbsége és szorzata is* **R***-beli szám. Ha egy* **K** *számgyűrű bármely két elemének hányadosa is* **K***-beli, akkor* **számtest***ről beszélünk.* (0-val természetesen nem lehet osztani.)

Feladatunk tehát egy számgyűrűben vizsgálni az egyértelmű prímtényezős felbontás lehetőségét. Ez azonban nem tárgyalható olyan magától értetődő módon, mint a természetes számok körében, és ezért szükség van arra, hogy néhány fogalmat pontosan definiáljunk.

Definíció: *Azt mondjuk, hogy az* **R***-beli a elem* **osztója** *az* **R***-beli b elemnek (illetve b* **többszöröse** *a-nak), ha létezik olyan* **R***-beli c elem, amelyre $b = a \cdot c$. (Az oszthatóság rendelkezik az egész számok körében már jól ismert tulajdonságokkal.)*

Egy **R** *számgyűrű valamely ε elemét* **egység***nek nevezzük, ha minden* **R***-beli elemnek osztója. – Ezzel ekvivalens az a definíció, hogy ε osztója 1-nek. (Az egész számok körében két egység van, $a\ +1$ és $a\ -1$.)*

Az **R** *számgyűrű egy p egységtől különböző elemét felbonthatatlannak (irreducibilisnek) nevezzük, ha $p = q \cdot t$ esetén ($q, t \in$ **R**) q és t valamelyike biztosan egység.*

Az **R** *számgyűrű p és q elemeit* **asszociáltak***nak nevezzük, ha mindegyik osztója a másiknak. – Ezzel ekvivalens az a definíció, hogy mindegyik a másik egységszerese.*

---

[1] Ennek a cikknek a megértéséhez szükségesek: A komplex számokra vonatkozó elemi ismeretek, az egyértelmű prímtényezős felbontás az egész számok körében, az egyismeretlenes magasabbfokú egyenletek egész és racionális gyökeinek a meghatározási módszere.

[2] Pierre FERMAT francia matematikus (1601–1665)

[3] „állítólag" az azt jelenti, hogy akik a bizonyítást átnézték és megértették, eddig még nem találtak benne hibát. Gondoljuk meg, hogy egy olyan bizonyítás megértése és ellenőrzése, amely több száz vagy ezer oldalra rúg, nem kis feladat!

Észrevehetjük, hogy a prímszám elnevezés helyett a felbonthatatlan szót használtuk. A felbonthatatlanság ugyanis a prímszámok egy igen jellemző tulajdonsága. Emellett van egy másik fontos tulajdonság, amely végső soron lehetővé teszi az egyértelmű faktorizáció (lásd a definíciót) bizonyítását.

Definíció: *Az* **R** *számgyűrű egy p eleme rendelekezik a* **prímtulajdonság***gal, ha bármely* **R***-beli a és b elemekre p csak akkor osztója az ab szorzatnak, ha e szorzat valamelyik tényezőjének is osztója.*

Könnyen belátható , hogy a 0 is és minden egység is prímtulajdonságú. Azt sem nehéz megmutatni, hogy ezenkívül csak a felbonthatatlan elemek rendelkezhetnek a prímtulajdonsággal. Az is igaz, hogy ha egy **R** számgyűrűben érvényes az egyértelmű faktorizáció, akkor a felbonthatatlan elemek mindegyike prímtulajdonságú.

Most még azt is definiáljuk, hogy mit értünk **egyértelmű faktorizáció**n.

Definíció: *Az* **R***-beli szám egy faktorizációján egy $a = p_1 \cdot \ldots \cdot p_r$ felbontást értünk, ahol $p_1, \ldots, p_r$* **R***-beli irreducibilis elemek.*

Az a elem egy $a = q_1 \cdot \ldots \cdot q_s$ faktorizációját az előbbivel ekvivalensnek nevezzük, ha $s = r$, és ez utóbbiban a tényezőket úgy tudjuk sorba rakni, hogy a kapott és az előbbi felbontásban az ugyanannyiadik helyen álló tényezők egymásnak asszociáltjai. (Pl. $6 = 2 \cdot 3$ és $6 = (-3) \cdot (-2)$ esetén ez utóbbi szorzatban felcseréljük a tényezőket.)

Az **R** *gyűrűben érvényes az egyértelmű faktorizáció, ha bármely 0-tól és egységektől különböző elemének van faktorizációja és bármely két faktorizációja ekvivalens.*

III. Számgyűrűk egyértelmű faktorizáció nélkül. Tudjuk, hogy az egész számok gyűrűjében érvényes az egyértelmű faktorizáció. Először Gauss[4] mutatott rá arra, hogy ez a tétel bizonyításra szorul, és ő maga több bizonyítást is adott rá. Ezzel a tétellel – legalább is az egész számok körében – az a probléma, hogy nem látjuk, hogy „miért ne volna igaz". A legismertebb és legegyszerűbb ellenpélda erre a páros számok gyűrűje. Itt ugyanis a 2, 6, 10 és 30 mindegyike felbonthatatlan (nem írhatóak fel páros számok szorzataként!), és így a $60 = 2 \cdot 30 = 6 \cdot 10$ felbontások faktorizációk, de nem ekvivalensek. Sajnos azonban ez a példa bizonyos értelemben csalás. Az egyértelmű faktorizációból ugyanis valamiképpen következik az, hogy a számgyűrűben benne kell lennie az 1-nek. Ha ilyen példát is akarunk találni, akkor már nehezebb dolgunk van. Ennek előkészületeként először egy olyan gyűrűt veszünk, amelyikben érvényes az egyértelmű faktorizáció.

Jelölje **G** az $a + bi$ alakú – úgynevezett *Gauss egészek* – gyűrűjét, ahol $a, b \in \mathbf{Z}$ (vagyis egész számok) és $i = \sqrt{-1}$. Ebben a gyűrűben elvégezhető a maradékos osztás. Persze itt a maradék nem csökkenhet, hanem a maradék „normá"-ja csökken. Az $\alpha = a + bi$ normája a $N(\alpha) = a^2 + b^2$.

Ha α-t a pozitív n egész számmal akarjuk maradékosan osztani, akkor elosztjuk először a-t és b-t úgy, hogy a maradék negatív is lehet, de ne legyen nagyobb mint $n/2$; $a = c \cdot n + p$ és $b = d \cdot n + q$, ahol $|p|, |q| \leq n/2$. Ekkor a $\gamma = c + di$ és $\varrho = p + qi$ Gauss egészekre $\alpha = \gamma \cdot n + \varrho$ és $N(\varrho) = p^2 + q^2 \leq n^2/4 + n^2/4 < n^2 = N(n)$. Ha α-t a 0-tól különböző $u + vi = \beta$-val akarjuk maradékosan osztani, akkor tekintjük a $\overline{\beta} = u - vi$ Gauss egészet, amelyre $\beta \cdot \overline{\beta} = N(\beta)$, és $\alpha \cdot \overline{\beta}$-t osztjuk el $N(\beta)$-val: $\alpha \cdot \overline{\beta} = \gamma \cdot N(\beta) + \varrho_1$. Könnyen belátható, hogy ϱ_1 felírható $\varrho \cdot \overline{\beta}$ alakban, ahol $N(\varrho) < N(\beta)$; és fennáll az $\alpha = \gamma \cdot \beta + \varrho$ összefüggés.

Tekintsük most az $a + 2bi$ alakú Gauss egészeket, ahol $a, b \in \mathbf{Z}$. Ezek között ott van az 1, és mégis a $4 = 2 \cdot 2 = (2i) \cdot (-2i)$ felbontások nem ekvivalens faktorizációk. Ugyanis a jobb oldali $2i$ a bal oldalon fellépő egyik tényezővel sem asszociált, mert hányadosuk i nem eleme a szóban forgó gyűrűnek. No persze ebből mindenki láthatja, hogy ismét csaltunk, mert „kidobtunk" egy számot, amelyiknek „bent kellett volna lennie".

Nézzünk most egy másik számgyűrűt, amelyikben szintén nem érvényes az egyértelmű faktorizáció. Előre elárulhatom, hogy itt is csalásról van szó; itt viszont nem olyan egyszerű észrevenni ezt.

Tekintsük az $a + b\sqrt{-3}$ alakú számokat, ahol $a, b \in \mathbf{Z}$. Jelöljük ezt a gyűrűt $\mathbf{Z}[\sqrt{-3}]$-mal (ez azt jelenti, hogy ez a legkisebb olyan gyűrű, amely az egészeken kívül a $\sqrt{-3}$-t is tartalmazza). Az $\alpha = a + b\sqrt{-3}$ szám konjugáltján az $\overline{\alpha} = a - b\sqrt{-3}$ számot értjük, normáján pedig az $N(\alpha) = \alpha \cdot \overline{\alpha} = a^2 + 3b^2$ számot. Könnyen beláthatók, hogy ha $\alpha \neq 0$, akkor normája sem 0, szorzat normája megegyezik a tényezők normájának a szorzatával, és ha α osztója β-nak, akkor$N(\alpha)$ is osztója $N(\beta)$-nak (de nem fordítva!). Ez azért hasznos, mert az oszthatóság csak úgy állhat fenn, ha a normákra vonatkozó oszthatóság teljesül. Mivel a normák természetes számok, ezért eleve csak nagyon kevés lehetőséget kell megvizsgálni, ha egy szám osztóit keressük. Így megállapíthatjuk, hogy a fenti gyűrűben 2, $1 + \sqrt{-3}$ és $1 - \sqrt{-3}$ mind felbonthatatlanok; és $2 \cdot 2 = (1 + \sqrt{-3}) \cdot (1 - \sqrt{-3})$ következtében itt sem érvényes az egyértelmű faktorizáció. Pedig egyáltalában nem látható, hogy valamit is kihagytunk volna!

A „kihagyott" számok megkereséséhez az az eljárás adja meg a kulcsot, amelynek a segítségével megállapíthatjuk, hogy egy egész együtthatós polinomnak mely egész vagy racionális számok lehetnek a gyökei. Itt ugyanis semmi más nincs felhasználva, csak az, hogy az egész számok körében érvényes az egyértelmű faktorizáció.

Mindenekelőtt a szóban forgó **R** számgyűrűhöz egy olyan számtestet is kell találni, amelyhez hasonló kapcsolat fűzi, mint az egész számokat a racionálisakhoz; amelyek éppen az egész számok hányadosai.

Definíció: *Az* **R** *számgyűrű* **hányadostest***ének nevezzük azt a számtestet, amely az* **R***-beli számok hányadosaiból áll.* [5]

[4] Carl Friedrich GAUSS német matematikus (1777–1855).

[5] Azt, hogy ez valóban számtest, mindenki könnyen bebizonyíthatja magának.

Szükségünk van bizonyos speciális polinomokra, amelyeknek külön nevük is van: Az **R**-beli együtthatós polinomot **normált**nak nevezzük, ha legmagasabbfokú tagjának az együtthatója 1.

Tétel: *Tegyük fel, hogy az* **R** *számgyűrűben érvényes az egyértelmű faktorizáció, és legyen* **K** *az* **R** *hányadosteste. Ekkor minden olyan* **K***-beli szám, amely egy* **R***-beli normált polinomnak a gyöke, maga is* **R***-ben van.*

Bizonyítás: Legyen $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ a szóban forgó polinom; és legyen p/q ennek gyöke. $p, q \in \mathbf{R}$, és feltehető, hogy ezek relatív prímek. Behelyettesítve és q^n-nel végigszorozva a

$$p^n + a_{n-1}p^{n-1}q + \ldots + a_1pq^{n-1} + a_0q^n = 0$$

egyenlőséghez jutunk. Itt az első tag után mindegyik tag osztható q-val, ezért az első tag is osztható vele. Legyen t a q-nak egy felbonthatatlan tényezője, ekkor t is osztója az első tagnak, p^n-nek. Mivel t prímtulajdonságú, ezért p-nek is osztója, amiből az következik, hogy t közös osztója p-nek és q-nak. Mivel e két szám relatív prím, ezért ilyen t nem létezhet, vagyis q csak egység lehet. Mivel egy egység minden **R**-beli számnak osztója, ezért valóban $p/q \in \mathbf{R}$. □

Tekintsük most az $x^2 - x + 1$ polinomot, amely nyilván normált és együtthatói a $\mathbf{Z}[\sqrt{-3}]$ (sőt a **Z**) számgyűrűből valóak. E polinomnak gyöke az $\dfrac{1+\sqrt{-3}}{2}$ szám, amely eleme a $\mathbf{Z}[\sqrt{-3}]$ számgyűrű hányadostestének, de nem eleme a $\mathbf{Z}[\sqrt{-3}]$ számgyűrűnek. Éppen ezért ebben a számgyűrűben nem is lehet érvényes az egyértelmű faktorizáció. Ha viszont a $\mathbf{Z}\left[\dfrac{1+\sqrt{-3}}{2}\right]$ számgyűrűt nézzük, amelynek elemei az $a+b\cdot\dfrac{1+\sqrt{-3}}{2}$ alakú számok (ahol $a, b \in \mathbf{Z}$), akkor már bizonyítható, hogy ebben a számgyűrűben igaz az egyértelmű faktorizáció. Mielőtt a következő ellenpéldára rátérnénk, megfogalmazzuk, hogy milyen számgyűrűkben célszerű az egyértelmű faktorizációt vizsgálni.

IV. Algebrai számok és algebrai egészek. A fenti példákban mindig olyan számokat vizsgáltunk, amelyek egy egész együtthatós – nem azonosan 0 – polinom gyökei voltak. Az ilyen számokat **algebrai számok**nak nevezzük. Azoknak a számgyűrűknek az elemei, amelyekben a fenti tétel igaz „lehet", mind egy normált egész együtthatós polinom gyökei.

Egy normált egészegyütthatós polinom gyökeit **algebrai egészek**nek nevezzük.

Bizonyítható a következő

Tétel: *az összes algebrai számok egy számtestet, az összes algebrai egészek egy számgyűrűt alkotnak.*

A fenti példákban csak „nagyon kicsi" számgyűrűket néztünk. Azt, hogy nagyon kicsi, pontosan meg is fogalmazzuk:

Létezik véges sok olyan algebrai szám, hogy a szereplő **R** számgyűrű a legkisebb olyan számgyűrű, amelyik **Z**-t és az adott véges sok algebrai számot tartalmazza. Az ilyen számgyűrűket a **Z véges bővítése**inek nevezzük.

A **Z** egy véges **R** bővítését **integrálisan zárt**nak mondjuk, ha minden eleme algebrai egész és tartalmazza a hányadostestében levő összes algebrai egészet.[6] Mint láttuk, a **Z** egy véges algebrai bővítésében csak akkor lehet igaz az egyértelmű faktorizáció, ha az integrálisan zárt.[7]

Nézzük most az $\mathbf{R} = \mathbf{Z}[\sqrt{-5}]$ gyűrűt, amelynek elemei tehát az $a + b\sqrt{-5}$ alakú számok ($a, b \in \mathbf{Z}$). Be lehet bizonyítani, hogy ez a gyűrű integrálisan zárt. Itt is definiálható a norma, amelynek segítségével könnyen megmutatható, hogy $2,\ 3,\ 1+\sqrt{-5},\ 1-\sqrt{-5}$ mind felbonthatatlanok. Így a $2 \cdot 3 = (1+\sqrt{-5}) \cdot (1-\sqrt{-5})$ egyenlőség azt mutatja, hogy itt „kijavíthatatlanul" nem igaz az egyértelmű faktorizáció.

V. Egy kisérlet az egyértelmű faktorizáció pótlására. Az egyértelmű faktorizációnál az egyértelműség bizonyítása azon múlik, hogy minden felbonthatatlan elem rendelkezik a prímtulajdonsággal. A maradékos osztás, vagy annak fent tárgyalt változatai azt biztosítják, hogy a legnagyobb közös osztó[8] létezik, és speciális alakban adható meg. Mint azonnal látni fogjuk, ez biztosítja, hogy minden felbonthatatlan elem rendelkezik a prímtulajdonsággal.

Tétel: *Ha az* **R** *számgyűrű bármely adott α és β eleméhez léteznek e számgyűrűben olyan ξ és η elemek, amelyekre $\delta = \alpha\xi + \beta\eta$ mindkét adott elemnek osztója, akkor* **R***-ben minden irreducibilis elem prímtulajdonságú.*[9]

Bizonyítás: Tegyük fel, hogy **R** egy π felbonthatatlan eleme osztója az **R**-beli α és β elemek szorzatának. Feltétel szerint az α és π elemeknek van egy $\delta = \alpha\xi + \pi\eta$ alakú közös osztója. Mivel π felbonthatatlan, ezért δ vagy asszociált hozzá, vagy egy egység (miért?). Az első esetben az oszthatóság elemi tulajdonságaiból azonnal következik, hogy $\pi \mid \alpha$. A második esetben alkalmas egységgel szorozva elérhető, hogy δ helyett 1 álljon, amikor is a felírt egyenlőséget β-val szorozva a $\beta = (\alpha\beta)\xi + \pi(\eta\beta)$ egyenlőséghez jutunk. A feltételezett oszthatóság miatt a jobb oldali két tag mindegyike osztható π-vel, és ezért $\pi \mid \beta$. □

Az előző tételben adott felírás alapján a δ szám **R**-beli többszörösei

$\delta\zeta = \alpha(\xi\zeta) + \beta(\eta\zeta)$ alakúak, ahol ζ az **R** elemein fut végig. A δ számot – asszociáltaktól eltekintve – egyértelműen meghatározzák a többszörösei. Az asszociáltság viszont nem okoz gondot, sőt az oszthatóságnál az asszociáltak

[6] A definícióban nem követelik meg azt, hogy minden elem algebrai egész legyen, mi csak azért tesszük hozzá, hogy ne kelljen erre egy külön elnevezést használni.

[7] Valójában nem egészen ezt láttuk, de amit beláttunk, az érezhetően közel áll ehhez a megfogalmazáshoz; viszont a bizonyítás elég hosszadalmas volna.

[8] Nem mindig beszélhetünk arról, hogy valamelyik osztó a „legnagyobb". Általában ezen egy olyan közös osztót értünk, amely minden közös osztónak többszöröse.

[9] Belátható, hogy δ az adott két elem bármely közös osztójának többszöröse.

„egyenjogúak". Éppen ezért a δ számot meghatározza az $\alpha\xi + \beta\eta$ alakú elemek halmaza, ahol ξ és η az $\mathbf{R}$ elemein fut végig.

Teljesen hasonlóan járhatunk el akkor, ha több szám legnagyobb közös osztóját akarjuk leírni. Ha δ az $\alpha_1, \ldots, \alpha_r \in \mathbf{R}$ számok legnagyobb közös osztója, akkor δ többszörösei éppen az $\alpha_1\xi_1 + \ldots + \alpha_r\xi_r$ alakú számok halmazának elemei, ahol $\xi_1, \ldots, \xi_r$ az $\mathbf{R}$ elemein futnak végig.

Ez a kép vezette Kummert[10] ahhoz a gondolathoz, hogy „hiányzó" legnagyobb közös osztó esetén a fenti halmazokat vizsgálja. Az $\alpha_1\xi_1 + \ldots + \alpha_r\xi_r$ alakú számok halmaza, ahol $\xi_1, \ldots, \xi_r$ az $\mathbf{R}$ elemein futnak végig, azzal a jellemző tulajdonsággal rendelkezik, hogy e halmaz bármely két elemének a különbsége is e halmazba esik, és ha egy halmazbeli elemet egy tetszőleges $\mathbf{R}$-beli elemmel szorzunk, akkor ismét a tekintett halmaz egy elemét kapjuk.

Definíció: *Az $\mathbf{R}$ gyűrű egy $\mathbf{A}$ – nem üres – részhalmazát* **ideál***nak nevezzük, ha*
(1) $\alpha, \beta \in \mathbf{A}$ *esetén* $\alpha - \beta \in \mathbf{A}$, *és*
(2) $\alpha \in \mathbf{A}$ *és* $\xi \in \mathbf{R}$ *esetén* $\alpha\xi \in \mathbf{A}$.

Ha $\mathbf{A}$ a legkisebb olyan ideál, amely az $\alpha_1, \ldots, \alpha_r$ számokat tartalmazza, akkor azt mondjuk, hogy $\mathbf{A}$ az $\alpha_1, \ldots, \alpha_r$ számok generálta ideál, és ebben az esetben az $\mathbf{A} = (\alpha_1, \ldots, \alpha_r)$ jelölést használjuk.

Véges sok szám generálta ideál neve **végesen generált ideál,** *az egy elem generálta ideált pedig* **főideál***nak nevezzük.*

Könnyen belátható, hogy az $(\alpha_1, \ldots, \alpha_r)$ ideál elemei pontosan az $\alpha_1\xi_1 + \ldots + \alpha_r\xi_r$ alakú számok.

Az ideál elnevezés onnét származik, hogy a „nemlétező" legnagyobb közös osztókat próbálták helyettesíteni e halmazokkal. Így egy „nemlétező" „ideális számot" kaptak; és ebből maradt meg az ideál elnevezés.

Hasonló dolog tapasztalható a projektív geometriában, ahol a „végtelen távoli pont" helyett az ideális pont elnevezés használatos. Ez valójában egy irány, amely a „végtelen távoli pontra mutat". Ebben is fennáll az analógia, az ideál arra a számra „mutat", amelyik generálja őt; e szám nincs benne, de ha létezne ilyen szám, akkor az ideál éppen ennek a többszöröseiből állna.

Ha egy olyan számgyűrűt nézünk, amelyben nem érvényes az egyértelmű faktorizáció (de $\mathbf{Z}$-nek véges bővítése), akkor mindig található benne olyan ideál, amelyik nem főideál. Egy ilyennek a megadása ekvivalens egy olyan felbontással, ahol az egyértelműség nem teljesül. Így például $\mathbf{Z}[\sqrt{-5}]$-ben a $(2,\ 1+\sqrt{-5})$ ideál nem főideál.

Ahhoz, hogy ez a fogalom egy jó általánosítás, azt kellene tudnunk, hogy az „ideális számokra" vagyis az ideálokra érvényes-e az egyértelmű faktorizáció. Persze ehhez meg szükség van az ideálok szorzatára, de ezt úgy kell definiálni, hogy ha az ideálok főideálok, akkor a szorzat pontosan a generátorelemek szorzata által generált főideált adja $((\alpha)\cdot(\beta) = (\alpha\beta)$ legyen); vagyis a szorzat a számok szorzatát általánosítsa. A kézenfekvő az volna, ha az $\mathbf{A} \cdot \mathbf{B}$ ideálszorzat az $\alpha\beta$ alakú elemek halmaza lenne, de sajnos ez általában nem egy ideál.

Definíció: *Az $\mathbf{A}$ és $\mathbf{B}$ ideálok $\mathbf{A} \cdot \mathbf{B}$ szorzatán a $\sum \alpha_i\beta_i$ alakú véges összegek halmazát értjük, ahol az α_i és β_i egymástól függetlenül megfelelően az $\mathbf{A}$* és a *$\mathbf{B}$ ideál elemein futnak végig.*

Könnyen be lehet látni, hogy ez a definíció a fent megfogalmazott mindkét követelménynek eleget tesz.

Az $\mathbf{R}$ számgyűrűben van két speciális ideál, a 0 generálta $\mathbf{O}$ ideál (amelynek egyetlen eleme a 0) és az 1 generálta ideál, amely maga az $\mathbf{R}$ számgyűrű. Ezekre bármely $\mathbf{A}$ ideál esetén érvényes a $\mathbf{O} \cdot \mathbf{A} = \mathbf{O}$ és $\mathbf{R} \cdot \mathbf{A} = \mathbf{A}$ összefüggés. Ezt a két ideált **triviális ideálok**nak is szokták nevezni, az összes többi ideál neve **valódi ideál.**

Ha az $\mathbf{A}$ ideál felbontható a $\mathbf{B}$ és $\mathbf{C}$ valódi ideálok szorzatára: $\mathbf{A} = \mathbf{B} \cdot \mathbf{C}$, akkor $\mathbf{A}$-t **felbontható ideál**nak nevezzük. A többi valódi ideál neve **felbonthatatlan ideál**.

Nos, ha már ennyire elbonyolítottuk a számfogalmat, akkor jó volna tudni, hogy ezekre érvényes-e az egyértelmű faktorizáció. A definícióhoz két dolog szükséges:

1. Ha az $\mathbf{R}$ számgyűrű minden $\mathbf{A}$ valódi ideálja felírható felbonthatatlan ideálok $\mathbf{A} = \mathbf{P}_1 \ \ldots \ \mathbf{P}_r$ szorzataként, akkor azt mondjuk, hogy $\mathbf{R}$-ben **érvényes a faktorizáció.**

2. Ha $\mathbf{R}$-ben érvényes a faktorizáció, és bármely $\mathbf{A}$ valódi ideált kétféleképpen felírva felbonthatatlan ideálok szorzatára, csupán a tényezők sorrendje különbözik, akkor azt mondjuk, hogy $\mathbf{R}$-ben **érvényes az egyértelmű faktorizáció.**

Tétel: *Ha $\mathbf{R}$ a $\mathbf{Z}$ véges bővítése és integrálisan zárt, akkor $\mathbf{R}$ ideáljaira érvényes az egyértelmű faktorizáció.*

Ennek a tételnek a bizonyítása már egyáltalában nem könnyű, és sok előismeretet is igényel.

Gondoljuk most meg, hogy mit jelent ez az eredeti egyértelmű faktorizációra nézve. Mivel egy-egy számot éppen egy főideál helyettesíthet, ezért pontosan azokban a számgyűrűkben igaz az egyértelmű faktorizáció, amelyekben minden ideál főideál. Eleve azonban még azt sem tudjuk, hogy az ideálokat véges sok szám generálja-e.

Nos, a következőket nem túlságosan bonyolult algebrai eszközökkel be lehet látni. A szóban forgó $\mathbf{R}$ gyűrűk $\mathbf{K}$ hányadostestében mindig található egy olyan α algebrai szám, hogy $\mathbf{K}$ a legkisebb olyan test, amely α-t tartalmazza. Ehhez az α számhoz mindig található olyan minimális fokú egész együtthatós polinom, amelynek α gyöke. E polinom foka egyértelműen meghatározott; ha ez n, az $\mathbf{R}$ gyűrű minden ideálja generálható n elemmel.

Ha még mélyebbre megyünk, akkor azt is kimutathatjuk, hogy az n-től és $\mathbf{R}$-től függetlenül minden ideál generálható két elemmel.

[10] Ernst Eduard KUMMER német matematikus 1810-1893.

Tessék meggondolni, milyen kevés hiányzik ahhoz, hogy érvényes legyen az egyértelmű faktorizáció! Persze, ezt a helyzetet úgy is értelmezhetjük, hogy „a végtelen sokkal közelebb van a 2-höz, mint 2 az 1-hez". Az értelmezés egyéni érzések kérdése.

VI. Megtaláljuk a hiányzó legnagyobb közös osztót. Vajon hány olyan ideál van az $\mathbf{R}$ számgyűrűben, amelyik nem főideál? Így ez a kérdés rosszul van fogalmazva. Hiszen, ha (α, β) nem főideál, akkor $\mathbf{R}$ tetszőleges γ elemét véve $(\alpha\gamma, \beta\gamma)$ sem főideál és viszont. Az ilyen kapcsolatban álló ideálokat tehát együtt érdemes vizsgálni.

Az $\mathbf{R}$ számgyűrű (α_1, β_1) és (α_2, β_2) ideáljait egy **ideálosztályba** soroljuk, ha léteznek olyan $\gamma_1, \gamma_2 \in \mathbf{R}$ számok, amelyekre $(\alpha_1\gamma_1, \beta_1\gamma_1) = (\alpha_2\gamma_2, \beta_2\gamma_2)$.

A hiányzó legnagyobb közös osztók számát tehát az ideálosztályok $\mathbf{h}$ száma adja meg. Nos, az erre vonatkozó mély és igen szép eredmény szerint $\mathbf{h}$ mindig véges.

Jelöljük az $\mathbf{A}$-t tartalmazó ideálosztályt $[\mathbf{A}]$-val. Könnyen belátható, hogy az ideálok szorzata átvihető az ideálosztályokra az $[\mathbf{A}] \cdot [\mathbf{B}] = [\mathbf{A} \cdot \mathbf{B}]$ definícióval. Az is világos, hogy a főideálok mind egyetlen osztályba tartoznak (és ebben az osztályban csak főideál lehet). Ez az osztály az $[(1)] = [\mathbf{R}]$ osztály. Ugyancsak nyilvánvaló az $[\mathbf{R}] \cdot [\mathbf{A}] = [\mathbf{A}]$ összefüggés is.

$\mathbf{h}$ végességének a bizonyításánál fontos szerepet játszanak az úgynevezett **törtideálok**. Ezek $\alpha_1\xi_1 + \ldots + \alpha_r\xi_r$ alakú számhalmazok, ahol a $\xi_1, \ldots, \xi_r$ számok ugyan az $\mathbf{R}$ gyűrűből valóak, de az $\alpha_1, \ldots, \alpha_r$ számok nem feltétlenül a $\mathbf{R}$ gyűrűből, hanem ennek a $\mathbf{K}$ hányadostestéből. Az ideálosztályokat a törtideálokra is értelmezhetjük, és meg lehet mutatni, hogy az ideálosztályok száma itt is ugyanaz a $\mathbf{h}$ szám, mint az $\mathbf{R}$ gyűrűnél. Amit itt nyerünk, az az, hogy a törtideálokra be lehet vezetni az osztást, és az ideálosztályok erre, valamint a szorzásra nézve úgynevezett csoportot alkotnak. A csoport definíciója most nem lényeges, csak az a tétel, hogy egy véges csoportban minden elemnek van olyan hatványa, amelyik az egységelem. Más szóval minden ideál $\mathbf{h}$-adik hatványa egy főideál.

Nézzük tehát az (α, β) ideál $\mathbf{h}$-adik hatványát. Ez egy (δ) főideál. Ebből arra következtethetünk, hogy az (α, β) ideál megegyezik a $(\sqrt[h]{\delta})$ főideállal. Persze $\sqrt[h]{\delta}$ általában nincs benne az $\mathbf{R}$ számgyűrűben. Mégis $\sqrt[h]{\delta}$-nak az $\mathbf{R}$-be eső többszörösei éppen az (α, β) ideál elemei. Itt „csak" az a probléma, hogy mit értünk a $\sqrt[h]{\delta}$ többszörösein. Erre is egészen egyszerű a válasz: algebrai egész-szereseket.

Nézzük meg hát végezetül a $\mathbf{Z}[\sqrt{-5}]$ számgyűrűbeli $(2,\ 1 + \sqrt{-5})$ ideált. Higyjük el, hogy ebben a gyűrűben az ideálosztályok száma $\mathbf{h} = 2$. Ezért a fenti ideál négyzetét kell nézni, amelyről kimutatható (egyáltalán nem könnyen), hogy a 2 generálta főideál. Ez azt jelenti, hogy a fenti két szám legnagyobb közös osztója a $\sqrt{2}$, ami persze nincs a vizsgált gyűrűben. Tegyük most fel, hogy δ osztója az ideál mindkét generátorának. Ekkor persze osztója a két generátorelem $1-\sqrt{-5} = 2-(1+\sqrt{-5})$ különbségének is. Ezért δ^2 osztója mind $2 \cdot 2 = 4$-nek, mind $(1+\sqrt{-5})(1-\sqrt{-5}) = 6$-nak. Ekkor viszont osztója ezek különbségének, ami 2. Ez azt jelenti, hogy ha δ osztója 2-nek is és $(1 + \sqrt{-5})$-nek is (az összes algebrai egész gyűrűjében), akkor δ^2 osztója 2-nek, azaz δ osztója $\sqrt{2}$-nek. $\sqrt{2}$ persze algebrai egész, mert az $x^2 - 2$ polinom gyöke. Ahhoz, hogy $\sqrt{2}$ valóban a legnagyobb közös osztó, azt kell már csak belátni, hogy a két adott szám mindegyikének osztója. $2/\sqrt{2} = \sqrt{2}$ miatt 2-nek osztója. Nézzük az $\alpha = (1 + \sqrt{-5})/\sqrt{2}$ számot. Mivel $\alpha^2 = -2 + \sqrt{-5}$, ezért α gyöke az $(x^2 + 2)^2 + 5$ egész együtthatós normált polinomnak, így valóban algebrai egész.

Ez az eljárás azt sugallja, hogy az összes algebrai egész gyűrűjében érvényes az egyértelmű faktorizáció. Legalábbis, mintha a fenti eljárás biztosítaná az egyértelműséget. Nos, ez a második állítás lényegében igaz is. Az viszont már nem igaz, hogy van faktorizáció. Ennek az az oka, hogy nincs is felbonthatatlan elem. Ha ugyanis α tetszőleges (nem-egység) algebrai egész, akkor azonnal látható, hogy a négyzetgyöke is (nem-egység) algebrai egész, és az $\alpha = \sqrt{\alpha} \cdot \sqrt{\alpha}$ felírás mutatja, hogy α nem felbonthatatlan.

Annyit azért be lehet bizonyítani, hogy ha egy algebrai egésznek van két szorzat előállítása, akkor a tényezőket úgy lehet tovább bontani, hogy a végén két, lényegében megegyező előállítást nyerjünk.

Fried Ervin

Megjegyzés. Bizonyára sokan tudnak a legújabb fejleményről: a világsajtó hírül adta, hogy Andrew Wiles, a cambridge-i Isaac Newton Institute 40 éves matematikusa bebizonyította a 300 éves Fermat-sejtést.

Számítógép nem kellett a bizonyításhoz, viszont olyan matematikai eszközöket használ, mint: moduláris formulák, elliptikus görbék, Galois-elmélet. A szerzőről és a korábbi bizonyítási kísérletekről következő számunkban olvashatnak. Egy bizonyos: Wiles nem követhette Fermat eredeti gondolatmenetét, mert 1000 oldalas bizonyítása nem férne el egyetlen könyv margóján sem, mint Fermat állítólagos „csodálatosan egyszerű" bizonyítása.

Szerk.