4. Az Algebrai Számelmélet Elemei

4.0. Bevezetés.

Az algebrai számelmélet legegyszerűbb kérdései az ún. aégebrai számtestek egészei gyűrűjének aritmetikai tulajdonságainak vizsgálata. Ezek legegyszerűbb példái a Gauss- és az Euler-egészek. Miután összegeztünk néhány szükséges absztrakt algebrai fogalmat és összefüggést, először ezekkel foglalkozunk.

Definíció. Legyenek M, L testek. Ha $L \subseteq M$, akkor azt mondjuk, hogy M az L *test bővítése.* Jelölése: $M|L$.

Megjegyzés. Egyszerűen látható, hogy ez esetben M vektortér az L test fölött.

Definíció. Ha $M|L$, akkor az M vektortér dimenzióját a *testbővítés fokának* nevezzük, jelölése: $\deg(M\colon L) = \dim_L M$.

Példa. $\deg(\mathbb{C}\colon \mathbb{R}) = 2$, $\deg(\mathbb{R}\colon \mathbb{Q}) = \infty$.

4.0.1. Tétel. *Tetszőleges $L \subseteq M \subseteq N$ testbővítés lánc esetén*

$$\deg(N\colon L) = \deg(N\colon M) \cdot \deg(M\colon L).$$

Definíció. Legyenek $L \subseteq M$ testek. Az $\alpha \in M$ elem *algebrai az L test fölött,* ha van olyan nemzéró $f \in L[x]$ polinom, hogy $f(\alpha) = 0$.

Példa. Az előző fejezetben említett algebrai számok a $\mathbb{C}$ test algebrai elemei a racionális számtest fölött, míg minden komplex szám algebrai elem mind a valós-, mind a komplex számok teste fölött.

Definíció. Legyen L részteste az M testnek. Az L fölött algebrai $\alpha \in M$ elem *minimálpolinomja* a(z egyik) legalacsonyabb fokú olyan $f \in L[x]$ polinom, amelyre $f(\alpha) = 0$. Az α fokszáma (foka), jelölése: $\deg \alpha$, $\deg f$.

Jelölés. Az $\alpha \in M \supseteq L$ elem minimálpolinomjára használni fogjuk az $m_{\alpha,L}$ jelölést.

4.0.2. Tétel. *Legyen $M|L$ testbővítés és $\alpha \in M$ algebrai elem. Ekkor*

(*i*) *az $m_{\alpha,L}$ minimálpolinom irreducibilis és konstans szorzótól eltekintve egyértelműen meghatározott;*

(*ii*) *valamely $f \in L[x]$ polinomra $f(\alpha) = 0$ pontosan akkor teljesül, ha $m_{\alpha,L}|f$;*

(*iii*) *egy $g \in L[x]$ polinom akkor és csak akkor minimálpolinomja α-nak, ha irreducibilis és $g(\alpha) = 0$.*

4.0.3. Tétel. *Ha $M|L$ testbővítésre $\deg(M\colon L) < \infty$, akkor M minden eleme algebrai L fölött.*

Definíció. Legyen $\vartheta \in \mathbb{C}$. A $\mathbb{Q}$ testnek a ϑ-vel történő *egyszerű testbővítése* a

$$\mathbb{Q}(\vartheta) = \left\{ \frac{g(\vartheta)}{h(\vartheta)} \colon f, h \in \mathbb{Q}[x],\ h(\vartheta) \neq 0 \right\}$$

alakú komplex számok halmaza.

Megjegyzés. Vegyük észre, hogy $\mathbb{Q}(\vartheta) = [\mathbb{Q} \cup \{\vartheta\}]_{\mathbb{C}}$.

4.0.4. Tétel. *Ha ϑ n-edfokú algebrai szám, akkor $\mathbb{Q}(\vartheta)$ elemei egyértelműen írhatók föl $a_0 + a_1\vartheta + a_2\vartheta^2 + \ldots + a_{n-1}\vartheta^{n-1}$ alakban, ahol $a_0, \ldots, a_{n-1} \in \mathbb{Q}$.*

4.0.5. Tétel. *Ha ϑ algebrai szám, akkor* $\deg(\mathbb{Q}(\vartheta)\colon \mathbb{Q}) = \deg \vartheta$.

E fejezetben a racionális számok testének másodfokú bővítéseivel fogunk foglalkozni. Ezt két klasszikus, speciális eset vizsgálatával kezdjük.

4.1. Gauss-egészek.

Definíció. Azon $a + bi$ alakú komplex számokat, amelyekre $a, b \in \mathbb{Z}$ *Gauss-egészeknek* nevezzük. Az összes Gauss-egészek halmazát az elkövetkezőkben $\mathbb{Z}[i]$ fogja jelölni.

Jelölés. Az egyértelmű megkülönböztetés érdekében az ún. *racionális egészeket*, azaz $\mathbb{Z}$ elemeit latin betűkkel, míg a Gauss-egészeket görög betűkkel fogjuk jelölni.

Definíció. Az $\alpha = a+bi$ Gauss-egész *normájának* nevezzük és $N(\alpha)$-val jelöljük α abszolút értékének négyzetét:

$$N(\alpha) = |\alpha|^2 = \alpha\overline{\alpha} = a^2 + b^2.$$

A Gauss-egészek definíniójából és a komplex számok abszolút értékére vonatkozó ismereteink alapján nyilvánvalók a következő tétel állításai.

4.1.1. Tétel. *Tetszőleges α, β Gauss-egészekre*

($\imath$) $N(\alpha)$ *nemnegatív egész,*

($\imath\imath$) $N(\alpha) = 0 \quad \Leftrightarrow \quad \alpha = 0,$

($\imath\imath\imath$) $N(\alpha\beta) = N(\alpha)N(\beta).$

Megmutatjuk, hogy a Gauss-egészekre lényegében ugyanolyan számelmélet építhető, mint a racionális (közönséges) egész számokra. Az első említésre méltó különbség a maradékos osztásoknál fog jelentkezni.

Definíció. Azt mondjuk, hogy az α Gauss egész *osztója* a β Gauss-egésznek, ha van olyan γ Gauss egész, hogy $\beta = \alpha\gamma$. Ez esetben alkalmazni fogjuk az ismert $\alpha \mid \beta$ jelölést.

4.1.2. Tétel. *Ha az $\alpha, \beta \in \mathbb{Z}[i]$-re $\alpha \mid \beta$, akkor $N(\alpha) \mid N(\beta)$ is teljesül a racionális egészek körében.*

Definíció. Azt mondjuk, hogy az ε Gauss-egész *egység*, ha minden Gauss- egésznek osztója.

Megjegyzés. Ez nem az integritástartománybeli egység szokásos definíciója, de a Gauss-egészek körében tradicionálisan így definiálják. A következő tételben megmutatjuk, hogy a két definíció ekvivalens.

4.1.3. Tétel. *Egy ε Gauss-egészre a következő állítások ekvivalensek.*

($\imath$) ε *egység.*

($\imath\imath$) $\varepsilon \mid 1.$

($\imath\imath\imath$) $N(\varepsilon) = 1.$

($\imath\nu$) $\varepsilon = \pm 1,$ *vagy* $\varepsilon = \pm i.$

Bizonyítás.

($\imath$) $\Rightarrow$ ($\imath\imath$) Azonnal adódik az egység iménti definíciójából.

($\imath\imath$) $\Rightarrow$ ($\imath\imath\imath$) Következik az 1.2. Tételből.

($\imath\imath\imath$) $\Rightarrow$ ($\imath\nu$) Az $N(a+bi) = a^2 + b^2 = 1$ egyenlőség a racionális egészek körében csak akkor teljesül, ha $a = \pm 1$ és $b = 0$, vagy $a = 0$ és $b = \pm 1$.

($\imath\nu$) $\Rightarrow$ ($\imath$) Bármely α Gauss-egészre

$$\alpha = 1\alpha = (-1)(-\alpha) = i(-i\alpha) = (-i)(i\alpha).$$

A következő tétel a Gauss-egészek maradékos (euklideszi) osztásáról szól

4.1.4. Tétel. *Tetszőleges α és $\beta \neq 0$ Gauss-egészekhez léteznek olyan γ, ϱ Gauss-egészek, hogy*

$$\alpha = \beta\gamma + \varrho \qquad \text{és} \qquad N(\varrho) < N(\beta). \tag{1}$$

Bizonyítás. Vegyük észre, hogy az (1) föltétel ekvivalens a következővel:

$$\frac{\alpha}{\beta} - \gamma = \frac{\varrho}{\beta} \quad \text{és} \quad |\varrho| < |\beta|, \quad \text{azaz} \quad \left|\frac{\varrho}{\beta}\right| < 1.$$

Ez azt jelenti, hogy olyan γ Gauss-egészt kell keresni, amelyre

$$\left|\frac{\alpha}{\beta} - \gamma\right| < 1. \tag{2}$$

A Gauss-egészek a sík egész koordinátájú rácspontjaival reprezentálhatók, így van a síkon olyan 1 oldalhosszúságú négyzet, amely belsejében, vagy a határán tartalmazza az $\frac{\alpha}{\beta}$ komplex számot reprezentáló pontot. Az elemi geometriából tudjuk, hogy van legalább egy olyan csúcspontja ezen négyzetnek, amelyik 1-nél kisebb távolságra van e ponttól (akár az összes csúcspont ilyen lehet). Ezek közül választhatjuk γ-t.

Legyen $\frac{\alpha}{\beta} = r + si$, és tekintsük a hozzá legközelebb eső csúcspontot (Gauss-egészt), jelölje ezt $\gamma = u + vi$. Világos, hogy u, v az r, s racionális számokhoz legközelebb eső egész.

Ekkor — ugyancsak elemi geometriai ismereteink alapján — kapjuk, hogy

$$\left|\frac{\alpha}{\beta} - \gamma\right| = (r-u)^2 + (s-v)^2 \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2}.$$

Megjegyzés. Eredményünk azt is jelenti, hogy a Gauss-egészek gyűrűje az imént bevezetett normával euklideszi gyűrű.

A Gauss-egészek — föltéve, hogy legalább az egyikük nemzéró — *legnagyobb közös osztóját* ugyanúgy definiáljuk, mint általában integritástartományokban, azaz *olyan közös oszó, amelynek mindegyik közös osztó osztója.* Világos, hogy a legnagyobb közös osztó csak egységszerestől eltekintve egyértelmű.

Bármely két Gauss-egésznek (ha legalább az egyik nem nulla) van legnagyobb közös osztója és egy legnagyobb közös meghatározható euklideszi algoritmussal, annak utolsó nemzéró maradéka. Ugyanúgy, mint korábban, ln. k. o.(α, β) az α, β Gauss-egészek bármely legnagyobb közös osztóját jelölheti.

Definiáljuk a Gauss-egészek körében is a fölbonthatatlan-(irreducibilis-), ill. a prím elemeket.

Definíció. A π egységtől különböző, nemzéró Gauss-egészt *Gauss-prímnek* nevezzük ha csak úgy lehet osztója két Gauss-egész szorzatának, ha legalább az egyik tényezőnek osztója. Azaz

$$\pi \mid \alpha\beta \qquad \Rightarrow \qquad \pi \mid \alpha \quad \text{vagy} \quad \pi \mid \beta.$$

Definíció. A π egységtől különböző, nemzéró Gauss-egészt *Gauss-fölbonthatatlannak* nevezzük ha csak úgy bontható föl két Gauss-egész szorzatára, hogy valamelyik tényező egység. Azaz

$$\pi = \alpha\beta \qquad \Rightarrow \quad \alpha \text{ vagy } \beta \text{ egység.}$$

4.1.5. Tétel. *Egy Gauss-egész pontosan akkor prím, ha fölbonthatatlan.*
Bizonyítás. Tegyük föl, hogy ϱ Gauss prím, és $\varrho = \alpha\beta$ valamely α, β Gauss egészekre. Világos, hogy $\varrho|\alpha\beta$, és mivel prím, valamely tényezőnek is osztója, mondjuk $\varrho|\alpha$. Ekkor $\alpha\beta|\alpha$ is áll, amiből $\alpha \neq 0$ révén $\beta|1$ következik, azaz β egység.

Most legyen ϱ fölbonthatatlan elem, és $\varrho|\alpha\beta$. Ha $\varrho|\alpha$, akkor készen vagyunk, ϱ prím. Ha pedig $\varrho \nmid \alpha$, akkor ln. k. o.$(\varrho, \alpha) = 1$. Ekkor van olyan γ, δ Gauss-egész, hogy $\varrho\gamma + \alpha\delta = 1$, amely hasonlóan igazolható, mint a racionális egészek körében. Ebből már egyszerűen adódik, hogy $\varrho|\beta$.
Megjegyzés. Mivel a Gauss-egészek körében a fölbonthatatlan elemek pontosann a prímelemek, ezért az elkövetkezőkben általában a prímelem, vagy egyszerűen a prím elnevezést részesítjük előnyben.

4.1.6. Tétel. (A számelmélet alaptétele) *Minden 0-tól és az egységektől különböző Gauss-egész fölbontható Gauss-fölbonthatatlanok szorzatára. A fölbontás a tényezők sorrendjétől és egységszeresektől eltekintva egyértelmű.*
Bizonyítás. Az egyértelműség bizonyítása a 4.1.5. Tétel segítségével ugyanúgy végezhető el, mint a racionális egészek esetén.

A felbonthatóság igazolásának menete is ugyanaz, csak az abszolút érték helyett a normát kell figyelembe venni.
Megjegyzés. Láttuk, hogy a számelmélet alaptételének igazolásakor a fölbontás létezését a racionális- és a Gauss-egészeknél lényegében ugyanúgy mutattuk meg, ugyanazt a gondolatmenetet követtük. Az egyértelműség bizonyításához vezető út lépései pedig a következő voltak:

Maradékos osztás $\Rightarrow$ létezik legnagyobb közös osztó (olyan osztó, amely minden közös osztónak osztója) $\Rightarrow$ minden fölbonthatatlan egyben prím is $\Rightarrow$ a fölbontás egyértelmű.

Megmutatható, hogy a (megfelelő értelemben vett) maradékos osztás létezéséből mindig következik, hogy az adott integritástartományban érvényes a számelmélet alaptétele, de a fordított irányú implikáció már nem.

A következő tétel teljesen leírja a Gauss-prímeket.

4.1.7. Tétel.
(*i*) *Minden π Gauss-prímhez pontosan egy olyan p pozitív (racionális) prím létezik, amelyre $\pi|p$.*
(*ii*) *Minden p pozitív (racionális) prímszám vagy maga is Gauss-prím, vagy két olyan Gauss-prím szorzata, amelyek normája p és egymás konjugáltjai.*
Bizonyítás. (*i*) π prím, így $N(\pi) > 1$, és így $N(\pi)$ fölbontható pozitív (racionális) prímek szorzatára: $N(\pi) = p_1 p_2 \dots p_r$. Ekkor

$$\pi \mid \pi\overline{\pi} = N(\pi) = p_1 p_2 \dots p_r.$$

Mivel π (Gauss-)prím, osztója a szorzat valamely tényezőjének, azaz valamelyik p_i-nek is.

A egyértelműség igazolásához legyenek p, q olyan különböző pozitív (racionális) prímek, amelyeknek π osztója. Mivel p, q relatív prímek, léteznek olyan u, v egész számok, hogy $1 = pu + qv$, amiből $\pi|p$ és $\pi|q$ miatt $\pi|1$ adódik, ami lehetetlen.

(*ii*) Ha a $p > 0$ prímszám nem Gauss-prím, akkor fölírható legalább két Gauss-prím szorzataként (4.1.6. Tétel):

$$p = \pi_1 \dots \pi_r \qquad r \geq 2.$$

Ez azt jelenti, hogy

$$p^2 = N(p) = N(\pi_1) \dots N(\pi_r),$$

ahol $N(\pi_i) > 1$. Mivel p^2 csak egyféleképp bomlik egynél nagyobb (racionális) egészek szorzatára, ezért $r = 2$, és $N(\pi_1) = N(\pi_2) = p$.

Mivel $p = \pi_1\pi_2$ és $p = N(\pi_1) = \pi_1\overline{\pi_1}$, a bizonyítandó $\pi_2 = \overline{\pi}_1$ egyenlőséget kapjuk.

A következő tételben megadjuk a Gauss-prímek „listáját".

4.1.8. Tétel. *Legyen $\varepsilon \in \mathbb{Z}[i]$ tetszőleges egység. Az alábbi Gauss-egészek adják az összes Gauss-prímet.*

(*i*) $\varepsilon(1 + i)$.

(*ii*) εq, *ahol q olyan pozitív (racionális) prím, amelyre* $q \equiv -1 \pmod 4$.

(*iii*) *Olyan π, amelyre $N(\pi) = p$ pozitív (racionális) prím, és* $p \equiv 1 \pmod 4$*; minden ilyen prímszámhoz egységszerestől eltekintve két Gauss-prím tartozik, amelyek egymás konjugáltjai, de nem egységszeresei.*

Példák.

(1) A $-1 + i = i(1 + i)$, $-7i$ Gauss-prímek.

(2) A $2-5i$ szintén gauss-prím, mert $N(2-5i) = 29$, amely racionális prím 1-gyel kongruens modulo 4.

(3) A -37, és a $9 + 2i$ nem Gauss-prímek.

Bizonyítás. A 4.1.7. Tétel alapján az összes Gauss-prímet a pozitív (racionális) prímek fölbontásából kapjuk attól függően, hogy e racionális prím a 2 (ez az (*i*) eset), $4k-1$ alakú (a (*ii*) eset), illetve $4k + 1$ alakú (a (*iii*) eset).

(*i*) A $2 = (1 + i)(1 - i) = i^2(1 + i)^2$ egyenlőségekből adódik.

(*ii*) Legyen q olyan pozitív prím, hogy $q \equiv -1 \pmod 4$. Ha nem Gauss-prím, akkor az 4.1.7. Tétel (*ii*) állítása szerint van olyan $\pi = a + bi$ Gauss-prím, hogy

$$q = N(\pi) = a^2 + b^2,$$

ami lehetetlen, mert a modulo 4 -1-gyel kongruens pozitív prímek nem bonthatók két négyzetszám összegére.

(*iii*) Legyen $p \equiv 1 \pmod 4$ pozitív prímszám. Korábbi számelméleti tanulmányainkból tudjuk, hogy az $x^2 + 1 \equiv 0 \pmod p$ kongruencia megoldható, azaz van olyan $c \in \mathbb{Z}$, hogy $p|c^2 + 1 = (c + i)(c - i)$. Ekkor, amennyiben p Gauss-prím, osztója valamelyik tényezőnek. Ez azonban nem teljesül, hiszen

$$\frac{c \pm i}{p} = \frac{c}{p} \pm \frac{1}{p}i$$

nem Gauss-egészek, lévén, hogy a képzetes részük nem egész.

Alkalmazzuk ismét az előző tételt. Ez alapján $p = \pi\overline{\pi}$, ahol a jobb oldalon álló két tényező Gauss-prím. Azt kell csak igazolnunk, hogy $\pi \neq \varepsilon\overline{\pi}$, ahol ε egység. Ez azonban egyszerű számolással adódik , ugyanis ε lehetséges értékei $\pm 1, \pm i$.

4.2. Euler-egészek.

Definíció. Az $\alpha = a + b\omega$ alakú komplex számokat, ahol $a, b \in \mathbb{Z}$ és $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, *Euler-egészeknek* nevezzük.

Megjegyzés. Vegyük észre, hogy ω harmadik primitív egységgyök, és $\omega^2 = -1-\omega$ szintén az, és így

$$x^3 = z^3 - y^3 = (z - y)(z - y\omega)(z - y\omega^2).$$

Ez azt (is) mutatja, hogy az Euler-egészek jó eséllyel alkalmazhatók a Fermat-probléma tárgyalásában az $n = 3$ esetben.

A következő két állítás egyszerűen igazolható.

4.2.1. Állítás. *Az összes Euler-egészek $\mathbb{Z}[\omega]$ halmaza, ahol ω harmadik primitív egységgyök, integritástartományt alkotnak a komplex számok ismert összeadásával és szorzásával.*

4.2.2. Állítás. *Az Euler-egészeknek megfelelő pontok egy olyan egységnyi oldalú rombuszrácsot alkotnak a számsíkon, amelynek szögei* 120 *és* 60 *fokosak.*

Definíció. Az $\alpha = a + b\omega$ Euler-egész *normájának* nevezzük, és $N(\alpha)$-val jelöljük α abszolút értékének négyzetét:

$$N(\alpha) = |\alpha|^2 = (a + b\omega)(a + b\omega^2) = a^2 - ab + b^2.$$

4.2.3. Állítás.

(*i*) *Tetszőleges $\alpha \in \mathbb{Z}[\omega]$-ra $N(\alpha) \in \mathbb{N}_0$, továbbá $N(\alpha) = 0 \quad \Leftrightarrow \quad \alpha = 0$.*

(*ii*) *Az $\alpha = a+b\omega$ Euler egész a^2-ab+b^2 normája mindig írható c^2+3d^2 alakban alkalmas c, d egészekkel.*

Bizonyítás.

(*ii*) Megmutatjuk, hogy az $x^2 - xy + y^2 = n$ diofantikus egyenlet pontosan akkor oldható meg, amikor az $x^2+3y^2 = n$ diofantikus egyenlet. Ebből nyilván már következik állításunk.

Legyen $n \in \mathbb{N}$ és $a, b \in \mathbb{Z}$ olyanok, hogy $a^2 + 3b^2 = n$. Fölhasználva a norma definícióját, $n = a^2 + 3b^2 = N(a + bi\sqrt{3})$ kapjuk, hogy

$$\begin{aligned} a^2 + 3b^2 &= N(a + b + 2\omega) = N(a + b(1 + 2\omega)) \\ &= N((a + b) + 2b\omega) \\ &= ((a + b) + 2b\omega)((a + b) + 2b\omega^2) \\ &= (a + b)^2 - (a + b)(2b) + (2b)^2, \end{aligned}$$

amiből világos, hogy $x = a + b$ és $y = 2b$ megoldása az $x^2 - xy + y^2 = n$ egyenletnek.

Megfordítva, tegyük föl, hogy $c, d \in \mathbb{Z}$ megoldása az $x^2 - xy + y^2 = n$ egyenletnek. Ha van olyan $a, b \in \mathbb{Z}$, hogy

$$c = a + b \qquad \text{és} \qquad d = 2b,$$

akkor az előbbi gondolatmeneten visszafelé haladva a bizonyítást elvégezhetjük. Ez természetesen csak akkor működik, ha c, d valamelyike páros (x, y szerepe szimmetrikus). Marad az az eset, amikor c, d páratlanok.

Mivel

$$\begin{aligned} n = c^2 - cd + b^2 &= N(c + d\omega) = N(c + d\omega^2) \\ &= N(c - d - d\omega) \\ &= (c-d)^2 - (c-d)(-d) + (-d)^2 \end{aligned}$$

látható hogy ez esetben — lévén most $c - d$ páros — kaptuk, hogy ez esetben $c - d$ és $-d$ is megoldás. Erre már alkalmazhatjuk az előbb leírtakat.

Megjegyzések.
(1) Az Euler-egészek körében a Gauss-egészeknél alkalmazott módon definiálhatók a következők: oszthatóság, egység, legnagyobb közös osztó, irreducibilis- és prím elem.
(2) A Gauss-egészeknél alkalmazott módszerek értelemszerű módosításával igazolhatók: a norma tulajdonságai, maradékos osztás (természetesen itt rácsnégyzet helyett rácsrombuszt kell használni), a prím és az irreducibilis ekvivalenciája, a számelmélet alaptétele, az egységek karakterizációja, a következő tétel figyelembe vételével. Az érdeklődő olvasó megtalálja e tételek bizonyítását Freud Róbert és Gyarmati Edit könyvében.

4.2.4. Tétel. *Az Euler-egészek gyűrűjében 6 egység van, amelyek a következők.*

$$\pm 1, \quad \pm\omega, \quad \pm\omega^2 = \mp(1+\omega).$$

Ezen éppen a hatodik egységgyökök.

4.2.5. Tétel. *Az Euler prímek a következők* (ε *tetszőleges egységet jelöl*).
(A) $\varepsilon(i\sqrt{3}) = \varepsilon(1 + 2\omega)$,
(B) εq, *ahol* $q \equiv 2 \pmod 3$ *pozitív (racionális) prímszám,*
(C) π, *ahol* $N(\pi) \equiv 1 \pmod 3$ *pozitív (racionális) prímszám; minden ilyen prímszámhoz egységszerestől eltekintve két Euler- prím tartozik, amelyek egymás konjugáltjai, de nem egymás egységszeresei.*

Ugyancsak az előbb említett könyvben olvasható, hogy hogyan alkalmazhatók az Euler-egészek a Fermat-sejtés igazolására az $n = 3$ esetben. A következő tétel bizonyítható ugyanis.

4.2.6. Tétel. *Az* $x^3 + y^3 + z^3 = 0$ *egyenletnek nincs zérótól különböző megoldása az Euler-egészek gyűrűjében.*

4.3. A racionális számtest másodfokú bővítései.

7.3.1. Tétel. *A racionális számok* $\mathbb{Q}$ *testének összes másodfokú bővítése* $\mathbb{Q}(\sqrt{t})$ *alakú, ahol* $t \in \mathbb{Z}$ *négyzetmentes szám és* $t \neq 1$. *Különböző ilyen* t *egészekhez különböző bővítések tartoznak.*
Megjegyzések.
(1) $t > 0$ esetén a bővítést valósnak, míg a $t < 0$ esetben képzetes (imaginárius) bővítésnek

nevezzük. Ha $t < 0$ és $\alpha^2 = t$, akkor $\mathbb{Q}(\alpha) = \mathbb{Q}(-\alpha)$ lévén $\sqrt{t}$ jelentse mindig a gyökvonás fölső félsíkbeli értékét, azaz $\sqrt{t} = i\sqrt{|t|}$.
(2) A racionális számok testének másodfokú bővítéseit gyakran *kvadratikus testeknek* nevezik. Ha a $T \subseteq \mathbb{C}$, kvadratikus test, akkor T nem algebrai elemeit szokás *kvadratikus irracionálisoknak* nevezni.
Bizonyítás. Legyen $M \subseteq \mathbb{C}$ olyan, hogy $[M : \mathbb{Q}] = 2$. Ekkor bármely $\alpha \in M$ irracionális szám másodfokú algebrai szám, és $M = \mathbb{Q}(\alpha)$.

Legyen $g = g_\alpha \in \mathbb{Z}[x]$ az α minimálpolinomja (világos, hogy racionális- helyett tekinthetünk egész együtthatósat!!!), $g = a_0 + a_x + a_2x^2$. A másodfokú egyenletek gyökképlete alapján $\alpha = r_0 + r_1\sqrt{s}$, ahol $r_0, r_1 \in \mathbb{Q}$, $r_1 \neq 0$ és $s \in \mathbb{Z}$. Ha $s = k^2t$, ahol t négyzetmentes és $t \neq 1$, akkor $\alpha = r_0 + r_1k\sqrt{t}$. Ebből már könnyen kapható, hogy $M = \mathbb{Q}(\alpha) = \mathbb{Q}(t)$.

Legyen ezután $\mathbb{Q}(\sqrt{t_1}) = \mathbb{Q}(\sqrt{t_2})$, akol t_1, t_2 négyzetmentes és különbözik 1-től. Mivel

$$\sqrt{t_2} \in \mathbb{Q}(\sqrt{t_1}) \qquad \Longrightarrow \qquad \sqrt{t_2} = a + b\sqrt{t_1},$$

ahol $a, b \in \mathbb{Q}$ kapjuk, hogy

$$t_2 = a^2 + t_1b^2 + 2ab\sqrt{t_1}.$$

Tekintettel arra, hogy $\sqrt{t_1} \notin \mathbb{Q}$ ez csak úgy lehetséges, hogy ha $b = 0$, vagy $a = 0$. Az első eset lehetetlen, hiszen belőle $\sqrt{t_2}$ racionális volta adódik. A második esetben pedig $\sqrt{t_2}/\sqrt{t_1} \in \mathbb{Q}$ adódik, ami t_1, t_2 négyzetmentessége miatt csak akkor lehetséges, ha $t_1 = t_2$.
Példák.
(1) A $\mathbb{Q}(i)$ test, az ún. Gauss-racionálisok teste másodfokú bővítése a racionális számtestnek, ekkor $t = -1$.
(2) Ha $\omega = \frac{-1+i\sqrt{3}}{2}$, azaz egy harmadik primitív egységgyök, akkor a $\mathbb{Q}(\omega)$ test, az Euler-racionálisok teste olyan másodfokú bővítésként kapható, ahol $t = -3$.

Definíció. A racionális számok $\mathbb{Q}$ testének másodfokú bővítéseit *kvadratikus testeknek* nevezzük.
Definíció. Egy algebrai számot *algebrai egésznek* mondunk, ha (egyik) minimálpolinomja egész együtthatós főpolinom (azaz kezdőegyütthatója 1).
Megjegyzés. Vegyük észre, hogy a Gauss-egészek éppen a $\mathbb{Q}(\sqrt{-1})$ kvadratikus test egész elemei.

Az elkövetkezőkben a kvadratikus testek, a racionális számok testének másodfokú bővítései, algebrai egészeivel foglalkozunk, különös tekintettel arra, hogy melyek azok a kvadratikus testek, amelyek egészei Gauss-gyűrűt alkotnak (érvényes körükben a számelmélet alaptétele).
4.3.2. Tétel. *Legyen $t \neq 1$ négyzetmentes szám. Ekkor a $\mathbb{Q}(\sqrt{t})$ bővítés algebrai egészei pontosan a $c + d\vartheta$ alakú számok, ahol $c, d \in \mathbb{Z}$ és*

$$\vartheta = \begin{cases} \sqrt{t}, & \text{ha} \quad t \not\equiv 1 \pmod 4; \\ \dfrac{1+\sqrt{t}}{2}, & \text{ha} \quad t \equiv 1 \pmod 4. \end{cases}$$

Más megfogalmazásban, valamely $a + b\sqrt{t}$ elem pontosan akkor egész eleme a $\mathbb{Q}(\sqrt{t})$ testnek, ha

(*i*) $t \not\equiv 1 \pmod 4$ *esetén* $a, b \in \mathbb{Z}$*;*
(*ii*) $t \equiv 1 \pmod 4$ *esetén* $a = \frac{u}{2},\ b = \frac{v}{2}$*, ahol* u, v *azonos paritású egészek.*

Bizonyítás. Az állítás a $\mathbb{Q}(\sqrt{t})$ test racionális elemeire nyilvánvaló, hiszen ezek pontosan akkor algebrai egészek, ha egész számok. Ezért elegendő csak az irracionális elemekkel foglalkoznunk.

Legyen $\alpha \in \mathbb{Q}(\sqrt{t})$ irracionális, így egyértelműen írható $\alpha = r_0 + r_1\sqrt{t}$ alakban, ahol $r_0, r_1 \in \mathbb{Q},\ r_1 \neq 0$. Nyilván e szám írható

$$\alpha = \frac{a + b\sqrt{t}}{c}, \qquad a, b, c \in \mathbb{Z},\ \text{ln. k. o.}(a, b, c) = 1,\ c > 0,\ b \neq 0$$

alakban. Ezt rendezve, majd négyzetre emelve

$$\alpha - \frac{a}{c} = \frac{b\sqrt{t}}{c}$$
$$\alpha^2 - \frac{2a}{c}\alpha + \frac{a^2 - tb^2}{c^2} = 0$$

adódik. Mivel α másodfokú elem, ezért a második egyenlőség alapján az α minimálpolinomja

$$g_\alpha = x^2 - \frac{2a}{c}x + \frac{a^2 - tb^2}{c^2}.$$

Így α pontosan akkor lesz algebrai egész, ha ezen minimálpolinom egész együtthatós, azaz

$$c|2a \qquad \text{és} \qquad c^2|a^2 - tb^2. \tag{1}$$

Azt kell belátnunk tehát, hogy ez utóbbi pontosan akkor teljesül, ha

(*i*) $t \not\equiv 1 \pmod 4$ estén $c = 1$;

(*ii*) $t \equiv 1 \pmod 4$ estén $c = 2$ és a, b páratlan, vagy $c = 1$.

Először azt mutatjuk meg, hogy (1)-ből $c = 1$, vagy $c = 2$ következik. Ezt úgy tesszük, hogy a $c > 2$ föltételezésből ellentmondást vezetünk le. Ez utóbbi föltételezés esetén vagy van a c-nek $p > 2$ prímosztója, vagy $4|c$.

Ha $p|c$ és $p > 2$ prím, akkor $p|2a \ \Rightarrow\ p|a$, továbbá $p^2|a^2 - tb^2$. Így $p^2|tb^2$ is áll. Mivel $p|a$, $\text{ln. k. o.}(a, b, c) = 1$ kapjuk, hogy $\text{ln. k. o.}(pb) = 1$, tehát $p^2|t$. Ez azonban ellentmond t négyzetmentes voltának. A $4|c$ eset ugyanígy vizsgálható, $p = 2$ alkalmazásával.

Maradnak a $c = 1, 2$ lehetőségek. Világos, hogy ha $c = 1$, akkor (1) bármely $a, b \in \mathbb{Z}$-re teljesül. Ha $c = 2$, akkor az első oszthatóság bármely a egészre igaz. A második oszthatósági föltétel pedig

$$a^2 - tb^2 \equiv 0 \pmod 4 \tag{2}$$

alakba írható át.

Vegyük észre, hogy az $\text{ln. k. o.}(a, b, c) = 1$ és a $c = 2$ föltételek miatt a, b nem lehet egyidejűleg páros. Legyen először a b páros és az a páratlan. Ekkor

$$a^2 - tb^2 \equiv 1 \pmod 4,$$

ha pedig fordítva van, akkor

$$a^2 - tb^2 \equiv -t \pmod 4,$$

tehát mindkettő ellentmond (2)-nek.

Marad az az eset, amikor a, b egyaránt páratlan. Ekkor

$$a^2 - tb^2 \equiv 1 - t \pmod 4,$$

azaz ez esetben (2) pontosan a $t \equiv 1 \pmod 4$ esetben teljesül. Ezzel a tételt bebizonyítottuk.

4.3.3. Következmény. *Jelölje a $\mathbb{Q}(\sqrt{t})$ bővítés algebrai egészeinek halmazát $E(\sqrt{t})$. Az előbbi tételünk szerint*

$$E(\sqrt{t}) = \{c + d\sqrt{t} \mid c, d \in \mathbb{Z}\}, \qquad \text{ha } t \not\equiv 1 \pmod 4, \tag{3a}$$

illetve

$$E(\sqrt{t}) = \left\{c + d\frac{1+\sqrt{t}}{2} \mid c, d \in \mathbb{Z}\right\}, \quad \text{ha } t \equiv 1 \pmod 4. \tag{3b}$$

Mivel az $E(\sqrt{t})$ halmaz integritástartomány, hiszen részgyűrűje $\mathbb{C}$-nek, érdeme megvizsgálni e gyűrű néhány számelméleti tulajdonságát. Világos, hogy az oszthatóság, az irreducibilis- és a prímelemek, a legnagyobb közös osztó és még számos hasonló tulajdonság, köztük az irreducibilis faktorizáció ugyanúgy vizsgálható, mint például a gauss-egészek körében. Midezekhez — hasonlóan a Gauss-egészekhez — most is hasznos lesz egy norma bevezetése.

Definíció. Legyen az $\alpha = a + b\sqrt{t} \in E(\sqrt{t})$ elem normája

$$N(\alpha) = a^2 - tb^2 = (a + b\sqrt{t})(a - b\sqrt{t}).$$

Megjegyzés. Világos, hogy az iménti norma egész szám.

A következőkben a tételeket csak megfogalmazzuk, esetenként kommentáljuk. A bizonyításokat az érdeklődő hallgatók megtalálhatják például Freud Róbert és Gyarmati Edit Számelmélet c. tankönyvében, vagy Megyesi László Bevezetés a Számelméletbe c. jegyzetében.

4.3.4. Tétel.

(A) *Egy $\varepsilon \in E(\sqrt{t})$ elemre*

$$\varepsilon | 1 \qquad \Leftrightarrow \qquad |N(\varepsilon)| = 1.$$

(B) *Ha $t > 0$, akkor $E(\sqrt{t})$-ben végtelen sok egység van.*

(C) *Ha $t < 0$ és $t \neq -1, -3$, akkor $E(\sqrt{t})$-ben az összes egység a ± 1.*

4.3.5. Tétel. *A számelmélet alaptétele érvényes az $E(\sqrt{2})$ gyűrűben, azaz e gyűrű Gauss-gyűrű, de nem érvényes az $E(\sqrt{-5})$ és $E(\sqrt{10})$ gyűrűkben.*

Megjegyzések.
(1) Viszonylag egyszerű számolással mutatható meg, hogy az $E(\sqrt{-5})$ gyűrűben a 2 és a 3 nem bontható föl, azaz irreducibilis, de a 3 nem prím.
(2) Annak a megmutatása sem bonyolult, hogy az $E(\sqrt{10})$ gyűrűben a -9-nek kétféle fölbontása van.

Az a kérdés, hogy mely kvadratikus testek egészeinek gyűrűje Gauss-gyűrű, azaz melyekben érvényes a számelmélet alaptétele meglehetősen nehéz kérdés, teljesen a mai napig megoldatlan. Ezek közül néhány eredményt, illetve megoldatlan kérdést említünk végezetül.

1. Megoldatlan, hogy létezik-e végtelen sok olyan $t > 0$ egész, hogy $E(\sqrt{t})$-ben érvényes az alaptétel.

2. Ismeretes az összes olyan $t > 0$ egész, amelyekre az $E(\sqrt{t})$ gyűrű euklideszi, azaz elvégezhető benne a norma abszolút értéke szerinti maradékos osztás. Ezek a következők:

$$t = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73.$$

Léteznek továbbá olyanok pozitív t-k, amelyekre igaz az alaptétel, például $t = 14, 22, 23, 31$.

3. Pontosan 9 olyan $t < 0$ létezik, amelyre $E(\sqrt{t})$-ben érvényes az alaptétel, nevezetesen

$$t = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

4. Az előbbiek közül pontosan 5 olyan van, amelyekben elvégezhető a norma négyzete szerinti maradékos osztás.