

5. AZ ALGEBRAI SZÁMELMÉLET ELEMEI

5.0. Bevezetés.

Az algebrai számelmélet legegyszerűbb kérdései az ún. algebrai 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: $\deg(M: L) = \dim_L M$.

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

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

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

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.

5.0.2. 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 $g(\alpha) = 0$.

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

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

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

alakú komplex számok halmaza.

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

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

5.0.5. Tétel. Ha ϑ algebrai szám, akkor $\deg(\mathbb{Q}(\vartheta) : \mathbb{Q}) = \deg \vartheta$.

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

5.2. 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.

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

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

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

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

5.2.3. Állítás.

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

(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

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

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 rácsháromszöget 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.

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

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

Ezek éppen a hatodik egységgyökök.

5.2.5. Tétel. *Az Euler prímek a következők (ε tetszőleges egységet jelöl).*

$$(A) \quad \varepsilon(i\sqrt{3}) = \varepsilon(1 + 2\omega),$$

$$(B) \quad \varepsilon q, \text{ ahol } q \equiv 2 \pmod{3} \text{ pozitív (racióális) prímszám,}$$

(C) π , ahol $N(\pi) \equiv 1 \pmod{3}$ pozitív (racióális) 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.

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

5.3. A racionális számtest másodfokú bővítései.

5.3.1. 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 felső 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 racionális 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 együtthatós polinom helyett tekinthetünk egész együtthatósat!!!), $g = a_0 + a_1x + a_2x^2$. 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 $M = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{t})$.

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

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

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 volna 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-rationálisok 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).

5.3.2. 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

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

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

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

alakban. Ezt rendezve, majd négyzetre emelve

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

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 együttthatható, azaz

$$c|2a \quad \text{és} \quad c^2|a^2 - tb^2. \quad (1)$$

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

(i) $t \not\equiv 1 \pmod{4}$ esetén $c = 1$;

(ii) $t \equiv 1 \pmod{4}$ esetén $c = 2$ 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 $c > 2$ feltételezésből ellentmondást vezetünk le. Ez utóbbi feltételezés 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 $p|a$, ln. k. o. $(a, b, c) = 1$ kapjuk, hogy ln. k. o. $(p, b) = 1$, 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 feltétel pedig

$$a^2 - tb^2 \equiv 0 \pmod{4} \quad (2)$$

alakba írható át.

Vegyük észre, hogy az ln. k. o. $(a, b, c) = 1$ és a $c = 2$ feltételek 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.

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

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

illetve

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

Mivel az $E(\sqrt{t})$ halmaz integritástartomány, hiszen részgyűrűje $\mathbb{C}$ -nek, érdemes 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.

5.3.4. Tétel.

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

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

(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 .

5.3.5. 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 további olyan 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 előbbiektől közül pontosan 5 olyan van, amelyekben elvégezhető a norma négyzete szerinti maradékos osztás.