1. Algebrai egészek

Az alábbiakban minden gyűrű szokásos, és ha $R \leq S$ gyűrűk, akkor feltesszük, hogy R és S egységeleme ugyanaz. Ilyenkor $\alpha_1, \ldots, \alpha_n \in S$ esetén $R[\alpha_1, \ldots, \alpha_n]$ jelöli az R és az $\alpha_1, \ldots, \alpha_n$ által generált részgyűrűt. Ez a $h(\alpha_1, \ldots, \alpha_n)$ elemek halmaza, ahol $h \in R[x_1, \ldots, x_n]$.

1.1. Definíció. Legyen R részgyűrűje S-nek. Azt mondjuk, hogy az $R \leq S$ bővítés *véges* modulusbővítés, ha az S, mint R-modulus, végesen generált.

Ez tehát azt jelenti, hogy van olyan $\alpha_1, \ldots, \alpha_n \in S$, hogy S minden eleme előáll ezen elemek R-beli együtthatós lineáris kombinációjaként.

1.2. Lemma. *Véges modulusbővítések egymásutánja is véges.*

Bizonyítás. Legyenek $R \leq S \leq U$ gyűrűk, ahol $R \leq S$ és $S \leq U$ véges modulusbővítések. Jelölje $\alpha_1, \ldots, \alpha_n$ az S-nek, mint R-modulusnak egy generátorrendszerét, és $\beta_1, \ldots, \beta_m$ az U-nak, mint S-modulusnak egy generátorrendszerét. Ekkor az nm darab $\alpha_i\beta_j$ szorzat generálja az ${}_RU$ modulust (a számolás ugyanaz, mint a testbővítések szorzástétele esetében). □

1.3. Definíció. Legyen R részgyűrűje S-nek. Az $\alpha \in S$ elem (algebrai) *egész* az R fölött, ha gyöke egy nem nulla, R-beli együtthatós, *normált* polinomnak. Ha speciálisan $R = \mathbb{Z}$ és $S = \mathbb{C}$, akkor a kapott egészeket *algebrai egész számoknak* nevezzük.

1.4. Lemma. *Legyen α egész R fölött. Ekkor $R[\alpha] \geq R$ véges modulusbővítés.*

Bizonyítás. Legyen $f \in R[x]$ egy olyan normált polinom, melynek α gyöke, és jelölje n az f fokát. Az $R[\alpha]$ elemei az $s = r_0 + r_1\alpha + \ldots + r_m\alpha^m$ alakú kifejezések, ahol $r_i \in R$. Ha itt $m \geq n$, akkor az $f(\alpha) = 0$ egyenlőséget α^{m-n}-nel szorozva azt kapjuk, hogy α^m, és így s is kifejezhető α alacsonyabb hatványaival és R elemeivel. Az eljárást ismételve s-et α legfeljebb $n-1$-edfokú R-beli együtthatós polinomjaként írhatjuk fel. Ezért az $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ elemek generátorrendszert alkotnak az ${}_RR[\alpha]$ modulusban. □

1.5. Lemma. *Ha $R \leq S$ gyűrűk, és ez véges modulusbővítés, akkor S minden eleme egész R fölött.*

Bizonyítás. Jelölje $\alpha_1, \ldots, \alpha_n$ az S-nek, mint R-modulusnak egy generátorrendszerét, és legyen $\alpha \in S$. Ekkor $\alpha\alpha_j$ felírható $r_{j1}\alpha_1 + \cdots + r_{jn}\alpha_n$ alakban, ahol $r_{ji} \in R$. Mivel nem minden α_j nulla, ez azt jelenti, hogy (az S hányadostestében gondolkozva), az $((r_{ji}))$ mátrixnak α sajátértéke. Ezért α gyöke e mátrix karakterisztikus polinomjának, aminek főegyütthatója $(-1)^n$, és $R[x]$-beli. Ennek $(-1)^n$-szerese mutatja, hogy α egész R fölött. □

1.6. Tétel. *Az algebrai egész számok gyűrűt alkotnak. Általánosabban, ha $R \leq S$ gyűrűk, akkor az S azon elemei, melyek egészek R fölött, részgyűrűt alkotnak.*

Bizonyítás. Tegyük fel, hogy $\beta, \gamma \in S$ egészek R fölött. Ekkor $U = R[\beta]$ végesen generált R-modulus, és $U[\gamma]$ végesen generált U-modulus, hiszen γ egész U fölött is. Ezért $R \leq U[\gamma]$ is végesen generált, és így minden eleme, speciálisan $\beta - \gamma$ és $\beta\gamma$ is egész R fölött. □

1.7. Tétel. *Algebrai egész együtthatós normált polinom gyökei is algebrai egészek. Általában, ha $R \leq S$ gyűrűk és $\alpha \in S$ gyöke egy olyan normált $f(x)$ polinomnak, melynek együtthatói egészek R fölött, akkor α is egész R fölött.*

Bizonyítás. Bővítsük R-et, mint gyűrűt sorban f együtthatóival, ekkor mindig véges modulusbővítést kapunk, ezért az eredmény is egy véges $R \leq U$ modulusbővítés, ahol $f \in U[x]$. Ekkor $U[\alpha] \geq U$ is véges, ezért $U \leq R$ is az, és így α egész R fölött. □

Az R gyűrű *egész-zárt*, ha a hányadostestének minden R fölött egész eleme R-beli.

1.8. Tétel. *Minden alaptételes gyűrű egész-zárt. Speciálisan ha egy algebrai egész szám egyben racionális szám is, akkor $\mathbb{Z}$-beli egész szám.*

Bizonyítás. Tegyük föl, hogy R hányadostestének p/q eleme gyöke az $f \in R[x]$ normált polinomnak. Mivel R alaptételes, érvényes a racionális gyökteszt tétele, azaz ha p és q relatív prímek, akkor q osztója f főegyütthatójának, és így q egység. Ezért $p/q \in R$. □

E tétel következő általánosítása segít eldönteni, hogy egy algebrai szám algebrai egész-e. Legyen $R \leq L$ gyűrűbővítés, ahol R alaptételes és L test. Jelölje T az R hányadostestét. Ez nem más, mint L-nek az a részteste, amely az R-beli elemek hányadosaiból áll. Például $R = \mathbb{Z}$ és $L = \mathbb{C}$ esetén $T = \mathbb{Q}$.

1.9. Tétel. *Az iménti jelölésekkel, ha R alaptételes, akkor L egy eleme akkor és csak akkor egész R fölött, ha a T fölötti (normált) minimálpolinomja R-beli együtthatós.*

Bizonyítás. Legyen $\alpha \in L$ egész R fölött és $f \in R[x]$ olyan normált polinom, melynek α gyöke. Mivel $R[x]$ alaptételes, az f felbomlik irreducibilis polinomok szorzatára. De f normált, ezért ezeknek az irreducibilis tényezőknek egység a főegyütthatója, speciálisan egyik sem lehet konstans, és így mindegyik irreducibilis R hányadosteste fölött is (hiszen így írtuk le az R fölött irreducibilis polinomokat). Van ezek között a tényezők között egy olyan, amelynek α gyöke. Ez tehát α minimálpolinomjának egységszerese, így ez a minimálpolinom is R-beli együtthatós. □

1.10. Tétel. *Minden algebrai szám előáll egy algebrai egész és egy $\mathbb{Z}$-beli egész hányadosaként. Általában, legyen $R \leq L$ gyűrűbővítés, ahol L test és T az R hányadosteste. Ekkor minden T fölött algebrai $\beta \in L$ felírható α/r alakban, ahol $\alpha \in L$ egész R fölött és $r \in R$.*

Bizonyítás. A β elem T fölötti minimálpolinomjának együtthatóit közös nevezőre hozva olyan $f(x) = r_0 + r_1 x + \ldots + r_n x^n \in R[x]$ polinomot kapunk, melynek β gyöke (és $r_n \neq 0$). Legyen $r = r_n$ és $\alpha = r\beta$. Ekkor az $f(\beta) = 0$ egyenletet r^{n-1}-nel beszorozva látjuk, hogy α gyöke az $x^n + r_{n-1}x^{n-1} + rr_{n-2}x^{n-2} + \ldots + r^{n-1}r_0$ polinomnak, és így egész R fölött. □

2. Hilbert nullhelytétele

Ha az $R \leq S$ gyűrűbővítésben R test, akkor a modulusgenerálás valójában vektortérgenerálás, és az algebrai elemek ugyanazok, mint az algebrai egész elemek (hiszen a főegyütthatóval végigoszthatjuk a polinomot, a gyökei nem változnak). Ha $\alpha \in S$ algebrai az R test fölött, akkor az $R[\alpha]$ gyűrűről nemcsak azt tudjuk, hogy R-nek véges modulusbővítése, hanem azt is láttuk a Galois-elméletben, hogy testet kapunk. Innen n szerinti indukcióval adódik, hogy ha $\alpha_1, \ldots, \alpha_n \in S$ algebraiak az R test fölött, akkor $R(\alpha_1, \ldots, \alpha_n) = R[\alpha_1, \ldots, \alpha_n]$, vagyis e testbővítés minden eleme az $\alpha_1, \ldots, \alpha_n$ elemek R-beli együtthatós polinomja, osztásra nincs szükség (és ez is véges modulusbővítése R-nek). Most megmutatjuk ennek az állításnak a megfordítását: ha gyűrűbővítésként testet kapunk, akkor algebrai elemekkel bővítettünk. Ehhez eszközként használjuk az algebrai egész elemeket.

2.1. Lemma. *Legyen $K \leq L$ testbővítés, amely mint gyűrűbővítés végesen generált. Ekkor ez véges bővítés (vektortérként is).*

Bizonyítás. Legyen $L = K[\beta_1, \ldots, \beta_n]$, azt kell belátni, hogy mindegyik β_i algebrai K fölött. Az n szám szerinti indukcióval bizonyítunk, a kezdőeset a triviális $n = 0$. Az elemek cseréjével feltehető, hogy β_1 transzcendens K fölött, ebből akarunk ellentmondásra jutni. Legyen $R = K[\beta_1] \cong K[x]$ és $T = K(\beta_1) \cong K(x)$.

Mivel $T[\beta_2, \ldots, \beta_n] = L$, az indukciós feltevés miatt $\beta_2, \ldots, \beta_n$ algebrai T fölött. Az 1.10. Tétel miatt $i \geq 2$ esetén β_i felírható α_i/f_i alakban, ahol α_i egész R fölött és $f_i \in R$ (hiszen T az R hányadosteste). Ha $s \in L$ tetszőleges, akkor $s = h(\beta_1, \ldots, \beta_n)$ alkalmas $h \in K[x_1, \ldots, x_n]$ polinomra. Írjuk be mindegyik β_i helyébe a megfelelő α_i/f_i-t, majd szorozzunk be az $f = f_2 \ldots f_n$ olyan nagy hatványával, hogy az f_i nevezők eltűnjenek. Ekkor $R[\alpha_2, \ldots, \alpha_n]$ egy elemét kapjuk, és ez egész R fölött, hiszen az egészek részgyűrűt alkotnak. Azaz beláttuk, hogy ha N elég nagy, akkor $f^N s$ egész R fölött.

Tudjuk, hogy R izomorf $K[x]$-szel, és β_1-nek x felel meg. Ezért $\beta_1 f + 1$ nem nulla, nem egység, és f^N-hez relatív prím R-ben. Mivel $s = 1/(\beta_1 f + 1) \in L$, van olyan N, hogy $f^N/(\beta_1 f + 1)$ egész R fölött. Az 1.8. Tétel miatt $\beta_1 f + 1$ egység, ami ellentmondás. □

Legyen $R = \mathbb{C}[x_1, \ldots, x_n]$ és $p = (z_1, \ldots, z_n) \in \mathbb{C}^n$. A „$p$ behelyettesítése" az az R-ből $\mathbb{C}$-be vezető φ gyűrűhomomorfizmus, amelyre $\varphi(f) = f(p)$. Ez a konstans polinomok miatt szürjektív, így ha $I_p = \mathrm{Ker}(\varphi)$, akkor a homomorfizmustétel szerint $R/I_p \cong \mathbb{C}$, és így I_p maximális ideál. Ebben az ideálban benne vannak az $x_i - z_i$ polinomok, és ezek generálják is, hiszen minden polinom egy konstanssal kongruens mod $(x_1 - z_1, \ldots, x_n - z_n)$. Azt mondjuk, hogy I_p a *p ponthoz kötött* maximális ideál, és hogy I_p elemei *eltűnnek* a p pontban.

2.2. Állítás. *Az $R = \mathbb{C}[x_1, \ldots, x_n]$ minden maximális ideálja ponthoz kötött.*

Bizonyítás. Legyen M maximális ideál R-ben és $L = R/M$, ez kommutatív, egységelemes, egyszerű gyűrű, és így test. Mivel a konstans polinomok páronként inkongruensek mod I, az L-nek van egy $\mathbb{C}$-vel izomorf K részteste. A $K \leq L$ gyűrűbővítést generálják K fölött az x_i polinomok maradékosztályai, tehát az előző lemma szerint ez egy véges bővítés. Mivel $\mathbb{C}$ algebrailag zárt, $K = L$. Ezért mindegyik x_i határozatlan kongruens egy alkalmas z_i konstans polinommal, és így $M = I_{(z_1, \ldots, z_n)}$. □

2.3. Tétel [Nullhelytétel]. *Legyen $f_1, \ldots, f_k \in \mathbb{C}[x_1, \ldots, x_n]$ és $V \subseteq \mathbb{C}^n$ az $f_1, \ldots, f_k$ polinomok közös gyökeinek a halmaza. Ekkor egy $f \in \mathbb{C}[x_1, \ldots, x_n]$ pontosan akkor tűnik el V minden elemén, ha van olyan $N > 0$, hogy $f^N \in (f_1, \ldots, f_k)$.*

Bizonyítás. Ha $f^N = g_1 f_1 + \ldots + g_k f_k$ alkalmas g_i polinomokra, akkor nyilván $f^N(p) = 0$ minden $p \in V$-re. Megfordítva, tegyük fel, hogy f eltűnik V-n. Vegyünk fel egy új y határozatlant, és tekintsük az $I = (f_1, \ldots, f_k, 1 - yf)$ ideált $\mathbb{C}[x_1, \ldots, x_n, y]$-ban. Belátjuk, hogy ez az egész gyűrű. Valóban, ha nem így lenne, akkor Krull tétele miatt létezne egy I-t tartalmazó maximális ideál, ami az előző állítás miatt egy $q = (z_1, \ldots, z_n, w) \in \mathbb{C}^{n+1}$ ponthoz kötött. Ezért q gyöke $f_1, \ldots, f_k, 1 - yf$ mindegyikének, azaz $p = (z_1, \ldots, z_n) \in V$ és $1 - f(p)w = 0$. De akkor $f(p) = 0$ a feltétel szerint, ami ellentmondás.

Tehát $1 \in I$, azaz $1 = g_1 f_1 + \ldots + g_k f_k + g(1 - yf)$ alkalmas $g_i, g \in \mathbb{C}[x_1, \ldots, x_n, y]$-ra. Helyettesítsünk ebbe az azonosságba y helyére $1/f$-et, ekkor az utolsó tag nulla lesz:

$$1 = \sum_{i=1}^{k} g_i\big(x_1, \ldots, x_n, (1/f)\big) f_i(x_1, \ldots, x_n)\,.$$

Az f alkalmas N hatványával szorozva f eltűnik mindegyik nevezőből. □