7. Gyűrűk

7.1 Alapfogalmak

7.1.1 Definíció: az $(R,+,\cdot)$ struktúra gyűrű, ha $(R,+)$ Abel-csoport, $(R,\cdot)$ félcsoport és a szorzás jobbról és balról egyaránt disztributív az összeadásra nézve. (Ez azt jelenti, hogy a gyűrű valamely elemével – jobbról vagy balról való – szorzás az additív csoport – $(R,+)$ – csoport egy endomorfizmusa.) Összefoglalva:

(R1) $+: R\times R\to R$
(R2) $\forall a,b,c\in R: a+(b+c)=(a+b)+c$
(R3) $\forall a,b\in R: a+b=b+a$
(R4) $\exists 0\in R: \forall a\in R: a+0=a$
(R5) $\forall a\in R: \exists(-a)\in R: a+(-a)=0$
(R6) $\cdot: R\times R\to R$
(R7) $\forall a,b,c\in R: a\cdot(b\cdot c)=(a\cdot b)\cdot c$
(R8) $\forall a,b,c\in R: a\cdot(b+c)=a\cdot b+a\cdot c$
(R9) $\forall a,b,c\in R: (a+b)\cdot c=a\cdot c+b\cdot c$

Az additív csoport egységelemét a gyűrű nullelemének nevezzük és 0-val jelöljük. Egy a elem ellentettje az additív inverze, jele $-a$. $a+(-b)$-t $(a-b)$-vel jelöljük és a két elem különbségének nevezzük. A gyűrű egységeleme – ha van – $(R,\cdot)$ egységeleme, jele 1. Baloldali ill. jobboldali egységelem névvel a multiplikatív félcsoport megfelelő elemeit illetjük. Amennyiben $(R,\cdot)$ kommutatív ill. egységelemes félcsoport, akkor R egységelemes ill. kommutatív gyűrű. Triviális gyűrűnek az egyelemű gyűrűt nevezzük. Mivel az állítások vagy triviálisan igazak rá, vagy triviálisan nem, ezzel a gyűrűvel a továbbiakban nem foglalkozunk.

A 0 minden többszöröse is 0, hiszen $\forall r\in R: 0\cdot r=0\cdot r+r\cdot r-r\cdot r=(0+r)r-r^2=r^2-r^2=0$ és hasonlóan $r\cdot 0=0$. Eszerint ha egy R gyűrűben a 0 jobb- vagy baloldali egységelem, akkor minden r elemre $r=r\cdot 0=0$ ill. $r=0\cdot r=0$, tehát R a triviális gyűrű.

7.1.2 Definíció: az R gyűrű a eleme bal- illetve jobboldali nullosztó, ha R valamely 0-tól különböző x elemére $ax=0$ ill. $xa=0$. Az R gyűrű nullosztómentes, ha egyetlen nullosztója a 0, azaz $(a\neq 0, b\neq 0)\Rightarrow ab\neq 0$. Ez ekvivalens azzal, hogy $(ab=0, a\neq 0)\Rightarrow b=0$.

7.1.3 Definíció: az R egységelemes gyűrű u eleme egység, ha valamely $v\in R$-re $uv=vu=1$. Ezek csoportot alkotnak a szorzásra nézve, jele $U(R)$.

Megjegyzés: ha u-nak van balinverze, akkor nem balnullosztó. Ugyanis a balinverzet v-vel jelölve $u\in U(R), ux=0$ esetén $x=(vu)x=v\cdot 0=0$. Hasonlóan egy jobbinverzzel rendelkező elem nem jobbnullosztó. Speciálisan $U(R)$-ben nincs nullosztó.

Megjegyzés: az előző definícióban fontos kikötni, hogy v kétoldali inverz legyen, mert megeshet egy egységelemes gyűrű elemével, hogy csak féloldali inverze van. Pl. ha V egy K feletti, megszámlálható dimenziós vektortér, akkor V endomorfizmusai gyűrűt alkotnak (ld. **7.2.8**). Rendelje az $(a_1,a_2,a_3,\ldots)$ vektorhoz a φ leképezés $(0,a_1,a_2,a_3,\ldots)$-t, ψ pedig $(a_2,a_3,a_4,\ldots)$-t. Ekkor $\varphi\psi$ az identitás, de ψ-nek nincs jobboldali inverze, hiszen $Im\,\psi\neq V$, φ-nek pedig nincs baloldali inverze, hiszen $Ker\,\varphi\neq\{0\}$. Sőt, π-vel jelölve az első koordináta-függvényt $\varphi\pi=\pi\psi=0$, azaz φ baloldali, ψ jobboldali nullosztó.

7.1.4 Definíció: az R gyűrű ferde test, ha R egységelemes és minden elemének van a szorzásra nézve inverze, azaz ha $mul(R)=(R\setminus\{0\},\cdot)$ csoportot alkot. Ha ez a csoport kommutatív, akkor R (kommutatív) test.

7.1.5 Definíció: R_1 részgyűrűje az R gyűrűnek, ha **(1)** mint halmaz részhalmaza R-nek és **(2)** gyűrűt alkot az R-beli műveletekre nézve. Jelölése $R_1\leq R$.

Azt állítjuk, hogy egy gyűrű valamely H részhalmaza pontosan akkor zárt az összedásra és az ellentettképzésre, ha bármely két elemének különbségét is tartalmazza. Az $(a-b)=a+(-b)$ definícióból az egyik irány következik. $H=\emptyset$ esetén a másik irány is triviális, legyen tehát $a\in H$. A második feltételt alkalmazva az a,a számpárra kapjuk, hogy $0\in H$, majd tetszőleges $b\in H$ esetén a $0,b$ párral $(-b)\in H$ és végül tetszőleges $b,c\in H$ párra $b,(-c)$ behelyettesítésével $b+c\in H$, ezzel a másik irányt is beláttuk.

7.1.6 Állítás: ha **7.1.5.1** teljesül, akkor **7.1.5.2**-vel ekvivalens, hogy **(2a)** R_1 nem üres, zárt az R-beli műveletekre és minden elemének ellentettjét is tartalmazza (azaz zárt a szorzásra és a kivonásra).

Ugyanis ha R_1 részgyűrű, akkor nem lehet üres (nincs 0 elemű gyűrű) és definíció szerint zárt a műveletekre. Ha pedig **(2a)** teljesül, akkor $\exists a\in R_1$. Ezért $0=(a-a)\in R_1$ és ez valóban nulleleme R_1-nek. Eszerint R_1 elemeinek van R_1-ben ellentettje R_1 nulleleme szerint, mégpedig az R-beli ellentettjük, így **(R4)** és **(R5)** teljesül R_1-re. Az $\{\mathbf{(R}i\mathbf{)}\,|\,i\in\{2,3,7,8,9\}\}$ műveleti szabályok átöröklődnek, **(R1)**-et és **(R6)**-ot pedig kikötöttük. Tehát R_1 valóban gyűrű lesz, állításunknak megfelelően.

Az imént azt is beláttuk, hogy a többi feltétel teljesülése esetén R_1 pontosan akkor nem üres, ha $0\in R_1$. Tehát:

7.1.7 Állítás: $R_1\leq R$ pontosan akkor teljesül, ha **(1)** $0\in R_1\subseteq R$ és **(2)** R_1 zárt a kivonásra és a szorzásra.

7.1.8 Állítás: részgyűrűk tetszőleges metszete részgyűrű. (Ellenőrizzük az előző állítás feltételeit!)

7.1.9 Definíció: az R gyűrű egy X részhalmaza által generált részgyűrű az X-et tartalmazó részgyűrűk metszete, jelölése $\langle X\rangle$. A fenti állítás szerint $X\subseteq\langle X\rangle\leq R$ és nyilván ez a legszűkebb ilyen részgyűrű. Ez nyilván megegyezik az X elemeiből a kivonás és szorzás műveletekkel véges sok lépésben megkapható elemek halmaza, azaz a disztributivitás figyelembevételével $\{\sum_{k=1}^{n}(\pm\prod_{i=1}^{s_k}x_{k,i})\,|\,n\in\mathbb{N},s_k\in\mathbb{Z}^+,x_{k,i}\in X\}$. (Az üres összeg definíció szerint 0.)

7.2 Példák, konstrukciók gyűrűkre

Egységelemes, nullosztómentes, kommutatív gyűrű az egész számok halmaza a szokásos műveletekkel, jele $\mathbb{Z}$. Nem egységelemes pl. $2\mathbb{Z}$, a páros számok gyűrűje.

7.2.1 Definíció: tetszőleges $(A,+)$ Abel-csoportra az A feletti zérógyűrű az az $(A,+,\cdot)$ gyűrű, ahol $\forall a,b\in A\colon a\cdot b=0$.

7.2.2 Definíció: legyen R tetszőleges gyűrű. Ekkor R oppozit gyűrűje az az R^{op} gyűrű, amelyre $(R^{\mathrm{op}},+)=(R,+)$ és az R^{op}-beli '$\circ$' szorzás $a\circ b=b\cdot a$. Ez általában nem izomorf (ld. később) R-el. Pl. ha az R-beli szorzás $a\cdot b:=b$ (ez gyűrűt ad), akkor R-ben minden elem baloldali egységelem és nincs jobboldali egységelem; R^{op}-ban ez pont fordítva van.

7.2.3 Definíció: tetszőleges R gyűrűre $M_n(R)$ az $n\times n$-es mátrixok gyűrűje (a pozíciónkénti összeadás, mátrixszorzás műveletekkel). $n=1$ esetben ez R, egyébként nem kommutatív, nem nullosztómentes. Pontosan akkor egységelemes, ha R az volt.

7.2.4 Definíció: $R[x]=\{\sum_{i=0}^{n}a_ix^i\,|\,n\in\mathbb{N},a_i\in R\}$ az R feletti polinomgyűrű. Ezt lehetőleg csak egységelemes R esetén használjuk. Ha R kommutatív és/vagy nullosztómentes, akkor $R[x]$ is az lesz. Egységeleme az azonosan 1 polinom, ha $\exists 1\in R$.

7.2.5 Definíció: az $x_1,\dots,x_n$ változókra $R[x_1,\dots,x_n]$ ezen változók polinomjainak halmaza, azaz $\{\sum_{i=1}^{r}c_i\cdot x_1^{s_i(1)}x_2^{s_i(2)}\dots x_n^{s_i(n)}\,|\,r\in\mathbb{N},s_i\colon\{1\dots n\}\to\mathbb{N},s_i\neq s_j \text{ ha } i\neq j\}$. Ez azonos $R[x_1][x_2]\dots[x_n]$-el és független az x_i-k sorrendjétől. Változók egy X halmazára $R[X]$ az X-beli változók polinomjainak halmaza. Ez éppen $\bigcup_{\mathbf{X}\subseteq X,\,|\mathbf{X}|\in\mathbb{N}}R[\mathbf{X}]$. Ha R kommutatív és/vagy nullosztómentes, akkor $R[X]$ is az. Ha R egységelemes, akkor $R[X]$-nek egységeleme az azonosan 1 polinom.

7.2.6 Definíció: $R[[x]]=\{\sum_{n\in\mathbb{N}}a_nx^n\,|\,a_n\in R\}$ az R feletti formális hatványsorok gyűrűje. Pontosan akkor egység-elemes, kommutatív vagy nullosztómentes, ha R az volt.

7.2.7 Definíció: legyen d négyzetmentes, 0-tól és 1-től különböző egész szám. Ekkor $\mathbb{Z}[\sqrt{d}]=\{a+b\sqrt{d}\in\mathbb{C}\,|\,a,b\in\mathbb{Z}\}$ a „logikus" műveletekkel (úgy teszünk, mintha $\sqrt{d}$ R feletti polinomjairól lenne szó, csak $(\sqrt{d})^2$ helyére mindig d-t írunk). Például $\mathbb{Z}[\sqrt{-1}]=\mathbb{Z}[i]$ a Gauss-egészek gyűrűje.

Megjegyzés: $R[q]$ tetszőleges gyűrű és benne nem szereplő elem esetén R q-val való bővítését jelenti; ebben úgy számolunk, mintha q polinomjairól lenne szó R felett, csak elvégezzük a lehetséges egyszerűsítéseket. (Pl. ha q-t egy R feletti p polinom R-en kívüli gyökének választottuk, akkor $p(q)$ többszöröseit 0-nak tekintjük. Ez erősen hasonlít arra, ahogy különböző csoportokat szabadcsoportok faktorcsoportjaként adtunk meg.) $R[H]$ jelöli azt a gyűrűt, melyet úgy kapunk R-ből, hogy sorra bővítjük H elemeivel.

A bővített gyűrű pontosan akkor egységelemes vagy kommutatív, ha R az volt.

7.2.8 Definíció: legyen $(A,+)$ Abel-csoport. Definiáljuk A endomorfizmusai között az alábbi műveleteket: $\varphi+\psi: a\mapsto a\varphi+a\psi$, $\varphi\cdot\psi: a\mapsto(a\varphi)\psi$. Könnyen ellenőrizhető, hogy egységelemes gyűrűt kapunk, ez A endomorfizmusgyűrűje. Jelölése $End(A)$

7.2.9 Definíció: legyen R egységelemes gyűrű, G csoport. Az RG csoportgyűrű alaphalmaza legyen a következő: $\{\sum_{i=1}^{k} r_i g_i \,|\, k\in\mathbb{N}, 0\neq r_i\in R, g_i\in G, g_i\neq g_j \text{ ha } i\neq j\}$. Az összeadást úgy végezzük, mintha G elemeinek R feletti polinomjairól lenne szó (tehát g_i együtthatóit adjuk össze). Szorzásnál a két összeget tagonként beszorozzuk, majd az $(r_ig_i)(r_jg_j)$ alakú szorzatok helyére rendre $(r_ir_j)(g_ig_j)$-t írunk és elvégezzük a szorzást a két gyűrűelem ill. a két csoportelem között; végül a kapott összeget G elemei szerint csoportosítjuk. Ha $R=K$ test, akkor KG-t csoportalgebrának hívjuk. Fontos speciális eset, ha $|G|=n<\infty$; ekkor $KG=\{\sum_{i=1}^{n}\alpha_i g_i \,|\, \alpha_i\in K, \{g_1,\dots,g_n\}=G\}$.

7.3 Ideál definíciója, alaptulajdonságai. Faktorgyűrű

7.3.1 Definíció: az R gyűrű L részhalmaza balideál, ha nem üres (ez a következő feltétel miatt ekvivalens lesz $0\in L$-el), bármely két elemének különbségét tartalmazza és $\forall a\in L, r\in R: r\cdot a\in L$. J jobbideál, ha teljesíti az első két feltételt és $\forall a\in J, r\in R: a\cdot r\in J$. Nyilván minden bal- és jobbideál részgyűrű. $I\subseteq R$ ideál, ha jobb- és balideál, azaz ha **(I1)** $0\in I\subseteq R$, **(I2)** $\forall a,b\in I: (a-b)\in I$ és **(I3)** $\forall a\in I, r\in R: r\cdot a\in I, a\cdot r\in I$. Jelölése $I\lhd R$. A bal- ill. jobbideálokat esetleg $L\lhd_b R, J\lhd_j R$, jelöli.

7.3.2 Definíció: az R gyűrű egyszerű, ha $R\neq\{0\}$ és $I\lhd R\Rightarrow(I=\{0\}$ vagy $I=R)$.

7.3.3 Állítás: Balideálok metszete balideál, jobbideálok metszete jobbideál, ideálok metszete ideál. (Ellenőrizzük a definíció feltételeit!)

7.3.4 Definíció: $X\subseteq R$ esetén az X által generált balideál / jobbideál / ideál az X-et tartalmazó ~ok metszete. Ez valóban egy X-et tartalmazó ~ lesz az előző állítás szerint és nyilván ezek közül a legszűkebb. A generált ideál jelölése (X). A generált bal- ill. jobbideált végszükség esetén $(X)_b$-vel ill. $(X)_j$-vel jelöljük.

7.3.5 Definíció: főideálnak nevezzük az egy elem által generált ideált.

Legyen most $a\in R$. Mi lesz $(a)_b$? Egy a-t tartalmazó balideálban benne kell legyen $\{na+r\cdot a \,|\, n\in\mathbb{Z}, r\in R\}$ minden eleme, hiszen zárt a kivonásra és bármely gyűrűelemmel való szorzásra. Szerencsére ez szemmel láthatóan egy a-t tartalmazó balideál, így épp a legszűkebb ilyen. Eszerint $(a)_b=\{na+r\cdot a \,|\, n\in\mathbb{Z}, r\in R\}$. Hasonlóan $(a)_j=\{na+a\cdot r \,|\, n\in\mathbb{Z}, r\in R\}$. Egységelemes gyűrűben a disztributivitás miatt $na=(n\cdot 1)\cdot a=a\cdot(n\cdot 1)$, így na előáll mind $r\cdot a$, mind $a\cdot r$ alakban, tehát $(a)_b=\{r\cdot a \,|\, r\in R\}$ és $(a)_j=\{a\cdot r \,|\, r\in R\}$ lesz.

Az a által generált ideál $(a)=\{na+r_0\cdot a+a\cdot s_0+\sum_{i=1}^{k} r_i\cdot a\cdot s_i \,|\, n\in\mathbb{Z}; k\in\mathbb{N}; r_i, s_i\in R\}$ lesz, mert egy a-t tartalmazó ideálban minden ilyen elemnek benne kell lennie, ez pedig ideál. Ha R egységelemes, akkor az „na" tag feleslegessé válik, továbbá $r_0\cdot a=r_0\cdot a\cdot 1$ és $a\cdot s_0=1\cdot a\cdot s_0$ miatt a második és harmadik tag is bevihető az összegbe, tehát $(a)=\{\sum_{i=1}^{k} r_i a s_i \,|\, \dots\}$. Ha R kommutatív, akkor $(a)=(a)_j=(a)_b$, ha pedig kommutatív és egységelemes, akkor $(a)=a\cdot R$.

7.3.6 Állítás: R pontosan akkor nullosztómentes, ha az $xa=b$ egyenletnek legfeljebb egy megoldása van tetszőleges $a\in R\setminus\{0\}, b\in R$ elemekre.

Bizonyítás: ha R nem nullosztómentes akkor $\exists a,b\in R\setminus\{0\}: ab=0$, tehát az $ax=0$ egyenletnek b és 0 két különböző megoldása. Ha pedig R nullosztómentes, $a\in R\setminus\{0\}, b\in R$ és $ax_1=ax_2=b$, akkor $a(x_1-x_2)=0$ miatt $x_1-x_2=0$, tehát a két megoldás azonos.

7.3.7 Állítás: az R gyűrűben $xa=b$ pontosan akkor oldható meg minden $a\in R\setminus\{0\}, b\in R$ esetén, ha R ferde test

Bizonyítás: ha ferdetest, akkor $x=ba^{-1}$ megoldás. Lássuk most a másik irányt, azaz legyen $xa=b$ megoldható, ha $b\neq 0$.

⊡ R nullosztómentes. Ehhez tegyük fel, hogy $ab=0, a\neq 0$ és lássuk be, hogy $b=0$. $a\neq 0\Rightarrow\forall x\,\exists y: ya=x$, azaz $\forall x: xb=yab=y\cdot 0=0$, így $\nexists x: xb=a$. A feltétel szerint tehát $b=0$. **7.3.6** szerint ⊡ az $xa=b$ egyenlet megoldása minden $a\in R\setminus\{0\}, b\in R$ párra egyértelmű. Jelölje ezt $[b/a]$.

Ha $a,b\in R$ nemnulla elemek, akkor $(a-a\cdot[b/b])\cdot b=ab-ab=0$, így ⊡ alapján $a\cdot[b/b]=a$, amiből ⊡ miatt $[a/a]=[b/b]$. Eszerint értelmes definíció $e:=[a/a]$, ahol a tetszőleges nem 0 elem és az így kapott e jobboldali egységelem. Ismét ⊡

szerint minden nem 0 elemnek van (egyértelmű) jobbinverze. Mint a csoportokról szóló fejezetben beláttuk, ebből következik, hogy $(R\setminus\{0\},\cdot)$ csoport. Ezzel az állítást beláttuk.

Ha R ferde test, akkor a feltétel nyilván teljesül.

7.3.8 Tétel: R-nek pontosan akkor nincs nem triviális balideálja (tehát ${}_RR$ pontosan akkor egyszerű, ld. később), ha R ferde test vagy prímrendű zérógyűrű.

Bizonyítás: $\Leftarrow$: ha R ferde test és az L balideáljára $\{0\}\neq L<R$, akkor $\exists a\in L: a\neq 0$. Tehát $L\supseteq RL\,(\text{komplexusszorzat})\supseteq Ra=R$. Ha R prímrendű zérógyűrű, akkor még nem triviális additív részcsoportja sincs.

$\Rightarrow$: ha R zérógyűrű, akkor minden additív részcsoport ideál. Ha nincs nem triviális ideálja, akkor $(R,+)$ egyszerű kell legyen; ez csak Z_p lehet. Marad az az eset, amikor R nem zérógyűrű.

$\nexists$ R nem nullosztómentes, azaz $\exists a\neq 0, b\neq 0: ab=0$. Ekkor $L=\{x\in R\,|\,xb=0\}$ balideál R-ben. $a\in L$ miatt $L\neq\{0\}\Rightarrow L=R$, azaz $Rb=\{0\}$. $I=\{y\in R\,|\,Ry=\{0\}\}$ ideál R-ben és $b\in I\Rightarrow I\neq\{0\}\Rightarrow I=R$. Így az $R\cdot R$ komplexusszorzat $\{0\}$, tehát R mégiscsak zérógyűrű, $\lightning$. R tehát nullosztómentes. Tekintsük Ra-t, ahol $a\neq 0$ tetszőleges. Ez egy balideál és nem $\{0\}$, mert R nullosztómentes és $a\neq 0$. Következésképp $Ra=R$, tehát $xa=b$ minden $b\in R$-re megoldható. Teljesül **7.3.7** feltétele, így R ferde test.

7.3.9 Állítás: ha $I,J\triangleleft R$, akkor az általuk generált ideál $(I,J)=I+J$.

Bizonyítás: legyen $H=I+J$. $0\in H$, mert $0=0+0$, ahol $0\in I$ és $0\in J$. Tetszőleges $x,y\in H$ elemek különbsége felírható $x-y=(a+b)-(a'-b')=(a-a')+(b-b')$ alakban, ahol $a,a'\in I; b,b'\in J$. Az első tag I-ben, a második J-ben van, hiszen ideálok, így $(x-y)\in H$. Tetszőleges $r\in R$ és $x=a+b\in H: a\in I, b\in J$ elemekre $xr=(a+b)r=ar+br\in H$ és $rx=r(a+b)=ra+rb\in H$. Tehát H teljesíti **(I1)**-t, **(I2)**-t és **(I3)**-t $\Rightarrow I\cup J\subseteq H\triangleleft R\Rightarrow (I,J)\subseteq H$. Másrészt (I,J) zárt kell legyen az összeadásra és tartalmazza I-t és J-t, így $(I,J)\supseteq H$. Ezzel az állítást beláttuk.

Ha I és J bal- ill. jobbideálok, akkor $I+J$ az általuk generált bal- ill. jobbideál.

7.3.10 Definíció: ha $I,J\triangleleft R$, akkor $I\cdot J$ ne a komplexusszorzatot jelölje (az nem feltétlenül ideál), hanem a komplexusszorzat által generált ideált. Ez könnyen ellenőrizhetően $P=\{\sum_{i=1}^{k}a_ib_i\,|\,a_i\in I, b_j\in J\}$. (Ennél szűkebb nem lehet és ez szerencsére ideál. Sőt, P már akkor is ideál lesz, ha I bal-, J pedig jobbideál.)

7.3.11 Állítás: ha $I,J\triangleleft R$, akkor $I\cdot J\subseteq I\cap J$. Ehhez elegendő, hogy a komplexusszorzat minden eleme a metszetben van. Legyen $a\in I, b\in J$ tetszőleges. Ekkor $ab\in I$, mert I balideál és $ab\in J$, mert J jobbideál $\Rightarrow ab\in I\cap J$, márpedig ab a komplexusszorzat egy tetszőleges eleme volt.

7.3.12 Definíció: legyen $I\triangleleft R$. Ekkor az R/I faktorgyűrű vagy maradékosztály-gyűrű elemei az $\{a+I\,|\,a\in R\}$ halmazok (ezek I mellékosztályai az $(R,+)$ csoportban). A műveletek: $(a+I)+(b+I):=(a+b)+I$ és $(a+I)(b+I):=ab+I$. Le kell persze ellenőrizni, hogy ez jóldefiniált (tehát a definíció nem függ a reprezentáló elemek választásától) és hogy a kapott struktúra gyűrű lesz. Íme:

Legyenek a és a' ill. b és b' ugyanazon maradékosztályok elemei, azaz $a-a'\in I, b-b'\in I$. Azt kell belátnunk, hogy $(a+b)+I=(a'+b')+I$ és $ab+I=a'b'+I$, azaz $(a+b)-(a'+b)\in I$ és $ab-a'b'\in I$. Az első kifejezést átalakítva $(a+b)-(a'+b')=(a-a')+(b-b')$ két I-beli elem összege, tehát I-beli. A második $ab-a'b'=(a-a')b+a'(b-b')$; itt az első tag azért van I-ben, mert jobbideál, a másik pedig azért, mert balideál, így az összegük is I-beli.

Megjegyzés: a bizonyításból látszik, hogy ha R nem kommutatív és I csak bal- vagy csak jobbideál, akkor a szorzás nem feltétlenül jóldefiniált. Az is látszik, hogy az $(a+I)$, $(b+I)$ maradékosztályok komplexusszorzata része $(ab+I)$-nek. Viszont nem feltétlenül azonos vele (pl. ha R zérógyűrű és $I\neq\{0\}$, akkor nem).

7.3.13 Definíció: a $\varphi: R_1\to R_2$ leképezés homomorfizmus, ha művelettartó. Ebből következik például, hogy $0\varphi=0$ és $(-a)\varphi=-a\varphi$. Viszont könnyen megeshet, hogy R_1 és R_2 is egységelemes, de $1\varphi\neq 1$ (ld. $R\to R^2$ injekció). A homomorfizmus képe $Im\,\varphi=\{a\varphi\,|\,a\in R_1\}$, magja $Ker\,\varphi=\{a\in R_1\,|\,a\varphi=0\}$. Nyilván $Im\,\varphi\leq R_2$.

7.3.14 Definíció: a $\varphi: R_1\to R_2$ leképezés izomorfizmus, ha homomorfimus és bijekció, jele $\varphi: R_1\xrightarrow{\sim} R_2$. Ha valamely R_1,R_2 gyűrűkhöz található ilyen izomorfizmus, akkor izomorfak, jele $R_1\simeq R_2$ vagy $R_1\overset{\varphi}{\simeq}R_2$. Ez nyilván ekvivalencia-reláció.

7.3.15 Állítás: $Ker\,\varphi\triangleleft R_1$. (A definíció feltételei egyszerű számolással ellenőrizhetőek.)

Az is látható, hogy minden I ideál előáll, mint az $R\to R/I$ természetes homomorfizmus ($\psi_I: a\mapsto a+I$) magja.

7.3.16 Homomorfizmus-tétel: legyen $\varphi: R_1\to R_2$ homomorfizmus. Ekkor $Im\,\varphi\simeq R_1/Ker\,\varphi$. Az eddigi homomorfizmus-tételekkel gyakorlatilag azonos módon bizonyítható.

7.4 Modulus, faktormodulus

7.4.1 Definíció: M baloldali R-modulus, ha Abel-csoport valamilyen összeadás műveletre, továbbá balról meg tudjuk szorozni M elemeit R elemeivel, ez a szorzás mindkét tényező szerint disztributív a megfelelő halmazbeli összedásra és asszociatív az R feletti szorzással. Azaz

(M1) $+: M\times M\to M$
(M2) $\forall m_1,m_2,m_3\in M: m_1+(m_2+m_3)=(m_1+m_2)+m_3$
(M3) $\forall m_1,m_2\in R: m_1+m_2=m_2+m_1$
(M4) $\exists 0\in M: \forall m\in M: m+0=m$
(M5) $\forall m\in R: \exists(-m)\in R: m+(-m)=0$
(M6) $\cdot: R\times M\to M$
(M7) $\forall r_1,r_2\in R, m\in M: r_1\cdot(r_2\cdot m)=(r_1r_2)\cdot m$
(M8) $\forall r\in R, m_1,m_2\in M: r\cdot(m_1+m_2)=r\cdot m_1+r\cdot m_2$
(M9) $\forall r_1,r_2\in R, m\in M: (r_1+r_2)\cdot m=r_1\cdot m+r_2\cdot m$

Hasonlóan definiáljuk a jobboldali R-modulusokat. (Ezek nem csak nevükben különböznek a baloldali modulusoktól. Ha ugyanis az $m\in M$ elemet megszorozzuk az r_1r_2 szorzattal, akkor jobboldali modulusnál az első, baloldaliaknál a második tényezővel kell először szorozni.) Kommutatív gyűrűnél a jobb - és baloldali modulusokat felesleges megkülönböztetni. Arra, hogy M bal- ill. jobboldali R-modulus, az ${}_RM$ ill. M_R jelölésekkel utalhatunk.

Az egyszerűség kedvéért (majdnem) minden állítást, definíciót stb. baloldali modulusokra fogalmazunk meg. Ugyanezeket el lehetne mondani jobboldali modulusokra is.

7.4.2 Definíció: az M R-modulus unitális, ha R egységelemes és az 1-el való szorzás identitás M-en, azaz $\forall m\in M: 1\cdot m=m$. Ha például R test, akkor az R feletti unitális modulusok a vektorterek.

7.4.3 Definíció: az R feletti M modulus N részhalmaza részmodulus, ha R-modulus az M-ből örökölt műveletekre nézve. Ez nyilván ekvivalens azzal, hogy **(1)** $0\in N$ és **(2)** zárt az M feletti kivonásra és az R elemeivel való szorzásra. Jelölése $N\le M$.

Megjegyzés: R-t tekinthetjük önmaga feletti (bal- vagy jobboldali) modulusnak („szabad modulus"). Ekkor a balideálok éppen ${}_RR$, a jobbideálok R_R részmodulusai.

7.4.4 Definíció: részmodulusok metszete nyilván részmodulus. Eszerint van értelme a $H\subseteq {}_RM$ halmaz által generált részmodulusról beszélni: ${}_R\langle H\rangle=\langle H\rangle := \bigcap_{H\subseteq N\le M} N$, a legszűkebb H-t tartalmazó részmodulus.

7.4.5 Definíció: legyen ${}_RN\le {}_RM$. Ekkor az M/N faktormodulus elemei $\{a+M \mid a\in M\}$. Az összeadás legyen az, amit az $(M,+)/(N,+)$ faktorcsoportból kapunk (tehát $(a+N)+(b+N):=(a+b)+N$). A szorzás $r\cdot(a+N):=r\cdot a+N$. A szokásos számolással belátható, hogy a szorzás jóldefiniált és a kapott struktúra baloldali R-modulus.

7.4.6 Definíció: legyen L balideál R-ben. Ekkor R/L alatt az ${}_RR/{}_RL$ faktormodulust értjük.

7.4.7 Definíció: a $\varphi: {}_RM\to {}_RN$ leképezés homomorfizmus, ha művelettartó. Izomorfizmus, ha még bijektív is; ekkor $M\simeq N$. Képe $Im\,\varphi=\{m\varphi \mid m\in M\}$, magja $Ker\,\varphi=\{m\in M \mid m\varphi=0\}$. Nyilván $Im\,\varphi\le N, Ker\,\varphi\le M$.

7.4.8 Homomorfizmus-tétel: ha M és N R-modulusok, φ pedig egy $M\to N$ homomorfizmus, akkor $Im\,\varphi\simeq M/Ker\,\varphi$. (Bizonyítása a szokásos.) Egyben észrevehetjük, hogy M minden M' részmodulusa előáll a $\varphi_{M'}(M\to M/M'): m\mapsto(m+M')$ természetes homomorfizmus magjaként.

7.4.9 Izomorfizmus-tétel: egy R-modulus M,N részmodulusaira $M+N/M\simeq N/N\cap M$. A csoportelméletnél szereplőhöz hasonló módon bizonyítható.

7.4.10 Definíció: az M modulus egyszerű, ha $M\neq\{0\}$ és $N\le M\Rightarrow(N=\{0\}$ vagy $N=M)$, azaz csak triviális részmodulusa van.

7.5 Modulusok, gyűrűk direkt összege. Féligegyszerű modulusok

7.5.1 Definíció: legyenek M_1, M_2 R-modulusok. Ezek $M_1 \oplus M_2 = M$ külső direkt összegének alaphalmaza $\{(a,b) \mid a \in M_1, b \in M_2\}$; az összeadás és az $r \in R$ elemmel való szorzás történjék komponensenként, azaz $(a,b)+(a',b') := (a+a', b+b')$ és $r \cdot (a,b) := (r \cdot a, r \cdot b)$.

Tekintsük most az $\{(a,0) \in M \mid a \in M_1\} = \overline{M}_1 \simeq M_1$ és az $\{(0,b) \in M \mid b \in M_2\} = \overline{M}_2 \simeq M_2$ részmodulusokat M-ben. Ezek metszete $\{0\}$ (vagy – ha jobban tetszik – $\{(0,0)\}$) és együtt generálják a direkt összeget, azaz $\overline{M}_1 + \overline{M}_2 = M$.

7.5.2 Definíció: M az M_1, M_2 részmodulusok belső direkt összege, ha **(1)** $M_1 \cap M_2 = \{0\}$ és **(2)** $M_1 + M_2 = M$. Akárcsak a csoportoknál, e két feltétel ekvivalens azzal, hogy M minden m eleme egyértelműen áll elő $m = a+b \; : \; a \in M_1, b \in M_2$ alakban. Az egyértelmű előállításból látható, hogy ekkor M izomorf az $M_1 \oplus M_2$ külső direkt összeggel. (Így hát jogosan használjuk ugyanazt a jelölést a kétféle direkt összegre.) Terjesszük ki a definíciót több tagra:

7.5.3 Definíció: M belső direkt összege az $\{M_\alpha \mid \alpha \in \mathbf{I}\}$ részmodulusainak, ha **(1)** $\langle M_\alpha \mid \alpha \in \mathbf{I} \rangle = M$ és **(2)** $\forall \alpha \in \mathbf{I}: M_\alpha \cap \langle M_\beta \mid \beta \in \mathbf{I} \setminus \{\alpha\} \rangle = \{0\}$. Jelölése $M = \bigoplus_{\alpha \in \mathbf{I}} M_\alpha$. Ez ekvivalens azzal, hogy M elemei egyértelműen állnak elő olyan véges összegként, melynek minden tagja különböző M_α részmodulusok eleme.

A többtényezős külső direkt összeg alaphalmaza az olyan $\mu: \mathbf{I} \to \bigcup M_\alpha, \forall \alpha: \mu_\alpha \in M_\alpha$ függvényekből áll, melyeknél véges sok α kivételével minden koordináta a megfelelő modulus nulleleme. (Ez utóbbi feltétel jelenti azt, hogy $\{M_\alpha \mid \alpha \in \mathbf{I}\}$ generálja M-et.) A műveleteket koordinátánként végezzük. Véges $\mathbf{I}$ esetén ez a definíció ugyanazt adja, mintha a $\oplus$ kétváltozós, izomorfia erejéig asszociatív és kommutatív műveletből definiáltuk volna.

Megjegyzés: a direkt összeg fenti definícióiban semmi meglepő újdonság nem szerepel. Az M_α tényezők direkt összegét úgy definiáltuk, hogy mint Abel-csoportokat tekintettük őket, csak azt is megköveteltük tőlük, hogy R-modulusok legyenek.

7.5.4 Definíció: az R_1, R_2 gyűrűk $R_1 \oplus R_2 = R$ külső direkt összegének alaphalmaza $\{(a,b) \mid a \in R_1, b \in R_2\}$, a műveletek a koordinátánkénti műveletek. Könnyen ellenőrizhető, hogy ez valóban gyűrű lesz. Az $\{(a,0) \in R \mid a \in R_1\} = \overline{R}_1 \simeq R_1$ és $\{(0,b) \in R \mid b \in R_2\} = \overline{R}_2 \simeq R_2$ ideálok metszete $\{0\}$ és együtt generálják R-t.

7.5.5 Állítás: legyenek R_1 és R_2 ideálok R-ben, továbbá ${}_R R = {}_R(R_1) \oplus_R (R_2)$. Ekkor $R \simeq R_1 \oplus R_2$.

Bizonyítás: a második feltétel szerint R minden r eleme egyértelműen áll elő $r = a+b \; : \; a \in R_1, b \in R_2$ alakban. Lássuk be, hogy $\varphi(R \to R_1 \oplus R_2): a+b \longmapsto (a,b)$ izomorfizmus! Az triviális, hogy bijekció, így elég, hogy művelettartó. Legyen a és b két tetszőleges R-beli elem, $a = a_1 + a_2, b = b_1 + b_2 \; : \; a_1, b_1 \in R_1; a_2, b_2 \in R_2$. Ekkor $(a+b)\varphi = (a_1 + a_2 + b_1 + b_2)\varphi = \big((a_1 + b_1) + (a_2 + b_2)\big)\varphi = (a_1 + b_1, a_2 + b_2) = a\varphi + b\varphi$, tehát φ az összeadást megtartja. $(ab)\varphi = (a_1 b_1 + a_2 b_2 + a_1 b_2 + a_2 b_1)\varphi$. Itt $a_1 b_2 \in R_1$, mert $a_1 \in R_1 \lhd R$, továbbá $a_1 b_2 \in R_2$, mert $b_2 \in R_2 \lhd R$. Viszont ${}_R(R_1) \cap {}_R(R_2) = \{0\}$, tehát $a_1 b_2 \in R_1 \cap R_2 = \{0\}$-ből $a_1 b_2 = 0$. Hasonlóan $a_2 b_1 = 0$. Ezt visszahelyettesítve: $(ab)\varphi = (a_1 b_1 + a_2 b_2)\varphi = (a_1 b_1, a_2 b_2) = (a_1, a_2) \cdot (b_1, b_2) = a\varphi \cdot b\varphi$. Így φ valóban homomorfizmus, az állítást beláttuk.

7.5.6 Definíció: R belső direkt összege az $\overline{R}_1, \overline{R}_2$ ideáloknak, ha $\overline{R}_1 \cap \overline{R}_2 = \{0\}$ és $\overline{R}_1 + \overline{R}_2 = R$.

Megjegyzés: **7.5.5** segítségével könnyen belátható, hogy a belső és a külső direkt szorzat lényegében ugyanaz. Definiálhatnánk a többtényezős direkt szorzatokat is, kimondhatnánk és bebizonyíthatnánk **7.5.5** többtényezős változatát – de nem tesszük.

7.5.7 Lemma: tegyük fel, hogy az M modulus minden részmodulusa direkt összeadandó, azaz $\forall N \leq M \; \exists N^* \leq M: N \oplus N^* = M$. Ekkor $M_1 \leq M \Rightarrow M_1$ minden részmodulusa direkt összeadandó M_1-ben.

Bizonyítás: legyen $N \leq M_1 \leq M$. Ekkor $\exists N^* \leq M: N \oplus N^* = M$. Lássuk be, hogy $M_1 = N \oplus N^{**}$, ahol $N^{**} = N^* \cap M_1$. Legyen $m \in M_1$ tetszőleges. $M = N \oplus N^*$ miatt m előáll $m = n + n^* \; (n \in N, n \in N^*)$ alakban. $n^* = m - n \; : \; m \in M_1, n \in N \leq M_1$ miatt $n^* \in M_1 \Rightarrow n^* \in M_1 \cap N^* = N^{**}$. Eszerint M_1 minden eleme előáll egy N-beli és egy N^{**}-beli elem összegeként és az előállítás $N \cap N^{**} \subseteq N \cap N^* = \{0\}$ miatt egyértelmű. Ezt akartuk belátni.

7.5.8 Lemma: ha M minden részmodulusa direkt összeadandó és $\{0\} \neq M_1 \leq M$, akkor M_1-nek van egyszerű részmodulusa.

Bizonyítás: legyen $m \in M_1 \setminus \{0\}$. Legyen most N egy olyan részmodulusa M_1-nek, amely nem tartalmazza m-et és erre a tulajdonságra nézve maximális. (Az ilyen tulajdonságú részmodulusok H halmaza nem üres, hiszen $\{0\} \in H$

és bármely $\mathcal{L}\subseteq\mathcal{H}$ láncra $(\bigcup\mathcal{L})\in\mathcal{H}$. A Zorn-lemma szerint tehát $\mathcal{H}$-nak van maximális eleme.) **7.5.7** szerint $\exists N^*\le M_1: M_1=N\oplus N^*$. Azt állítjuk, hogy N^* egyszerű. ↑ N^*-nak van egy nem triviális L részmodulusa. Ismét **7.5.7** alapján $N^*=L\oplus L^*$, ahol sem L, sem L^* nem $\{0\}$. Ekkor $N\oplus L$ és $N\oplus L^*$ (jogos a direkt összeg jelölése, hiszen $L,L^*\le N^*$ miatt N-el vett metszetük $\{0\}$) egyaránt bővebb N-nél. Feltételeink szerint ez csak úgy lehetséges, ha mindkettő tartalmazza m-et. Ekkor m felírható $m=n_1+l\ :\ n_1\in N, l\in L\subseteq N^*$ és $m=n_2+l^*\ :\ n_1\in N, l^*\in L^*\subseteq N^*$ alakban is. De m egyértelműen áll elő egy N-beli és egy N^*-beli elem összegeként, azaz $l=l^*$. Ez benne kell legyen $L\cap L^*=\{0\}$ -ban $\Rightarrow$ $m=n_1=n_2\in N$, ami N választása miatt ↯. N^*-nak tehát csak triviális részmodulusa lehet, így valóban egyszerű.

7.5.9 Tétel: egy M R-modulusra nézve ekvivalens az alábbi három feltétel:

(1) M előáll egyszerű modulusok direkt összegeként, azaz $M=\bigoplus_{\alpha\in\mathbf{I}} S_\alpha$ alakban, ahol $\forall\alpha\in\mathbf{I}: S_\alpha$ egyszerű.

(2) M-et generálja néhány egyszerű részmodulusa: $M=\sum_{\alpha\in\mathbf{I}} S_\alpha=\langle S_\alpha \mid \alpha\in\mathbf{I}\rangle$, ahol $\forall\alpha\in\mathbf{I}: (S_\alpha\le M, S_\alpha$ egyszerű$)$.

(3) $\forall N\le M\ \exists N^*\le M: M=N\oplus N^*$.

Bizonyítás: **(1)** $\Rightarrow$ **(3)**: legyen $\forall\alpha\in\mathbf{I}: S_\alpha$ egyszerű, $M=\bigoplus_{\alpha\in\mathbf{I}} S_\alpha$ és $N\le M$. Legyen $\mathbf{J}\subseteq\mathbf{I}$ olyan, hogy $\underline{\boxdot}\ N\cap\langle S_\alpha \mid \alpha\in\mathbf{J}\rangle=\{0\}$, továbbá legyen erre a tulajdonságra nézve maximális. Ilyen $\mathbf{J}$ létezését a Zorn-lemmával bizonyítjuk. $\mathbf{J}=\emptyset$ nyilván teljesíti $\boxdot$-t. Tekintsünk egy $\mathcal{L}\subseteq\mathcal{P}(\mathbf{I})$ láncot, melynek minden $\mathbf{J}$ eleme teljesíti $\boxdot$-t és lássuk be, hogy az uniójuk is.

↑ $\exists m\in N\cap\langle S_\alpha \mid \alpha\in\bigcup\mathcal{L}\rangle$ nem 0 elem. Ekkor m előáll $(\bigcup_{\alpha\in\bigcup\mathcal{L}} S_\alpha)$-beli elemek véges összegeként: $\underline{\boxdot}\ m=m_{\alpha(1)}+\ldots+m_{\alpha(k)}$, ahol $m_{\alpha(i)}\in S_{\alpha(i)}$ és $\alpha(i)\in\bigcup\mathcal{L}$. A $\mathbf{H}=\{\alpha(i)\mid 1\le i\le k\}$ véges indexhalmazt L elemeinek uniója lefedi. Ez azonban csak úgy lehetséges, ha L-nek létezik olyan $\mathbf{J}^*$ eleme, amely fedi $\mathbf{H}$-t. A $\boxdot$ felírás szerint ekkor $m\in\langle S_\alpha \mid \alpha\in\mathbf{J}^*\rangle$, azaz $m\in N\cap\langle S_\alpha \mid \alpha\in\mathbf{J}^*\rangle$ és $m\ne 0$. Az L-re tett feltevés szerint ez ↯, tehát ha egy $\mathcal{L}\subseteq\mathcal{P}(\mathbf{I})$ lánc minden $\mathbf{J}$ eleme teljesíti $\boxdot$-t, akkor az uniójuk is. Teljesülnek tehát a Zorn-lemma feltételei, így létezik a feltételnek megfelelő és emellett maximális $\mathbf{J}$.

Legyen most $N^*=\langle S_\alpha \mid \alpha\in\mathbf{J}\rangle$. Most bizonyítottuk, hogy $N\cap N^*=\{0\}$, így csak azt kell belátnunk, hogy N és N^* együtt már generálja M-et. Legyen $\alpha\in\mathbf{I}\setminus\mathbf{J}$ tetszőleges. $\mathbf{J}$ maximalitása miatt $(S_\alpha\oplus N^*)\cap N=(S_\alpha\oplus\bigoplus_{\beta\in\mathbf{J}} S_\beta)\cap N\ne\{0\}$. Tehát $\exists m\in N$ nem 0 elem, ami előáll $m=m_\alpha+m^*\ :\ m_\alpha\in S_\alpha, m^*\in N^*$ alakban. $N\cap N^*=\{0\}$ miatt $m_\alpha\ne 0$, azaz $0\ne m_\alpha=m-m^*\in(N\oplus N^*)\cap S_\alpha$, speciálisan $(N\oplus N^*)\cap S_\alpha\ne\{0\}$. Ez a metszet részmodulusa az S_α egyszerű modulusnak, tehát maga S_α. Mivel α tetszőleges volt, azt kaptuk, hogy $\forall\alpha\in\mathbf{I}\setminus\mathbf{J}: S_\alpha\subseteq N\oplus N^*$. Másrészt N^* definíciójából $\forall\alpha\in\mathbf{J}: S_\alpha\subseteq N^*\subseteq N\oplus N^*$ $\Rightarrow$ az M-et generáló egyszerű részmodulusok mind benne vannak $N\oplus N^*$-ban $\Rightarrow$ $N\oplus N^*$ valóban generálja M-et.

(3) $\Rightarrow$ **(2)**: vegyük M egyszerű részmodulusainak egy olyan $\mathcal{H}=\{S_\alpha \mid \alpha\in\mathbf{I}\}$ halmazát, amely rendelkezik azzal a Γ tulajdonsággal, hogy az elemei által generált részmodulus a direkt összegük és erre a tulajdonságra nézve maximális. Először is lássuk be, hogy ilyen létezik. Tekintsünk egy $\mathcal{L}$ láncot, melynek minden eleme Γ tulajdonságú és lássuk be, hogy $\bigcup\mathcal{L}$ is az.

Vegyük észre, hogy Γ éppen azt jelenti, hogy $\forall\alpha\in\mathbf{I}: S_\alpha\cap\langle S_\beta \mid \beta\in\mathbf{I}\setminus\{\alpha\}\rangle=\{0\}$. ↑ ez nem teljesül az $\mathbf{I}=\bigcup\mathcal{L}$ halmazra és valamely $\alpha\in\mathbf{I}$ indexre. Ekkor található $m_\alpha\in S_\alpha$, amely felírható $\underline{\boxdot}\ m_\alpha=m_{\alpha(1)}+\ldots+m_{\alpha(k)}$ alakban, ahol $m_{\alpha(i)}\in S_{\alpha(i)}$ és $\alpha\ne\alpha(i)\in\bigcup\mathcal{L}$. $\bigcup\mathcal{L}$ fedi a $\mathbf{H}=\{\alpha\}\cup\{\alpha(i)\mid 1\le i\le k\}$ véges halmazt, ami csak úgy lehetséges, ha már valamely $\mathbf{J}\in\mathcal{L}$ is fedi. Viszont ez a **J** – feltevéseinkkel ellentétben – nem lehet Γ tulajdonságú $\boxdot$ miatt. ↯, így $\bigcup\mathcal{L}$ is Γ tulajdonságú. Alkalmazhatjuk tehát a Zorn-lemmát, amely szerint létezik maximális N, ha létezik Γ tulajdonságú halmaz. Ilyen pedig van, pl. $\emptyset$.

↑ $\bigoplus_{\alpha\in\mathbf{I}} S_\alpha\ne M$. Jelölje $\bigoplus_{\alpha\in\mathbf{I}} S_\alpha$-t N. Ekkor **(3)** szerint $\exists N^*\le M: M=N\oplus N^*$ és $N^*\ne\{0\}$. **7.5.8** szerint található $S^*\le N^*$ egyszerű részmodulus. Ekkor azonban $\mathcal{H}\cup\{S^*\}$ egy $\mathcal{H}$-nál bővebb, M egyszerű részmodulusaiból álló Γ tulajdonságú halmaz lenne, ami $\mathcal{H}$ választása miatt ↯. Tehát $M=\bigoplus_{\alpha\in\mathbf{I}} S_\alpha\ \Rightarrow\ M=\langle S_\alpha \mid \alpha\in\mathbf{I}\rangle$, a bizonyítandó állítás.

(2) $\Rightarrow$ **(1)**: legyen $M=\sum_{\alpha\in\mathbf{I}} S_\alpha$, ahol $\forall\alpha\in\mathbf{I}: (S_\alpha\le M, S_\alpha$ egyszerű$)$. Akárcsak az előbb, vegyük M $\{S_\alpha \mid \alpha\in\mathbf{I}\}$-beli részmodulusainak egy olyan $\mathcal{H}=\{S_\beta \mid \beta\in\mathbf{J}\subseteq\mathbf{I}\}$ halmazát, amely Γ tulajdonságú és emellett maximális. Legyen $\alpha\in\mathbf{I}\setminus\mathbf{J}$ tetszőleges. Ha $S_\alpha\cap(\bigoplus_{\beta\in\mathbf{J}} S_\beta)=\{0\}$, akkor $\mathcal{H}\cup\{S_\alpha\}$ létezése ellentmond $\mathcal{H}$ maximalitásának. Ezért $S_\alpha\cap(\bigoplus_{\beta\in\mathbf{J}} S_\beta)\ne\{0\}$ $\Rightarrow$ ez S_α egy nem $\{0\}$ részmodulusa, ami S_α egyszerűsége miatt csak S_α lehet. Tehát $\forall\alpha\in\mathbf{I}: S_\alpha\subseteq\bigoplus_{\beta\in\mathbf{J}} S_\beta$, azaz $M=\sum_{\alpha\in\mathbf{I}} S_\beta\subseteq\bigoplus_{\beta\in\mathbf{J}} S_\beta$. Persze $M\supseteq\bigoplus_{\beta\in\mathbf{J}} S_\beta$ is teljesül, ezzel az állítást beláttuk.

7.5.10 Definíció: a fenti feltételeknek eleget tevő modulusokat féligegyszerű modulusnak hívjuk.

7.5.11 Definíció: az R egységelemes gyűrű féligegyszerű, ha ${}_RR$ féligegyszerű modulus. (Itt fontos, hogy R-t mint baloldali R-modulust tekintjük.) Mivel ${}_RR$ egyszerű részmodulusai a minimális balideálok, ekkor R előáll néhány minimális balideáljának direkt összegeként. (Vigyázat, itt a direkt összeg nem gyűrűk direkt összegét jelenti – az összeadandók nem feltétlenül ideálok –, hanem a modulusok (vagy Abel-csoportok) feletti direkt összeget. A legkényelmesebb megfogalmazás az, hogy kiválasztható R minimális balideáljainak egy olyan $\{L_\alpha \mid \alpha\in\mathbf{I}\}$ halmaza, hogy R minden r eleme egyértelműen áll elő $r=x_{\alpha(1)}+\ldots+x_{\alpha(k)}$ alakban, ahol $k\in\mathbb{N}, \alpha(i)\in\mathbf{I}, x_{\alpha(i)}\in L_{\alpha(i)}\setminus\{0\}$ és $\alpha(i)\neq\alpha(j)$ ha $i\neq j$.

7.6 Noether-gyűrű, artin-gyűrű

7.6.1 Definíció: az R gyűrűben teljesül a balideálokra a minimumfeltétel, ha az alábbi két (nyilván ekvivalens) feltétel fennáll: **(1)** balideálok bármely nemüres halmazában van minimális elem ill. **(2)** nem létezik balideálok végtelen, szigorúan monoton fogyó ($L_1\supset L_2\supset\ldots\supset L_n\supset\ldots$) sorozata. Ezt úgy is mondjuk, hogy R (bal-)artin. Ha ugyanez a jobbideálokra teljesül, akkor R jobb-artin.

7.6.2 Definíció: az R gyűrűben teljesül a balideálokra a maximumfeltétel, ha az alábbi három (ekvivalens, ld. később) feltétel fennáll: **(1)** balideálok bármely nemüres halmazában van maximális elem; **(2)** nem létezik balideálok végtelen, szigorúan monoton növő ($L_1\subset L_2\subset\ldots\subset L_n\subset\ldots$) sorozata; **(3)** minden L balideál végesen generált, azaz található hozzá $\mathbf{X}\subseteq R$ véges halmaz, hogy $(\mathbf{X})_\mathrm{b}=L$. Ekkor R (bal-)noether. Ha mindez a jobbideálokra teljesül, akkor R jobb-noether.

Be kell még látnunk, hogy a három feltétel ekvivalens. **(1)** $\Leftrightarrow$ **(2)** triviális. **(3)** $\Rightarrow$ **(2)**: legyen $\{L_n\in\mathbb{N}\}$ balideálok monoton növő sorozata. $L^*=\bigcup_{n\in\mathbb{N}}L_n$ végesen generált: $L^*=(\mathbf{X})_\mathrm{b}$, $|\mathbf{X}|<\infty$. Ekkor létezik olyan k, melyre $|\mathbf{X}|\subseteq L_k$, mert $|\mathbf{X}|\subseteq\bigcup L_n$. Eszerint $L=(\mathbf{X})_\mathrm{b}\subseteq L_k$, ezért $\forall n\geq k: L_k\subseteq L_n\subseteq L\subseteq L_k$, azaz a sorozat nem lehet szigorúan monoton növő.

(2) $\Rightarrow$ **(3)**: tegyük fel, hogy nem teljesül **(3)**, azaz létezik egy L balideál, amely nem végesen generált. L_1 legyen $\{0\}$. Tegyük most fel, hogy már van egy $L_1\subset L_2\subset\ldots\subset L_n$ sorozatunk, ahol $\forall k\in\{1,\ldots,n\}: L_k=(r_1,\ldots,r_{k-1})_\mathrm{b}$ és $r_1,\ldots,r_{k-1}\in L$. Ekkor persze $L_n\subseteq L$. Mivel L nem végesen generált, $\exists r_n\in L\setminus L_n$. Válasszunk egy ilyen elemet és legyen $L_k=(r_1,\ldots,r_n)_\mathrm{b}$. Ezt az algoritmust megszámlálható sokszor ismételve egy $\{L_n\mid n\in\mathbb{N}\}$ szigorúan monoton növő balideál-sorozatot kapunk, tehát **(2)** sem teljesülhet. Ezt akartuk bizonyítani.

Megjegyzés (Hopkins-tétel): ha R egységelemes bal-artin gyűrű, akkor bal-noether is.

Példa: a Z_{p^∞} feletti zérógyűrűre nem teljesül a maximumfeltétel, hiszen minden részcsoportja ideál és nincs maximális részcsoportja. A Z_p^∞ feletti zérógyűrű sem noether, hiszen nem végesen generált.

Megjegyzés: egységelemes, kommutatív gyűrűben (**7.6.2.2** $\Rightarrow$ **7.6.2.3**)-hoz nem kell a kiválasztási axióma.

7.6.3 Tétel (Hilbert bázistétele): ha az R egységelemes, kommutatív gyűrű noether, akkor $R[x]$ is noether.

Bizonyítás: azt fogjuk belátni, hogy minden $I\triangleleft R[x]$ ideál végesen generált. Legyen $A_n=\{a_n\in R\mid\exists f\in I: f=a_nx^n+\ldots\}$. Nyilván $A_n\triangleleft R$, mert $0\in I$ miatt $0\in A_n$, ha pedig $a,b\in A_n$ az $f,g\in I$ polinomok révén és $r\in R$ tetszőleges, akkor $f\pm g, r\cdot f\in I$ miatt $a\pm b, ra\in A_n$. $\forall k\in\mathbb{N}: A_k\subseteq A_{k+1}$, hiszen ha $a\in A_k$ az $f\in I$ polinom miatt, akkor $xf\in I$-ből következik $a\in A_{k+1}$.

Az $A_0\subseteq A_1\subseteq A_2\subseteq\ldots$ monoton növő R-beli ideálsorozat stabilizálódik, mert R noether; legyen maximális eleme A_m. $A_1\ldots A_m$ mindegyike végesen generált. Legyen $A_k=(a_{ki}\mid i\in\mathbf{H}_k)$, ahol $\mathbf{H}_k$ minden esetben véges indexhalmaz. Minden a_{ki}-hez található egy $f_{ki}=(a_{ki}x^k+\ldots)\in I$ polinom. Azt állítjuk, hogy $J=(f_{ki}\mid 0\leq k\leq m, i\in\mathbf{H}_k)$ jelöléssel $I=J$.

$J\subseteq I$ triviális, tehát azt kell belátni, hogy ha $f\in I$, akkor $f\in J$. Ezt f fokszáma szerinti indukcióval bizonyítjuk. Az I-beli nulladfokú polinomok éppen A_0 elemei (a 0-t kivéve), ezeket tehát generálja $\{a_{0,i}\mid i\in\mathbf{H}_0\}\subseteq J$.

Legyen most $f\in I$ t-edfokú és tegyük fel, hogy J generálja I alacsonyabb fokú polinomjait. Jelölje f főegyütthatóját a. Ekkor $a\in A_t$, azaz $s=\mathbf{min}(t,m)$ választással $a\in A_s$, így előáll $a=\sum_{i\in\mathbf{H}(s)}r_ia_{si}$ alakban, ahol $r_i\in R$. Ezért $g=f-\sum_{i\in\mathbf{H}(s)}r_ix^{t-s}\cdot f_{si}$-ben x^t együtthatója 0 $\Rightarrow$ $\deg g<t$. $g\in I$, így az indukciós feltevés következtében $g\in J$. $\sum(\ldots)\in J$ miatt tehát $f=g+\sum(\ldots)\in J$.

7.6.4 Következmény: $K[x_1,x_2,\ldots,x_n]$ és $\mathbb{Z}[x_1,x_2,\ldots,x_m]$ noether, pedig egyik sem főideálgyűrű (definíciója: ld. **7.8.2**) (ha $n\geq 2$ ill. $m\geq 1$), hiszen $(x,y)\triangleleft K[x,y]$ és $(2,x)\triangleleft\mathbb{Z}[x]$ egyike sem főideál.

7.7 Radikál, prímideál, maximális ideál

7.7.1 Definíció: $a\in R$ nilpotens, ha $\exists n\geq 1: a^n=0$.

7.7.2 Definíció: legyen R egységelemes, kommutatív gyűrű. Ekkor R nilradikálja $N(R)=\{a\in R \mid \exists n\geq 1: a^n=0\}$. Ez ideál, mert ha $a^n=0$, akkor $\forall r\in R: (ra)^n=r^n\cdot a^n=0$ és ha $a^n=b^k=0$, akkor $(a+b)^{n+k-1}$-t kifejtve minden tag 0, mert vagy a kitevője legalább n benne, vagy b kitevője legalább k (és nem üres, mert $0\in N(R)$).

Megjegyzés: a kommutativitás nem felesleges, mert $M_2(K)$-ban $\left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right)$ és $\left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right)$ egyaránt nilpotensek, de összegük nem az.

7.7.3 Állítás: $N\left(R/N(R)\right)=\{0\}$. Ha ugyanis $r+N$ nilpotens a faktorgyűrűben, akkor $\exists n\in\mathbb{Z}^+: 0=(r+N)^n=(r^n+N)$, azaz $r^n\in N$. Eszerint r^n nilpotens: $r^{nk}=0$, ahol $k\in\mathbb{Z}^+$. Persze $nk\in\mathbb{Z}^+$, így r is nilpotens $\Rightarrow$ $r\in N$ $\Rightarrow$ $(r+N)=0$. Ez tehát a faktorcsoport egyetlen nilpotens eleme.

7.7.4 Definíció: legyen R egységelemes, kommutatív. Ekkor $P\trianglelefteq R$ prímideál, ha $x,y\in R, xy\in P \Rightarrow (x\in P$ vagy $y\in P)$. (Az elnevezés onnan ered, hogy $(n)\triangleleft\mathbb{Z}$ pontosan akkor prímideál, ha n prím vagy $n=0$.)

7.7.5 Definíció: legyen R egységelemes, kommutatív és $I\triangleleft R$. Ekkor I radikálja $\sqrt{I}=\{r\in R \mid \exists n\in\mathbb{N}: r^n\in I\}$. Könnyen beláthatóak az alábbiak: **(1)** $I\subseteq\sqrt{I}\triangleleft R$, **(2)** $N(R/\sqrt{I})=\{0\}$, **(3)** $\sqrt{\sqrt{I}}=\sqrt{I}$, **(4)** $\sqrt{I\cap J}=\sqrt{I}\cap\sqrt{J}$, **(5)** $\sqrt{I}=(1)\Rightarrow I=(1)$, **(6)** $\sqrt{I+J}=\sqrt{\sqrt{I}+\sqrt{J}}$, **(7)** ha P prímideál, akkor $\sqrt{P^n}=P$ minden $n\in\mathbb{N}$-re.

7.7.6 Definíció: $I\triangleleft R$ maximális ideál, ha $I\neq R$ és $\nexists J\trianglelefteq R: I<J$. Hasonlóan definiáljuk a maximális bal- és jobbideál fogalmát.

7.7.7 Állítás: legyen R egységelemes és kommutatív, $I\trianglelefteq R$. Ekkor **(1)** I prímideál $\Leftrightarrow$ R/I nullosztómentes és **(2)** I maximális ideál $\Leftrightarrow$ R/I test.

Bizonyítás: **(1)** I nem prímideál $\Leftrightarrow$ $(\exists x,y\in R\setminus I: xy\in I)$ $\Leftrightarrow$ $(\exists x,y\in R\setminus I: (x+I)(y+I)=I)$ $\Leftrightarrow$ R/I nem nullosztómentes. **(2)** R/I kommutatív és egységelemes. Így **7.3.8** szerint pontosan akkor test, ha nincs nem triviális ideálja. Mivel R/I ideáljai kölcsönösen egyértelműen megfelelnek R I-t tartalmazó ideáljainak, ez pontosan akkor teljesül, ha nincs I és R között ideál, azaz ha I maximális ideál.

7.7.8 Következmény: egységelemes, kommutatív gyűrűben minden maximális ideál prímideál, hiszen ha R/I test, akkor nullosztómentes. Ennek a megfordítása nem igaz. (Pl. (0) minden nullosztómentes gyűrűben prímideál, de csak testben maximális ideál. Továbbá $K[x,y]$-ban $(0)<(x)\trianglelefteq K[x,y]$ és ezek mind prímideálok, hiszen a faktorgyűrűk – rendre $K[x,y], K[y]$ és K – nullosztómentesek.)

7.7.9 Állítás: legyen R egységelemes kommutatív gyűrű. Ekkor minden $a\in R\setminus U(R)$ elem és minden R-nél szűkebb I ideál (azaz minden, kivéve az egységeket) belefoglalható egy maximális ideálba.

Bizonyítás: $1\notin aR$, mert $a\notin U(R)$ és tudjuk, hogy $(a)=aR$. Elég tehát az állítás második felét belátni, hiszen az alapján az a által generált ideál belefoglalható maximális ideálba. Álljon az $\mathcal{L}$ lánc olyan R-beli ideálokból, melyek I-t tartalmazzák, de 1-et nem. Ekkor $\cup\mathcal{L}$ is ilyen ideál lesz. A Zorn-lemma szerint tehát az I-t fedő, 1-et nem tartalmazó ideálok között van maximális. Legyen M ilyen. M választása miatt egy M-nél bővebb ideál mindenképp tartalmazza 1-et, tehát maga R $\Rightarrow$ M maximális ideál.

7.7.10 Következmény: egységelemes kommutatív gyűrűben van maximális ideál, hiszen (0) belefoglalható maximális ideálba. Ez **7.7.8** alapján egyben prímideál is.

7.7.11 Tétel: egységelemes, kommutatív gyűrűben $N(R)$ a prímideálok metszete. (Ez az előbbi következmény szerint nem üres metszet.)

Bizonyítás: tegyük fel, hogy $a\in N(R)$, azaz valamely $n\in\mathbb{Z}^+$-re $a^n=0$. Ekkor az $a\cdot a\cdot\ldots\cdot a=0$ szorzat tetszőleges P prímideálnak eleme. Ez csak úgy lehetséges, ha valamely tényezője P-beli, azaz ha $a\in P$. Eszerint a eleme minden prímideálnak, így a metszetüknek is. a a nilradikál egy tetszőleges eleme volt, azaz $N(R)\subseteq\left(\bigcap_{P \text{ prímideál}} P\right)$.

Legyen most $f\notin N(R)$ és keressünk hozzá egy olyan P prímideált, amelynek nem eleme. $f\notin N(R)$ $\Rightarrow$ $0\notin F=\{f^n \mid n\in\mathbb{Z}^+\}$. Legyen P olyan ideál R-ben, amely diszjunkt F-től és erre a tulajdonságra nézve maximális. (A $\{0\}$

ideál ilyen tulajdonságú és egy ilyen tulajdonságú ideálokból álló $\mathcal{L}$ lánc elemeinek uniója is, így a Zorn-lemma szerint létezik megfelelő P.) Azt állítjuk, hogy P prímideál.

Azt kell belátni, hogy tetszőleges $x,y\in R\setminus P$ elemekre $xy\notin P$. P maximalitása miatt $F\cap(P+(x))\neq\emptyset$, azaz $\exists k\in\mathbb{Z}^+: f^k\in P+(x)$. Eszerint f^k felírható $u+rx : u\in P, r\in R$ alakban. Hasonlóan $\exists m\in\mathbb{Z}^+ f^m=v+sy : v\in P, s\in R$. Összeszorozva $f^{k+m}=(uv+rxv+syu)+rs\cdot xy$. A zárójelben lévő kifejezés P-ben van, mert minden tagban van P-beli tényező és P ideál. $f^{k+m}\notin P \Rightarrow rs\cdot xy\notin P \Rightarrow xy\notin P$, kész vagyunk.

7.7.12 Definíció: legyen R egységelemes, kommutatív gyűrű. Ekkor R Jacobson-radikálja $J(R)=\bigcap_{\text{ideál } R\text{-ben}}^{M \text{ maximális}} M$.

7.7.13 Állítás: $x\in J(R) \Leftrightarrow \forall y\in R: 1-xy$ egység.

Bizonyítás: $\Rightarrow$: $\nearrow$ $x\in J(R)$ és $\exists y\in R: 1-xy$ nem egység. Ekkor **7.7.9** szerint $1-xy$ belefoglalható egy M maximális ideálba. $x\in J(R) \Rightarrow x\in M \Rightarrow xy\in M$ és M választása miatt $1-xy\in M$. Eszerint az összegük is M-beli, azaz $(1-xy)+xy=1\in M \Rightarrow M=R$, $\lightning$.

$\Leftarrow$: $\nearrow$ $\forall y\in R: 1-xy$ egység, de $x\notin J(R)$. Ez utóbbi szerint $\exists M\trianglelefteq R$ maximális ideál, amely nem tartalmazza x-et. Ha pedig maximális, akkor $R=(M,x)=M+(x)$, speciálisan 1 felírható $m+xy$ $(m\in M, y\in R)$ alakban. Így $1-xy=m\in M$. Mivel $1-xy$ egység, ebből következik $1\in M \Rightarrow M=R$, $\lightning$.

Megjegyzés: $N(R)\subseteq J(R)$, hiszen minden maximális ideál prímideál, így a prímideálok metszete nem lehet bővebb a maximális ideálok metszeténél. Az alábbi példán láthatjuk, hogy nem mindig azonosak.

Legyen $R=\{\frac{a}{b}\in\mathbb{Q} \,|\, (a,b)=1, b \text{ páratlan}\}$. $N(R)=\{0\}$, mert nullosztómentes. $U(R)=\{\frac{a}{b} \,|\, (a,b)=1, a \text{ és } b \text{ páratlan}\}$, hiszen pontosan ezeknek van inverzük. Egy R-től különböző ideál diszjunkt kell legyen $U(R)$-től, tehát $I\trianglelefteq R \Rightarrow I\subseteq\{\frac{2a}{b} \,|\, (2a,b)=1\}=(2)$. Ez tehát az egyetlen maximális ideál, így személyesen $J(R)$.

7.7.14 Definíció: R (egységelemes, kommutatív gyűrű) lokális gyűrű, ha pontosan egy maximális ideálja van. Ez ekvivalens azzal, hogy a nem-egységek ideált alkotnak. (Minden maximális ideál részhalmaza $R\setminus U(R)$-nek, mert nem tartalmazhat egységet. Ha pedig csak egy maximális ideál van, akkor abban minden nem-egység szerepel **7.7.9** miatt.) ($\exists$nek olyan emberek, akik szerint R akkor lokális gyűrű, ha emellett még noether is.)

7.8 Egységelemes integritási tartományok

7.8.1 Definíció: integritási tartomány egy kommutatív, nullosztómentes gyűrű.

7.8.2 Definíció: R főideálgyűrű (PID, principal ideal domain), ha integritási tartomány és minden ideálja főideál. Ekkor persze noether.

7.8.3 Tétel: legyen R integritási tartomány. Ekkor létezik olyan legszűkebb K test, amelyben R részgyűrű.

Bizonyítás: tekintsük az $\{(a,s) \,|\, a\in R, s\in R\setminus\{0\}\}$ halmazt. Definiáljuk efelett az alábbi relációt: $(a,s)\sim(b,t) \Leftrightarrow at-bs=0$. Ez ekvivalencia-reláció lesz. Jelölje (a,s) ekvivalencia-osztályát $\overline{(a,s)}$. Legyenek K elemei az ekvivalencia-osztályok, a műveletek pedig a következők: $\overline{(a,s)}+\overline{(b,t)}=\overline{(at+bs,st)}$ és $\overline{(a,s)}\cdot\overline{(b,t)}=\overline{(ab,st)}$. Mivel R nullosztómentes, $st\neq0$, azaz a műveletek eredménye egy K-beli elem. Ellenőrizhető, hogy a műveletek jóldefiniáltak, kommutatívak. $\overline{(0,s)}$ nullelem, $\overline{(s,s)}$ egységelem, $-\overline{(a,s)}=\overline{(-a,s)}$ és ha $a\neq0$, akkor $\overline{(a,s)}^{-1}=\overline{(s,a)}$. Az $\overline{(as,s)}$ elemet a-val jelölve látszik, hogy R részgyűrűje K-nak.

Legyen K' egy tetszőleges, R-t részgyűrűként tartalmazó test. Rendelje a $\varphi: K\to K'$ leképezés az $\overline{(a,s)}\in K$ elemhez $as^{-1}\in K'$-t. Ez homomorfizmus lesz és a K-ba ágyazott R egy $a=\overline{(as,s)}$ elemének képe $ass^{-1}=a$, azaz φ $R\subseteq K$-ra megszorítva identitás. Továbbá φ injektív, mert ha $a_1s_1^{-1}=as^{-1}$, akkor $\overline{(a_1,s_1)}=\overline{(a,s)}$. Tehát K valóban a lehető legszűkebb.

7.8.4 Definíció: a fenti K testet R hányadostestjének hívjuk.

Megjegyzés: ha R nullosztómentes, nem kommutatív gyűrű, akkor nem feltétlenül ágyazható ferde testbe.

Az alábbiakban jelöljön R egységelemes integritási tartományt.

7.8.5 Definíció: definiáljuk R elemei közt az alábbi relációt: a osztja b-t (b többszöröse a-nak), ha $\exists c\in R: ac=b$. Jelölése $a\,|\,b$. Az egységek éppen 1 osztói, azaz $u\in U(R) \Leftrightarrow u\,|\,1 \Leftrightarrow \forall r\in R: u\,|\,r$. A reláció reflexív és tranzitív, viszont ($a\,|\,b$ és $b\,|\,a$)-ból nem következik $a=b$. Ezért bevezetünk még egy relációt:

7.8.6 Definíció: $a,b\in R$ asszociáltak – jelölése $(a\sim b)$, ha $\exists u\in U(R)\colon au=b$. Ez ekvivalencia-reláció, mert $U(R)$ csoport. Nyilván $a\sim b \Leftrightarrow (a\,|\,b \text{ és } b\,|\,a) \Leftrightarrow \big(b\in(a) \text{ és } a\in(b)\big) \Leftrightarrow (a)=(b)$. Az a elem ekvivalencia-osztályát jelölje $\bar a$.

7.8.7 Állítás: az oszthatóság részbenrendezés az ' ~' reláció ekvivalencia-osztályai felett.

Azt kell belátnunk, hogy az ekvivalencia-osztályokra átörökíthető az oszthatóság, tehát ha $a\sim a',b\sim b'$ és $a\,|\,b$, akkor $a'\,|\,b'$. Beírva a definíciókat $\exists u,v\in U(R),c\in R\colon au=a',bv=b',ac=b$. Mivel u egység, van inverze, így $a=a'u^{-1}$. Ekkor $a'(u^{-1}cv)=acv=bv=b'$, azaz $a'\,|\,b'$. A reflexivitás és a tranzitivitás öröklődik, azt pedig már kimondtuk, hogy $(a\,|\,b \text{ és } b\,|\,a) \Leftrightarrow a\sim b$, ami az ekvivalencia-osztályokon $(\bar a\,|\,\bar b \text{ és } \bar b\,|\,\bar a) \Leftrightarrow \bar a=\bar b$-nek felel meg.

7.8.8 Definíció: legyen $a,b,d\in R$. Ekkor d-t a és b legnagyobb közös osztójának nevezzük, ha **(1)** $d\,|\,a,d\,|\,b$ és **(2)** $(d'\,|\,a,d'\,|\,b)\Rightarrow d'\,|\,d$. Jelölése $d=(a,b)$, esetleg $d\sim(a,b)$.

Tetszőleges a,b elemekhez nem feltétlenül létezik ilyen d. Ha létezik, akkor asszociáltság erejéig egyértelmű, hiszen ha d és d' egyaránt legnagyobb közös osztói a-nak és b-nek, akkor **(2)** szerint $d'\,|\,d$ és $d\,|\,d'$.

7.8.9 Definíció: legyen $a,b,m\in R$. Ekkor m-et a és b legkisebb közös többszörösének nevezzük, ha **(1)** $a\,|\,m,b\,|\,m$ és **(2)** $(a\,|\,m',b\,|\,m')\Rightarrow m\,|\,m'$. Jelölése $m=[a,b]$, esetleg $m\sim[a,b]$. Legnagyobb közös osztó sem mindig létezik, de ha van, akkor asszociáltság erejéig egyértelmű.

Megjegyzés: $[a,b]=0 \Leftrightarrow (a=0 \text{ vagy } b=0)$.

Bizonyítás: $\Rightarrow$: ha $a,b\neq0$, akkor $ab\neq0$ közös többszöröse a-nak és b-nek, viszont nem többszöröse 0-nak. Így 0 nem lehet a legkisebb közös többszörös. $\Leftarrow$: ha a,b valamelyike 0, akkor minden közös többszörösük is 0.

7.8.10 Állítás: $\exists[a,b]\Rightarrow\exists(a,b)$ és $[a,b](a,b)=ab$.

Bizonyítás: ha $[a,b]=0$, akkor az előbbi megjegyzés szerint a,b egyike (pl. a) 0. Ekkor $(a,b)=b$ és az állítás igaz. Legyen tehát $[a,b]=m\neq0$. ab közös többszörös, tehát osztható m-el, így $\exists d\in R\colon md=ab$. Mivel m többszöröse a-nak, megfelelő b'-re $m=ab'$. Ekkor $ab=adb'$. Ebből $a\neq0$ miatt következik $b=db'$, azaz $d\,|\,b$ és hasonlóan $d\,|\,a$. Tehát d valóban közös osztó.

Legyen most d' egy tetszőleges közös osztó, $a=a'd'$ és $b=b'd'$. Ekkor $m'=a'b'd'$-re $a\,|\,m'=ab'$ és $b\,|\,m'=a'b$, ez tehát egy közös többszörös. m választása miatt $m\,|\,m'$, azaz $m'=mc$. Ekkor $md=ab=a'd'b'd'=m'd'=mcd'$. Mivel $m\neq0$, ebből következik $d=d'c\Rightarrow d'\,|\,d$, állításunknak megfelelően.

7.8.11 Definíció: legyen $d\in\mathbb{Z}\setminus\{0,1\}$, négyzetmentes. Ekkor $\mathbb{Q}(\sqrt d)=\{r+s\sqrt d\in\mathbb{C}\,|\,r,s\in\mathbb{Q}\}$. Ez test lesz és $\mathbb{Q}<\mathbb{Q}(\sqrt d)<\mathbb{C}$.

Az $\alpha=r+s\sqrt d\in\mathbb{Q}(\sqrt d)$ elem konjugáltja legyen $\bar\alpha=r-s\sqrt d$. (Ha $d<0$, akkor ez a komplex konjugált, különben nem.) Normája legyen $N(\alpha)=\|\alpha\|=\alpha\bar\alpha=r^2-s^2d$. Ez multiplikatív, azaz $\|\alpha\beta\|=\|\alpha\|\cdot\|\beta\|$ és $\|\alpha\|=0\Leftrightarrow\alpha=0$. Ha $d<0$ $d<0$, akkor $\|\alpha\|\geq0$.

7.8.12 Állítás: $\alpha\in\mathbb{Z}[\sqrt d]$ egység $\Leftrightarrow$ $N(\alpha)=\pm1$

Bizonyítás: $\Rightarrow$: α egység $\Rightarrow$ $\exists\beta\in\mathbb{Z}[\sqrt d]\colon\alpha\beta=1$, ekkor $N(\alpha)\cdot N(\beta)=1$. Ezek egész számok, tehát $N(\alpha)\,|\,1$. $\Leftarrow$: $N(\alpha)=\pm1\Rightarrow\alpha\bar\alpha=\pm1$. Mivel $\pm\bar\alpha\in\mathbb{Z}[\sqrt d]$, α egység.

Ha $d<0$, akkor persze $N(\alpha)$ nem lehet -1, csak 1.

Következmény: $\mathbb{Z}[i]$ egységei ±1 és $\pm i$, hiszen $N(a+bi)=a^2+b^2$ csak ezekre lehet 1.

7.8.13 Definíció: $p\in R$ prím, ha $p\,|\,ab\Rightarrow(p\,|\,ab \text{ vagy } p\,|\,b)$. Mivel $(p)=pR=\{r\in R\colon p\,|\,r\}$, ez ekvivalens azzal, hogy (p) prímideál. (A 0-t és az egységeket nem tekintjük prímnek.)

7.8.14 Definíció: $a\in R$ irreducibilis avagy felbonthatatlan, ha $a=bc\Rightarrow b,c$ egyike egység, a másik a asszociáltja. (Tehát a minden osztója vagy asszociált, vagy egység. A 0-t és az egységeket nem tekintjük irreducibilisnek.)

7.8.15 Állítás: $p\in R$ prím $\Rightarrow p$ irreducibilis.

Bizonyítás: tegyük fel, hogy $p=bc$. Ekkor $p\,|\,bc$, így definíció szerint $p\,|\,b$ vagy $p\,|\,c$. Az első esetben $p\sim b$, amiből $bc=p=bu$ $(u\in U(R))$. **7.3.6** szerint ekkor $c=u$, azaz c egység. A második esetben $p\sim c$ és b egység.

Az állítás megfordítása nem igaz. Például $\mathbb{Z}[\sqrt{-5}]$-ben **7.8.12** alapján csak ±1 egység. Tekintsük a $2\cdot3=(1+\sqrt{-5})(1-\sqrt{-5})$ egyenlőséget. A normák rendre $4,9,6,6$. Ha valamelyik a tényező nem lenne irreducibilis, akkor felbomlana $a=bc$ alakban, ahol b,c egyike sem egység. Tehát $N(a)=N(b)\cdot N(c)$, ahol $1<N(b),N(c)<N(a)$, mind pozitív egészek. Ez viszont lehetetlen, mert $\mathbb{Z}[\sqrt{-5}]$-ben nincs sem 2, sem 3 normájú elem. Tehát mind a négy tényező irreducibilis és egyik sem prím, hiszen mindegyik osztja a másik oldalon lévő szorzatot, de a normák miatt egyik tagját sem oszthatja.

7.9 UFD, euklideszi gyűrű

Jelöljön R továbbra is egységelemes integritási tartományt.

7.9.1 Definíció: R UFD (unique factorization domain), ha minden (nem 0) eleme lényegében egyértelműen bomlik fel irreducibilis elemek szorzatára, azaz **(1)** $\forall a\in R\ \exists t\in\mathbb{N}, u,p_1,\dots,p_t\in R: a=u\cdot p_1\cdot\dots\cdot p_t$, ahol minden p_i irreducibilis és u egység (az üres szorzat értéke definíció szerint 1), továbbá ha **(2)** ha $a=u\cdot p_1\cdot\dots\cdot p_t=v\cdot q_1\cdot\dots\cdot q_s$ két ilyen felbontás, akkor $s=t$ és alkalmas átrendezéssel $p_i\sim q_i$.

UFD például $K[x],\mathbb{Z},\mathbb{Z}[i]$. Nem UFD $\mathbb{Z}[\sqrt{-5}]$, hiszen a 6-nak nemrég megadtuk két lényegesen különböző felbontását $\mathbb{Z}[\sqrt{-5}]$-ben.

7.9.2 Állítás: ha R UFD, akkor $\forall a,b\in R: \exists(a,b)$ és $\exists[a,b]$.

Legyenek $p_1,\dots,p_s$ mindazok az irreducibilis elemek, melyek szerepelnek a vagy b felbontásában. (Az asszociáltakat csoportosítsuk egybe. Ez a felbontásban szereplő egység változtatásával megoldható.) Ekkor $a=u\cdot p_1^{\alpha_1}\cdot\dots\cdot p_s^{\alpha_s}$ és $b=v\cdot p_1^{\beta_1}\cdot\dots\cdot p_s^{\beta_s}$, ahol $\alpha_i,\beta_i\in\mathbb{N}$. Könnyen ellenőrizhető, hogy $(a,b)=\prod_{k=1}^{s}p_k^{\mathbf{min}(\alpha_k,\beta_k)}$ és $[a,b]=\prod_{k=1}^{s}p_k^{\mathbf{max}(\alpha_k,\beta_k)}$.

7.9.3 Definíció: R euklideszi, ha található egy olyan $\varphi: R\setminus\{0\}\to\mathbb{N}$ leképezés, amelyre **(1)** $\varphi(ab)\geq\varphi(a)$ és **(2)** $\forall a\in R, b\in R\setminus\{0\}\ \exists q,r\in R: a=bq+r$, ahol vagy $r=0$, vagy $\varphi(r)<\varphi(b)$. (Ez utóbbi feltétel azt jelenti, hogy R-ben lehet maradékosan osztani.)

Megjegyzés: az első feltétel nem igazán fontos, csak kényelmes. Ha ugyanis $\psi: R\setminus\{0\}\to\mathbb{N}$ teljesíti **(2)**-t, akkor $\varphi: x\mapsto\mathbf{min}_{y\in R\setminus\{0\}}\psi(xy)$ mindkét feltételnek megfelel, ez némi számolással ellenőrizhető.

7.9.4 Tétel: ha R euklideszi, akkor főideálgyűrű.

Bizonyítás: legyen $I\lhd R$ és lássuk be, hogy főideál. Ha $I=(0)$, akkor kész vagyunk. Ha nem, akkor legyen a egy olyan elem I-ben, amelyre $\varphi(a)$ minimális. Azt állítjuk, hogy $I=(a)$, amihez elég $I\subseteq(a)$. Legyen $b\in I$ tetszőleges és lássuk be, hogy $b\in(a)$. Osszuk el maradékosan b-t a-val, azaz legyen $b=aq+r$, ahol $r=0$ vagy $\varphi(r)<\varphi(a)$. $r=(b-aq)\in I$, tehát a választása miatt $\varphi(r)<\varphi(a)$ nem állhat fenn. Eszerint $b=aq\in(a)$.

7.9.5 Állítás: R UFD $\Leftrightarrow$ **(1)** minden elem előáll irreducibilisek szorzataként és **(2)** minden irreducibilis elem prím.

Bizonyítás: $\Rightarrow$ **(1)** az UFD definíciójából. $\Rightarrow$ **(2)**: legyen p irreducibilis és $p\mid ab$, azaz $pq=ab$. Legyen $a=u\cdot\prod a_i$, $b=v\cdot\prod b_i$, $q=w\cdot\prod q_i$ az a,b,q számok felbontása irreducibilis elemek szorzatára. A $w\cdot(p\cdot\prod q_i)=ab=(uv)\cdot\prod a_i\cdot\prod b_i$ felbontások lényegében azonosak, tehát valamely a_i vagy b_i asszociáltja p-nek. Ekkor p osztója a-nak vagy b-nek.

$\Leftarrow$: tegyük fel, hogy a-t felbontottuk kétféleképp irreducibilis elemek szorzatára és lássuk be, hogy ez a két felbontás lényegében azonos. Legyen tehát $a=u\cdot p_1\cdot\dots\cdot p_s=v\cdot q_1\cdot\dots\cdot q_t, s\leq t$. Tudjuk, hogy minden irreducibilis elem prím, speciálisan p_1 is. Osztja a jobb oldali szorzatot, tehát osztja valamelyik tényezőjét; feltehető, hogy ez q_1. Egy irreducibilis elem viszont csak úgy oszthat egy másikat, ha asszociáltak, azaz $q_1=w_1p_1$ (w_1 egység). Ezt beírva $p_1\cdot(u\cdot p_2\cdot\dots\cdot p_s)=p_1\cdot(vw_1)(q_2\cdot\dots\cdot q_t)$, amiből $p_1\neq0$ alapján $v_1=uw_1$ jelöléssel (persze v_1 is egység) $u\cdot p_2\cdot\dots\cdot p_s=v_1\cdot q_2\cdot\dots\cdot q_t$. Ugyanezt a gondolatmenetet folytatva $q_2=w_2p_2,\dots,q_s=w_sp_s$ (w_i egység) és marad $u=v_s\cdot q_{s+1}\cdot\dots\cdot q_t$, ahol v_s egység. Ez csak úgy lehetséges, ha $q_{s+1}\cdot\dots\cdot q_t$ üres szorzat, azaz $t=s$. Közben kijött, hogy $p_i\sim q_i$, a két felírás tehát lényegében azonos.

7.9.6 Állítás: **(1)** ha R-ben teljesül a főideálokra a maximumfeltétel (nem létezik főideálok szigorúan monoton növekvő végtelen sorozata), akkor minden elem felbomlik irreducibilisek szorzatára. **(2)** ha R UFD, akkor a főideáljaira teljesül a maximumfeltétel.

Bizonyítás: **(1)** $\nexists\, a_0 \in R$ nem bomlik fel irreducibilis elemek szorzatára. Ekkor ő maga sem irreducibilis, tehát szorzattá bontható úgy, hogy egyik tényező sem asszociáltja, azaz $a_0 = xy$, ahol $a_0 \nmid x$ és $a_0 \nmid y$. $x \mid a_0$ miatt $(a_0) \subseteq (x)$ és $a_0 \nmid x$ miatt nem állhat fenn egyenlőség; hasonlóan $(a_0) \subset (y)$. Mivel a_0 nem bomlik fel irreducibilisek szorzatára, x és y között is kell legyen olyan, amely nem bomlik fel irreducibilisek szorzatára; legyen ez a_1. Ezt az algoritmust megszámlálható sokszor megismételve egy végtelen $(a_0) \subset (a_1) \subset (a_2) \subset \dots$ sorozatot kapunk, $\lightning$.

(2) Jelölje $a \in R$-re $s(a)$ az a felbontásában szereplő irreducibilis faktorok számát. Ez jóldefiniált, mert R UFD. Természetesen $s(a) \in \mathbb{N}$. Továbbá $s(ab) = s(a) + s(b)$, mert az $ab = a \cdot b$ egyenlet két oldala ugyanannyi irreducibilis szorzatára bomlik. Nyilván $s(u) = 0 \Leftrightarrow u$ egység, továbbá $a \sim b \Rightarrow s(a) = s(b)$.

Azt állítjuk, hogy $(a) \subset (b) \Rightarrow s(a) > s(b)$. Ugyanis $(a) \subset (b) \Leftrightarrow (b \mid a$ és $b \nmid a) \Leftrightarrow (\exists x \in R: a = bx,\ x$ nem egység$) \Leftrightarrow (\exists x: a = bx, s(x) > 0)$. Ekkor $s(a) = s(b) + s(x) > s(b)$.

Eszerint ha létezne egy végtelen $(a_0) \subset (a_1) \subset (a_2) \subset \dots$ sorozat, akkor $s(a_i)$ egy természetes számokból álló, szigorúan monoton csökkenő végtelen sorozat lenne, ilyen viszont nincs.

Megjegyzés: ha R főideálgyűrű, akkor noether-gyűrű, hiszen minden ideál végesen generált. Tehát (fő)ideáljaira teljesül a maximumfeltétel, így **7.9.6.1** szerint minden eleme felbomlik irreducibilis elemek szorzatára.

7.9.7 Állítás: ha R főideálgyűrű, akkor minden $a, b \in R$-nek van legnagyobb közös osztója és az előáll $ax + by \ :\ x, y \in R$ alakban.

Bizonyítás: tekintsük az (a, b) ideált. Ez főideál, tehát előáll $(a, b) = (d)$ alakban. Azt állítjuk, hogy d legnagyobb közös osztó. $(a) \subseteq (a, b) = (d) \Rightarrow d \mid a$ és hasonlóan $d \mid b$, tehát közös osztó. $d \in (a, b) = (a) + (b) = \{ax + by \mid x, y \in R\}$, azaz d előáll $ax + by$ alakban. Így $d' \mid a, b \Rightarrow d' \mid ax + by = d$, tehát d valóban legnagyobb közös osztó.

Persze a többi legnagyobb közös osztó (ezek d asszociáltjai) is előáll $ax' + by'$ alakban: $ud = a \cdot ux + b \cdot uy$.

7.9.8 Állítás: ha $a, b \in R$ legnagyobb közös osztója létezik és előáll $d = ax + by$ alakban, akkor létezik m legkisebb közös többszörösük is és $md = ab$.

Bizonyítás: $d = 0$ érdektelen. Ha $d \neq 0$, akkor legyen $m = a'b'd$, ahol $a = a'd$ és $b = b'd$. Ez többszöröse a-nak is és b-nek is, hiszen $m = ab' = a'b$. Legyen most m' is közös többszörös. $a, b \mid m' \Rightarrow ab \mid am', bm' \Rightarrow ab \mid (ax + by)m'$, azaz $dm \mid dm'$. Ebből $d \neq 0$ miatt következik $m \mid m'$, így m minden közös többszörösnek osztója.

A generált ideáltól való megkülönböztethetőség végett a és b legnagyobb közös osztóját ideiglenesen $\overline{(a, b)}$-vel fogjuk jelölni.

7.9.9 Állítás: ha $\exists \overline{(a, b)}$ és előáll $d = ax + by$ alakban, akkor $\forall c \in R: c \cdot \overline{(a, b)} \sim \overline{(ca, cb)}$.

Bizonyítás: cd nyilván osztója ca, cb-nek. Másrészt ha $d' \mid ca, cb$, akkor $d' \mid cax + cby = cd$, tehát cd legnagyobb közös osztó.

7.9.10 Állítás: ha R főideálgyűrű, akkor UFD.

Bizonyítás: **7.9.6.1** és az azt követő megjegyzés, továbbá **7.9.5** alapján elég belátni, hogy ha p irreducibilis, akkor prím, azaz ha $p \mid ab$ és $p \nmid a$, akkor $p \mid b$. Mivel R főideálgyűrű, (p, a) előáll (d) alakban. Itt d osztója p-nek, tehát vagy asszociáltja, vagy egység. Asszociált nem lehet, mert d osztója a-nak, p pedig nem. Így $(p, a) = (1)$.

Az előző néhány állítás felhasználásával $(p) \supseteq (pb, ab)$, mert $pb, ab \in (p)$. $(pb, ab) = b \cdot (a, p) = b \cdot (1) = (b)$. Összefoglalva $(p) \supseteq (b)$, azaz $p \mid b$.

Beláttuk tehát, hogy minden euklideszi gyűrű főideálgyűrű és minden főideálgyűrű UFD.

7.9.11 Állítás: $\mathbb{Z}[i]$ euklideszi gyűrű.

Bizonyítás: azt állítjuk, hogy φ-nek a normát választva teljesülnek a feltételek. $N(\alpha\beta) = N(\alpha) \cdot N(\beta) \geq N(\alpha)$, az első feltételnek megfelel. Legyen most $\alpha, \beta \in \mathbb{Z}[i], \beta \neq 0$ tetszőleges, majd lássuk be, hogy megfelelő γ, δ választással $\alpha = \beta\gamma + \delta$ és $\delta = 0$ vagy $N(\delta) < N(\alpha)$.

β többszörösei egy $r = \sqrt{N(\beta)}$ élű négyzetrács csúcsai a komplex számsíkon. Vegyünk körül minden ilyen csúcsot egy r sugarú nyílt körlappal. Ezek bőven lefedik a teljes síkot, tehát α beleesik egy ilyen körlapba, ennek a

középpontja legyen $\beta\gamma$. Ekkor $\delta=\alpha-\beta\gamma$ választással $|\delta|<|\beta| \Rightarrow N(\delta)<N(\beta)$. Ha $\delta=0$, akkor kész vagyunk és ha nem, akkor is.

Ha a síkot $\frac{r}{\sqrt{2}}$ sugarú zárt körlapokkal fedtük volna le, akkor az erősebb $\delta=0$ vagy $N(\delta)\le\frac{1}{2}N(\alpha)$ feltételt kaptuk volna.

7.9.12 Definíció: legyen $d\in\mathbb{Z}\setminus\{0,1\}$ négyzetmentes. Ekkor $d\equiv 2,3\ (mod\ 4)$ esetén $R_d:=\mathbb{Z}[\sqrt{d}]$, $d\equiv 1\ (mod\ 4)$-nél pedig $R_d:=\{a+b\sqrt{d}\,|\,a,b\in\mathbb{Z}$ vagy $a-\frac{1}{2},b-\frac{1}{2}\in\mathbb{Z}\}=\mathbb{Z}[\omega]$, ahol $\omega=\frac{-1+\sqrt{d}}{2}$. Például R_{-3} az Euler-egészek gyűrűje.

7.10 Testbővítések

7.10.1 Definíció: az L test bővítése a K testnek, ha $K\subseteq L$ és az L feletti műveleteket K-ra megszorítva a K feletti műveleteket kapjuk. (Eddigi elnevezéseink mintájára ezt mondhatnánk úgy is, hogy K részteste L-nek.) Jelölése $L\ge K$. A K test L bővítését $L|K$-val szoktuk jelölni.

7.10.2 Definíció: az $L|K$ testbővítés foka L dimenziója, ha mint K feletti vektorteret tekintjük. Jelölése $(L:K)$. Ha $(L:K)$ véges, akkor $L|K$-t véges bővítésnek nevezzük.

7.10.3 Tétel: legyenek $M|L$, $L|K$ testbővítések. Ekkor az $M|K$ bővítésre $(M:K)=(M:L)\cdot(L:K)$.

Bizonyítás: legyen $\mathbf{B}_1=\{m_i\,|\,i\in\mathbf{I}\}$ bázis az M_L vektortérben és $\mathbf{B}_2=\{l_j\,|\,j\in\mathbf{J}\}$ bázis L_K-ban. Azt akarjuk belátni, hogy különböző $i\in\mathbf{I},j\in\mathbf{J}$ indexpárokra az $l_jm_i\in M$ elemek különbözőek és $\mathbf{B}=\{l_jm_i\,|\,i\in\mathbf{I},j\in\mathbf{J}\}$ bázis M_K-ban. Ha ez sikerül, akkor kész vagyunk, mert $\mathbf{B}$ egy $|\mathbf{I}|\cdot|\mathbf{J}|=dim_LM\cdot dim_KL$ számosságú bázis M_K-ban.

Ha $l_jm_i=l_{j^*}m_{i^*}$, akkor ez egy M-beli elem két felírása $\mathbf{B}_1$-beli elemek L feletti nem triviális $(l_i\neq 0)$ lineáris kombinációjaként. Ilyen felírás viszont csak egyféle van, tehát $l_j=l_{j^*}$ és $m_i=m_{i^*}$, amiből $j=j^*$ és $i=i^*$.

Legyen $m\in M$. Ekkor előáll $m=\sum_{i\in\mathbf{I}(m)}\lambda_im_i$ alakban, ahol $\mathbf{I}(m)\subset\mathbf{I}$ véges indexhalmaz és $\lambda_i\in L$. λ_i előáll $\lambda_i=\sum_{j\in\mathbf{J}(\lambda_i)}\kappa_{ij}l_j$ alakban, ahol $\mathbf{J}(\lambda_i)\subset\mathbf{J}$ véges és $\kappa_{ij}\in K$. Tehát $m=\sum_{i\in\mathbf{I}(m),j\in\mathbf{J}(\lambda_i)}\kappa_{ij}(l_jm_i)$, azaz $\mathbf{B}$ generálja M_K-t

Tegyük fel, hogy valamely $\mathbf{I}^*\subset\mathbf{I}$ és $\mathbf{J}^*\subset\mathbf{J}$ véges indexhalmazokra és $\kappa_{ij}\in K$ együtthatókra $\sum_{i\in\mathbf{I}^*,j\in\mathbf{J}^*}\kappa_{ij}(l_jm_i)=0$. Ekkor $\sum_{i\in\mathbf{I}^*}(\sum_{j\in\mathbf{J}^*}\kappa_{ij}l_j)m_i=0$. $\mathbf{B}_1$ lineáris független L felett, ezek az együtthatók pedig L-ben vannak. Ez tehát csak úgy lehetséges, ha minden együttható 0, azaz $\forall i\in\mathbf{I}^*:\sum_{j\in\mathbf{J}^*}\kappa_{ij}l_j=0$. Minthogy $\mathbf{B}_2$ lineárisan független az L_K vektortérben, itt is minden együttható 0, azaz $\forall i\in\mathbf{I}^*\forall j\in\mathbf{J}^*:\kappa_{ij}=0$. Így $\mathbf{B}$ lineárisan független M_K-ban, kész vagyunk.

7.10.4 Definíció: $L_1|K$ izomorf $L_2|K$-val, ha létezik olyan $\varphi:L_1\to L_2$ művelettartó bijekció, amely K-ra megszorítva identitás. Jelölése $L_1|K\simeq L_2|K$. $L_1|K_1$ és $L_2|K_2$ izomorfiáját akkor definiáljuk, ha $K_1\simeq K_2$ és van egy előre rögzített $\psi:K_1\xrightarrow{\sim}K_2$ izomorfizmusunk. Ez esetben $L_1|K_1\simeq L_2|K_2$, ha ψ kiterjeszthető $\bar{\psi}:L_1\xrightarrow{\sim}L_2$ izomorfizmussá.

Az $L_k\ge L_{k-1}\ge\ldots\ge L_1\ge L_0$ és $K_k\ge\ldots\ge K_0$ bővítésláncok izomorfak, ha van egy előre rögzített $\psi:L_0\xrightarrow{\sim}K_0$ izomorfizmusunk, ami lépésenként kiterjeszthető egy $\bar{\psi}:L_k\xrightarrow{\sim}K_k$ izomorfizmussá.

7.10.5 Definíció: $\alpha\in L|K$ algebrai (K felett), ha van olyan K feletti p polinom, amelynek gyöke.

Legyen $\alpha\in L|K$ algebrai és tekintsük az $I=\{p\in K[x]\,|\,p(\alpha)=0\}$ halmazt. Látható $I\lhd K[x]$. Tudjuk, hogy minden test feletti polinomgyűrű euklideszi a $\varphi:p\mapsto degp$ leképezéssel, tehát főideálgyűrű. Így hát I előáll (p^*) alakban. $I\neq(0)$, mert α algebrai, azaz $p^*\neq 0$. $K[x]$ egységei $K\setminus\{0\}$ elemei, tehát p^*-nak pontosan egy olyan p_α asszociáltja van, amelynek a főegyüttható ja 1. $I=(p_\alpha)$ éppen azt jelenti, hogy p_α minden K feletti polinomot oszt, amelynek gyöke α, sőt, pontosan ezeket osztja. Ez a legkisebb fokú polinom $K[x]$-ben, aminek gyöke α, tehát irreducibilis K felett.

7.10.6 Definíció: a fenti p_α polinomot α minimálpolinomjának hívjuk. Ez pontosan akkor elsőfokú, ha $\alpha\in K$. Ha hangsúlyozni akarjuk, hogy az 1 főegyüttható jú minimálpolinomról beszélünk, akkor α kanonikus polinomjának nevezzük.

7.10.7 Definíció: az $L|K$ bővítés egyszerű, ha $\exists\alpha\in L:K(\alpha)=L$.

7.10.8 Definíció: legyen $\alpha\in L|K$ algebrai K felett, a minimálpolinomja n-edfokú (ekkor $n\ge 1$). Ekkor K α-val való bővítése $K(\alpha)=\{a_0+a_1\alpha^2+\ldots+a_{n-1}\alpha^{n-1}\,|\,a_i\in K\}$. Az összeadást úgy végezzük, mintha α polinomjairól lenne szó. A szorzásnál viszont a szorzatpolinomot maradékosan elosztjuk p_α-val és az így kapott polinom lesz a szorzás

eredménye. Kiszámolható, hogy így testet kapunk és nyilván $K(\alpha)\big|K$. A bővítés foka $(K(\alpha):K)=n=deg\, p_\alpha$, mert $\{\alpha^k\big|0\le k<n\}$ bázisa $K(\alpha)_K$-nak.

7.10.9 Állítás: legyen $\alpha\in L\big|K$, $\beta\in M\big|K$ és legyen a minimálpolinomjuk azonos. Ekkor $K(\alpha)\big|K\simeq K(\beta)\big|K$.

Bizonyítás: rendelje φ a $(\sum_{k=0}^{n-1}a_k\alpha^k)\in K(\alpha)$ elemhez $(\sum_{k=0}^{n-1}a_k\beta^k)\in K(\beta)$-t. Szerencsénk van, izomorfizmus.

Az állítás megfordítása nem igaz, mert $\mathbb{C}\big|\mathbb{Q}$-ban $\mathbb{Q}(\sqrt{2})=\mathbb{Q}(1+\sqrt{2})$, de a minimálpolinomok x^2-2 és x^2-2x-1.

7.10.10 Definíció: legyen p n-edfokú, irreducibilis polinom K felett. Létre szeretnénk hozni egy $K(\alpha)$ testet, amely K (lehetőleg véges) bővítése és amelyben p-nek van egy α gyöke: legyen $K(\alpha)=K[x]/(p)$. Azt akarjuk belátni, hogy **(1)** $K(\alpha)$ test, **(2)** $K(\alpha)\ge K$, **(3)** $[K(\alpha):K]$ véges és **(4)** van olyan α $K(\alpha)$-ban, ami algebrai K felett és minimálpolinomja p.

(1): Jelölje a $K(x)=K[x]/(p)$ természetes homomorfizmusban egy a elem képét $\bar{a}$. Legyen $\bar{q}\ne 0$, ekkor $p\nmid q$. $K[x]$ euklideszi, tehát $\exists(p,q)$ legnagyobb közös osztó és előáll $pu=qv$ alakban. Ez csak 1 lehet, mert p irreducibilis. Azaz $pu=qv=1$, amiből $\bar{p}\bar{u}+\bar{q}\bar{v}=\bar{1}=1$. $\bar{p}=0$ miatt ez azt jelenti, hogy $\bar{v}=\bar{q}^{-1}$, azaz $\bar{q}$-nak van inverze. Mivel $\bar{q}$ tetszőleges nem 0 eleme volt a faktorgyűrűnek, ebben minden nem 0 elemnek van inverze. Kommutatív, tehát test. Másképp: ha $q\notin(p)$, akkor $1\in(p,q)$, azaz (p) maximális ideál $K[x]$-ben, ezért a faktorgyűrű test.

(2): p legalább elsőfokú, tehát K elemei páronként különböző mellékosztályokban vannak. A műveletek valóban a $K(\alpha)$-beli műveletek megszorításai, tehát $K(\alpha)\ge K$.

(3): A maradékos osztás miatt (p) minden additív mellékosztályában pontosan egy olyan elem van, melynek foka alacsonyabb n-nél, azaz a mellékosztályok megfelelnek az n-nél alacsonyabb fokú K feletti polinomok vektorterének, a bővítés foka éppen n.

(4): $\alpha=\bar{x}$ gyöke p-nek, mert a művelettartás miatt $p(\bar{x})=\overline{p(x)}$, ami 0. Eszerint α minimálpolinomja osztja p-t. Ez irreducibilis, tehát azonosak (konstans szorzó erejéig a főegyüttható miatt).

A fentiekből **7.10.9** szerint következik, hogy ha K valamely L bővítésében β gyöke p-nek, akkor L-ben bővítve K-t β-val egy $K(\alpha)$-val izomorf bővítést kapunk. Ez azért jó, mert így fedő test nélkül is tudunk bővíteni egy poli nom gyökével. Erre az eljárásra azt mondjuk, hogy p gyökét adjungáljuk K-hoz.

7.10.11 Definíció: $K(x)$ a K feletti racionális törtfüggvények teste, $K(x)=\{\frac{p(x)}{q(x)}\big|p(x),q(x)\in K[x],q\ne 0\}$. (Ez $K[x]$ hányadosteste.)

7.10.12 Definíció: α transzcendens K felett, ha nem gyöke egyetlen K feletti polinomnak sem.

7.10.13 Állítás: ha $\alpha\in L\big|K$ transzcendens K felett, akkor $K(\alpha)\simeq K(x)$. Ugyanis a $\frac{p(x)}{q(x)}\mapsto\frac{p(\alpha)}{q(\alpha)}$ leképezés könnyen ellenőrizhetően izomorfizmus.

Az ilyen bővítéseket transzcendens bővítéseknek nevezzük. Transzcendens bővítés foka mindig végtelen, hiszen $\{\alpha^k\big|k\in\mathbb{N}\}$ lineárisan független. (Ha ezek K feletti nem triviális lineáris kombinációjaként előállna a 0, az egy nem 0 polinomot adna K felett, aminek α gyöke.) Transzcendens például $\pi,e\in\mathbb{C}\big|\mathbb{Q}$.

Beláttuk, hogy minden $p\in K[x]$ irreducibilis polinomhoz található egy olyan $L\big|K$ véges bővítés, ahol p-nek van gyöke. Ekkor persze minden polinomhoz van ilyen L, mert ha valamelyik r irreducibilis faktorához megkonstruáljuk a megfelelő L-t, r gyöke egyben az az eredeti polinomnak is gyöke. Ennél azonban több is igaz:

7.10.14 Tétel: legyen $p\in K[x]$. Ekkor létezik K-nak egy olyan L véges bővítése, ahol p a főegyüttható tól eltekintve gyöktényezők szorzatára bomlik.

Bizonyítás: legyen p foka n és legyen k gyöke K-ban. Legyen q_1 egy irreducibilis faktora. Adjungáljuk K-hoz q_1 egy gyökét. A kapott L_1 test véges bővítése K-nak és itt már legalább $k+1$ gyöke van. Bontsuk p-t irreducibilis faktorokra L_1 felett, legyen az egyik tényező q_2. Adjungáljuk L_1-hez q_2 egy gyökét, így kapjuk L_2-t. Ez véges bővítése L_1-nek, így **7.10.3** szerint véges bővítése K-nak. Folytassuk ezt addig, amíg a kapott L_m testben p-nek már n gyöke van. Itt p gyöktényezőkre bomlik, $p=a_n(x-\alpha_1)\cdot\ldots\cdot(x-\alpha_n)$. Vegyük most $L_m\big|K$-t és ebben bővítsük K-t sorra $\alpha_1,\ldots,\alpha_n$-el. (Ezt azért csináljuk, hogy az L_m-be belekeveredett „felesleges" elemektől megszabaduljunk, tehát egy „nem túl nagy" L-hez jussunk.) Az így kapott $\bar{L}=K(\alpha_1,\ldots,\alpha_n)$ test megfelel az állítás feltételeinek. El is nevezzük:

7.10.15 Definíció: $\bar{L}|K$ felbontási teste $p\in K[x]$-nek, ha p $\bar{L}$-ben felbomlik $a_n(x-\alpha_1)\cdot\ldots\cdot(x-\alpha_n)$ alakban gyöktényezők szorzatára és $\bar{L}=K(\alpha_1,\ldots,\alpha_n)$.

7.10.16 Állítás: ha $\bar{L}_1|K$ és $\bar{L}_2|K$ egyaránt felbontási teste p-nek, akkor $\bar{L}_1|K\simeq\bar{L}_2|K$.

Bizonyítás: feltehetjük, hogy a főegyüttható 1. Legyen $\bar{L}_1$-ben $p=\prod_{k=1}^{n}(x-\alpha_k)$, $\bar{L}_2$-ben $p=\prod_{k=1}^{n}(x-\beta_k)$. Legyen továbbá K-ban $p=\prod_{k=1}^{s}p_k$, ahol a tényezők irreducibilisek. α_1 $\bar{L}_1$-ben gyöke valamelyik p_k-nak, hiszen gyöke a szorzatuknak. p_k gyöktényezők szorzatára bomlik $\bar{L}_2$-ben, azaz gyöke valamelyik β_i, például β_1. Ekkor α_1 és β_1 minimálpolinomja azonos (mégpedig p_k), tehát **7.10.9** szerint $K(\alpha_1)|K\simeq K(\beta_1)|K$. Legyen az ehhez tartozó izomorfizmus φ_1.

Ez a φ_1 izomorfizmus természetes módon kiterjed egy $K(\alpha_1)[x]\rightsquigarrow K(\beta_1)[x]$ izomorfizmussá, ami $K[x]$-re megszorítva az identitás. Bontsuk fel p-t $K(\alpha_1)$-ben irreducibilisek szorzatára: $p=(x-\alpha_1)\cdot\prod_{k=1}^{t}q_k$. Ekkor $p\varphi_1=(x-\alpha_1)\varphi_1\cdot\prod_{k=1}^{t}(q_k)\varphi_1$ és két polinomgyűrű izomorfiája miatt a $q_k\varphi_1$ tényezők irreducibilisek. $p\varphi_1=p$, mert $\varphi_1|_{K[x]}$ identitás. $(x-\alpha_1)\varphi_1=x-\alpha_1\varphi_1=x-\beta_1$. $\bar{L}_1$-ben α_2 gyöke valamelyik q_m-nek. $\bar{L}_2$-ben valamelyik β_{i^*} gyöke $(q_m)\varphi_1$-nek, legyen ez β_2. Ekkor β_2 minimálpolinomja $\bar{L}_2|K(\beta_1)$-ben azonos α_2 $\bar{L}_1|K(\alpha_1)$-beli minimálpolinomjának φ_1 szerinti képével. **7.10.9** bizonyítása átvihető erre az esetre is és kapjuk, hogy $K(\alpha_1)(\alpha_2)|K(\alpha_1)\simeq K(\beta_1)(\beta_2)|K(\beta_1)$.

Ezt folytatva az $\alpha_3,\ldots,\alpha_n$ $\bar{L}_1$-beli gyökökre kapjuk, hogy a $\bar{L}_1=K(\alpha_1\ldots\alpha_n)\geq K(\alpha_1\ldots\alpha_{n-1})\geq\ldots\geq K(\alpha_1)\geq K$ és $\bar{L}_2=K(\beta_1\ldots\beta_n)\geq\ldots\geq K(\beta_1)\geq K$ bővítésláncok izomorfak, speciálisan $\bar{L}_1|K\simeq\bar{L}_2|K$.

7.10.17 Tétel: minden K testnek van olyan $L|K$ bővítése, ahol $K[x]$ minden eleme felbomlik gyöktényezők szorzatára.

7.10.18 Definíció: $L|K$ algebrai, ha $\forall\alpha\in L$ algebrai K felett.

Minden véges bővítés algebrai, mert ha $(L:K)=n$ és $\alpha\in L$, akkor $\{1,\alpha,\alpha^2,\ldots,\alpha^n\}\subset L_K$ lineárisan összefüggő, így α gyöke egy legfeljebb n-edfokú K feletti polinomnak. Sőt, $L\geq K(\alpha)\geq K$-ra alkalmazva **7.10.3**-at $K(\alpha)|K$ osztója n-nek, tehát α minimálpolinomjának foka n osztója.

7.10.19 Állítás: ha $L|K$ és $M|L$ algebrai, akkor $M|K$ is az, tehát algebrai bővítés algebrai bővítése algebrai.

Bizonyítás: azt igazoljuk, hogy ha $L|K$ algebrai bővítés és α algebrai K felett, akkor L felett is algebrai. Legyen hát α gyöke az L feletti $p(x)=\sum_{k=0}^{n}a_kx^k$ polinomnak. Legyen $L_k=K(a_0,a_1,\ldots,a_k)$ $(k=0,\ldots,n+1)$ és $L'=L_n(\alpha)$. Ekkor a **7.10.10**-ben megadott konsrtukcióból $(M_0:K)$, $(L_{k+1}:L_k)$: $0\leq k\leq n$ és $(L':L_n)$ rendre végesek, azaz **7.10.3** szerint $L'|K$ is véges bővítés. Az előbbi definícióhoz fűzött megjegyzésünk értelmében $L'|K$ algebrai, így $\alpha\in L'$ algebrai K felett.

7.10.20 Állítás: legyen $L|K$ tetszőleges bővítés, $K_1=\{\alpha\in L|\,\alpha$ algebrai K felett$\}$. Ekkor K_1 résztestje L-nek.

Bizonyítás: azt kell belátnunk, hogy ha $\alpha,\beta\in L|K$ algebrai K felett, akkor $\alpha+\beta,\alpha+\beta,\alpha\beta,\frac{\alpha}{\beta}$ is algebrai K felett. Mindezek az elemek benne vannak a $K(\alpha,\beta)|K$ véges, tehát algebrai bővítésben. Eszerint valóban algebraiak K felett.

7.10.21 Tétel: minden K testnek van olyan $L|K$ algebrai bővítése, ahol $K[x]$ minden eleme felbomlik gyöktényezők szorzatára.

Bizonyítás: tudjuk (pontosabban elhittük), hogy létezik egy $L^*|K$ nem feltétlenül algebrai bővítés, ahol $K[x]$ minden eleme felbomlik. Legyen L az $L^*|K$-beli algebrai elemek halmaza. Ez **7.10.20** szerint algebrai bővítése K-nak és itt is felbomlik $K[x]$ minden eleme gyöktényezőkre, hiszen a gyökök mind algebraiak, így L-ben vannak.

Definíció: az algebrai számok halmaza kifejezés alatt általában $\mathbb{C}|\mathbb{Q}$ algebrai elemeinek $\mathbb{A}$ testét értjük.

7.10.22 Definíció: $\alpha\in\mathbb{C}$ algebrai egész, ha gyöke egy 1 főegyütthatójú $p\in\mathbb{Z}[x]$ polinomnak. Az algebrai egészek halmazát Ω-val jelöljük.

7.10.23 Állítás: $\alpha\in\mathbb{Q}\Leftrightarrow$ kanonikus polinomja egész együtthatós.

Bizonyítás: $\Rightarrow$: legyen α kanonikus polinomja q. Tudjuk, hogy $\exists p=x^n+\sum_{k=0}^{n-1}a_kx^k\in\mathbb{Z}[x]$, hogy $p(\alpha)=0$. Eszerint $q|p$ (mint $\mathbb{Q}$ feletti polinom), azaz $\exists r\in\mathbb{Q}[x]$: $p=qr$. p és q főegyütthatója 1, tehát r főegyütthatója is. Tudjuk, hogy egyértelműen léteznek olyan $c,c'\in\mathbb{Q}^+$ konstansok, hogy cq és $c'r$ primitív egész együtthatós polinomok. Ekkor $cc'\cdot p=cq\cdot c'r$. Primitív polinomok szorzata primitív, tehát $cc'\cdot p$ primitív. p már eredetileg is primitív volt, mert egész

együtthatós és 1 a főegyütthatója, tehát $cc'=1$. c és c' rendre a $cq, c'r \in \mathbb{Z}[x]$ polinomok főegyütthatói, tehát pozitív egészek. Így hát $c=c'=1 \Rightarrow q=qc \in \mathbb{Z}[x]$, a bizonyítandó állítás.

$\Leftarrow$: ha a kanonikus polinom $q \in \mathbb{Z}[x]$, akkor $q(\alpha)=0$ miatt $\alpha \in \Omega$, hiszen q főegyütthatója 1.

Megjegyzés: $\Omega \cap \mathbb{Q}=\mathbb{Z}$, mert $q \in \mathbb{Q}$ kanonikus polinomja $x-q$, ami pontosan akkor egész együtthatós, ha $q \in \mathbb{Z}$. Eszerint $\Omega \subset \mathbb{A}$ valódi tartalmazás.

7.10.24 Állítás: Ω részgyűrűje $\mathbb{C}$-nek, de nem test.

1. Lemma: legyen $\alpha_1, \dots, \alpha_n \in \Omega$. Ekkor található olyan S részgyűrű $\mathbb{C}$-ben, hogy $\mathbb{Z} \leq S < \mathbb{C}$, $\alpha_1, \dots, \alpha_n \in S$ és S mint $\mathbb{Z}$-modulus végesen generált.

Bizonyítás: legyen α_i kanonikus polinomjának foka $n(i)$, azaz $\alpha_i^{n(i)}=b_{i,n(i)-1}\alpha_i^{n(i)-1}+\dots+b_{i,1}\alpha_i+b_{i,0}$. Ekkor a $\{\prod_{i=1}^{n}\alpha_i^{k(i)} \mid 0 \leq k(i) \leq n(i)\}$ véges halmaz elemeinek összes $\mathbb{Z}$ együtthatós lineáris kombinációi egyrészt gyűrűt alkotnak, másrészt egy $\alpha_1, \dots, \alpha_n$-t és $\mathbb{Z}$-t tartalmazó $\mathbb{Z}$-modulust. Ez tehát megfelel S-nek.

2. Lemma: ha S olyan részgyűrű $\mathbb{C}$-ben, amelyre $\mathbb{Z} \leq S < \mathbb{C}$ és ami mint $\mathbb{Z}$-modulus végesen generált, továbbá $\alpha \in S$, akkor $\alpha \in \Omega$.

Bizonyítás: legyen ${}_{\mathbb{Z}}S={}_{\mathbb{Z}}\langle y_1, \dots, y_n \rangle$. S gyűrű $\Rightarrow$ $\alpha y_i \in S$ $\Rightarrow$ előáll $\alpha y_i=\sum_{j=1}^{n} a_{ij}y_j$: $a_{ij} \in \mathbb{Z}$ alakban. Tehát az $a_{i1}x_1+\dots+(a_{ii}-\alpha)x_i+a_{in}x_n=0$ $(i=1 \dots n)$ homogén lineáris egyenletrendszernek van nem triviális megoldása, nevezetesen $(y_1, \dots, y_n)$. Mátrixának determinánsa tehát 0. Ennek a mátrixnak a főátlójában az $(a_{ii}-\alpha)$ elemek vannak, minden más elem egész. A determinánst kifejtve tehát egy $(-1)^n$ főegyütthatójú egész együtthatós polinomját kapjuk α-nak, ami 0. Ekkor α definíció szerint algebrai egész.

Bizonyítás: legyen $\alpha, \beta \in \Omega$. Készítsük el az első lemma szerint létező S részgyűrűt $\mathbb{C}$-ben, ami fedi $\mathbb{Z}$-t, α-t, β-t és mint $\mathbb{Z}$-modulus végesen generált. Ebben benne lesz $\alpha+\beta, \alpha-\beta$ és $\alpha\beta$, így ezek a második lemma szerint algebrai egészek.

Megjegyzés:

Ω nyilván egységelemes integritási tartomány. Persze nagyon megörülnénk, ha tudnánk csinálni neki egy számelméletet, csak sajnos nem lehet, mert nincsenek benne irreducibilis elemek. Ugyanis ha $\alpha \in \Omega$, akkor nyilván $\sqrt{\alpha} \in \Omega$, így $\alpha=\sqrt{\alpha}\cdot\sqrt{\alpha}$. Ez vagy egy nem triviális felbontása α-nak, vagy $\sqrt{\alpha} \in U(\Omega)$. Ez utóbbi esetben viszont α is egység, tehát nem nevezzük irreducibilisnek.

Sokkal érdekesebbek a $K \cap \Omega$ gyűrűk, ahol $K \mid \mathbb{Q}$ egy véges (n-edfokú) bővítés. Ezt a témakört hívják az algebrai egészek számelméletének. $n=1$ esetén $K=\mathbb{Q}$, tehát $\mathbb{Z}$-t kapjuk (ezért szokták $\mathbb{Z}$-t néha „racionális egészek" névvel illetni).

Ha $n=2$, akkor $K=\mathbb{Q}(\alpha)$ egyszerű bővítés, ahol α kanonikus polinomja másodfokú, $x^2+2ax+b$: $a, b \in \mathbb{Q}$. Ennek $\exists \beta=(-a+\sqrt{d}) \in \mathbb{C}$ gyöke, ahol $d=a^2-b$. Ekkor $\mathbb{Q}(\alpha) \simeq \mathbb{Q}(\beta)=\mathbb{Q}(\sqrt{d})$. Feltehető, hogy d négyzetmentes egész, továbbá nem 0 vagy 1 (ez a két eset érdektelen). Az is látszik, hogy ha d_1 és d_2 különböző, a fenti feltételeknek megfelelő számok, akkor $\mathbb{Q}(\sqrt{d_1}) \neq \mathbb{Q}(\sqrt{d_2})$, mert x^2-d_1 pontosan az egyikben bomlik fel.

7.10.25 Állítás: $\mathbb{Q}(\sqrt{d}) \cap \Omega = R_d$.

Bizonyítás: $\mathbb{Q}(\sqrt{d})$ egy tetszőleges α eleme egyértelműen írható fel $\alpha=\frac{a+b\sqrt{d}}{c}$ alakban, ahol $a, b \in \mathbb{Z}, c \in \mathbb{Z}^+$ és $(a, b, c)=1$. Ekkor $c^2\alpha^2-2ca\cdot\alpha+a^2-b^2d=0$, tehát α kanonikus polinomja $x^2-\frac{2a}{c}\cdot x+\frac{a^2-db^2}{c^2}$. Kiszámolható, hogy ez $d \equiv 2, 3 \pmod 4$ esetén pontosan akkor egész együtthatós, ha $c=1$. Ha $d \equiv 1 \pmod 4$, akkor ezen kívül még akkor is, ha $c=2$ és a, b páratlan. Éppen R_d elemeit kaptuk.

7.11 Transzcendens valós számok

Ebben a részben azt bizonyítjuk be, hogy léteznek transzcendens valós számok. Először megemlítünk néhány állítást bizonyítás nélkül.

Definíció: az $r=\frac{p}{q} \in \mathbb{Q}$ szám $f(q)$ pontossággal közelíti az $\alpha \in \mathbb{R}$ számot, ha $|r-\alpha| < f(q)$.

Tétel: minden α irracionális szám végtelen sok racionális számmal közelíthető $\frac{1}{\sqrt{5}\cdot q^2}$ pontossággal. Ez a becslés éles, mert $\frac{1+\sqrt{5}}{2}$ nem közelíthető ennél jobban ($\frac{1}{\sqrt{5}}$-nél kisebb konstansra vagy 2-nél nagyobb kitevőre csak véges sok esetben).

Tétel (Liouville, 1844): ha α $n-$edfokú algebrai, akkor csak véges sok racionális szám közelítheti $\frac{1}{q^{n+1}}$ pontossággal. Ezért $\sum_{n\in\mathbb{N}}\frac{1}{k^{n!}}$ transzcendens, mert részletösszegei túl jól közelítik (k 1-nél nagyobb pozitív egész).

Tétel (Thue-Siegel): ha α $n-$edfokú algebrai és $c\in\mathbb{R}$ tetszőleges, akkor α-t csak véges sok racionális szám közelítheti $\frac{c}{q^n}$ pontossággal.

Tétel (Roth): ha α $n-$edfokú algebrai, $n\geq 3$ és $\varepsilon>0$, akkor α-t csak véges sok racionális szám közelítheti $\frac{1}{q^{2+\varepsilon}}$ pontossággal.

7.11.1 Tétel (Cantor, 1874): $|\mathbb{A}|=\aleph_0<|\mathbb{R}|$, tehát nem lehet minden valós szám algebrai.

Bizonyítás: leellenőrizhető, hogy megszámlálható sok egész együtthatós egy főegyütthatós polinom van és mindegyiknek véges sok gyöke. Így az összes ilyen gyök még mindig megszámlálható, $\mathbb{A}$ pedig ezek halmaza.

Ez utóbbi tétel apró szépséghibája, hogy nem mutat nekünk egyetlen transzcendens számot sem. Liouville tételéből pedig csak egy felettébb érdektelen számról tudtuk meg, hogy transzcendens. Ezzel persze nem elégszünk meg.

7.11.2 Tétel (Hermite, 1873): e transzcendens.

Bizonyítás: e azon tulajdonságát fogjuk használni, hogy $\frac{\mathrm{d}}{\mathrm{d}x}(e^x)=e^x$. (Meg persze több analízisbeli tételt.)

$\lightning\ e\in\mathbb{A}$, azaz $\boxdot\ a_m e^m+a_{m-1}e^{m-1}+\ldots+a_1 e+a_0=0$, ahol $a_i\in\mathbb{Z}$ és $a_0\neq 0$. Legyen $g(x)=x^{p-1}(x-1)^p(x-2)^p\ldots(x-m)^p$ és $f(x)=\frac{g(x)}{(p-1)!}$; mindkettő $(mp+p-1)$-edfokú polinom. Legyen $F(x)=f(x)+f'(x)+f''(x)+\ldots+f^{(mp+p-1)}(x)$. Ekkor

$$\frac{\mathrm{d}}{\mathrm{d}x}\left(e^{-x}F(x)\right)=e^{-x}(F'(x)-F(x))=-e^{-x}f(x). \qquad \text{Ezt felhasználva:}$$

$$a_j e^j\cdot\int_0^j e^{-x}f(x)dx=a_j e^j\cdot\left[e^{-x}F(x)\right]_{x=0}^{j}=a_j\cdot e^j\cdot\left(F(0)-e^{-j}F(j)\right) \qquad \text{Összegezve } j=0,1,\ldots,m\text{-re:}$$

$$\sum_{j=0}^{m}a_j e^j\cdot\int_0^j e^{-x}f(x)dx=F(0)\cdot\left(\sum_{j=0}^{m}a_j e^j\right)-\sum_{j=0}^{m}a_j\cdot F(j) \qquad \text{Jelölje a ezt } S_p.$$

A jobb oldal első tagja $\boxdot$ szerint 0. A másik összeget kibontva $S_p=-\sum_{j=0}^{m}\sum_{i=0}^{mp+p-1}a_j f^{(i)}(j)$. Azt állítjuk, hogy a $j=0, i=p-1$ eset kivételével ennek a kettős összegnek minden tagja egy $p-$vel osztható egész szám.

Tekintsük először a $j\neq 0$ esetet. Ekkor a $g(x)=x^{p-1}(x-1)^p\ldots(x-j)^p\ldots(x-m)^p$ szorzatot $i-$szer deriválva egy soktagú összeget kapunk. Ennek minden $\xi(x)$ tagjában szerepel tényezőként $(x-j)^p$ valahanyadik (k_ξ-edik) deriváltja. Ha $k_\xi>p$, akkor $\left((x-j)^p\right)^{(k_\xi)}=0$, tehát $\xi\equiv 0$. Ha $k_\xi<p$, akkor $(x-j)$ osztja $\left((x-j)^p\right)^{(k_\xi)}$-t, tehát annak gyöke $x=j$, így $\xi(j)=0$. Így a tagok összegét elosztva $(p-1)!$-al továbbra is 0-t kapunk, másrészt $a_j f^{(i)}(j)$-t, ezért az 0. Ha $k_\xi=p$, akkor $\left((x-j)^p\right)^{(p)}=p!$ miatt $\xi(j)$ osztható $p!$-al, így $(p-1)!$-al osztva is p többszöröse lesz.

Ha $j=0$, de $i\neq p-1$, akkor a $g(x)$ szorzat i-edik deriváltjának egy $\zeta(x)$ tagja a fenti módon csak akkor nem 0-t vesz fel $x=j=0$-ban, ha x^{p-1} pontosan $p-1$-szer deriválva szerepel benne. Ez csak $i\geq p$ esetén fordulhat elő, azaz ζ-ben még legalább egy $(x-k)^p$-nek legalább az első deriváltja szerepel tényezőként. Így hát

$$\zeta(x)=\left(x^{p-1}\right)^{(p-1)}\cdot\ldots\cdot\left((x-k)^p\right)^{(d)}\cdot\ldots=(p-1)!\cdot\ldots\cdot\left(p(p-1)\ldots(p-d+1)\right)\cdot\ldots=p!\cdot\ldots,$$

ahol minden ki nem írt tényező egész együtthatós polinomja $x-$nek. Tehát $\zeta(x_0)$ minden ζ tagra és minden egész x_0 $-$ra osztható lesz $p!$-al, így az összegük, $g(x)$ is. Ezt alkalmazva $x_0=j$-re, elosztva $(p-1)!$-al és megszorozva $a_j\in\mathbb{Z}$ -vel kapjuk, hogy $a_j f^{(i)}(j)$ p-vel osztható egész.

A $j=0, i=p-1$ esetben is csak úgy kaphatunk nem 0 tagot $g(x)$ i-edik deriváltjában az $x=j=0$ behelyettesítésnél, ha a tagban x^{p-1} $(p-1)$-edik deriváltja szerepel. Egyetlen ilyen tag van, mégpedig $\vartheta(x)=\left(x^{p-1}\right)^{(p-1)}\cdot(x-1)^p\ldots(x-m)^p$. Tehát $g^{(p-1)}(0)=\vartheta(0)=(p-1)!\cdot(-1)^p\cdot(-2)^p\cdot\ldots\cdot(-m)^p=(p-1)!\cdot(-1)^{pm}\cdot(m!)^p$, azaz $a_0 f^{(p-1)}(0)=a_0(-1)^{pm}\cdot(m!)^p$.

Ha p egy $\mathbf{max}(|a_0|,m)-$nél nagyobb prím, akkor ez egy $p-$vel nem osztható egész, míg S_p összegalakjának többi tagja osztható p-vel. Eszerint $S_p\in\mathbb{Z}, p\nmid S_p\ \Rightarrow\ S_p\in\mathbb{Z}\setminus\{0\}\ \Rightarrow\ \boxdot\ |S_p|\geq 1$.

Tekintsük S_p baloldali felírását. Vegyük észre, hogy $0\leq x\leq m$ esetén $|f(x)|\leq\frac{1}{(p-1)!}\cdot m^{mp+p-1}$. Ezt minden tagra alkalmazva

$$|S_p| = \left|\sum_{j=0}^{m} a_j e^j \cdot \int_0^j e^{-x} f(x)\mathrm{d}x\right| \le \sum_{j=0}^{m} \left|a_j e^j \cdot \int_0^j \frac{m^{mp+p-1}}{(p-1)!}\right| \le \left(\sum_{j=0}^{m} |a_j e^j \cdot j|\right) \cdot \frac{m^{mp+p-1}}{(p-1)!}$$

Ha $p\to\infty$, akkor ez a kifejezés 0-hoz tart, mert p exponenciális függvényének és $(p-1)!$-nak a hányadosa. Viszont ⚀ szerint tetszőlegesen nagy p található, amelyre $|S_p|\ge 1$, ↯.

7.11.3 Tétel (Lindemann, 1882): π transzcendens.

Bizonyítás: elég belátni, hogy $i\cdot\pi$ transzcendens. Ehhez többek közt azt használjuk, hogy $e^{i\alpha}=\cos\alpha+i\cdot\sin\alpha$, tehát $e^{i\pi}+1=0$. ↑ $\vartheta_1(x)=\prod_{j=1}^{n}(x-\alpha_i)\in\mathbb{Q}[x]$, melynek gyöke $i\pi$, azaz pl. $\alpha_1=i\pi$. Legyen $H=\{\alpha_1,\alpha_2,\dots,\alpha_n\}$. Ekkor $(e^{\alpha_1}+1)(e^{\alpha_2}+1)\dots(e^{\alpha_n}+1)=0$, hiszen az első tényező 0. Kiszorozva $\sum_{G\subseteq H}\left(e^{\sum_{\alpha\in G}\alpha}\right)=0$. Legyen $\vartheta_s(x)$ $(2\le s\le n)$ az az 1 főegyütthatós polinom, melynek gyökei az α_j-k s tagú összegei, azaz $\{\sum_{\alpha\in G}\alpha : G\subseteq H, |G|=s\}$. $\vartheta_s(x)$ együtthatói előjeltől eltekintve gyökei elemi szimmetrikus polinomjai. A gyökök választása miatt ezek egész együtthatós szimmetrikus polinomjai $\alpha_1\dots\alpha_n$-nek, tehát egész együtthatós polinomjai $\alpha_1\dots\alpha_n$ elemi szimmetrikus polinomjainak, melyek ϑ_1 együtthatói, azaz racionálisak.

Eszerint $\vartheta^*(x)=\prod_{j=1}^{n}\vartheta_j(x)\in\mathbb{Q}[x]$. Ahányszor 0 előáll, mint néhány (legalább 0) különböző α_j összege, annyiszoros (jelölje k) gyöke ϑ^*-nak 0. Minthogy 0 darab α_j összege 0, $k\ge 1$. Leosztva ϑ^*-t x^k-al és megszorozva együtthatói közös nevezőjével egy $\vartheta(x)=cx^r+c_1x^{r-1}+\dots+c_r\in\mathbb{Z}[x]$ polinomot kapunk, ahol $c,c_r\ne 0$ és a $\beta_1,\beta_2,\dots,\beta_r$ gyökökre teljesül $0=(e^{\alpha_1}+1)(e^{\alpha_2}+1)\dots(e^{\alpha_n}+1)=e^{\beta_1}+e^{\beta_2}+\dots+e^{\beta_r}+(e^0+\dots+e^0)$, ahol a zárójelben pontosan k darab $e^0=1$ van. Tehát

⚀ $$e^{\beta_1}+e^{\beta_2}+\dots+e^{\beta_r}=-k.$$

Legyen $g(x)=x^{p-1}(\vartheta(x))^p$, $f(x)=\frac{c^{rp}}{(p-1)!}\cdot g(x)$ és $F(x)=f(x)+f'(x)+\dots+f^{(rp+p-1)}(x)$. Ekkor $\frac{\mathrm{d}}{\mathrm{d}x}(e^{-x}\cdot F(x))=-e^{-x}\cdot f(x)$, amiből $-\int_0^x e^{-y}f(y)dy=e^{-x}\cdot F(x)-F(0)$. Beszorozva e^x-el és $y=\lambda x$-et helyettesítve

$$F(x)-e^x\cdot F(0)=-x\cdot\int_0^1 e^{(1-\lambda)x}f(\lambda x)\mathrm{d}\lambda \qquad /\textstyle\sum(\dots): x=\beta_1,\beta_2,\dots,\beta_r;\ ⚀$$

⚀ $$k\cdot F(0)+\sum_{j=1}^{r}F(\beta_j)=\sum_{j=1}^{r}F(\beta_j)-\sum_{j=1}^{r}e^{\beta_j}\cdot F(0)=\sum_{j=1}^{r}\beta_j\cdot\int_0^1 e^{(1-\lambda)\beta_j}f(\lambda\beta_j)\mathrm{d}\lambda.$$

Tekintsük $\sigma_t=\sum_{j=1}^{r}g^{(t)}(\beta_j)$-t. $0\le t<p$ esetén ezt osztja ϑ, hiszen g-t osztja ϑ^p. ϑ-nak gyöke β_j, így $\sigma_t=0$.

Legyen most $p\le t\le rp+p-1$. Csak azokkal a tagokkal kell foglalkoznunk, ahol ϑ^p legalább p-szer deriválva szerepel tényezőként. Ezek összegéből kiemelve a $(\vartheta^p)^{(p)}$-ből származó $p!$ szorzótényezőt a maradék szimmetrikus, egész együtthatós és legfeljebb rp fokú polinomja $\beta_1\dots\beta_r$-nek, tehát előáll azok elemi szimmetrikus polinomjainak legfeljebb rp fokú egész együtthatós polinomjaként és $\sigma_i(\beta_i\dots\beta_r)=\frac{c_i}{c}\cdot(-1)^i$. Így ha a teljes összeget megszorozzuk $\frac{c^{rp}}{(p-1)!}$-el, akkor a nevezők elszállnak, $p!$-ból pedig marad még p, tehát egy p-vel osztható egész számot kapunk, másrészt $\sum_{j=1}^{r}f^{(t)}(\beta_j)$-t. Eszerint $\sum_{j=1}^{r}F(\beta_j)=\sum_{j=1}^{r}\sum_{t=0}^{rp+p-1}f^{(t)}(\beta_j)$ egy p-vel osztható egész szám.

$f^{(t)}(0)$ p-vel osztható egész, ha $t\ne p-1$. (Ha egy ξ tagban x^{p-1}-t nem pont $p-1$-szer deriváljuk, akkor 0-ban ξ eltűnik. Ha pont ennyiszer és $t\ne p-1$, akkor ϑ^p-t legalább egyszer. x^{p-1} deriválásából jön egy $(p-1)!$ szorzó, ami kiejti a nevezőt, ϑ^p deriválásából jön egy p szorzó és minden tényező egész, ha x egész.) $t=p-1$ esetén $f^{(t)}(0)=c^{rp}\cdot c_r^p$. Ezek szerint $F(0)=\sum_{t=0}^{rp+p-1}f^{(t)}(0)$ egész és $F(0)\equiv c^{rp}\cdot c_r^p \pmod p$.

Összefoglalva: ⚀ bal oldala egész és $\equiv k\cdot c^{rp}\cdot c_r^p \pmod p$, ami $p>\mathbf{max}(k,|c|,|c_r|)$ prím esetén nem osztható p-vel, hiszen $k,c,c_r\ne 0$. Így hát $|\textit{bal oldal}|\ge 1$ ha p ilyen.

Legyen $m(j)=\mathbf{sup}_{0\le\lambda\le 1}|\vartheta(\lambda\beta_j)|$. Így ha $0\le\lambda\le 1$, akkor $|f(\lambda\beta_j)|\le\frac{1}{(p-1)!}\cdot|c|^{rp}\cdot|\beta_j|^{p-1}\cdot|m(j)|^p$ és ⚀ jobb oldalának abszolútértéke felülről becsülhető $\frac{1}{(p-1)!}\cdot\sum_{j=1}^{r}|c|^{rp}\cdot|\beta_j|^{p-1}\cdot|m(j)|^p$-vel. Ez $p\to\infty$ esetén 0-hoz tart. Viszont végtelen sok $p\in\mathbb{N}$ számra lesz az abszolútérték legalább 1, ↯.

7.12 Szerkeszthetőség

A euklideszi síkon szerkesztés alatt azt értjük, hogy valamilyen adott pontokból és távolságokból (megjegyzés: egy d távolságot meg lehet adni két ponttal, tehát elég pontokat megadni) kiindulva véges sok lépést végzünk, melyek mindegyike az alábbiak valamelyike:

(1) két ismert egyenes metszésponjának kijelölése (egy egyenes ismert, ha adott két pontja);

(2) egy ismert körvonal és egy ismert egyenes metszéspontjának kijelölése (egy kör ismert, ha adott a középpontja és a sugara, azaz a középpontja és a kerület egy pontja);

(3) két ismert körvonal metszéspontjának kijelölése.

Egy d hosszúság ismert, ha ismert két pont, melyekről tudjuk, hogy távolságuk $|d|$. Egy φ szög szerkeszthető, ha tudunk olyan egyenespárt szerkeszteni, melyek szöge φ.

7.12.1 Definíció: α szerkeszthető a $H\subset\mathbb{R}$ halmazból, ha tudunk szerkeszteni egy α ($\alpha<0$ esetén $-\alpha$) hosszú szakaszt, amennyiben adott számunkra minden $a\in H$-ra egy a hosszú szakasz. (Általában $1\in H$-t megköveteljük.) Vegyük észre, hogy ha $K\subset\mathbb{R}$ minden eleme szerkeszthető H-ból és α szerkeszthető K-ból, akkor H-ból is.

7.12.2 Tétel: $H=\{1\}$-ből tetszőleges $\frac{p}{q}\in\mathbb{Q}^+$ szerkeszthető. (Ld. párhuzamos szelők tétele.)

7.12.3 Tétel: $\{a,b,c\}$-ből szerkeszthető $a\pm b,\frac{ab}{c},\sqrt{ab}$ és bármilyen $\frac{p}{q}\in\mathbb{Q}$ racionális *szám*hoz (értsd: nem távolságként adott, hanem mint két egész szám hányadosa) $\frac{p}{q}\cdot a$.

Bizonyítás: $a\pm b$ triviálisan, $\frac{ab}{c}$ és $\frac{p}{q}\cdot a$ a párhuzamos szelők tételével. $\sqrt{ab}$-hez vegyünk fel az e egyenesen sorra A,B,C pontokat úgy, hogy $\overline{AB}=a,\overline{BC}=b$ legyen. Messük el az $\overline{AC}$ szakasz felezőpontja közepű $\frac{a+b}{2}$ sugarú kört az e-re B-ben állított merőleges egyenessel, a metszéspontok legyenek M és N. Ekkor $\overline{BM}=\sqrt{ab}$ lesz.

Következmény: ha $1,a,b\in H$, akkor H-ból szerkeszthető $a^{-1},ab,\sqrt{a},\frac{a}{b}$.

7.12.4 Következmény: ha $1\in H$, akkor a H-ból szerkeszthető szakaszok K halmaza résztestje $\mathbb{R}$-nek és bővítése $\mathbb{Q}$-nak.

Minthogy $1\in H$ feltételezése legfeljebb a sík átskálázását jelenti, a fenti következmény miatt szoríthozhatunk azokra az esetekre, ahol $H=K$ az $\mathbb{R}|\mathbb{Q}$ bővítés egy közbülső teste..

Megjegyzés: tekinthetjük továbbá a síkot $\mathbb{C}$-nek is. Ez esetben $z\in\mathbb{C}$ definíció szerint akkor szerkeszthető a $H\subset\mathbb{C}$ halmazból, ha megszerkeszthető, amennyiben adottak H pontjai a komplex síkon (a komplex síkhoz automatikusan jár origó). Ismét elég az $1\in H$ esettel foglalkozni, hiszen z pontosan akkor szerkeszthető H-ból, ha $z\alpha^{-1}$ szerkeszthető $H\cdot\alpha^{-1}$-ből. Persze $H=\{1\}$-ből már minden racionális koordinátájú pont megszerkeszthető, speciálisan a valós tengely is. Ha pedig van valós tengely, akkor lehet rá tükrözni, azaz konjugálni. Így az alábbi műveletek elvégezhetőek szerkesztéssel: összeadás, ellentettképzés, konjugálás, valós és képzetes rész képzése, szorzás, osztás; továbbá a négyzetgyökvonás is. Ismét elég tehát a $\mathbb{C}|\mathbb{Q}$ bővítés közbülső testei közül választani H-t. Vegyük észre, hogy a másodfokú polinom megoldóképlete szerint a K közbülső testből minden K feletti legfeljebb másodfokú polinom gyökei szerkeszthetőek. Könnyen láthatóan ugyanakkor szerkeszthető K-ból $z=r(\cos\varphi+i\cdot\sin\varphi)$, $\{r,\varphi\}$ vagy $\{\mathrm{Re}\,z,\mathrm{Im}\,z\}$. Speciálisan $\alpha\in\mathbb{R},K<\mathbb{R}$ esetén a szerkeszthetőségre adott két definíciónk ekvivalens.

7.12.5 Tétel: **(1)** ha $\alpha\in\mathbb{R}$ szerkeszthető a $K<\mathbb{R}$ résztestből, akkor $(K(\alpha):K)$ 2-hatvány és **(2)** ha $z\in\mathbb{C}$ szerkeszthető a $K<\mathbb{C}$ résztestből, akkor $(K(z):K)$ 2-hatvány. Speciálisan ha α ill. z szerkeszthető $\mathbb{Q}$-ból, akkor $gr_{\mathbb{Q}}(\alpha)$ ill. $gr_{\mathbb{Q}}(z)$ 2-hatvány.

(Előbbi megjegyzésünk vége szerint elég lenne **(2)**-t belátni. Azért belátjuk külön **(1)**-et is.)

Bizonyítás: **(1)** legyenek a távolságok úgy megadva, hogy adott egy e egyenes, azon egy O pont és $\forall d\in K$-ra adott egy $P_d\in e$ pont O-tól d távolságra. Helyezzük el a síkot egy Descartes-féle koordináta-rendszerbe úgy, hogy az origó O, az x tengely e legyen. Most minden fellépő távolság és minden ismert pont mindkét koordinátája 2-hatvány rendű $\mathbb{R}|K$-ban (mind K-beli). Azt akarjuk belátni, hogy ez a tulajdonság tetszőleges szerkesztési alaplépés során megmarad. Minthogy a távolságok előállnak a koordinátákból összeadás, kivonás, szorzás és gyökvonás segítségével (Pitagorasz-tétel), elegendő a koordinátákra vonatkozó tulajdonság megmaradását belátni.

Két egyenes metszéspontja egy olyan 2×2-es lineáris egyenletrendszer megoldása, melynek együtthatói az ismert pontok koordinátáiból az alapműveletekkel megkaphatóak. Ez benn marad a K kiindulási testben.

Egy ismert egyenes és kör metszéspontjai előállnak egy $x^2+y^2+ax+by+c=0$, $Ax+By+C=0$ alakú egyenletrendszer megoldásaiként, ahol az együtthatók – mint fent – K-beliek. A megoldások koordinátái legfeljebb másodfokúak $\mathbb{R}|K$-ban, tehát benne vannak egy $L|K$ 2-hatvány rendű bővítésben.

Két kör metszéspontjai előállnak egy $x^2+y^2+ax+by+c=0$, $x^2+y^2+Ax+By+C=0$ alakú egyenletrendszer megoldásaként. Ez ekvivalens az $x^2+y^2+ax+by+c=0$, $(a-A)x+(b-B)y+(c-C)=0$ egyenletrendszerrel, amelyiknek megoldásai ismét 2-hatvány rendű bővítései K-nak. Ezzel az állítást beláttuk.

(2) Ugyanígy belátható, hogy minden szerkesztési lépés egy első- vagy másodfokú polinom megoldását jelenti, tehát 2-hatvány rendű bővítést eredményez.

Megjegyzés: a tétel megfordítása nem igaz – z pontosan akkor szerkeszthető K-ból, ha $K(z)\big|K$ megkapható másodfokú bővítések egymásutánjaként, ami nem minden 2-hatvány rendű z-re áll fenn.

7.12.6 Tétel: az alábbi szerkesztési feladatok nem oldhatóak meg:

(1) adott egy kocka (mármint az éle). Szerkesszünk olyan kockát (az élét), melynek térfogata a megadott kocka térfogatának kétszerese;

(2) harmadoljunk el egy megadott szöget;

(3) "környégyszögesítés" – adott egy kör, szerkesszünk vele azonos területű négyzetet.

Bizonyítás:

(1) válasszuk egységnek a megadott kocka élét. Feladatunk $\sqrt[3]{2}$ szerkesztése, de $gr_{\mathbb{Q}}(\sqrt[3]{2})=3$.

(2) azt látjuk be, hogy 20° nem szerkeszthető $\mathbb{Q}$-ból, pedig 60° igen. φ pontosan akkor szerkeszthető $\mathbb{Q}$-ból, ha $\cos\varphi$ szerkeszthető. A $\cos(3\varphi)=4\cos^3\varphi-3\cos\varphi$ képletből $\cos(3\cdot 20^\circ)=\frac{1}{2}$ felhasználásával $\alpha=\frac{\cos 20^\circ}{2}$ gyöke az $x^3-3x-1=0$ egyenletnek. Ez sajnos irreducibilis, tehát $gr_{\mathbb{Q}}(\alpha)=3$, $\cos 20^\circ$ nem szerkeszthető.

(3) válasszuk egységnek a kör sugarát, ekkor feladatunk $\sqrt{\pi}$ szerkesztése $\mathbb{Q}$-ból, de $\sqrt{\pi}$ transzcendens.

7.12.7 Tétel (Gauss): pontosan azon $n\in\mathbb{N}\ (n\geq 3)$ számokra szerkeszthető szabályos n-szög, melyek $2^k\cdot\prod p_i$ alakba írhatóak, ahol $k\in\mathbb{N}$ és a p_i-k $2^{2^k}+1$ alakú (ún. Fermat-)prímek.

Ehhez elég az állítást páratlan prímek hatványaira belátni, azaz hogy $p\geq 3$ prímre szabályos p^k-szög pontosan akkor szerkeszthető, ha p Fermat-prím és $k=1$. Mi csak azt látjuk be (nagyjából), hogy a feltétel szükséges.

Pontosan akkor tudunk szabályos p^k-szöget szerkeszteni, ha meg tudjuk szerkeszteni valamelyik p^k-adik primitív egységgyököt, ε_{p^k}-t. Ha ε_p szerkeszthető, akkor foka 2-hatvány. Kanonikus polinomja $\Phi_p(x)$, mert ez irreducibilis, egész együtthatós, 1 a főegyüttható és gyöke ε_p. Ennek foka $p-1$, tehát p mindenesetre 2^m+1 alakú kell legyen. Ha m-nek lenne egy 1-nél nagyobb páratlan osztója, azaz $m=q\cdot(2r+1)$ állna fenn valamely $q,r\in\mathbb{Z}^+$ számokra, akkor $a=2^q$ jelöléssel $p=\left(a^{2r+1}-(-1)^{2r+1}\right)=(a+1)\cdot\left(\sum_{i=0}^{2r}(-a)^i\right)$ – mivel mindkét tényező 1-nél nagyobb – ellentmodana annak, hogy p prím. Tehát m 2-hatvány és $p=2^m+1=2^{2^k}+1$. Ha valamely $k\geq 2$-re szerkeszthető szabályos p^k-szög, akkor $k=2$-re is, tehát szerkeszthető ε_{p^2}. Ez gyöke a

$$\Phi_{p^2}(x)=\frac{x^{p^2}-1}{x^p-1}$$

polinomnak. Némi fáradsággal belátható, hogy Φ_{p^2} irreducibilis, így $gr_{\mathbb{Q}}(\varepsilon_{p^2})=deg(\Phi_{p^2})=p\cdot(p-1)$, ami nem 2-hatvány. Így ε_{p^2} nem szerkeszthető.