Megoldások a Bolyai Kollégium szemináriumán
1999 március 4-én részben megbeszélt feladatokhoz

A John H. Conway "On numbers and games " című könyve 6. fejezete alapján.

Definició:
Legyen $L(H)$ a H halmazban nem szereplő legkisebb rendszám (legkisebb kizárt).
Definiáljuk rekurzióval a rendszámokon a következő összeadást és szorzást:

$$a+b = L(\{a'+b | a' < a\} \cup \{a+b' | b' < b\})$$

$$ab = L(\{(a'b+ab')+a'b' | a' < a, b' < b\}).$$

Jelölés: Egyszerűsítjük a jelölést, a' mindig az a-nál kisebb rendszámokon fut végig, b' a b-nél kisebbeken, stb., így a fenti definició egyszerübben:

$$a+b = L(a'+b, a+b')$$

$$ab = L(a'b+ab'-a'b').$$

Itt a $-$ másik jel a $+$-ra, a zárójelezést az asszociativitás miatt hagyhattuk el, amit majd igazolunk.
A feladatok arra vonatkoztak, hogy lássuk be, a rendszámok így testet alkotnak, és tudjunk meg minál többet erről a testről.

Egy soros bizonyítás egy állításra olyan induktív bizonyítás, ahol formális átalakítások során korábban bizonyítottakat használunk, és a bizonyítandót egyszerűbb esetben. Ilyen majdnem minden alábbi bizonyítás. Itt egyszerűbbnek akkor tekintünk egy rendszám k-ast, egy másiknál, ha minden eleme kisebb vagy egyenlő, és az egyik kisebb. Ez a részben rendezés van a rekurzív definició mögött, és a 13–14 egyszerű kiterjesztések is erre hivatkoznak.

I. Összeadás
1. Nullelem: $a+0 = a$
Biz: $a+0 = L(a'+0) = L(a') = a$.
2. Kommutativitás: $a+b = b+a$
Biz: $a+b = L(a'+b, a+b') = L(b+a', b'+a) = b+a$.
3. Technikai: Ha $a = L(H_a)$ és $b = L(H_b)$, akkor $a+b = L(a''+b, a+b'')$ ahol a'' H_a elemein fut végig, b'' pedig H_b elemein.
Biz: H_a-ban szerepel minden a-nál kisebb rendszám és esetleg néhány a-nál nagyobb, és hasonló H_b és b viszonya. Tehát elég belátni, hogy $a'' > a$, illetve $b'' > b$ esetén $a''+b \neq a+b$ illetve $b''+b \neq a+b$. De $a''+b$ definiciója szerint a legkisebb kizárt egy olyan halmazban, ami tartalmazza $a+b$-t, így az első állítás igaz. A második hasonlóan belátható, vagy következik a kommutativitásból.
4. Asszociativitás: $a+(b+c) = (a+b)+c$.
Biz: $a+(b+c) = L(a'+(b+c), a+(b'+c), a+(b+c')) = L((a'+b)+c, (a+b')+c, (a+b)+c') = (a+b)+c$. Itt az $a+(b+c)$ és $(a+b)+c$ felírásához nem a definiciót használtuk, hanem 3-at a $b+c = L(b'+c, b+c')$ és az $a+b = L(a'+b, a+b')$ halmazokkal.
5. Az exponens 2: $a+a = 0$
Biz: $a+a = L(a'+a, a+a')$, így az kell, hogy $a'+a \neq 0 \neq a+a'$, ami igaz, hisz mind a kettő legkisebb kizárt egy halmazban, amiben szerepel $a'+a' = 0$.
1–5: A rendszámok a $+$-ra kettő exponensű Abel-csoportot adnak, melynek 0 a nulleleme.

II. Szorzás

6. Nullelem: $a \cdot 0 = 0$

Biz: $a \cdot 0 = L(\emptyset) = 0$. Nem is kéne bizonyítani, mert következik 10-ből.

7. Egységelem: $1 \cdot a = a$

Biz: $1 \cdot a = L(0 \cdot a + 1 \cdot a' - 0 \cdot a') = L(1 \cdot a') = L(a') = a$.

8. Kommutativitás: $ab = ba$.

Biz: $ab = L(a'b + ab' - a'b') = L(ba' + b'a - b'a') = L(b'a + ba' - b'a') = ba$.

9. Technikai, mint 3: Ha $a = L(H_a)$ és $b = L(H_b)$, akkor $ab = L(a''b + ab'' - a''b'')$ ahol a'' H_a elemein fut végig, b'' pedig H_b elemein.

Biz: Mint 3-nál, itt is elég belátni, hogy $a'' \neq a$, $b'' \neq b$ esetén $a''b + ab'' - a''b'' \neq ab$. Legyen a_0 a kisebb, a_1 a nagyobb a és a'' közül, hasonlóan legyen b_0 a kisebb, b_1 a nagyobb b és b'' közül. Az a_1b_1 szorzat definiciója szerint a legkisebb kizárt egy halmazban, melyben szerepel $a_0b_1 + a_1b_0 - a_0b_0$, így $a_1b_1 \neq a_0b_1 + a_1b_0 - a_0b_0$, amiből átrendezéssel adódik $a''b + ab'' - a''b'' \neq ab$.

10. Disztributivitás: $a(b + c) = ab + ac$

Biz: $a(b + c) = L(a'(b + c) + a(b' + c) - a'(b' + c), a'(b + c) + a(b + c') - a'(b + c')) = L((a'b + a'c) + (ab' + ac) - (a'b' + a'c), (a'b + a'c) + (ab + ac') - (a'b + a'c')) = L((a'b + ab' - a'b') + ac, ab + (a'c + ac' - a'c')) = L(ab + ac)$. Itt az $a(b + c)$ felírásához nem a definiciót használtuk, hanem 9-et, $ab + ac$-hez 3-at.

11. Asszociativitás: $a(bc) = (ab)c$.

Biz: $a(bc) = L(a'(bc) + a(b'c + bc' - b'c') - a'(b'c + bc' - b'c')) = L(a'(bc) + a(b'c) + a(bc') - a(b'c') - a'(b'c) - a'(bc') + a'(b'c')) = L((a'b)c + (ab')c + (ab)c' - (ab')c' - (a'b')c - (a'b)c' + (a'b')c') = L((a'b + ab' - a'b')c + (ab)c' - (a'b + ab' - a'b')c') = L((ab)c)$. Itt használjuk 9-et, 10-et, és persze 1–5-öt is.

12. Nullosztómentesség: Ha $a \neq 0 \neq b$, akkor $ab \neq 0$.

Biz: ab a legkisebb kizártja egy halmaznak, melyben szerepel $0 \cdot a + a \cdot 0 - 0 \cdot 0 = 0 + 0 - 0 = 0$.

1–12. a rendszámok az új műveletekkel egy kettő karakterisztikájú integritási tartományt adnak. A nullelem 0, az egységelem 1.

III. Egyszerű kiterjesztési szabalyok

Jelöljük az x-nél kisebb rendszámok halmazát (mint halmazelméletben szokás) x-szel (és reménykedjünk, hogy ez nem okoz félrértést).

13. Ha x nem zárt az összeadásra, akkor $x = a + b$ minden minimális (a, b) párra, melynek nincs összege x-ben.

Biz: Feltettük, hogy $a + b \geq x$, így $a + b = L(a' + b, a + b')$ miatt elég belátni, hogy $a' + b \neq x$ és $a + b' \neq x$, de mindkét bal oldal a minimalitás miatt x-nél kisebb.

14. Ha x zárt az összeadásra, de nem a szorzásra, akkor $x = ab$ minden minimalis (a, b) párra, amelynek nincs szorzata x-ben.

Biz: Mint az előbb, itt is elég belátni, hogy $a'b + ab' - a'b' \neq x$. A baloldal itt a minimalitás és az összeg-zártság miatt x-beli.

15. Ha $x > 1$ gyűrű, de nem test, akkor $x = 1/a$ a minimális $a > 0$-ra, melynek nincs reciproka x-ben.

Biz: Kell, hogy $ax = L(a'x + ax' - a'x') = 1$. Nyilvan $a' = x' = 0$ választás 0-t ad, így csak az kell, hogy $a'x + ax' - a'x' = 1$ nem lehet. Ha $a' = 0$, akkor ez $ax' = 1$ lenne, ami nem lehet, mert a-nak nincs reciproka x-ben. Ha $a' \neq 0$, akkor a minimalitás miatt van $b < x$, hogy $a'b = 1$, és ezzel szorozva $a'x + ax' - a'x' = 1$-et $x = b + x' - abx'$ adódna, ami nem lehet, mert a jobb oldal az x gyűrűben marad.

16. A rendszámok testet alkotnak az új műveletekkel.

Biz: 1-12 után csak a reciprok létezése kell. Ha x-nek nem lenne reciproka, akkor 13–15 szerint minden rendszám az x-nél kisebbek és azok reciprokai által generált gyűrűben lenne, ami számossági okokból nem megy ("több rendszám van").

17. Technikai: Ha x test, akkor x polinomjai x-beli együtthatókkal lesznek az első rendszámok, méghozzá lexikografikus sorrendben, egészen addig, amíg a polinomok értéke páronként különböző. (A lexikografikus sorrendben két polinom közül az a kisebb, aminek a legnagyobb fokú eltérő együtthatója kisebb, így például kisebb fokú polinom kisebb. Vegyük észre, hogy ez jólrendezés.)

Biz: Természetesen indukcióval:

Konstansokra, és x-re triviális. Legyen most $y > x$, és tegyük fel, hogy $y = \{p(x)|p < r\}$, ahol p az x-beli együtthatós r-nél (lexikografikusan) kisebb polinomokon fut végig. Feltesszük, hogy $r(x)$ nem szerepel y-ban, és bizonyítani kell, hogy $y = r(x)$.

Ha r nem monom, akkor $r(t) = at^l + s(t)$ alakú, ahol $l \geq 1$, $s \neq 0$, és s foka l-nél kisebb. y nem zárt összeadásra, és $(ax^l, s(x))$ 14 szerinti minimális pár y-ban, így $y = ax^l + s(x) = r(x)$.

Ha $r(t) = ax^t$, ahol a nem zárt az összeadásra, akkor 14 szerint $a = b + c$ tetszőleges minimális a-ban alatt összeadhatatlan (b, c) párra. Ekkor (bx^l, cx^l) minimalis y-ban nem összedható pár, így ugyancsak 14 szerint $y = bx^l + cx^l = ax^l = r(x)$.

Ha $r(t) = at^l$, ahol $a > 1$ és a zárt az összeadásra, akkor y is zárt az összeadásra, és (a, x^l) minimális pár, melynek nincs szorzata y-ban, így 15 szerint $y = ax^l = r(x)$.

Ha $r(t) = t^l$, ahol $1 < l$, akkor y zárt az összeadásra, és (x, x^{l-1}) minimális pár, melyek szorzata nincs y-ban, így 15 szerint $y = x \cdot x^{l-1} = r(x)$.

18. Ha x test, de nem algebrailag zárt, akkor x minimálpolinomja x felett lexikografikusan legkisebb polinom x felett, aminek nincs gyöke x-ben.

Biz: Legyen x felett a legkisebb gyökmentes polinom $p(t)$. Ennek főegyütthatója nyilván 1 (egyébként egy konstanssal megszorozva kisebb polinom adódna), így $p(t) = t^l - q(t)$, ahol $l \geq 2$ és q foka kisebb l-nél.

Nyilván x transzcendens x felett vagy minimálpolinomja legalább l-ed fokú, így az l-nél kisebb fokú r polinomokra x felett $r(x)$ mindig különböző, így 17 szerint ezek r szeinti lexikografikus sorrendben adják az első valahány rendszámot, mondjul az y-nál kisebbeket (nyilván y az x rendszám szokásos — régi — értelemben vett l-edik hatványa lesz).

Legyen $z = x^{l-1}$. Ekkor $x^l = xz = L(x'z + xz' - x'z')$, és itt z' az $r(x)$ értékeken fut végig, ahol r $(l-1)$-nél kisebb fokú polinom x felett. Nézzük meg, hogy fix x' és l-nél kisebb fokú x feletti s polinom esetén mikor oldható meg $x'z + xz' - x'z' = s(x)$ valamely $z' = r(x)$-szel. Mivel itt végig az $y[t]$ polinomgyűrű l-nél kisebb fokú polinomjai közt mozgunk, ezért akkor, ha $x't^{l-1} + tr(t) - x'r(t) = s(t)$ megoldható, vagyis ha $x't^{l-1} - s(t)$-t osztja $t - x'$, ami viszont akkor teljesül, ha $t = x'$ gyöke $x't^{l-1} - s(t)$-nek azaz $x'^l = s(x')$, azaz x' gyöke a $t^l - s(t)$ polinomnak. A fentiek szerint x^l az első $s(x)$ értékkel egyezik meg, amit nem kapunk meg így, azaz amelyre $t^l - s(t)$-nek nincs gyöke x-ben. Ez q definiciója és 17 alapján pont $q(x)$, tehát $p(x) = x^l - q(x) = 0$, ahogy állítottuk.

19. A rendszámok algebrailag zárt testet alkotnak.

Biz: Pont, mint 16-nál. Ha ugyanis az x beli p polinomnak nem lenne gyöke, akkor 13–15 és 18 alapján az összes rendszám x algebrai lezártjába esne, ami számossági okokból nem megy.

20. Ha x algebrailag zárt testet alkot, akkor x transzcendens x felett.

Biz: Jobb híján... Csak a kerekség kedvéért írtam ide.

IV. Természetes számok

Szögletes zárójelen belül a régi műveletek érvényesek.

21. Összeadásra zárt $n < \omega$ akkor és csak akkor, ha $n = [2^k]$ alakú. Páronként különböző $[2^k]$ alakú számok összege és [összege] egyenlő (sok tagú összeg is). De persze $[2^k] + [2^k] = 0$.

Biz: 13-ból folyik. Az utolsó állítás 5 speciális esete. Egyébként rendszámhatványozás szerinti magasabb 2-hatványokra is igaz.

22. $n < \omega$ test akkor és csak akkor, ha $n = [2^{2^k}]$ alakú. Páronként különböző ilyen számok szorzata és [szorzata] egyenlő (sok tényezős szorzat is). De $[2^{2^k}][2^{2^k}] = [(3/2)2^{2^k}]$.

Biz: A prímtest 2, tegyük fel induktívan, hogy $[2^{2^k}]$ test ($k < \omega$). Ez véges test, így tökéletes, tehát a 18 szerinti legkisebb gyökmentes polinomja legalábbmásodfokú és nem t^2-a alakú $a < [2^{2^k}]$-ra. Tehát $[2^{2^k}]$ minimálpolinomja $t^2 - t - a$ alakú a legkisebb $a < [2^{2^k}]$-ra, amire ez gyökmentes ha van ilyen a. Kis számolás adja, hogy ez az a pont $[2^{2^k-1}]$, így a generált testbővítés négyzetes (a következő test $[2^{2^{k+1}}]$), és a szorzási szabályok is folynak.

21–22, (valamint a gyűrű-tulajdonságok) megadják a műveleteket ω-n. Próbáljátok pl. 4 hatványait ennek alapján végigszámolni.

V. ω

23. ω kvadratikusan zárt. (Minden másodfokú polinomnak van gyöke.)

Biz: Legyen p másodfokú polinom ω felett. Ekkor p már $[2^{2^k}]$ felett is polinom elég nagy k-ra, így mivel ez utóbbi $GF([2^{2^k}])$ gyöke már $GF([2^{2^{k+1}}])$-ben megjelenik, ami persze maga $[2^{2^{k+1}}]$.

24. $\omega^3 = 2$

Biz: 18 alapján ω minimálpolinomja a legkisebb gyökmentes polinom ω felett. 23 alapján ez minimum harmadfokú, és persze nem t^3 vagy $t^3 - 1$, mert azok gyöke 0, illetve 1. Elég belátni, hogy $t^3 - 2$-nek nincs gyöke ω-ban. Ha volna $n < \omega$ gyök, akkor n multiplikatív rendje 9 lenne, mert $n^9 = 2^3 = 1$, de $n^3 = 2 \neq 1$. De n egy $[2^{2^k}]$ elemű test eleme, így rendje osztja, $[2^{2^k} - 1]$-et, ami ellentmondás.

VI. Továbbiak

15–18 alapján sokáig követhető a test szerkezete. Szögletes zárójelben a szokásos rendszámműveletek érvényesek, immár a rendszámhatványozást is használjuk.

Első rendszámok, amik testet adnak:

$$2, 4, 16, \ldots, [2^{2^k}], \ldots$$

$$\omega, [\omega^3], [\omega^9], \ldots, [\omega^{3^k}], \ldots$$

$$[\omega^\omega], [\omega^{\omega\cdot 5}], [\omega^{\omega\cdot 25}], \ldots, [\omega^{\omega\cdot 5^k}], \ldots$$

$$[\omega^{\omega^2}], [\omega^{\omega^2\cdot 7}], [\omega^{\omega^2\cdot 49}], \ldots, [\omega^{\omega^2\cdot 7^k}], \ldots$$

Azaz először az összes kvadratikus bővités, majd az összes harmadrendű, stb. Végül $[\omega^{\omega^\omega}]$ a prímtest algebrai lezártja.

Ezután 17 és 20 alapján $\left[\left(\omega^{\omega^\omega}\right)^\omega\right] = \left[\omega^{\omega^{\omega+1}}\right]$ a következő gyűrű, de ez még nem test. Ez az első eset, hogy 15 "alkalmazódik", azaz

$$\left[\omega^{\omega^{\omega+1}}\right] = \frac{1}{[\omega^{\omega^\omega}]}.$$

A következő test hirtelen nagy ugrással már $\left[\omega^{\omega^{\omega^\omega}}\right]$ (számolj utána). Ez nem tökéletes test, így

$$\left[\omega^{\omega^{\omega^\omega}}\right]^2 = \left[\omega^{\omega^\omega}\right].$$

Stb.