Algebra és számelmélet

Definíciók

1. Definiálja az oszthatóság, a maradékos osztás, a legnagyobb közös osztó, illetve legkisebb közös többszörös fogalmát az egész számok körében.
2. Definiálja a modulo m kongruencia fogalmát.
3. Definiálja a maradékosztály, illetve redukált maradékosztály fogalmát modulo m.
4. Definiálja a teljes, illetve redukált maradékrendszer fogalmát modulo m.
5. Definiálja az Euler-féle φ függvényt a redukált maradékosztályok segítségével.
6. Definiálja a gyengén multiplikatív számelméleti függvény fogalmát.
7. Definiálja a tökéletes szám, illetve a Mersenne-prím fogalmát.
8. Definiálja számelméleti függvény összegzési, illetve megfordítási függvényét.
9. Definiálja két számelméleti függvény konvolúcióját.
10. Definiálja a Möbius-féle μ függvényt.
11. Definiálja egy komplex szám kanonikus alakját, valós és képzetes részét és konjugáltját, valamint abszolút értékét és trigonometrikus alakját.
12. Definiálja egy komplex szám n-edik gyökét és a komplex n-edik egységgyököket. Mit nevezünk primitív n-edik egységgyöknek?
13. Definiálja az oszthatóság, a maradékos osztás, a legnagyobb közös osztó, illetve legkisebb közös többszörös fogalmát test feletti polinomgyűrűben.
14. Definiálja az irreducibilis polinom fogalmát test feletti polinomgyűrűben.
15. Definiálja a polinom helyettesítési értékét, gyökét, valamint a polinomfüggvény fogalmát.
16. Hogyan definiáljuk test feletti polinom k-szoros gyökét, többszörös gyökét?
17. Definiálja tetszőleges test fölötti polinom deriváltját.
18. Mikor mondunk szimmetrikusnak egy n határozatlanú polinomot?
19. Definiálja, mit nevezünk algebrai, illetve transzcendens számnak.
20. Definiálja tetszőleges determinánsban az adott elemhez tartozó komplementer aldeterminánst és adjungált aldeterminánst.
21. Mit értünk egy mátrix inverzén? Mikor mondjuk azt, hogy két mátrix hasonló?
22. Mit értünk lineáris egyenletrendszer mátrixán és bővített mátrixán? Milyen mátrixot, illetve egyenletrendszert nevezünk lépcsős alakúnak?
23. Definiálja a vektortér fogalmát.
24. Mit értünk vektortér alterén és két altér összegén?
25. Mit értünk vektorok lineáris kombinációján és vektorok nemtriviális lineáris kombinációján? Definiálja a vektorhalmaz által generált alteret és a vektortér generátorrendszerét.
26. Mikor mondjuk azt, hogy egy vektorrendszer lineárisan független, illetve lineárisan függő?
27. Definiálja a véges dimenziós vektorteret, a bázist, a dimenziót, valamint egy vektor adott bázisra vonatkozó koordinátáit.
28. Definiálja a vektorrendszer rangját, valamint a mátrix sor-, oszlop- és determinánsrangját.
29. Definiálja a lineáris leképezés fogalmát, valamint a lineáris leképezés magját és képterét.
30. Definiálja a lineáris leképezés mátrixát adott bázisokban.
31. Definiálja a két bázis közötti áttérés mátrixát.
32. Definiálja a csoport fogalmát, valamint csoportokban az elem rendjének fogalmát.
33. Definiálja a részcsoport és a generátorrendszer fogalmát.
34. Mikor nevezünk egy csoportot ciklikus csoportnak?
35. Definiálja a részcsoport szerinti osztályozást és a részcsoport indexének fogalmát.
36. Definiálja a normálosztó és a faktorcsoport fogalmát.
37. Mely csoportokat nevezzük egyszerű csoportoknak?
38. Definiálja a csoportok közötti homomorfizmus, izomorfizmus fogalmát.
39. Definiálja két, illetve véges sok csoport „külső” és „belső” direkt szorzatát. Mikor mondjuk, hogy egy csoport direkt felbonthatatlan?
40. Mely algebrai struktúrákat nevezzük gyűrűknek, illetve testeknek?
41. Definiálja a részgyűrű, ideál, főideál, faktorgyűrű fogalmát.

Tételek, alkalmazások

1. Mondja ki a maradékos osztás tételét az egész számok gyűrűjében. Milyen kapcsolatban van ez a tétel azzal, hogy a természetes számok megadhatók különböző számrendszerekben?
2. Ismertesse az euklideszi algoritmust az egész számok gyűrűjében, és mondja meg, hogy milyen kapcsolatban áll az egész számok legnagyobb közös osztójával.
3. Mondja ki a kétismeretlenes lineáris diofantoszi egyenlet megoldhatóságának szükséges és elegendő feltételét, valamint adja meg a megoldások általános alakját.
4. Mondja ki a számelmélet alaptételét, valamint azt a következményét, hogy hogyan lehet két egész szám legnagyobb közös osztóját, illetve legkisebb közös többszörösét kiszámítani a prímtényezős felbontásuk segítségével.
5. Mondja ki az $ax \equiv b \pmod{m}$ lineáris kongruencia megoldhatóságának szükséges és elegendő feltételét, valamint írja le, hogyan kapható meg egy megoldás ismeretében az összes megoldás modulo m.
6. Mondja ki a kínai maradéktételt.
7. Mondja ki Wilson tételét.
8. Mondja ki az Euler–Fermat-tételt (kis Fermat-tételt).
9. Hogyan lehet kiszámítani egy n természetes szám osztóinak számát, osztóinak összegét, illetve $\varphi(n)$ értékét n prímtényezős felbontása segítségével?
10. Mondja ki a páros tökéletes számokat leíró tételt.
11. Mondja ki a Möbius-féle megfordítási tételt.
12. Sorolja fel a komplex számok azon tulajdonságait, amelyek a konjugálás, az abszolút érték, valamint a műveletek kapcsolatára vonatkoznak.
13. Írja fel trigonometrikus alakban megadott komplex számok konjugáltját, szorzatát, hányadosát, pozitív egész kitevős hatványát.
14. Adja meg trigonometrikus alakban tetszőleges komplex számok n-edik gyökeit. Adja meg az n-edik egységgyököket, és jelezze, hogy melyek a primitív n-edik egységgyökök.
15. Mondja ki a maradékos osztás tételét test fölötti polinomgyűrűkben. Ismertesse az euklideszi algoritmust, és mondja meg, hogy milyen kapcsolatban áll a polinomok legnagyobb közös osztójával.
16. Fogalmazza meg a test fölötti polinomgyűrűk faktorizációs tételét (a számelmélet alaptételének megfelelőjét), valamint azt a következményét, hogy hogyan lehet két polinom legnagyobb közös osztóját, illetve legkisebb közös többszörösét kiszámítani irreducibilis felbontásuk ismeretében.
17. Fogalmazza meg Bézout tételét és annak következményét a test feletti n-edfokú polinom gyökeinek számáról, illetve a test feletti legfeljebb harmadfokú irreducibilis polinomokról.
18. Mondja ki a klasszikus algebra alaptételét és következményét a komplex, illetve a valós számtest fölötti irreducibilis polinomokról. Hogyan szól a faktorizációs tétel a komplex, illetve a valós számtest fölötti polinomgyűrűben?
19. Mondja ki a Schönemann–Eisenstein-tételt. Milyen fontos következménye van ennek a tételnek a racionális számtest fölötti irreducibilis polinomok fokszámával kapcsolatban?
20. Mondja ki azt a tételt, amely módszert ad egész együtthatós polinomok racionális gyökeinek megkeresésére.
21. Hogyan lehet eldönteni, hogy két komplex számtest fölötti polinomok van-e közös gyöke?
22. Fogalmazza meg, mi a kapcsolat valamely komplex számtest fölötti polinom k-szoros gyökének létezése és a polinom többszörös deriváltjai között.
23. Mondja ki a szimmetrikus polinomok alaptételét.
24. Milyen struktúrát alkotnak az algebrai számok?
25. Mit értünk egy determináns i-edik sora szerinti kifejtésén?
26. Sorolja fel a determinánsok értékének kiszámolásakor használatos tulajdonságokat.
27. Fogalmazza meg a determinánsok szorzástételét. Adja meg determináns segítségével az inverzmátrix létezésének szükséges és elegendő feltételét.
28. Fogalmazza meg a Cramer-szabályt.
29. Fogalmazza meg a kicserélési tételt. Mi a kapcsolat a bázis, a maximális lineárisan független vektorrendszer és a minimális generátorrendszer között?

30. Fogalmazza meg az alterekre vonatkozó dimenziótételt. Mi a kapcsolat egy vektorrendszer rangja és a vektorrendszer által generált altér dimenziója között?
31. Fogalmazza meg a mátrixok rangszámtételét és a Kronecker–Capelli tételt.
32. Fogalmazza meg a lineáris leképezések magterére és képterére vonatkozó dimenziótételt. Mit tud a véges dimenziós vektorterek injektív, illetve szürjektív lineáris transzformációiról?
33. Hogyan kaphatók meg lineáris leképezések skalárszorosának, összegének és szorzatának mátrixai a leképezések mátrixaiból?
34. Mi a kapcsolat lineáris leképezések különböző bázisokban felírt mátrixai és a bázisok közötti átmenetmátrixok között?
35. Mondja ki Lagrange csoportokra vonatkozó tételét.
36. Mondja ki Cayley tételét.
37. Hogyan kaphatók meg a generátorrendszer elemei segítségével a generált részcsoport elemei?
38. Fogalmazza meg a ciklikus csoportokat izomorfia erejéig leíró tételt.
39. Fogalmazza meg a ciklikus csoportok részcsoportjait megadó tételt.
40. Adja meg a normálosztók különböző jellemzéseit, és fogalmazza meg a normálosztóknak és a csoportok kongruenciáinak kapcsolatára vonatkozó tételt.
41. Mondja ki a homomorfiatételt csoportokra.
42. Fogalmazza meg azt a tételt, amely különböző módon jellemzi azt, hogy mikor áll elő egy csoport két, illetve véges sok adott normálosztójának direkt szorzataként.
43. Mondja ki a véges Abel-csoportok alaptételét.

A megértést ellenőrző kérdések, feladatok

1. Az alábbi három állítás közül melyikből melyik következik *tetszőleges* a természetes szám és *tetszőleges* p prímszám esetén:
   (a) $a \nmid p$,
   (b) $p \nmid a$,
   (c) $\operatorname{lnko}(a, p) = 1$?
2. Az alábbi három állítás közül melyikből melyik következik *tetszőleges* olyan a, b, c természetes számokra, ahol a és b relatív prím:
   (a) $a \mid b$,
   (b) $a \mid c$,
   (c) $a \mid bc$?
3. Milyen n természetes számok esetén relatív prím egymáshoz a $3n + 2$ és $4n + 1$ természetes szám? Ha nem relatív prímek, akkor mi lehet a legnagyobb közös osztójuk?
4. Léteznek-e olyan a, b, c egész számok, amelyekre az $ax+by = c$ diofantoszi egyenletnek pontosan 2008 megoldása van?
5. (a) Írja fel a tízes számrendszerbeli 2008 számot ötös számrendszerben.
   (b) Írja fel a hármas számrendszerbeli 1021101 számot tízes számrendszerben.
6. Adjon szabályt a 3-mal való oszthatóságra négyes számrendszerben. Döntse el ennek segítségével, hogy osztható-e 3-mal a négyes számrendszerben felírt 320232321201 szám.
7. Ekvivalens-e egymással a $30x \equiv 48 \pmod{58}$ és a $30x \equiv 48 \pmod{29}$ kongruencia?
8. Vannak-e olyan a, b egész számok, amelyekre az $ax \equiv b \pmod{10}$ kongruenciának pontosan két különböző megoldása van modulo 10, mégpedig
   (a) $x \equiv 3 \pmod{10}$ és $x \equiv 7 \pmod{10}$;
   (b) $x \equiv 2 \pmod{10}$ és $x \equiv 7 \pmod{10}$?
9. Adjon meg olyan egész számokat, amelyek teljes maradékrendszert alkotnak modulo 8, és egyúttal redukált maradékrendszert alkotnak modulo 15.
10. Igaz-e minden p prímszámra a $p \mid ((p-1)!)^2 + (p-1)!$ oszthatóság?
11. Az
    (a) 852^{42},
    (b) 853^{42},
    (c) 855^{85},
    (d) 861^{85}

hatványok közül melyek adnak 86-tal oszva egyet maradékul? Mi a többi hatvány maradéka 86-tal oszva?

12. Adjon meg három tökéletes számot.
13. Legyen f gyengén multiplikatív számelméleti függvény, és jelölje az összegzési függvényét F. Határozza meg $F(45)$ értékét, ha $f(3) = 2, f(5) = 7, f(45) = 21$.
14. Legyen f gyengén multiplikatív számelméleti függvény, és jelölje az összegzési függvényét F. Határozza meg $f(45)$ értékét, ha $F(3) = 2, F(5) = 7, F(45) = 21$.
15. Határozza meg az identikus függvényből és a konstans 1 függvényből (mint számelméleti függvényekből) képezhető mind a négy kéttényezős konvolúciót.
16. Határozza meg a $\sum_{d|n} d \cdot \mu\left(\frac{n}{d}\right)$ összeget tetszőleges pozitív egész n-re (μ a Möbius-féle függvény).
17. Határozza meg az összes olyan p prímszámot, amelyre
    (a) $p + 3$,
    (b) $p + 7$
    is prím.
18. Határozza meg az $1 - i$, $-2 - 2\sqrt{3}i$ és $\cos\alpha - i\sin\alpha$ komplex számok trigonometrikus alakját.
19. Adja meg kanonikus alakban az $1 - i$ komplex szám ezredik hatványát, valamint az $\frac{1-i}{1+i}$ komplex számot.
20. Adja meg kanonikus alakban a nyolcadik egységgyököket, és mondja meg, melyek primitívek.
21. A z komplex számra teljesül, hogy $z^{50} = 1$. Igaz-e, hogy z
    (a) 100-adik egységgyök,
    (b) 100-adik primitív egységgyök?
22. Legyen $f, g \in \mathbb{Q}[x]$, és jelölje r az f polinom g-vel való maradékos osztásánál fellépő maradékot. Igaz-e, hogy ha f és g relatív prímek, akkor f és r is az?
23. Igaz-e, hogy ha az f valós együtthatós polinomnak gyöke az i komplex szám, akkor $x^2 + 1 \mid f$?
24. Igaz-e, hogy az $x^4 + 2x^3 - 3x^2 + x + 14$ egész együtthatós polinomnak minden racionális gyöke egész?
25. Irreducibilis-e az
    (a) $x^3 + x^2 - 5x + 3$,
    (b) $x^6 - 6x - 12$
    polinom a racionális számtest fölött?
26. Legyen $f \in \mathbb{Q}[x]$. Igaz-e, hogy
    (a) ha f irreducibilis $\mathbb{Q}$ fölött, akkor irreducibilis $\mathbb{R}$ fölött is,
    (b) ha f irreducibilis $\mathbb{R}$ fölött, akkor irreducibilis $\mathbb{Q}$ fölött is?
27. Igaz-e, hogy ha az f legalább másodfokú racionális együtthatós polinomnak nincsen racionális gyöke, akkor f irreducibilis a racionális számtest fölött?
28. Határozza meg az $x^6 + 2$ polinom irreducibilis felbontását a racionális, a valós és a komplex számtest fölött.
29. Mutasson $\mathbf{Z}_4[x]$-ben olyan polinomot, amely gyökeinek száma nagyobb, mint a fokszáma.
30. Van-e olyan test, amely fölött létezik két különböző olyan polinom, amelyekhez ugyanaz a polinomfüggvény tartozik?
31. Igaz-e, hogy bármely ötödfokú komplex együtthatós f polinomot egyértelműen meghatározza hat különböző helyen vett helyettesítési értéke?
32. Igaz-e, hogy ha az $f \in \mathbb{Q}[x]$ polinomra $f'(1) = f''(1) = 0$, akkor 1 legalább háromszoros gyöke f-nek?
33. Szimmetrikusak-e az
    (a) $f = 2xy + 2xz$,
    (b) $g = xyz$,
    (c) $h = 5$
    polinomok a $\mathbb{Q}[x, y, z]$, illetve a $\mathbb{Q}[x, y, z, u]$ gyűrűben?
34. Határozza meg az $f = x^3 + 3x + 2 \in \mathbb{C}[x]$ polinom gyökeinek négyzetösszegét.
35. Melyek algebrai számok az alábbi komplex számok közül:
    (a) $\sqrt{2}$,
    (b) π,

(c) $\sqrt{2}+i\sqrt{3}$,
(d) $\sqrt{\pi}$,
(e) az x^5-4x+2 polinom gyökei?

36. Döntse el, hogy az egész számok halmaza ideált alkot-e az egész együtthatós polinomok gyűrűjében.
37. A $\mathbb{Z}_2[x]$ polinomgyűrűben jelölje I az x^2+x+1 polinom által generált főideált. Hány eleme van a $\mathbb{Z}_2[x]/I$ faktorgyűrűnek? Test-e ez a faktorgyűrű?
38. Legyen A és B két azonos méretű négyzetes mátrix. Szimmetrikus-e az $AB^{\mathrm{T}}+BA^{\mathrm{T}}$ mátrix?
39. Egy n-edrendű determináns mellékátlója fölött minden elem nulla, és a mellékátlóban rendre az $a_1,\dots,a_n$ elemek szerepelnek. Adja meg a determináns értékét.
40. Legyen D olyan n-edrendű determináns, melynek első sorában lévő elemeihez tartozó komplementer aldeterminánsok rendre megegyeznek a második sorában lévő elemekhez tartozó komplementer aldeterminánsokkal, azaz $D_{1i}=D_{2i},\ i=1,\dots,n$. Igazolja, hogy D értéke 0.
41. Írja fel a $V(1,-1,2,-2)$ Vandermonde-determinánst, és számolja ki az értékét a Vandermonde-determinánsokra tanult képlet segítségével.
42. Milyen ismert algebrai struktúrát alkot a T test feletti $n\times n$-es mátrixok $T^{n\times n}$ halmaza
    (a) a mátrixok összeadására és a mátrixok T-beli elemekkel való szorzására nézve,
    (b) a mátrixok összeadására és a mátrixok szorzására nézve?
43. Igaz-e tetszőleges A,B azonos méretű négyzetes mátrixra, hogy ha $AB=\underline{0}$, akkor $A=\underline{0}$ vagy $B=\underline{0}$?
44. Igaz-e tetszőleges A,B azonos méretű négyzetes mátrixok esetén, hogy ha az A mátrixnak van inverze, a B mátrixnak pedig nincs inverze, akkor az AB szorzatnak sincs inverze?
45. Igaz-e a következő két állítás?
    (a) Ha egy lineáris egyenletrendszernek több egyenlete van mint ismeretlene, akkor nincs megoldása.
    (b) Ha egy lineáris egyenletrendszernek kevesebb egyenlete van mint ismeretlene, akkor van megoldása.
46. Van-e egy ötdimenziós vektortérben hét vektorból álló lineárisan független vektorrendszer?
47. Igaz-e, hogy minden lineárisan független vektorrendszer minimális generátorrendszer az általa generált altérben?
48. Adjon meg olyan háromelemű vektorrendszert, amelynek rangja
    (a) 1,
    (b) 0.
49. Igaz-e, hogy ha U és V két véges dimenziós altér egy vektortérben, melyekre $\dim(U+V)=\dim U+\dim V$, akkor $U\cap V=\{\underline{0}\}$?
50. Igaz-e, hogy egy T test fölötti $n\times n$-es mátrix rangja pontosan akkor kisebb, mint n, ha a mátrix determinánsa 0?
51. Létezik-e két hasonló 3×3-as valós mátrix, melyek rangja különböző?
52. Legyen φ a térnek (azaz az $\mathbb{R}$ fölötti $\mathbb{R}^3$ vektortérnek) azon lineáris transzformációja, mely minden vektorhoz hozzárendeli az XZ síkra vonatkozó merőleges vetületét. Adja meg az $\operatorname{Im}\varphi$ és $\operatorname{Ker}\varphi$ altereket, valamint mindkét altér dimenzióját.
53. Van-e egy 7-dimenziós vektortérnek olyan φ lineáris transzformációja, melyre $\dim(\operatorname{Ker}\varphi)=4$ és $\operatorname{Ker}\varphi\subseteq\operatorname{Im}\varphi$?
54. Legyen φ a térnek (azaz az $\mathbb{R}$ fölötti $\mathbb{R}^3$ vektortérnek) azon lineáris transzformációja, mely minden vektorhoz hozzárendeli a Z tengelyre vonatkozó tükörképét. Adja meg φ mátrixát
    (a) a standard bázisban,
    (b) a $(0,0,1),(1,0,0),(0,1,0)$ bázisban,
    (c) az $(1,0,0),(1,1,0),(1,0,1)$ bázisban.
55. Igaz-e, hogy ha egy véges dimenziós vektortéren értelmezett lineáris transzformáció mátrixa valamely bázisban nemelfajuló, akkor a lineáris transzformáció bijektív?
56. Igaz-e, hogy ha egy véges dimenziós vektortéren értelmezett lineáris transzformáció
    (a) bijektív,
    (b) injektív,
    (c) szürjektív,

    akkor mátrixa bármely bázisban nemelfajuló?

57. Adja meg az $\mathbb{R}$ fölötti $\mathbb{R}^3$ vektortér standard bázisról a $(0,1,0),(0,0,1),(1,0,0)$ bázisra való áttérés mátrixát, és a fordított irányú áttérés mátrixát is.
58. Egy 28 elemű csoport a eleméről tudjuk, hogy $a^4 \neq 1$ és $a^{14} \neq 1$. Meghatározható-e ennek alapján az a elem rendje?
59. Van-e olyan csoport, amelyben hatodrendű elem van, de harmadrendű elem nincsen?
60. Az egészek számok additív csoportjában adja meg a $\{4,6\}$ halmaz által generált részcsoportot. Ciklikus-e ez a részcsoport?
61. Van-e olyan nyolcadrendű csoport, amelyben van $1,2,4$ és 8 rendű részcsoport is?
62. Egy G véges csoportban van $2,3,4$ és 5 rendű elem is. Legalább mekkora kell, hogy legyen G rendje?
63. Melyek azok a csoportok, amelyeknek nincsen valódi nemtriviális részcsoportjuk?
64. Kompatibilis osztályozás-e az A_4 alternáló csoportban a következő osztályokból álló osztályozás: $\{\mathrm{id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$, $\{(1\,2\,3), (1\,3\,4), (2\,4\,3), (1\,4\,2)\}$ és $\{(1\,3\,2), (2\,3\,4), (1\,2\,4), (1\,4\,3)\}$.
65. Mutassa meg, hogy az S_3 szimmetrikus csoportban normálosztó az $(1\,2\,3)$ elem által generált H részcsoport, és adja meg az S_3/H faktorcsoport művelettáblázatát.
66. Van-e az S_3 szimmetrikus csoportnak olyan faktorcsoportja, amely izomorf a $H = (\{-1,1\};\cdot)$ csoporttal?
67. Homomorf képe-e a C_4 csoport a
    (a) C_6,
    (b) C_8
    csoportnak?
68. Adjon egy-egy példát kommutatív és nemkommutatív egyszerű csoportra.
69. Melyek izomorfak és melyek nem izomorfak a következő csoportok közül:
    (a) C_4,
    (b) $C_2 \times C_2$,
    (c) S_4,
    (d) a komplex negyedik egységgyökök multiplikatív csoportja?
70. Direkt felbonthatatlan-e a
    (a) $G = C_9$,
    (b) $G = C_{10}$
    csoport? Ha G direkt felbontható, akkor adjon is meg egy nemtriviális direkt felbontását.
71. Adja meg izomorfia erejéig az összes 40 elemű Abel-csoportot.