Logikai alapok – Halmazelméleti alapfogalmak

1. Mondjon legalább három példát predikátumra.

Síkbeli predikátum pl: E(x):= „x egyenes”; P(x):= „x pont”; I(x,y):= „x illeszkedik y-ra”.

2. Sorolja fel a logikai jeleket.

Logikai formulák alkotóelemei: ¬:= „nem”; ^:= „és”; ˅:= „vagy”, =>:= „ha… akkor…”; <=>:= „akkor és csak akkor”.

3. Milyen kvantorokat ismer? Mi a jelük?

A logikai formulák alkotóelemei a ∃:= „létezik” egzisztenciális kvantor és a ∀:= „minden” univerzális kvantor.

4. Hogyan kapjuk a logikai formulákat?

A logikai formulákat, vagy mondatokat az adott elmélet predikátumaiból épülnek fel, a logikai jelek, valamint a két kvantor segítségével.

5. Mikor van egy változó két kvantor hatáskörében?

Egy formula egy (∃xA) vagy (∀xA) típusú részformulája esetén az x változó minden, a két zárójel közötti előfordulására (a kvantor után vagy A-ban) azt mondjuk, hogy a kvantor hatáskörében van.

6. Mik a nyitott és mi a zárt formulák?

Ha egy formulában egy változó egy adott előfordulás egy kvantor hatáskörében van, akkor azt mondjuk, hogy az adott előfordulás kötött előfordulás, egyébként az adott előfordulás szabad előfordulás. Ha egy változónak egy formulában van szabad előfordulása, akkor azt mondjuk, hogy a változó szabad változó. Ha egy formulának nincs szabad változója, akkor a formulát zárt formulának, egyébként nyitott formulának mondjuk.

7. Mondjon két példát nyitott formulára!

A síkgeometria példájánál maradva az ((E(x) ^ P(y))^I(x,y)) és a ((P(x)^P(y))^¬x=y) formulában az x és az y szabad változók, így ezek nyitott formulák.

8. Mondjon egy példát zárt formulára.

A ∀x(E(x) => ∃y(P(y)^I(x,y))) zárt formula, mert nincs szabad változója.

9. Definiálja a részhalmaz és a valódi részhalmaz fogalmát és adja meg a jelöléseiket.

Akkor mondjuk, hogy az A halmaz részhalmaza a B halmaznak, ha A minden eleme a B halmaznak is eleme. Jele: $A \subset B$ vagy $B \supset A$. Ha A részhalmaza B-nek, de nem egyenlő vele, akkor azt mondjuk, hogy A valódi részhalmaza B-nek. Jele: $A \subsetneq B$ vagy $B \supsetneq A$.

10. Milyen tulajdonságokkal rendelkezik a „részhalmaz” fogalom?

Minden halmaz részhalmaza saját magának (reflexivitás), és ha $A \subset B$, $B \subset C$, akkor $A \subset C$ (tranzitivitás). Ha $A \subset B$ és $B \subset A$, akkor a meghatározottsági axioma szerint az is teljesül, hogy $A = B$ (antiszimmetria).

11. Milyen tulajdonságokkal rendelkezik a halmazok egyelősége?

A halmazok egyenlősége reflexív, tranzitív, antiszimmetrikus, és még az is teljesül, hogy ha $A = B$, akkor $B = A$ (szimmetria).

12. Írja le a részhalmaz fogalmát. Milyen jelölést használunk részhalmazok megadására?

Akkor mondjuk, hogy az A halmaz részhalmaza a B halmaznak, ha A minden eleme a B halmaznak is eleme. Jele: $A \subset B$ vagy $B \supset A$. Ha A részhalmaza B-nek, de nem egyenlő vele, akkor azt mondjuk, hogy A valódi részhalmaza B-nek. Jele: $A \subsetneq B$ vagy $B \supsetneq A$.

13. Írja le az üres halmaz fogalmát.

Van olyan halmaz, amelynek nincs eleme.

14. Igaz-e, hogy csak egy üres halmaz van?

Igen. A meghatározottság axiómája miatt csak egy üres halmaz van.

15. Írja le két halmaz unióját és a megfelelő jelöléseket.

Ha A és B halmazok, akkor azt a halmazt, amelynek pontosan azok a dolgok az elemei, melyek elemei A-nak vagy B-nek (vagy mindkettőnek), $A \cup B$-vel jelöljük, és a két halmaz uniójának nevezzük.

16. Írja le halmazrendszer unióját és a megfelelő jelöléseket.

Ha $\mathcal{A}$ egy halmaz, amelynek elemei mind halmazok, akkor azt a halmazt amely pontosan azokat a dolgokat tartalmazza, amelyek $\mathcal{A}$ valamely elemének az elemei, az $\mathcal{A}$ uniójának nevezzük. Ennek jelölése: $\cup\mathcal{A}\ vagy\ \cup\{A : A \in \mathcal{A}\}$ vagy $\cup_{A\in\mathcal{A}}A$.

17. Fogalmazza meg a halmazok uniójának alaptulajdonságait.

Ha A, B, C halmazok, akkor:

(1) $A \cup \emptyset = A$;
(2) $A \cup B = B \cup A$ (kommutativitás);
(3) $A \cup (B \cup C) = (A \cup B) \cup C$ (asszociativitás);
(4) $A \cup A = A$ (idempotencia)
(5) $A \subset B$ akkor és csak akkor, ha $A \cup B = B$.

18. Definiálja halmazrendszer és két halmaz metszetét, és adja meg a jelöléseiket.

Ha A és B halmazok, legyen $A \cap B := \{x \in A : x \in B\}$. Általánosan, ha $\mathcal{A}$ halmazok egy nem üres rendszere, akkor a halmazrendszer metszetét a $\cap\mathcal{A} := \{x : x \in A \text{ minden } A \in \mathcal{A}\text{-ra}\}$ összefüggéssel definiáljuk.

19. Definiálja a diszjunktság és a páronként diszjunktság fogalmát.

Ha $A \cap B = \emptyset$, akkor azt mondjuk, hogy A és B diszjunktak (vagy idegenek). Általábosabban, ha egy nem üres $\mathcal{A}$ halmazrendszer metszete az üres halmaz, akkor azt mondjuk, hogy a halmazrendszer diszjunkt. Ha a halmazrendszer bármely két halmazának metszete üres, akkor azt mondjuk, hogy elemei páronként diszjunktak. (Más szóhasználatban a páronként diszjunkt halmazokból álló halmazrendszert nevezzük diszjunktnak.)

20. Fogalmazza meg a halmazok metszetének alaptulajdonságait.

Ha A, B, C halmazok, akkor:

(1) $A \cap \emptyset = \emptyset$;
(2) $A \cap B = B \cap A$ (kommutativitás);
(3) $A \cap (B \cap C) = (A \cap B) \cap C$ (asszociativitás);
(4) $A \cap A = A$ (idempotencia)
(5) $A \subset B$ akkor és csak akkor, ha $A \cap B = A$.

21. Fogalmazza meg az unió és a metszet disztributivitását.

Ha A, B, C halmazok, akkor:

(1) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (a metszet disztributivitása az unióra nézve);
(2) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (az unió disztributivitása a metszetre nézve).

22. Definiálja a halmazok különbségét, szimmetrikus differenciálját és komplementerét.

Az A és B halmazok különbségét (vagy differenciálját) az $A \backslash B := \{x \in A : x \notin B\}$ összefüggéssel definiáljuk. A két halmaz szimmetrikus differenciálját az $A \triangle B := (A \backslash B) \cup (B \backslash A)$ összefüggéssel definiáljuk. Ha $A \subset X$, akkor az $X \backslash A$ halmazt néha A'-val jelöljük, és az A halmaz X-re vonatkozó komplementerének nevezzük. Ez természetesen nem csak A-tól, hanem az X „alaphalmaztól" is függ, ami az A' jelölésben nem jut kifejezésre.

23. Fogalmazza meg a halmazok komplementerének alaptullajdonságait.

Ha $A, B \subset X$, akkor

(1) $(A')' = A$
(2) $\emptyset' = X$
(3) $X' = \emptyset$
(4) $A \cap A' = \emptyset$
(5) $A \cup A' = X$
(6) $A \subset B$ akkor és csak akkor, ha $B' \subset A'$
(7) $(A \cup B)' = A' \cap B'$
(8) $(A \cap B)' = A' \cup B'$

24. Írja le a hatványhalmaz fogalmát. Milyen jelölések kapcsolódnak hozzá?

Ha A halmaz, akkor azt a halmazrendszert, melynek elemei A részhalmazai, az A hatványhalmazának nevezzük. Jele: $\rho(A)$. Tehát minden A halmazhoz létezik egy olyan halmazrendszer, amelynek elemei pontosan A részhalmazai.

Relációk

25. Definiálja a rendezett pár fogalmát és koordinátáit.

Bármely x, y esetén legyen $(x, y) := \{\{x\}, \{x, y\}\}$. Az (x, y) rendezett pár első koordinátája x, a második koordinátája y.

26. Definiálja két halmaz Descartes-szorzatát.

Az X, Y halmazok Descartes-szorzatán az $X \times Y := \{(x, y) : x \in X, y \in Y\}$ halmazt értjük.

27. Definiálja a binér reláció fogalmát és adja meg a kapcsolódó jelöléseket.

Egy halmazt binér relációnak (vagy kétváltozós relációnak) nevezünk, ha minden eleme rendezett pár. Ha R egy binér reláció, akkor $(x, y) \in R$ helyett gyakran azt írjuk, hogy xRy, és azt mondjuk, hogy x és y között fennáll az R reláció.

28. Adjon három példát binér relációra.

Ha R egy binér reláció, akkor pl.: R={(Anna, Elemér), …}; R={(x,x), x ∈ X}; R ⊆ X x Y.

29. Mit jelent az, hogy R reláció X és Y között? Mit jelent az, hogy R egy X-beli reláció?

Ha valamely X és Y halmazokra $R \subset X \times Y$, akkor azt mondjuk, hogy R reláció X és Y között. Ha $X = Y$, akkor azt mondjuk, hogy R egy X-beli binér reláció (homogén binér reláció).

30. Definiálja a binér reláció értelmezési tartományát és értékkészletét, és adja meg a kapcsolódó jelöléseket.

Az R binér reláció értelmezési tartományát a $dmn(R) := \{x : van\ olyan\ y, hogy\ (x, y) \in R\}$, értékkészletét pedig a $rng(R) := \{y : van\ olyan\ x, hogy\ (x, y) \in R\}$ összefüggéssel értelmezzük. A jelölések a „domain” illetve „range” szóra utalnak; dom vagy D, illetve ran, R vagy im (az „image” szóból) is szokásosak.

31. Definiálja a binér reláció kiterjesztését, leszűkítését és leszűkítését egy halmazra és adja meg a kapcsolódó jelöléseket.

Az R binér relációt az S binér reláció kiterjesztésének, illetve S-et az R leszűkítésének (vagy megszorításának) nevezzük, ha $S \subset R$. Ha X egy halmaz, az R reláció X-re való leszűkítésén (vagy megszorításán) az $R_{|X} := \{(x, y) \in R : x \in X\}$ relációt értjük.

32. Definiálja egy binér reláció inverzét, és sorolja fel az inverz három egyszerű tulajdonságát.

Egy R binér reláció inverzén az $R^{-1} := \{(b, a) : (a, b) \in R\}$ binér relációt értjük.

(1) $(R^{-1})^{-1} = R$;
(2) ha R reláció X és Y között, akkor R^{-1} reláció Y és X között;
(3) $dmn(R^{-1}) = rng(R)$ és $rng(R^{-1}) = dmn(R)$

33. Definiálja halmaz képét és inverz képét binér relációnál és adja meg a kapcsolódó jelöléseket.

Legyen R egy binér reláció és A egy halmaz. Az A halmaz képe az $R(A) := \{y : van\ olyan\ x \in A, hogy\ (x, y) \in R\}$ halmaz. $R(A)$ pontosan akkor üres, ha A és $dmn(R)$ diszjunktak. Az A halmaz inverz képe az R relációnál $R^{-1}(A)$. Ha $A = \{a\}$, akkor $R(\{a\})$ helyett $R(a)$-t írunk.

34. Definiálja a binér relációk kompozícióját. Lehet-e a kompozíció üres?

Az R és S binér relációk összetételén (kompozícióján, szorzatán) az
$R \circ S \coloneqq \{(x,y)$: $van\ olyan\ z, hogy\ (x,z) \in S\ és\ (z,y) \in R\}$ relációt értjük. Két reláció kompozíciója lehet üres: ez a helyzet, ha $rng(S)$ és $dmn(R)$ diszjunktak.

35. Fogalmazzon meg három, binér relációk kompozíciójára vonatkozó állítást.

Legyenek R, S és T binér relációk. Ekkor:

(1) ha $rng(S) \supset dmn(R)$, akkor $rng(R \circ S) = rng(R)$;
(2) $R \circ (S \circ T) = (R \circ S) \circ T$ (asszociativitás);
(3) $(R \circ S)^{-1} = S^{-1} \circ R^{-1}$.

36. Mint jelent az, hogy egy reláció tranzitív, szimmetrikus, illetve dichotom? Ezek közül mi az, ami csak a reláción múlik?

Legyen R egy X-beli binér reláció. Azt mondjuk, hogy R

(1) tranzitív, ha minden x, y, z-re $(x,y) \in R$ és $(y,z) \in R$ esetén $(x,z) \in R$;
(2) szimmetrikus, ha minden x, y-ra $(x,y) \in R$ esetén $(y,x) \in R$;
(3) dichotom, ha minden $x, y \in X$ esetén $(x,y) \in R$ vagy $(y,x) \in R$ (esetleg mindkettő), azaz bármely két elem összehasonlítható.

Ezek közül a tranzitivitás és a szimmetrikusság függ csak a relációtól.

37. Mit jelent az, hogy egy reláció intranzitív, antiszimmetrikus, illetve trichotóm? Ezek közül mi az, ami csak a reláción múlik?

Legyen R egy X-beli binér reláció. Azt mondjuk, hogy R

(1) intranzitív, ha minden x, y, z-re $(x,y) \in R\ és\ (y,z) \in R$ esetén $(x,z) \notin R$;
(2) antiszimmetrikus, ha minden x, y-ra $(x,y) \in R$ és $(y,x) \in R$ esetén $x = y$;
(3) trichotóm, ha minden $x, y \in X$ esetén $x = y, (x,y) \in R$ vagy $(y,x) \in R$ közül pontosan egy teljesül.

Ezek közül az intranzitivitás és az antiszimmetrikusság függ csak a relációtól.

38. Mint jelent az, hogy egy reláció szigorúan antiszimmetrikus, reflexív illetve irreflexív? Ezek közül mi az, ami csak a reláción múlik?

Legyen R egy X-beli binér reláció. Azt mondjuk, hogy R

(1) reflexív, ha minden $x \in X$ esetén $(x,x) \in R$;
(2) irreflexív, ha minden $x \in X$ esetén $(x,x) \notin R$;
(3) szigorúan antiszimmetrikus, ha minden x, y-ra $(x,y) \in R$ és $(y,x) \notin R$;

Ezek közül a szigorúan antiszimmetrikusság függ csak a relációtól.

39. Definiálja az ekvivalenciarelációt, illetve az osztályozás fogalmát.

Legyen X egy halmaz. Az X-beli binér relációt ekvivalenciarelációnak nevezzük, ha reflexív, szimmetrikus és tranzitív. Az X részhalmazainak egy O rendszerét X osztályozásának nevezzük, ha O páronként diszjunkt nem üres halmazokból álló halmazrendszer, amelyre $\cup\, O = X$.

40. Mi a kapcsolat az ekvivalenciarelációk és az osztályozások között?

Valamely X halmazon értelmezett $\sim$ ekvivalenciareláció X-nek egy osztályfelbontását adja. Megfordítva, az X halmaz minden osztályfelbontása egy $\sim$ ekvivalenciarelációt hoz létre.

41. Definiálja a részbenrendezés és a részbenrendezett halmaz fogalmát. Mit mondhatunk egy részbenrendezett halmaz egy részhalmazáról?

Egy X halmazbeli részbenrendezés egy tranzitív, reflexív, és antiszimmetrikus X-beli reláció. Egy X részbenrendezett halmaz, illetve rendezett halmaz tulajdonképpen az $(X, \leq)$ pár. Egy X részbenrendezett halmaz minden Y részhalmaza is részbenrendezett, ha a $\leq$ relációt csak ennek az elemei között tekintjük, azaz a $\leq \cap (Y \times Y)$ relációval.

42. Definiálja a rendezés, a rendezett halmaz és a lánc fogalmát.

Egy X halmazbeli részbenrendezés egy tranzitív, reflexív, és antiszimmetrikus X-beli reláció. Egy X részbenrendezett halmaz, illetve rendezett halmaz tulajdonképpen az $(X, \leq)$ pár. Egy X részbenrendezett halmaz minden Y részhalmaza is részbenrendezett, ha a $\leq$ relációt csak ennek az elemei között tekintjük, azaz a $\leq \cap (Y \times Y)$ relációval. Ha az Y részhalmaz ezzel a relációval rendezett, akkor láncnak nevezzük.

Ha a $\leq$ részbenrendezési reláció dichotom is, azaz ha X bármely két eleme összehasonlítható, akkor rendezésnek nevezzük.

43. Mondjon példát részbenrendezett de nem rendezett halmazra.

A valós számok halmaza – és így a természetes, egész és racionális számok halmaza is – rendezett a szokásos rendezéssel. A természetes számok körében az „n osztja m-et” reláció részbenrendezés, de nem rendezés.

44. Definiálja egy relációnak megfelelő szigorú illetve gyenge reláció fogalmát.

Egy X-beli reláció R relációhoz definiálhatunk egy X-beli S relációt úgy, hogy xSy akkor álljon fenn, ha xRy de $x \neq y$, ez az R-nek megfelelő szigorú reláció. Megfordítva, egy X-beli R relációhoz a megfelelő T gyenge relációt úgy definiáljuk, hogy legyen xTy, ha xRy vagy $x = y$.

45. Definiálja a szigorú részbenrendezést és fogalmazza meg kapcsolatát a részbenrendezéssel.

Egy $\leq$ részbenrendezés esetén a megfelelő szigorú relációt $<$-el jelöljük; ez tranzitív, irreflexív és szigorúan antiszimmetrikus. Megfordítva ha $<$ egy X-beli szigorú részbenrendezés, amin egy tranzitív és szigorúan antiszimmetrikus reláció értünk, akkor a megfelelő gyenge reláció egy részbenrendezés.

46. Mi az, hogy kisebb, nagyobb, megelőzi, követi? Adja meg a kapcsolódó jelöléseket.

Ha $x < y$, akkor azt mondjuk, hogy x kisebb, mint y vagy y nagyobb, mint x, illetve hogy x megelőzi y-t vagy y követi x-et. A gyenge reláció esetén hozzátesszük, hogy „vagy egyenlő”.

47. Definiálja az intervallumokat és adja meg a kapcsolódó jelöléseket.

Legyen X egy részbenrendezett halmaz. Ha $x \leq z$ és $z \leq y$, akkor azt mondjuk, hogy z az x és y közé esik, ha pedig $x < z$ és $z < y$, akkor azt mondjuk, hogy z szigorúan x és y közé esik. Az összes ilyen elemek halmazát $[x, y]$, illetve $]x, y[$ jelöli.

48. Mi az, hogy közvetlenül követi illetve közvetlenül megelőzi?

Ha $x < y$, de ugyanakkor nem létezik szigorúan x és y közé eső elem, akkor azt mondjuk, hogy x közvetlenül megelőzi y-t, vagy y közvetlenül követi x-et.

49. Definiálja a kezdőszelet fogalmát, és adja meg a kapcsolódó jelöléseket.

Legyen X egy részbenrendezett halmaz. Egy x elemhez tartozó kezdőszeletnek a $\{y \in X : y < x\}$ részhalmazt nevezzük. A kezdőszelet logikus, de nem elterjedt jelölése $]\leftarrow, x[$.

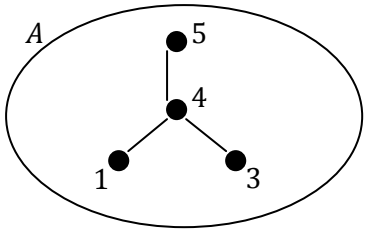
50. Definiálja a legkisebb és a legnagyobb elem fogalmát.

Az X részbenrendezett halmaz legkisebb (vagy első) elemén egy olyan $x \in X$ elemet értünk, amelyre $x \leq y \; minden \; y \in X$-re. Nem biztos, hogy van ilyen elem, de ha van, akkor egyértelmű. Hasonlóan, X legnagyobb (vagy utolsó) elemén egy olyan x elemet értünk, amelyre $y \leq x \; minden \; y \in X$-re. Nem biztos, hogy van ilyen elem, de ha van, akkor egyértelmű.

51. Definiálja a minimális és maximális elem fogalmát, és adja meg a kapcsolódó jelöléseket.

Legyen x eleme X. Az x-et minimálisnak nevezzük, ha nincs nála kisebb elem, maximálisnak pedig akkor, ha nincs nála nagyobb elem. Maximális és minimális elem lehet több is. Jelölések: $\min X$, $\max X$.

52. Adjon meg olyan részbenrendezett halmazt, amelyben több minimális elem van.



Az A részbenrendezett halmaz Hasse-diagramja a következő. Ezen esetben két minimális elem létezik: $1,3$.

53. Adjon meg olyan részbenrendezett halmazt, amelyben nincs maximális elem.

A természetes számok halmaza ilyen a szokásos rendezéssel.

54. Igaz-e, hogy rendezett halmazban a legkisebb és a minimális elem fogalma egybeesik?

Igen.

Minimális és maximális elem több is lehet, és hogy ha X rendezett, akkor a legkisebb és a minimális elem fogalma, illetve a legnagyobb és a maximális elem fogalma egybeesik, de egyébként nem feltétlenül.

55. Definiálja az alsó és a felső korlát fogalmát.

Egy X részbenrendezett halmaz egy x elemét az Y részhalmaz alsó korlátjának nevezzük, ha minden $y \in Y$-ra $x \leq y$. Ha minden $y \in Y$-ra $y \leq x$, akkor x az Y felső korlátja. Ha létezik alsó illetve felső korlát, akkor azt mondjuk, hogy Y alulról illetve felülről korlátos.

56. Igaz-e, hogy ha egy részbenrendezett halmaz egy részhalmaza tartalmaz a részhalmaz alsó korlátjai közül elemeket, akkor csak egyet?

Igen, ha az alsó korlátok között van olyan, mely eleme a részhalmaznak, úgy csak egy ilyen van.

57. Definiálja az alsó és felső határ tulajdonságot.

(x, ≤) alsó határ tulajdonságú, ha minden nem üres alulról korlátos részhalmazának van alsó határa.

(x, ≤) felső határ tulajdonságú, ha bármely nem üres, felülről korlátos részhalmazának van felső határa.

58. Igaz-e, hogy ha egy részbenrendezett halmaz egy részhalmaza tartalmazza a részhalmaz egy alsó korlátját, akkor az a részhalmaznak minimális eleme?

Igen, ha az alsó korlátok között van olyan, mely eleme a részhalmaznak, úgy csak egy ilyen van, és ez a részhalmaz legkisebb eleme (minimális eleme).

59. Definiálja az infimum és szuprémum fogalmát.

Az alsó korlátok halmazában van legnagyobb elem, akkor azt Y legnagyobb alsó korlátjának nevezzük, idegen szóval ez az infimum, és $inf\ Y$-al jelöljük. Hasonlóan, ha Y felső korlátjai halmazában van legkisebb elem, akkor azt Y legkisebb felső korlátjának nevezzük, idegen szóval ez a szuprémum, és $sup\ Y$-al jelöljük.

60. Definiálja a jólrendezés és jólrendezett halmaz fogalmát.

Egy X részbenrendezett halmazt jólrendezezznek, részbenrendezését pedig jólrendezésnek nevezzük, ha X bármely nem üres részhalmazának van legkisebb eleme. Jól rendezett halmaz mindig rendezett.

61. Adjon meg olyan rendezett halmazt, amely nem jólrendezett.

Az egész, racionális és valós számok halmaza nem jólrendezett de rendezett a szokásos rendezéssel.

62. Adjon példát jólrendezett halmazra.

A természetes számok halmaza jólrendezett a szokásos rendezéssel.

63. Adjon meg két részbenrendezett halmaz Descartes-szorzatán a halmazok részbenrendezései segítségével két részbenrendezést.

Legyenek X és Y részbenrendezett halmazok. Az $X \times Y$-ban legyen $(x, y) \leq (x', y')$, ha $x \leq x'$ az X-ben, és $y \leq y'$ az Y-ban. Így egy részbenrendezést kapunk.

64. Két jólrendezett halmaz Descartes-szorzatán a lexikografikus rendezést értjük. Mit állíthatunk erről?.

Legyen $(x, y) \leq (x', y')$, ha $x < x'$ vagy $x = x'$ és $y \leq y'$. $X \times Y$-nak ezt a részbenrendezését lexikografikus rendezésnek nevezzük.

Függvények

65. Definiálja a függvény fogalmát. Ismertesse a kapcsolódó jelöléseket.

Egy függvény egy olyan f reláció, amelyre ha $(x, y) \in f$ és $(x, y') \in f, akkor\ y = y'$, másszóval minden x-hez legfeljebb egy olyan y létezik, amelyre $(x, y) \in f$. Jelölések: $f(x) = y$. Az y elemet az f függvény x helyén (argumentumában) felvett értékének nevezzük. Egyéb jelölés: $f : x \mapsto y$.

66. Mi a különbség a között, hogy $f \in X \to Y$ és hogy $f : X \to Y$?

Annak kifejezésére, hogy az f függvény értelmezési tartománya a teljes X halmaz, értékkészlete pedig az Y halmaznak részhalmaza az $f : X \to Y$ jelölés szolgál, amit úgy olvasunk ki, hogy f az X-et Y-ba képező függvény. Ez nem ugyanaz, mint $f \in X \to Y$, mert utóbbi esetben $dmn(f) \subsetneq X$ is lehetséges.

67. Mikor nevezünk egy függvényt kölcsönösen egyértelműnek?

Az f függvényt kölcsönösen egyértelműnek nevezzük, ha $f(x) = y$ és $f(x') = y$ esetén $x = x'$. Ez azzal ekvivalens, hogy az f^{-1} reláció függvény. Másnéven injektívnek nevezzük a kölcsönösen egyértelmű függvényeket.

68. Igaz-e, hogy az identikus leképezés mindig szürjektív?

Igen. Ezt I_X-ként jelöljük, és X-nek X-re való identikus leképezésének nevezünk.

69. Definiálja a permutáció fogalmát.

Egy X halmaz önmagára való kölcsönösen egyértelmű leképezéseit az X permutációinak nevezzük.

70. Igaz-e, hogy két függvény összetétele függvény?

Igen. Ha f és g függvények, akkor $f \circ g$ is. Ha f és g kölcsönösen egyértelmű függvény, akkor $g \circ f$ is az. Ha az f függvény X-et Y-ra, a g függvény pedig Y-t Z-re képezi le, akkor $g \circ f$ az X-et Z-re képzi le.

71. Mikor állíthatjuk, hogy két függvény összetétele injektív, szürjektív illetve bijektív?

Ha f és g kölcsönösen egyértelmű függvények, akkor $f \circ g$ is. Ha az f függvény X-et Y-ra képezi le, a g függvény pedig Y-t Z-re képezi le, akkor $g \circ f$ az X-et Z-re képezi le. Ha két függvény összetétele injektív és szürjektív, akkor bijektív is.

72. Mi a kapcsolat függvények és ekvivalenciarelációk között?

Ha az X halmazon adott egy ekvivalenciareláció, akkor az x elemhez az ekvivalenciaosztályát rendelő leképezést kanonikus leképezésnek nevezzük. Megfordítva, ha $f : X \to Y$ egy függvény, akkor az $x \sim x',\ ha\ f(x) = f(x')$ reláció egy ekvivalenciareláció.

73. Mikor nevezünk egy függvényt monoton növekedőnek illetve monoton csökkenőnek?

Legyenek X és Y részbenrendezett halmazok. Az $f : X \to Y$ függvényt monoton növekedőnek nevezzük, ha $x, y \in X,\ x \leq y\ esetén\ f(x) \leq f(y)$ illetve monoton csökkenőnek nevezzük, ha $x, y \in X,\ x \leq y\ esetén\ f(x) \geq f(y)$.

74. Mikor nevezünk egy függvényt szigorúan monoton növekedőnek illetve szigorúan monoton csökkenőnek?

Legyenek X és Y részbenrendezett halmazok. Az $f : X \to Y$ függvényt szigorúan monoton növekedőnek nevezzük, ha $x, y \in X,\ x < y\ esetén\ f(x) < f(y)$, illetve szigorúan monoton csökkenőnek nevezzük, ha $x, y \in X,\ x < y\ esetén\ f(x) > f(y)$.

75. Mi a kapcsolat szigorúan monoton növekedő függvények és a kölcsönösen egyértelmű között?

Ha X, Y rendezettek, akkor szigorúan monoton növekedő (illetve csökkenő) függvény nyilván kölcsönösen egyértelmű. Megfordítva, ha X és Y rendezettek, akkor egy $f : X \to Y$ kölcsönösen egyértelmű monoton növekedő (illetve csökkenő) leképezés szigorúan monoton növekedő (illetve csökkenő) is.

76. Mit állítunk a monoton növekvő függvények inverz függvényéről?

A monoton növekvő függvények inverz függvénye monoton növekvő f(X)-en: valóban, ha x < y, akkor f(x) ≤ f(y), de f(x) = f(y) nem lehetséges, és ha u, v ∈ f(X), u < v, x = f^{-1}(u), y = f^{-1}(v), akkor x ≥ y nem lehetséges, mert ebből f(x) ≥ f(y), azaz u = f(x) < f(y) = v következne.

77. Mit értünk indexhalmaz, indexezett halmaz és család alatt?

Egy x függvény i helyen felvett értékét neha x_i-vel jelöljük. Ilyenkor gyakran a függvény I értelmezési tartományát indexhalmaznak, az elemeit indexeknek, értékkészletét indexelt halmaznak, az x függvényt magát pedig családnak nevezzük.

78. Definiálja a halmazcsaládok unióját és metszetét.

Ha az értékkészlet elemei halmazok, akkor halmazcsaládról beszélünk. Egy $X_i, i \in I$ halmazcsalád unióját a $\cup_{i\in I} X_i := \cup \{X_i : i \in I\}$ összefüggéssel értelmezzük. Rövidebb jelölése: $\cup_i X_i$. Ha $I \neq \emptyset$, akkor a halmazcsalád metszetét is definiáljuk a $\cap_{i\in I} X_i := \cap \{X_i : i \in I\}$

79. Fogalmazza meg a halmazcsaládokra vonatkozó De Morgan-szabályokat.

Ha $X_i, i \in I$ az X halmaz részhalmazainak egy nem üres családja (azaz $I \neq \emptyset$), akkor az X-re vonatkozó komplementert vesszővel jelölve,

(1) $(\cup_{i\in I} X_i)' = \cap_{i\in I} X_i'$;
(2) $(\cap_{i\in I} X_i)' = \cup_{i\in I} X_i'$.

80. Definiálja véges sok halmaz Descartes-szorzatát és ismertesse a kapcsolódó jelöléseket.

Ha az $(x_1, x_2, \dots, x_n)$ elem n-eseket az {1,2,...,n} halmaz, azaz N^+-nak az $n \in N^+$-nál nem nagyobb elemei által indexelt családokkal azonosítjuk, akkor az $X_1 \times X_2 \times \dots \times X_n$ Descartes-szorzatot mint az összes olyan x_i, $i \in \{1,2, \dots, n\}$ családok halmazát definiálhatjuk, amelyekre $x_i \in X_i, ha\ i \in \{1,2, \dots, n\}$.

81. Definiálja a (nem feltétlenül binér) reláció fogalmát és a kapcsolódó jelöléseket.

Ha az $(x_1, x_2, \dots, x_n)$ elem n-eseket az $\{1,2, \dots, n\}$ halmaz, azaz N^+-nak az $n \in N^+$-nál nem nagyobb elemei által indexelt családokkal azonosítjuk, akkor az $X_1 \times X_2 \times \dots \times X_n$ Descartes-szorzatot mint az összes olyan x_i, $i \in \{1,2, \dots, n\}$ családok halmazát definiálhatjuk, amelyekre $x_i \in X_i$, ha $i \in \{1,2, \dots, n\}$. Ilyen szorzathalmazok részhalmazait n-változós relációknak nevezzük.

82. Definiálja tetszőleges halmazcsalád Descartes-szorzatát és ismertesse a kapcsolódó jelöléseket.

Az $X_i, i \in I$ halmazcsalád $\times_{i\in I} X_i$ Descartes-szorzata a halmazcsaládhoz tartozó összes kiválasztási függvénynek halmaza. Jelölése: $\times_i X_i$.

83. Definiálja a binér, unér és nullér művelet fogalmát és ismertesse a kapcsolódó jelöléseket.

Legyen X egy halmaz. Egy X-beli binér műveleten egy $*\colon X \times X \to X$ leképezést értünk. Ha $x, y \in X$, akkor $*(x, y)$ a művelet eredménye, x és y pedig az operandusai. Rendszerint a binér művelet jelét az operandusok közé írjuk: $x * y$.

Egy X-beli unér művelet egy $* : X \to X$ leképezés.

Mivel $X^0 = \{\emptyset\}$, egy nullér művelet egy $* : \{\emptyset\} \to X$ leképezés, ami tulajdonképpen X egy elemének a kijelölését jelenti, operandusa nincs, csak eredménye.

84. Adjon meg egy binér és egy unér műveletet táblázattal.

Binér:

=>	↑	↓
↑	↑	↓
↓	↑	↑

Unér:

	↑	↓
¬	↓	↑

85. Hogyan definiálunk műveleteket függvények között?

Legyen X tetszőleges halmaz, Y pedig egy halmaz a $*$ binér művelettel. Ekkor az X-et Y-ba képező függvények között is értelmezünk „pontonként” egy binér műveletet (amit ugyanazzal a jellel szokás jelölni) az $(f * g)(x) \coloneqq f(x) * g(x)$ minden $x \in X$-re, ha $f, g\colon X \to Y$ összefüggéssel. Hasonlóan definiálunk unér, illetve nullér műveleteket függvénytereken.

86. Adjon példát műveletekre függvények között.

Egy adott X halmazon értelmezett egész, racionális, illetve valós értékű függvények esetén az összeadást, kivonást és a szorzást „pontonként” értelmezzük függvényekre is, de két függvény hányadosa nincs mindenütt definiálva. Függvény ellentettjét is pontonként definiáljuk. A 0 illetve az 1 kijelentéséből mint nullér műveletből az azonosan 0, illetve azonosan 1 függvény adódik.

87. Definiálja a művelettartó leképezés fogalmát.

Legyen $*$ binér művelet az X, és legyen $*'$ binér művelet az X' halmazon. Egy $\varphi : X \to X'$ leképezést művelettartónak nevetünk, ha $\varphi(x * y) = \varphi(x) *' \varphi(y)\ minden\ x, y \in X$-re. Hasonlóan értelmezzük a művelettartást unér és nullér műveletre is.

88. Adjon példát művelettartó leképezésre.

Ha a > 1, az $x \mapsto a^x$ leképezés művelettartó és kölcsönösen egyértelmű leképezés az összeadással tekintett valós számoknak a szorzással tekintett pozitív valós számokra. Ez a leképezés művelettartó leképezése az ellentett képzéssel tekintett valós számoknak a reciprokképzéssel tekintett pozitív valós számokra, valamint a 0-t 1-be viszi át, így ezen unér műveletekre is művelettartó.

Természetes számok

89. Fogalmazza meg a rekurziótételt.

Legyen X egy halmaz, $a \in X$ és $f : X \to X$ egy függvény. Ha a Peano-axiómák teljesülnek, akkor egy és csak egy olyan N-et X-be képező g függvény létezik, amelyre $g(0) = a$ és $g(n^+) = f\big(g(n)\big)$ minden $n \in N$-re.

90. Definiálja a karakterisztikus függvény fogalmát és ismertesse a kapcsolódó jelöléseket.

Legyen X egy halmaz, és ha $Y \subset X$, legyen $\chi_Y(x) = 1$, ha $x \in Y$ és $\chi_Y(x) = 0$, ha $x \in X \backslash Y$. A χ_Y függvényt az Y halmaz (X-en értelmezett) karakterisztikus függvényének nevezzük. Az $Y \to \chi_Y$ leképezés kölcsönösen egyértelmű leképezése $\rho(X)$-nek az X-en értelmezett karakterisztikus függvények $\{0,1\}^X$ halmazára. (Emiatt szokás $\rho(X)$-et 2^X-el is jelölni.)

91. Definiálja a baloldali semleges elem, a jobboldali semleges elem és a semleges elem fogalmát.

Legyen $*$ egy binér művelet a G halmazon. A G halmazt a $*$ művelettel, (azaz, ha pontosak akarunk lenni, a $(G,*)$ párt) szokás grupoidnak is nevezni. A G egy s elemét bal, illetve jobb oldali semleges elemnek nevezzük, ha $s * g = g$, illetve $g * s = g$ minden $g \in G$-re. Ha s bal és jobb oldali semleges elem is, akkor semleges elemnek nevezzük.

92. Definiálja a félcsoport, a balinverz, a jobbinverz és az inverz fogalmát.

Ha a $*$ binér művelet a G halmazon asszociatív, azaz $x, y, z \in X$ esetén $(x * y) * z = x * (y * z)$, akkor a G-t (pontosabban a $(G,*)$ párt) félcsoportnak nevezzük. Ha a G félcsoportban s semleges elem, és $g, g^* \in G$-re $g * g^* = s$, akkor azt mondjuk, hogy g a g^* balinverze, g^* pedig a g jobbinverze. Ha a g^* a g bal- és jobbinverze is, akkor azt mondjuk, hogy a g inverze. Ekkor nyilván g meg a g^* inverze.

93. Igaz-e, hogy egy egységelemes multiplikatív félcsoportban ha h-nak és g-nek van inverze, akkor hg-nek is, és ha igen, mi?

Igen. Ha g-nek g^* az inverze, és h-nak h^* az inverze, akkor a $g * h$ inverze $h^* * g^*$.

94. Definiálja a csoport és az Abel-csoport fogalmát.

Ha a $*$ binér művelet a G halmazon, $g, h \in G$ és $g * h = h * g$, akkor azt mondjuk, hogy g és h felcserélhetőek. Ha G bármely két eleme felcserélhető, akkor a $*$ műveletet kommutatívnak nevezzük. A kommutatív csoportokat Abel-csoportnak nevezzük. Ha X tetszőleges halmaz, akkor $(\rho(X),\Delta)$ Abel-csoport.

95. Igaz-e, hogy ha X tetszőleges halmaz, akkor $(\rho(X),\cap)$ egy egységelemes félcsoport?

Nem. $(\rho(X),\cap)$ kommutatív egységelemes félcsoport.

96. Igaz-e, hogy ha X tetszőleges halmaz, akkor $(\rho(X),\cup)$ egy csoport?

Nem. $(\rho(X),\cup)$ kommutatív egységelemes félcsoport.

97. Igaz-e, hogy ha X tetszőleges halmaz, akkor $(\rho(X),\Delta)$ egy félcsoport?

Nem. $(\rho(X),\Delta)$ egy Abel-csoport.

98. Igaz-e, hogy ha X tetszőleges halmaz, akkor az X-beli binér relációk a kompozícióval egységelemes félcsoportot alkotnak?

Igaz. Ez általában nem kommutatív és nem is csoport, bár vannak invertálható elemei.

99. Igaz-e, hogy ha X tetszőleges halmaz, akkor az X-et X-re képező bijektív leképezések kompozícióval, mint művelettel csoportot alkotnak?

Igaz. Ha csak az összes injektív, illetve az összes szürjektív leképezéseket tekintjük, akkor is egységelemes félcsoportot kapunk. Az összes bijektív leképezések csoportot alkotnak.

100. Fogalmazza meg a természetes számokra a ≤ relációt és a műveletek kapcsolatát leíró tételt.

Ha $m, n \in N$, akkor azt mondjuk, hogy $m \leq n$, ha van olyan k természetes szám, hogy $m + k = n$.

Legyen $k, m, n \in N$. Ekkor

(1) n^+ közvetlenül követi n-et;
(2) $m \leq n$ akkor és csak akkor, ha $m + k \leq n + k$;
(3) $k \neq 0$ esetén $m \leq n$ akkor és csak akkor, ha $m \cdot k \leq n \cdot k$;
(4) $m < n$ akkor és csak akkor, ha $m + k < n + k$;
(5) $k \neq 0$ esetén $m < n$ akkor és csak akkor, ha $m \cdot k < n \cdot k$;
(6) $ha\ m \cdot k = n \cdot k\ és\ k \neq 0$, akkor $m = n$ (egyszerűsítési szabály vagy törlési szabály $k \neq 0$-ra).

101. Definiálja a véges sorozatokat.

Ha $n \in N$, akkor a $[0, n] \subset N$ vagy $[1, n] \subset N^+$ halmazon értelmezett függvényeket véges sorozatnak nevezzük. Az x véges sorozatot úgy is jelöljük, hogy $x_0, x_1, \dots, x_n$ vagy $x_i,\ i = 0,1,2, \dots, n$, illetve $x_1, x_2, \dots, x_n$ vagy $x_i,\ i = 1,2, \dots, n$.

102. Fogalmazza meg az általános rekurziótételt.

Legyen adott egy X halmaz és egy f függvény, amelynek értékkészlete X részhalmaza, értelmezési tartománya pedig az összes olyan függvények halmaza, amelyek értékkészlete X részhalmaza, értelmezési tartománya pedig N valamely kezdőszelete. Ekkor egyértelműen lézetik egy $g : N \to X$ függvény, amelyre $g(a) = f\left(g|_{]\leftarrow, a[}\right)$ minden $a \in N$-re.

103. Hogyan használható az általános rekurziótétel a Fibonacci-számok definiálására?

Legyen $X = N$, és legyen az $n \mapsto n^-$ leképezése N^+-nak N-re az $n \mapsto n^+$ leképezés inverze, $f(\emptyset) = 0, f(\{(0, k)\}) = 1$ bármely $k \in N$-re, és ha $n > 1$, $h :] \leftarrow, n[\to N$ egy függvény, akkor legyen $f(h) = h(n^-) + h(n^{--})$. $(n = min(N \backslash dmn(h)))$

104. Definiálja véges sok elem szorzatát félcsoportban és egységelemes félcsoportban.

Ha G egy félcsoport, $x :\ N^+ \to G$ egy sorozat, akkor az általános rekurziótételt alkalmazva definiálhatjuk a $\Pi_{k=1}^n x_k,\ n \in N^+$ szorzatokat úgy, hogy $\Pi_{k=1}^1 x_k = x_1\ és\ \Pi_{k=1}^{n+1} x_k = (\Pi_{k=1}^n x_k) \cdot x_{n+1}$. Ha G egységelemes félcsoport e egységelemmel, akkor $\Pi_{k=1}^0 x_k = e$.

105. Fogalmazza meg a hatványozás két tulajdonságát félcsoportban és egységelemes félcsoportban.

A sorozatok tulajdonságaiból következik, vagy indukcióval bizonyítható, hogy $g^{m+n} = g^m \cdot g^n\ és\ (g^m)^n = g^{mn}$ minden $m, n \in N^+$-ra, ha G egységelemes félcsoport, akkor minden $m, n \in N$-re.

106. Fogalmazza meg a hatványozásnak azt a tulajdonságát, amely csak felcserélhető elemekre érvényes.

Ha g, h a G félcsoport felcseréhető elemei, akkor indukcióval $(gh)^n = g^n h^n$ minden $n \in N^+$-ra, ha G egységelemes félcsoport, akkor minden $n \in N$-re.

107. Hogyan értelmeztük, a $\sum_{a\in A} x_a$ jelölést?

Ha G kommutatív, akkor additív írásmódot is használhatunk, ilyenkor a szorzat helyett $\sum_{k=1}^{n} x_k$ összeget írunk. Ha G kommutatív félcsoport 0 nullelemmel, akkor $\sum_{k=1}^{0} x_k = 0$. Ha $x_k = g$ minden n-re, akkor $\sum_{k=1}^{n} x_k$ helyett ng-t írunk, n az együttható. Gyakran $\sum_{k=1}^{n} x_k$ helyett azt írjuk, hogy $x_1 + x_2 + \cdots + x_n$. Ha $x : A \to G$ egy tetszőleges függvény, és van olyan $\varphi : \{k \in N : 1 \leq k \leq n\} \to A$ kölcsönösen egyértelmű leképezés, amely A-ra képez, akkor a kommutativitást és asszociativitást felhasználva indukcióval belátható, hogy minden ilyen leképezésre $\sum_{k=1}^{n} x_{\varphi(k)}$ ugyanaz. (Ez az általános kommutativitás tétele.) Ezt a közös értéket $\sum_{a\in A} x_a$-val is jelöljük.

108. Fogalmazza meg a maradékos osztás tételét.

Legyen $n > 0$ természetes szám. Minden m természetes szám egyértelműen felírható $m = qn + r$ alakban, ahol $q, r \in N$ és $r < n$.

109. Definiálja a hányadost és a maradékot természetes számok osztásánál, a páros és páratlan természetes számokat.

Legyen $n > 0$ természetes szám. Minden m természetes szám egyértelműen felírható $m = qn + r$ alakban, ahol $q, r \in N$ és $r < n$.

E tétel szerint egyértelműen létező q számot hányadosnak, r számot pedig maradéknak nevezzük az m szám n-el való maradékos osztásánál. Ha az m természetes szám 2-vel való maradékos osztásánál a maradék 0, akkor m-et párosnak, egyébként páratlannak nevezzük.

110. Fogalmazza meg a számrendszerekre vonatkozó tételt.

Legyen $q > 1$ természetes szám. Minden $m > 0$ természetes számhoz egy és csak egy olyan n természetes szám és $a_0, a_1, \ldots, a_n \in [0, q[\subset N$ sorozat létezik, amelyre $a_n \neq 0$ és $m = \sum_{i=0}^{0} a_i \cdot q^i$.

Számfogalom bővítése

Egész számok

111. Mikor mondjuk, hogy egy binér művelet kompatibilis egy osztályzással? Adjon ekvivalens megfogalmazást, és definiálja a relációt az osztályok között.

Legyen $*$ egy binér művelet X-en, és legyen adott X egy osztályozása, illetve a megfelelő $\sim$ ekvivalencia-reláció. Azt mondjuk, hogy a $*$ művelet kompatibilis az osztályozással, illetve az ekvivalenciarelációval, ha $x \sim x'$ és $y \sim y'$ esetén $x * y \sim x' * y'$. Az ekvivalenciareláció tulajdonságai miatt elég azt megkövetelni, hogy $x * y \sim x' * y$ és $x * y \sim x * y'$ teljesüljön.

Ha a művelet kompatibilis az osztályozással, akkor az ekvivalenciaosztályok terén, $X^{\sim}$-on bevezethetünk egy $*^{\sim}$ műveletet a $x^{\sim} *^{\sim} y^{\sim} = (x * y)^{\sim}$ definícióval.

112. Definiálja a nullgyűrű és a zérógyűrű fogalmát.

Egy R halmazt egy $(+,\cdot)$ binér műveletekből álló párral gyűrűnek nevezünk, ha az összeadással Abel-csoport (a nullelemet 0 fogja jelölni), a szorzással félcsoport, és teljesül mindkét oldali disztributivitás.

A nullgyűrű csak egy elemet tartalmaz, ez pedig a 0.

A zérógyűrű olyan Abel-csoport, melyben bármely két elem szorzatát nullának értelmezzük.

113. Definiálja a bal és jobb oldali nullosztó és nullosztópár fogalmát.

Ha x, y egy R gyűrű nullától különböző elemei, és $xy = 0$, akkor azt mondjuk, hogy x és y egy nullosztópár, x bal oldali nullosztó, y pedig jobb oldali nullosztó.

114. Definiálja az integritási tartomány fogalmát.

Kommutatív nullosztómentes gyűrűt integritási tartománynak nevezünk.

115. Definiálja a rendezett integritási tartomány fogalmát.

Az R-et rendezett integritási tartománynak nevezzük, ha rendezett halmaz, integritási tartomány, és

(1) ha $x, y, z \in R$ és $x \leq y$, akkor $x + z \leq y + z$ (az összeadás monoton);
(2) ha $x, y \in R$ és $x, y \geq 0$, akkor $x \cdot y \geq 0$ (a szorzás monoton).

116. Fogalmazzon meg szükséges és elégséges feltételt arra vonatkozóan, hogy egy integritási tartomány rendezett integritási tartomány legyen.

Egy rendezett halmaz, amely integritási tartomány, akkor és csak akkor rendezett integritási tartomány, ha az alábbi feltételek fennállnak:

(1') ha $x, y, z \in R$ és $x < y$, akkor $x + z < y + z$ (az összeadás szigorúan monoton);

(2') ha $x, y \in R$ és $x, y > 0$, akkor $x \cdot y > 0$ (a szorzás szigorúan monoton).

117. Fogalmazza meg a rendezett integritási tartományban az egyenlőtlenségekkel való számolás szabályait leíró tételt.

Legyen R rendezett integritási tartomány. Ekkor

(1) ha $x > 0$, akkor $-x < 0$, és ha $x < 0$, akkor $-x > 0$;
(2) ha $x < y$ és $z > 0$, akkor $xz < yz$;
(3) ha $x < y$ és $z < 0$, akkor $xz > yz$;
(4) ha $x \neq 0$, akkor $x^2 > 0$; speciálisan, ha van egységelem, akkor az pozitív;
(5) ha 1 az egységelem, $0 < x < y$, és x-nek is, y-nak is van multiplikatív inverze, akkor $0 < \frac{1}{y} < \frac{1}{x}$.

Racionális számok

118. Definiálja a test fogalmát és adjon három példát testre.

Minden test integritási tartomány, hiszen testben minden nulla elemnek van inverze, invertálható elem pedig nem lehet nullosztó.

pl.: $\mathbb{Q}$; kételemű test: {0, 1}; 0 + 0 = 1 + 1 = 0, 0 + 1 = 1, összefüggéssel megadott összeadással és a $0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0$, $1 \cdot 1 = 1$ összefüggéssel megadott kommutatív szorzással.

119. Definiálja a rendezett test fogalmát és adjon példát olyan testre, amely nem tehető rendezett testté.

Egy testet rendezett testnek nevezünk, ha test és rendezett integritási tartomány.

Például a kételemű testen nincs olyan rendezés, amellyel rendezett test, mert rendezett testben $1 > 0$ és $-1 < 0$, de a kételemű testben $-1 = 1$.

Valós számok

121. Fogalmazza meg az Arkhimédészi tulajdonságot.

Egy F rendezett testet arkhimédészi tulajdonságúnak nevezünk, ha $x, y \in F,\ x > 0$ esetén van olyan $n \in N$, amelyre $nx \geq y$.

121. Mi a kapcsolata az arkhimédészi tulajdonságnak a felsőhatár tulajdonsággal?

Egy F rendezett testet felső határ tulajdonságúnak nevezünk, ha minden nem üres felülről korlátos részhalmazának létezik legkisebb felső korlátja. Egy F rendezett testet arkhimédészi tulajdonságúnak nevezünk, ha $x, y \in F,\ x > 0$ esetén van olyan $n \in N$, amelyre $nx \geq y$.

122. Fogalmazza meg a racionális számok felső határ tulajdonságára és az Arkhimédészi tulajdonságára vonatkozó tételt.

A racionális számok rendezett teste arkhimédészi tulajdonságú, de nem felső határ tulajdonságú.

123. Fogalmazza meg a valós számok egyértelműségét leíró tételt.

Létezik felső határ tulajdonságú test. Egy felső határ tulajdonságú testet valós számoknak nevezünk.

Legyen R' és R'' két felsőhatár tulajdonságú test. Ekkor létezik egy φ kölcsönösen egyértelmű leképezése R'-nak R''-re, amely monoton növekedő, összeadás és szorzástartó.

124. Definiálja a bővített valós számokat.

A bővített valós számok halmaza: $\overline{\mathbb{R}} \coloneqq \mathbb{R} \cup \{-\infty; +\infty\}$

125. Fogalmazza meg a valós számok létezését leíró tételt.

Létezik felsőhatár tulajdonságú test.

126. Fogalmazza meg a valós számok körében a gyökvonásra vonatkozó tételt.

Minden x ≥ 0 valós számhoz és n ∈ $\mathbb{N}^+$ természetes számhoz pontosan egy olyan y ≥ 0 valós szám található, melyre $y^n = x$. Az y számot az x n-edik gyökének nevezzük és $\sqrt[n]{x}$-el jelöljük (n=2 esetén $\sqrt{x}$-el is) vagy $x^{\frac{1}{n}}$-el jelöljük.

127. Fogalmazza meg a valós számok körében a szorzat gyökére vonatkozó állítást.

Komplex számok

128. Definiálja a komplex számok halmazát a műveletekkel.

A komplex számok halmaza $C = R \times R$, a valós számpárok halmaza az $(x, y) + (x', y') = (x + x', y + y')$ összeadással és az $(x, y) \cdot (x', y') = (xx' - y'y, y'x + yx')$ szorzással mint műveletekkel. A C test a fenti műveletekkel: a nullelem a $(0,0)$ pár, az (x, y) pár additív inverze a $(-x, -y)$ pár, egységelem az $(1,0)$ pár, és a nullelemtől különböző (x, y) pár multiplikatív inverze az $(x/(x^2+y^2), -y/(x^2+y^2))$ pár.

129. Adja meg R beágyazását C-be.

Ha $x, x' \in R$, akkor $(x, 0) + (x', 0) = (x + x', 0), (x, 0) \cdot (x', 0) = (xx', 0)$, így az $x \mapsto (x, 0)$ leképezés kölcsönösen egyértelmű, összeadás- és szorzástartó leképezése R-nek C-be, ezért az összes $(x, 0), x \in R$ alakú komplex számok halmazát azonosíthatjuk R-el.

130. Definiálja i-t, komplex szám valós és képzetes részét, konjugáltját és a képzetes számok fogalmát.

Jelölje i a $(0,1)$ komplex számot. Az $i^2 = -1$, az i segítségével az (x, y) komplex számot $x + iy$ alakban írhatjuk, és ez a felírás természetesen egyértelmű. Ezt a szám algebrai alakjának nevezzük. Ha $z = x + iy \in C$, ahol $x, y \in R$, akkor x-et a z valós részének, az y-t pedig a z képzetes részének nevettük. A z konjugáltja a $z = x - iy$ komplex szám. Egy komplex szám pontosan akkor valós, ha megegyezik a konjugáltjával. Ha egy komplex szám valós része nulla, akkor képzetesnek nevezzük.

131. Fogalmazza meg a komplex konjugálás tulajdonságait.

Legyen $z = x + iy \in C$ és $x, y \in R$.

A z konjugáltja a $\bar{z} = x - iy$ komplex szám. Egy komplex szám pontosan akkor valós, ha megegyezik a konjugáltjával. Ha egy komplex szám valós része nulla, akkor képzetesnek nevezzük. Következnek a $\bar{\bar{z}} = z$, $\overline{z + w} = \bar{z} + \bar{w}$, $\overline{zw} = \bar{z}\bar{w}, \overline{1/z} = 1/\bar{z}$ $z + \bar{z} = 2\Re(z)$, $z - \bar{z} = 2i\Im(z)$ összefüggések, ahol $z, w \in C$.

132. Definiálja komplex szám abszolút értékét. Milyen tételt használt?

Legyen az $(x, y) \in R \times R$ komplex szám abszolút értéke $|(x, y)| = \sqrt{x^2 + y^2}$.

Felhasznált tétel: ha $x \in R$, $x \geq 0$, $n \in N^+$, akkor egy és csak egy olyan y nem negatív valós szám létezik, amelyre $y^n = x$. Az y számot az x szám n-edik gyökének nevezzük, és $\sqrt[n]{x}$ -szel jelöljük.

133. Fogalmazza meg komplex számok abszolút értékének tulajdonságait.

Ha $z, w \in C$, akkor $zz = |z|^2$, $|0| = 0$, és $z \neq 0$ esetén $|z| > 0$, $|z| = |\bar{z}|$, $|zw| = |z||w|$, teljesülnek a háromszög-egyenlőtlenségek, illetve $|\Re(z)| \leq |z|$, $|\Im(z)| \leq |z|$ és $|z| \leq |\Re(z)| + |\Im(z)|$.

134. Definiálja komplex számokra a sgn függvényt és fogalmazza meg tulajdonságait.

Legyen $sgn(0) = 0$, és legyen $sgn(z) = \frac{z}{|z|}$, ha $0 \neq z \in C$.

Nyilván $sgn(\bar{z}) = \overline{sgn(z)}$ és $|sgn(z)| = 1$, ha $z \neq 0$.

135. Definiálja komplex számok trigonometrikus alakját és argumentumát.

Ha $0 \neq z \in C$, akkor van olyan t valós szám, amelyre $sgn(z) = \cos t + i \sin t$. Ha ez az összefüggés fennáll t-re, akkor a $t + 2k\pi$, $k \in Z$ számokra is, és csak ezekre. Ekkor $z = |z|(\cos t + i \sin t)$, ez a komplex szám trigonometrikus alakja.

Ha $0 \neq z \in C$, akkor legyen a z argumentuma, $\arg(z)$ az az egyetlen t valós szám, amelyre $-\pi < t \leq \pi$ és $sgn(z) = \cos t + i \sin t$; ez az egyetlen t valós szám, amelyre $-\pi < t \leq \pi$ és $z = |z|(\cos t + i \sin t)$.

136. Írja fel két komplex szám szorzatát és hányadosát trigonometrikus alakjuk segítségével.

Legyen $z, w \in C$, $z = |z|(\cos t + i \sin t)$ és $w = |w|(\cos s + i \sin s)$ ahol $t, s \in R$. Ekkor zw trigonometrikus alakja $zw = |zw|(\cos(t + s) + i \sin(t + s))$.

Ha $w \neq 0$, akkor $\frac{1}{w} = \frac{\bar{w}}{|w^2|}$, ebből $\frac{z}{w} = \frac{|z|}{|w|}(\cos(t - s) + i \sin(t - s))$.

137. Ha $n \in N^+$ és $w \in C$, írja fel a $z^n = w$ egyenlet összes megoldását.

Indukcióval $|w| = |z|^n$. Ebből $w = 0$ esetén $z = 0$. Egyébként, ha $t = \arg(w)$, akkor a

$$z_k = \sqrt[n]{|w|}\left(\cos\left(\frac{t + 2k\pi}{n}\right) + i \sin\left(\frac{t + 2k\pi}{n}\right)\right), \qquad k = 0,1, \dots, n - 1$$

különböző komplex számok, és csak ezek azok, amelyek n-edik hatványa w.

138. Írja fel az n-edik komplex egységgyököket. Mit értünk primitív n-edik egységgyök alatt?

Ha $w = 1$, akkor az $\epsilon^n = 1$ feltételnek az $\epsilon_k = \cos\left(\frac{2k\pi}{n}\right) + i \sin\left(\frac{2k\pi}{n}\right)$, $k = 0,1, \dots, n - 1$ komplex számok tesznek eleget. Ezeket n-edik komplex egységgyököknek nevezzük. Bizonyos n-edik egységgyökök hatványaiként az összes többi előáll (például $\epsilon_k = \epsilon_1^k$, $k = 0,1, \dots, k - 1$), ezeket n-edik primitív egységgyököknek nevezzük.

139. Ha $n \in N^+$ és $w \in C$, írja fel a $z^n = w$ egyenlet összes megoldását az n-edig egységgyök segítségével.

Ezek $z\epsilon_0, z\epsilon_1, \dots, z\epsilon_{n-1}$.

140. Fogalmazza meg az algebra alaptételét.

Ha $n \in N^+$, valamint $c_0, c_1, \dots, c_n$ komplex számok, $c_n \neq 0$, akkor van olyan z komplex szám, amelyre $\sum_{k=0}^{n} c_k z^k = 0$.

Véges halmazok

141. Definiálja halmazok ekvivalenciáját és sorolja fel tulajdonságait.

Az X és Y halmazokat ekvivalensnek nevezzük, ha létezik X-et Y-ra leképező kölcsönösen egyértelmű leképezés. Jelölése: $X \sim Y$.

Legyenek X, Y és Z halmazok. Ekkor

(1) $X \sim X$ (reflexivitás);
(2) ha $X \sim Y$, akkor $Y \sim X$ (szimmetria);
(3) ha $X \sim Y$ és $Y \sim Z$, akkor $X \sim Z$ (tranzitivitás).

142. Ha az X és X' illetve Y és Y' halmazok ekvivalensek, milyen más halmazok ekvivalenciájára következtethetünk még ebből?

Hogy Y^X és $Y'^{X'}$ ekvivalensek illetve $X \times Y$ és $X' \times Y'$ is ekvivalnesek.

143. Definiálja a véges és a végtelen halmazok fogalmát.

Egy X halmazt végesnek nevezünk, ha valamely n természetes számra ekvivalens a $\{1,2, \dots, n\}$ halmazzal, egyébként végtelennek nevezzük.

144. Definiálja egy véges halmaz elemeinek számát. Hogyan jelöljük? Mit használt fel a definícióhoz?

Azt az egyértleműen meghatározott természetes számot, amelyre egy adott X véges halmaz ekvivalens $\{1,2, \dots, n\}$-nel, az X halmaz elemei számának vagy számosságának nevezzük, és $card(A)$-val jelöljük.

145. Fogalmazza meg a véges halmazok és elemszámuk tulajdonságait leíró tételt.

Legyenek X és Y halmazok. Ekkor

(1) ha X véges és $Y \subset X$, akkor Y is véges, és $card(Y) \leq card(X)$;
(2) ha X véges és $Y \subsetneq X$, akkor $card(Y) < card(X)$;
(3) ha X és Y végesek és diszjunktak, akkor $X \cup Y$ is véges, és $card(X \cup Y) = card(X) + card(Y)$;
(4) ha X és Y végesek, akkor $card(X \cup Y) + card(X \cap Y) = card(X) + card(Y)$;
(5) ha X és Y végesek, akkor $X \times Y$ is véges, és $card(X \times Y) = card(X) \cdot card(Y)$;
(6) ha X és Y végesek, akkor X^Y is véges, és $card(X^Y) = card(X)^{card(Y)}$;
(7) ha X véges halmaz, akkor $\rho(X)$ is véges, és $card\big(\rho(X)\big) = 2^{card(X)}$;
(8) ha X véges, és az f függvény X-et Y-ra képezi, akkor Y is véges, $card(Y) \leq card(X)$, és ha f nem kölcsönösen egyértelmű, akkor $card(Y) < card(X)$.

146. Fogalmazza meg a skatulyaelvet.

Ha X és Y véges halmazok, és $card(X) > card(Y)$, akkor egy $f: X \to Y$ leképezés nem lehet kölcsönösen egyértelmű.

147. Mit mondhatunk véges halmazban minimális és maximális elem létezéséről?

Részben rendezett halmaz bármely nem üres véges részhalmazának van maximális és minimális eleme.

Kombinatorika

148. Mit mondhatunk véges halmaz összes permutációinak számáról?

Ha egy A halmaz ekvivalens {1,2,…,n}-nel, akkor permutációinak halmaza ekvivalens {1,2,…,n} permutációinak halmazával. Ha A={a_1,a_2,…,a_n} és p_1,p_2,…,p_n az {1,2,…n} egy permutációja, akkor az A megfelelő permutációja az $a_i \rightarrow a_{p_i}$ leképezés. Így A permutációinak száma csak n=card(A)-tól függ. Jelölje ezt a számot P_n=n!.

149. Mit értünk egy véges halmaz variációin és mit mondhatunk az összes variációk számáról?

Az A halmaz elemeiből készíthető, különböző tagokból álló a1,a2,…,an sorozatokat, azaz {1,2,…,n}-t A-ba képező kölcsönösen egyértelmű leképezéseket az A halmaz k-ad osztályú variációinak nevezzük. Ha A véges halmaz, card(A)=n, akkor ezek V_k^n száma megegyezik az {1,2,…,n}-t {1,2,…,n}-be képző, kölcsönösen egyértelmű leképezések számával. $V_k^n = \frac{n!}{(n-k)!} = n(n-1)\dots(n-k+1)$, ha k ≤ n és nulla egyébként.

150. Definiálja az ismétléses variációk fogalmát. Mit mondhatunk egy véges halmaz összes ismétléses variációinak számáról?

Az A halmaz elemeiből készíthető $a_1, a_2, \dots, a_k$ sorozatokat, azaz $\{1,2,\dots,k\}$-t A-ba képező leképezéseket az A halmaz k-ad osztályú ismétléses variációinak nevezzük. Ha A véges halmaz, $?(A) = n$, akkor ezek ${}^iV_n^k$ számáról (a $V_n^{k,i}$ jelölés is szokásos) már tudjuk, hogy n^k.

151. Mit értünk egy véges halmaz kombinációin, és mit mondhatunk az összes kombinációk számáról?

Ha $k \in \mathbb{N}$, akkor A halmaz k elemű részhalmazait az A halmaz k-ad oszályú kombinációinak nevezzük. Ha A vége halmaz, akkor card(A)=n, akkor ezek $C_n^k = \frac{n!}{k!(n-k)!} = \binom{n}{k}$, ha k ≤ n, és nulla egyébként.

152. Mit értünk egy véges halmaz ismétléses kombinációin, és mit mondhatunk az összes ismétléses kombinációk számáról?

Ha $k \in \mathbb{N}$, akkor A halmazból k elemet kiválasztva, de ismétléseket is megengedve, tekintet nélkül a sorrendre, az A halmaz k-ad osztályú ismétléses kombinációit kapjuk. Az ismétléses kombinációi az {1,2,…,k}-t {1,2,…,n}-be képező monoton növekvő függvények között, így ezek száma az A ismétléses kombinációinak ${}^iC_n^k$száma. ${}^iC_n^k = \binom{n+k-1}{k}$

153. Mit értünk egy véges halmaz ismétléses permutációin, és mit mondhatunk az összes ismétléses permutációk számáról?

Ha r,i_1,i_2,…i_r∈ $\mathbb{N}$, akkor az a_1,a_2,…,a_r (különböző) elemek i_1,i_2,…,i_r ismétlődésű ismétléses permutációi az olyan n=i_1+i_2+…+i_r tagú sorozatok, amelyekben az aj elemei ij szer fordul elő. Az A={a_1,a_2,…,a_r} jelöléssel ezek olyan {1,2,…,n}-et A-ba képző leképzések, amelyeknél a_j teljes inverz képei i_j elemű. Ezek száma: $P_n^{i_1,i_2,\dots,i_r} = \frac{n!}{i_1!i_2!\dots i_r!}$.

Binomiális és polinomiális tétel, szita formula

154. Fogalmazza meg a binomiális tételt.

Legyenek x, y egy R kommutatív egységelemes gyűrű elemei, $n \in N$. Ekkor

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} .$$

155. Írja fel a Pascal-háromszög első 8 sorát.

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1
1 6 15 20 15 6 1
1 7 21 35 35 21 7 1

156. Mennyi a binomiális együtthatók összege, illetve változó előjellel vett összege?

$$\sum_{K=0}^{n} \binom{n}{k} = 2^n \qquad \text{és} \qquad \sum_{k=0}^{n} \binom{n}{k} (-1)^k = 0$$

157. Fogalmazza meg a polinomiális tételt.

Legyen $r \in N$, $x_1, x_2, \dots, x_r$ egy R kommutatív egységelemes gyűrű elemei, $n \in N$. Ekkor

$$(x_1 + x_2 + \cdots + x_r)^n = \sum_{\substack{i_1+i_2+\cdots+i_r=n \\ i_1,i_2,\dots i_r \in \mathbb{N}}} P_n^{i_1,i_2,\dots,i_r} x_1^{i_1} x_2^{i_2} \dots x_r^{i_r}$$

158. Fogalmazza meg a logikai szita formulát.

Legyenek $X_1, X_2, \dots, X_k$ az X véges halmaz részhalmazai, f az X-en értelmezett, értékeket egy Abel-csoportban felvevő függvény.

Ha $1 \le i_1 < i_2 < \cdots < i_r \le k$, akkor legyen

$$Y_{i_1,i_2,\dots,i_r} = X_{i_1} \cap X_{i_2} \cap \dots \cap X_{i_r} .$$

Legyen továbbá

$$S = \sum_{x \in X} f(x) .$$

$$S_r = \sum_{1 \le i_1 < i_2 < \cdots < i_r \le k} \quad \sum_{x \in X_{i_1} \cap X_{i_2} \cap \dots \cap X_{i_r}} f(x) ,$$

és legyen

$$S_0 = \sum_{x \in X \setminus \cap_{i=1}^{k} X_i} f(x) .$$

Ekkor

$$S_0 = S - S_1 + S_2 - S_3 + \cdots + (-1)^k S_k .$$

Számelmélet

Oszthatóság

159. Definiálja a természetes számok körében az oszthatóságot és adja meg jelölését.

Az m természetes számot az n természetes szám osztójának, az n-et pedig m többszörösének nevezzük, illetve azt mondjuk, hogy n osztható m-el, ha van olyan k természetes szám, hogy $n = mk$; jelölése $m|n$.

160. Sorolja fel a természetes számok körében az oszthatóság alaptulajdonságait.

A természetes számok körében

(1) ha $m|n$ és $m'|n'$, akkor $mm'|nn'$;
(2) a nullának minden természetes szám osztója;
(3) a nulla csak saját magának osztója;
(4) az 1 minden természetes számnak az osztója;
(5) ha $m|n$, akkor $mk|nk$ minden $k \in N$-re;
(6) ha $k \in N^+$ és $mk|nk$, akkor $m|n$;
(7) ha $m|n_i$ és $k_i \in N, (i = 1,2, \dots, j)$, akkor $m|\sum_{i=1}^{j} k_i n_i$;
(8) bármely nem nulla természetes szám bármely osztója kisebb vagy egyenlő, mint a szám;
(9) az $|$ reláció reflexív, tranzitív és antiszimmetrikus, azaz részbenrendezés.

161. Definiálja a természetes számok körében a prímszám és a törzsszám fogalmát. Mi a kapcsolat a két fogalom között?

Ha egy $n > 1$ természetes szám csak $1 \cdot n = n \cdot 1$ alakban írható fel természetes számok szorzataként, akkor törzsszámnak (vagy felbonthatatlannak, illetve irreducibilisnek) nevezzük. Ekkor n-nek nincs más osztója, mint 1 és saját maga. A $p > 1$ természetes számot prímszámnak nevezzük, ha $p|km$ $(k, m \in N)$ esetén $p|k$ vagy $p|m$.

162. Definiálja egységelemes integritási tartományban az oszthatóságot és adja meg jelölését.

Legyen R egységelemes integritási tartomány. Ha $a, b \in R$, azt mondjuk, hogy b az a osztója, vagy a a b többszöröse, illetve hogy a osztható b-val, ha van olyan $c \in R$, hogy $a = bc$; jelölése $b|a$.

163. Sorolja fel egységelemes integritási tartományban az oszthatóság alaptulajdonságait.

Egy egységelemes integritási tartomány elemei körében

(1) ha $b|a$ és $b'|a'$, akkor $bb'|aa'$;
(2) a nullának minden természetes szám osztója;
(3) a nulla csak saját magának osztója;
(4) az 1 minden elemnek az osztója;
(5) ha $b|a$, akkor $bc|ac$ minden $c \in R$-re;
(6) ha $bc|ac$;s $c \neq 0$, akkor $b|a$;
(7) ha $b|a_i$ és $c_i \in R, (i = 1,2, \dots, j)$, akkor $b|\sum_{i=1}^{j} c_i a_i$;
(8) az $|$ reláció reflexív és tranzitív.

164. Definiálja az asszociáltak fogalmát és sorolja fel ennek a kapcsolatnak a tulajdonságait.

Legyen R egységelmes integritási tartomány. Ha $a|b$ és $b|a$, akkor azt mondjuk, hogy a és b asszociáltak. Ez a reláció reflexív, szimmetrikus és tranzitív, azaz ekvivalenciareláció, továbbá kompatibilis a szorzással. A nullának nincs más asszociáltja, csak saját maga. Az | reláció kompatibilis ezzel az ekvivalenciarelációval, és az ekvivalenciaosztályokon tekintve részbenrendezést kapunk.

165. Definiálja az egységek fogalmát és sorolja fel az egységek halmazának tulajdonságait.

Egy elem asszociáltját leírhatjuk az 1 asszociáltjai segítségével, amelyek nem mások, mint 1 osztói, hiszen 1 bárminek osztója; ezeket egységeknek nevezzük. Az egységek R azon elemei, amelyeknek van a szorzásra nézve inverzük. Az egységek a szorzásra nézve Abel-csoportot alkotnak, a gyűrű egységcsoportját. Az egységek bármely $a \in R$-nak osztói, mert $1a$-nak osztói.

166. Mi a kapcsolat az egységek és az asszociáltak között?

Az $a \in R$ asszociáltjai az εa alakú elemek, ahol ε egység.

167. Mi a kapcsolat a természetes számok és az egész számok körében vett oszthatóság között?

Mivel ha $k, m \in \mathbb{Z}$, akkor |km|=|k||m|, az egész számok körében m|n pontosan akkor teljesül, ha |m|||n| az $\mathbb{N}$-ben. Az egészek körében az egységek ± 1, az m egész szám asszíciáltjai $\pm$m, továbbá $n \in \mathbb{Z}$ pontosan akkor felbonthatatlan az egész számok körében, ha |n| törzsszám $\mathbb{N}$-ben, és $p \in \mathbb{Z}$ pontosan akkor prímelem, ha |p| prímszám $\mathbb{N}$-ben. Ennek alapján az oszthatóságra vonatkozó $\mathbb{N}$-beli állításokat átfogalmazhatjuk $\mathbb{Z}$-beli állításokká és viszont. A 2-vel osztható egészeket párosaknak, a többit páratlannak hívjuk.

168. Definiálja a Gauss-egészek gyűrűjét. Igaz-e, hogy két egységelem van?

A $G = \{n + im : n, m \in Z\} \subset C$ úgynevezett Gauss-egészek egységelemes gyűrűt alkotnak. A ∓ 1 és $\mp i$ egységek. Mivel $|bc|^2 = |b|^2|c|^2$, azt kapjuk, hogy $b|a$ esetén $|b|^2||a|^2$, így nincs is más egység.

169. Definiálja egységelemes integritási tartományban a prímelem és az irreducibilis elem fogalmát. Mi a kapcsolat a két fogalom között?

Legyen R egységelemes integritási tartomány. Egy $0 \neq a \in R$ elemet felbonthatatlannak nevezünk, ha nem egység, és csak triviális módon írható fel szorzatként, tehát $a = bc$, $b, c \in R$ esetén b vagy c egység.

A $0 \neq p \in R$ elemet prímelemnek nevezzük, ha nem egység és $p|ab$ $(a, b \in R)$ esetén $p|a$ vagy $p|b$.

Kapcsolat: minden prímelem felbonthatatlan, mert ha $p = xy$, akkor $p|x$ esetén $x = pz = x(yz)$ miatt $yz = 1$, ahonnan y és z egységek, x és p pedig asszociáltak, és hasonlóan $p|y$ esetén x egység, y és p pedig asszociáltak.

170. Mit értünk egységelemes integritási tartományban legnagyobb közös osztó alatt?

Azt mondjuk, hogy az R egységelmes integritási tartományban az $a_1, a_2, \dots, a_n \in R$ elemeknek a $b \in R$ elem legnagyobb közös osztója, ha $i = 1,2, \dots, n$ esetén $b|a_i$, és ha $i = 1,2, \dots, n$ esetén $b'|a_i$, akkor $b'|b$.

171. Mikor mondjuk egységelemes integritási tartomány elemeire, hogy relatív prímek?

R egységelemes integritási tartomány, és az $a_1, a_2, \dots, a_n \in R$. Ha az $a_1, a_2, \dots, a_n$ elemek legnagyobb közös osztói egységek, akkor azt mondjuk, hogy $a_1, a_2, \dots, a_n$ relatív prímek.

172. Mit értünk egységelemes integritási tartományban legkisebb közös többszörös alatt?

R egységelemes integritási tartomány. Azt mondjuk, hogy $b \in R$ az $a_1, a_2, \dots, a_n \in R$ elemek legkisebb közös többszöröse, ha $i = 1,2, \dots, n$ esetén $a_i | b$, és ha $i = 1,2, \dots, n$ esetén $a_i | b'$, akkor $b | b'$.

173. Egyértelmű-e az egész számok körében a legnagyobb közös osztó? Ismertesse a kapcsolódó jelölést.

Ha létezik az $a_1, a_2, \dots, a_n \in Z$ számoknak legnagyobb közös osztója, akkor a legnagyobb közös osztók közül az egyik nemnegatív, ezt $lnko(a_1, a_2, \dots, a_n)$-nel jelöljük.

174. Egyértelmű-e az egész számok körében a legkisebb közös többszörös? Ismertesse a kapcsolódó jelölést.

Ha létezik az $a_1, a_2, \dots, a_n \in Z$ számoknak legkisebb közös többszöröse, akkor a legkisebb közös többszörözök közül az egyik nemnegatív, jelölje ezt $lkkt(a_1, a_2, \dots, a_n)$-nel jelöljük.

175. Ismertesse a bővített euklideszi algoritmust.

Ez az eljárás meghatározza az $a, b \in Z$ egészek egy d legnagyobb közös osztóját, valamint az $x, y \in Z$ egész számokat úgy, hogy $d = ax + by$ teljesüljön.

(1) [inicializálás] Legyen $x_0 \leftarrow 1, y_0 \leftarrow 0,\ r_0 \leftarrow a, x_1 \leftarrow 0,\ y_1 \leftarrow 1,\ r_1 \leftarrow b,\ n \leftarrow 0.$
(2) [vége?] Ha $r_{n+1} = 0$, akkor $x \leftarrow x_n,\ y \leftarrow y_n,\ d \leftarrow r_n$, és az eljárás véget ért.
(3) [ciklus] Legyen $q_{n+1} \leftarrow \left\lfloor \frac{r_n}{r_{n+1}} \right\rfloor, r_{n+2} \leftarrow r_n \bmod r_{n+1} = r_n - r_{n+1}q_{n+1},\ x_{n+2} \leftarrow x_n - x_{n+1}q_{n+1},\ y_{n+2} \leftarrow y_n - y_{n+1}q_{n+1},\ n \leftarrow n + 1$ és menjünk (2)-re.

176. Mely tétel alapján számolhatjuk ki véges sok egész szám legnagyobb közös osztóját prímfelbontás nélkül?

Bármely $a_1, a_2, \dots, a_n \in Z$ számoknak létezik legnagyobb közös osztója, és $lnko(a_1, a_2, \dots, a_n) = lnko(lnko(a_1, a_2), a_3, a_4, \dots, a_n)$.

177. Fogalmazza meg a számelmélet alaptételét.

Minden pozitív természetes szám a sorrendtől eltekintve egyértelműen felbontható prímszámok szorzataként.

178. Definiálja prímtényezős felbontásnál a kanonikus alakot.

A számelmélet alaptételében szereplő prímtényezős felbontást gyakran $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ alakban írjuk, ahol $p_1, p_2, \dots, p_k$ különböző prímek, a kitevők pedig N^+ elemei. Ezt nevezzük a szám kanonikus alakjának.

179. Hogyan határozhatók meg természetes számok esetén az osztók, a legnagyobb közös osztó és a legkisebb közös többszörös a prímtényezős felbontás segítségével?

Ha mindnek adott a prímtényezős felbontása, akkor közös osztóik, valamint hasonlóan közös többszöröseik is leolvashatóak. Ez a kanonikus alak: $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ ahol $p_1, p_2, \dots, p_k$ különböző prímek, a kitevők pedig N^+ elemei.

180. Mi a kapcsolat két egész szám legnagyobb közös osztója és legkisebb közös többszöröse között?

Tetszőleges $a, b \in Z$ számoknak létezik legkisebb közös többszöröse, és $lnko(a, b) \cdot lkkt(a, b) = |ab|$.

181. Hogyan számolhatjuk ki véges sok egész szám legkisebb közös többszörösét prímfelbontás nélkül?

Tetszőleges $a_1, a_2, \dots, a_n \in Z$ számoknak létezik legkisebb közös többszöröse, és $lkkt(a_1, a_2, \dots, a_n) = lkkt(lkkt(a_1, a_2), a_3, a_4, \dots, a_n)$.

182. Ismertesse Eratoszthenész szitáját.

Ha egy adott n-ig az összes prímet meg akarjuk találni, a következő egyszerű eljárás hatékony módszert ad: írjuk fel a számokat 2-től n-ig. Az első szám, a 2 prím, összes (valódi) többszöröse összetett, ezeket húzzuk ki. A megmaradó számok közül az első a 3, ez prím, ennek minden (valódi) többszöröse összetett, ezeket húzzuk ki stb. Az eljárás végén az n-nél nem nagyobb prímek maradnak meg.

Kongruenciák

183. Definiálja egész számok kongruenciáját és adja meg a kapcsolódó jelöléseket.

Ha $a, b, m \in Z$ és m osztója $a - b$ –nek, akkor azt mondjuk, hogy a és b kongruensek modulo m; ezt úgy jelöljük, hogy $a \equiv b \ (mod\ m)$.

184. Fogalmazza meg az egész számok kongruenciájának egyszerű tulajdonságait.

Ha a és b nem kongruensek modulo m, akkor azt mondjuk, hogy inkongruensek modulo m, és azt írjuk, hogy $a \not\equiv b \ (mod\ m)$. Nyilván, ha $a \equiv b \ (mod\ m)$ és $d|m$, akkor $a \equiv b \ (mod\ d)$ is teljesül. Ha $0 \neq d \in Z$, akkor $a \equiv b \ (mod\ m)$ ekivalens azzal, hogy $ad \equiv bd \ (mod\ md)$.

Az oszthatóság tulajdonságaiból következik, hogy bármely adott $m \in Z$-re a kongruencia ekvivalenciareláció Z-ben. Az m és a $-m$ szerinti kongruencia ugyanazt jelenti.

185. Definiálja a maradékosztály, redukált maradékosztály, teljes és redukált maradékrendszer fogalmát.

Egy $m \in Z$ modulus szerinti kongruencia ekvivalenciaosztályait maradékosztályoknak nevezzük. Ha egy maradékosztály valamelyik eleme relatív prím a modulushoz, akkor mindegyik, és ekkor a maradékosztály redukált maradékosztálynak nevezzük. Páronként inkongruens egészek egy rendszerét maradékrendszernek nevezzük. Ha egy maradékrendszer minden maradékosztályából tartalmaz elemet, akkor teljes maradékrendszernek nevezzük. Ha egy maradékrendszer pontosan a redukált maradékosztályokból tartalmaz elemet, akkor redukált maradékrendszernek nevezzük.

186. Definiálja Z_m-et. Milyen algebrai struktúra Z_m?

Egy $m \in Z$ modulus szerinti kongruencia ekvivalenciaosztályait maradékosztályoknak nevezzük.

A kongruencia kompatibilis az összeadással és a szorzással. Az ekvivalenciaosztályok kommutatív egységelemes gyűrűt alkotnak az összeadással és a szorzással. Ezt a gyűrűt Z_m-el jelöljük.

187. Ismertesse a komplemens ábrázolásokat?

Negatív számok számítógépes ábrázolására elterjedt a komplemens ábrázolás. Csak bináris gépek esetével foglalkozunk. Egy n-bites számítógépen használt lehetőségek $0 \leq k < 2^{n-1}$ esetén –k ábrázolása:

1. –k mod(2^n-1) kettes számrendszerbeli alakját tároljuk. ezt úgy kapjuk, hogy k kettes számrendszerbeli alakját levonjuk 2^n-1 kettes számrendszerbeli alakjából. Mivel ez utóbbi csupa egyesből áll, a kivonás során nincs átvitel, k kettes számrendszerbeli alakját csak bitenként komplementáljuk. (egyesekre komplentálás)
2. Kettes komplementálás: k mod 2^n kettes számrendszerbeli alakját tároljuk. Ezt úgy kapjuk, hogy k kettes számrendszerbeli alakjának vesszük a bitenkénti komplementerét, majd hozzáadunk 1-et.

188. Fogalmazza meg a Z_m gyűrű tulajdonságait leíró tételt.

Legyen $m > 1$ egész. Ha $1 < lnko(a, m) < m$, akkor a maradékosztálya nullosztó Z_m-ben.

Ha $lnko(a, m) = 1$, akkor a maradékosztályának van multiplikatív inverze Z_m-ben. Speciálisan, ha m prímszám, akkor Z_m test.

189. Ismertesse a diszkrét logaritmus problémát.

Z_m-ben nem nehéz hatványozni. Azonban a tapasztalat szerint még ha m prím is, Z_m invertálható elemeinek multiplikatív csoportjában egy a alap és egy a^k hatvány ismeretében nehéz meghatározni a k kitevőt, legalábbis ha m-1-nek vannak nagy prímtényezői: ez a diszkrét logaritmus probléma. A probléma számos más csoport esetén is nehéznek tűnik.

190. Ismertesse a diszkrét logaritmus problémát.

A felhasználók megállapodnak egy nagy Sophie Germain prímben, azaz olyan p prímben, amelyre q=2p+1 is prím, valamint egy 1<g<p-1 alapban. Ha a két felhasználó valamely szokásos rejtjelezési rendszer, például az AES felhasználásával titkosított üzenetet akar váltani, akkor szükségük van egy véletlenszerű közös kulcsra. Választanak egy 1<a<p illetve 1<b<p véletlen kitevőt, kiszámolják, és közzéteszik a g^a mod q illetve g^b mod q értékeket. Mindketten ki tudják számolni a g^{ab} mod q értékét, ez lesz a titkos kulcs. Az eljárás biztonsága azon múlik, hogy a, g^a mod q és g^b mod q ismeretében sem látszik jobb megoldás g^{ab} mod q meghatározásában, mint az a és b megkeresése, ez viszont nehéz diszkrét logaritmus probléma. (Ezt a kulcscsere módszert használja az ssh, az SSL, és a TLS.)

191. Definiálja az Euler-féle φ függvényt.

Legyen $m > 0$ egész szám, és jelölje $\varphi(m)$ a modulo m redukált maradékosztályok számát; φ az Euler-féle φ függvény.

192. Mit mondhatunk az aa_i+b számokról, ha a_i egy maradékrendszer, illetve egy redukált maradékrendszer elemeit futja be?

Legyen m > 1 egész szám, a relatív prím m-hez. Ha $a_1,a_2,\dots,a_m$ teljes maradékrendszer modulo m és $b \in \mathbb{Z}$, akkor aa_1+b, aa_2+b is teljes maradékrendszer modulo m. Ha $a_1,a_2,\dots, a_{\varphi(m)}$ is redukált maradékrendszer modulo m.

193. Fogalmazza meg az Euler Fermat-tételt.

Legyen $m > 1$ egész szám, a relatív prím m-hez. Ekkor $a^{\varphi(m)} \equiv 1 \ (mod\ m)$.

194. Fogalmazza meg a Fermat-tételt.

Legyen p prímszám. Ha $a \in Z$ és $p \nmid a$, akkor $a^{p-1} \equiv 1 \ (mod\ p)$. Ha $a \in Z$ tetszőleges, akkor $a^p \equiv a \ (mod\ p)$.

195. Mit értünk diofantikus problémán?

Ha egy egyenlet vagy egyenletrendszer egész megoldásait keressük, akkor diofantikus problémáról beszélünk.

196. Mondjon két példát diofantikus problémára.

Például az $x^2 + y^2 = -4$ problémának valós megoldása nincs, az $x^4 - 4y^4 = 3$ egyenlet egyik oldala pedig modulo 4 kongruens 0-val vagy 1-el, a másik oldala pedig 3-mal, emiatt az egyenletnek nincs egész megoldása. Az $x^2 + y^2 = z^2$ egyenlet megoldásai a pitagoraszi számhármasok, míg ha $n > 2$ egész, akkor a Fermat-sejtés szerint az $x^n + y^n = z^n$ egyenletnek nincsenek nem triviális egész megoldásai.

197. Fogalmazza meg a kínai maradéktételt.

Legyenek $m_1, m_2, \dots, m_n$ egynél nagyobb, páronként relatív prím természetes számok, $c_1, c_2, \dots, c_n \in Z$. Az $x \equiv c_j \pmod{m_j}$, $j = 1,2, \dots, n$ kongruenciarendszer megoldható, és bármely két megoldása kongruens modulo $m_1 m_2 \dots m_n$.

~~***198. Ismertesse az RSA eljárást.***~~

~~***199. Ismertesse az RSA eljárás felhasználását digitális aláírásra.***~~

~~***200. Ismertesse az RSA eljárás felhasználását bizonyítványok kiállítására.***~~