Οργάνωση τμήματος: άρτιοι ΑΜ

http://eclass.di.uoa.gr/

- Τρίτη, 09:00-11:00 (αίθουσα Α2) και Πέμπτη 09:00-11:00 (αμφιθέατρο).
  Διακριτά Μαθηματικά, Σ. Κολλιόπουλος, σύγγραμμα **Liu**.
  80% βαθμού,
  όπου το 30% από υποχρεωτική πρόοδο και το 70% από την τελική εξέταση.
- Δευτέρα 11:00-12:00 (αμφιθέατρο).
  Θεωρία αριθμών, Π. Τσαγκάρης, σύγγραμμα Τσαγκάρη.
  20% βαθμού.
- Τμήμα περιττών ΑΜ: Διδάσκων Α. Κιαγιάς.

Φροντιστήρια άρτιων ΑΜ

Για φοιτητές με άρτιο Αριθμό Μητρώου και μόνο: Τετάρτη 13:00-14:00 (αίθουσα Α2).

Έναρξη φροντιστηρίων

Το φροντιστήριο ΔΕΝ θα ξεκινήσει αμέσως. Θα προηγηθεί ανακοίνωση στο μάθημα η οποία θα αναρτηθεί και στην ιστοσελίδα.

Τί είναι τα Διακριτά Μαθηματικά;

Είναι η μελέτη διακριτών μαθηματικών αντικειμένων:

- σύνολα, π.χ. {α,ε,η,ι,ο,υ,ω},
- γράφοι,
- ακέραιοι αριθμοί και υποσύνολά τους π.χ. $\{0, 2, 4, 8, 16, 32, \dots\}$,
- πρώτοι αριθμοί 2,3,5,7,11,13,...,
- αριθμητικές συναρτήσεις, δηλ. με πεδίο ορισμού τους ακεραίους.

Τα διακριτά αντικείμενα αναπαρίστανται με ακρίβεια στον Υπολογιστή!

Τι ΔΕΝ εξετάζουμε στα Διακριτά Μαθηματικά;
Συνεχή αντικείμενα, Μαθηματική ανάλυση.

Αντιστοιχία διακριτών/συνεχών αντικειμένω

Διακριτά $\neq$	Συνεχή αντικείμενα
$\mathbb{Z}$, $\mathbb{Q}$	$\mathbb{R}$, $\mathbb{C}$
σύνολο $\{0,1,2,3\}$, ακολουθία $(0,1,2,3)$	διάστημα $[0,3]$ ή $(0,3)$
άθροισμα $\sum_{k=0}^{N} k = \frac{N(N+1)}{2} = \frac{N^2}{2} + \frac{N}{2}$	ολοκλήρωμα $\int_0^N t\,dt = \frac{t^2}{2}\|_0^N = \frac{N^2}{2}$
διακριτή $\neq$ γεγονός $\in$ δειγματικό χώρο $\Delta = \{K, \Gamma\}$	συνεχής πιθανότητα $\Delta = [0,1]$

Γιατί μελετάμε τα Διακριτά Μαθηματικά;

Α. Αλγόριθμοι και Πολυπλοκότητα:

- ανάλυση πολυπλοκότητας μέσω αριθμητικών συναρτήσεων,
- πιθανοκρατικοί αλγόριθμοι: αποφεύγουν χείριστη περίπτωση,
- βελτιστοποίηση στην επιχειρησιακή έρευνα, π.χ. δρομολόγια αεροπορικών εταιριών,
- γεωμετρικοί αλγόριθμοι, π.χ. κυρτό περίβλημα, διάγραμμα **Voronoi**.

Β. Κρυπτογραφία, κωδικοποίηση και ασφάλεια:

- πρώτοι αριθμοί, π.χ. πιστωτικές κάρτες, **ssh, putty**,
- αλγεβρικοί αλγόριθμοι.

Γιατί μελετάμε τα Διακριτά Μαθηματικά;

Γ. Τηλεπικοινωνιακά δίκτυα:

- αλγόριθμοι σε γράφους,
- συνδυαστική και πιθανότητες.

Δ. Δομές και βάσεις δεδομένων:

- γράφοι, π.χ. ισορροπημένα δένδρα,

Ε. Γλώσσες προγραμματισμού και μεταγλωττιστές:

- θεωρία γράφων (γραφημάτων),
- λογικές προτάσεις, θεωρία συνόλων.

1 ΣΥΝΟΛΑ

[Liu, κεφ.1]

Ορισμός συνόλου

Σύνολο είναι μια συλλογή διακεκριμένων (δηλ. διαφορετικών) αντικειμένων.
Π.χ. $\{a, b\}$, $\mathbb{N} = \{0, 1, 2, 3, 4, 5, \dots\}$, $[0, 1] \subset \mathbb{R}$.
Π.χ. $A = \{a \in \mathbb{R} \ : \ 0 \leq a \leq 1\}$.
Π.χ. $\{1, 2, 4, 8, 16 \dots\} = \{x = 2^k \ : \ k = 0, 1, 2, 3, 4, \dots\}$.

Τα αντικείμενα που συνθέτουν το σύνολο καλούνται στοιχεία ή μέλη του συνόλου· συμβολίζουμε $a \in \{a, b\}$, $c \notin \{a, b\}$.

Ένα οποιοδήποτε αντικείμενο είτε ανήκει σε δεδομένο σύνολο είτε δεν ανήκει (αλλά ποτέ και τα δύο).

Το πλήθος των στοιχείων συνόλου καλείται πληθικός αριθμός.
Π.χ. $|\{a, b\}| = 2$, $|[0, 1]| = \infty$.

Τρόπος ορισμού

Ένα σύνολο ορίζεται

- με απαρίθμηση των στοιχείων του, π.χ. {1,2,3},
- με περιγραφή των στοιχείων του, π.χ. $\{a \in \mathbb{Z} : 1 \leq a \leq 3\}$,
- μέσω πράξεων σε σύνολα που έχουμε ήδη ορίσει (π.χ. ένωση, τομή).

Τα στοιχεία ενός συνόλου:

- δεν επαναλαμβάνονται, δηλ. το $\{a, a, b\}$ ΔΕΝ έχει νόημα, εκτός απο ειδικές περιπτώσεις.
- δεν είναι ταξινομημένα, δηλ. $\{a, b\} = \{b, a\}$,
- μπορεί να είναι διαφορετικού είδους, ακόμη και σύνολα, π.χ. $\{a, 1, \frac{3}{4}, \{K, \Gamma\}, \text{Περσεφόνη}, \{\}\}$.

Υποσύνολα

Ορ. Ένα σύνολο P καλείται υποσύνολο του Q (συμβολικά $P \subseteq Q$) αν $\forall p \in P$ ισχύει πως $p \in Q$.

Π.χ. $\{a\} \subseteq \{a, b\}, \{a, c\} \not\subseteq \{a, b\}$.

Παρατήρηση.

- Για κάθε σύνολο A, ισχύει $A \subseteq A$.
- Μπορεί να ισχύει $A \subset B$ και $A \in B$, π.χ. $A = \{a, b\}, B = \{a, b, \{a, b\}\}$.

Γνήσιο υποσύνολο $A \subset B$ καλείται το υποσύνολο A αν $A \neq B$.
Ισοδύναμα, $A \subset B \Leftrightarrow (A \subseteq B \,\&\, A \neq B)$.

Κενό σύνολο

Ορ. Κενό καλείται το σύνολο {}, που δεν περιέχει κανένα στοιχείο· συμβολίζεται με $\emptyset$. Ισοδύναμα, για κάθε a ισχύει $a \notin \emptyset$.

Θεώρ. $\emptyset \subseteq P$, για κάθε σύνολο P.

Απόδειξη: Ο ορισμός του υποσυνόλου ικανοποιείται τετριμμένα.

Άσκ. ΔΕΝ ισχύει πως, για κάθε σύνολο P, $\emptyset \in P$.
Απόδειξη με αντιπαράδειγμα: Υπάρχει σύνολο $\{a, b\}$ όπου δεν ανήκει το $\emptyset$.

Ισότητα Συνόλων

Ορ. $P = Q$ αν $\forall p, (p \in P \Leftrightarrow p \in Q)$.

Ισοδύναμα, $P = Q \Leftrightarrow (P \subseteq Q \;\&\; Q \subseteq P)$.

Π.χ. $\{a \in \mathbb{R} \;:\; 0 \leq a \leq 1\} = [0, 1]$.
Π.χ. $\{1, 2, 4, 8, 16 \dots\} = \{x = 2^k \;:\; k = 0, 1, 2, 3, 4, \dots\}$.
Π.χ. $\{a, b\} \neq \{a, b, \emptyset\}$.

Υπενθύμιση. $a \Leftrightarrow b$ σημαίνει πως

- το a είναι επαρκής συνθήκη για το b, δηλ. $a \Rightarrow b$ και, επίσης,
- το a είναι αναγκαία συνθήκη για το b, δηλ. $a \Leftarrow b$.

Ορισμός ένωσης και τομής συνόλων

$P \cup Q := \{a \;:\; a \in P \text{ ή } a \in Q\}$,
$P \cap Q := \{a \;:\; a \in P \text{ και } a \in Q\}$.

Π.χ. $\{a, b\} \cup \{a, c\} = \{a, b, c\}$, $\{a, b\} \cap \{a, c\} = \{a\}$,
$\{0, 2, 4, 6, 8, \dots\} \cap \{a : a = 2k + 1, k \in \mathbb{N}\} = \emptyset$.

Παρατηρήσεις.

- $\forall\, A, A \cup A = A$, $A \cap A = A$,
- $A \subseteq B \Rightarrow (A \cup B = B$, $A \cap B = A)$,
- $A \subseteq A \cup B$, $A \cap B \subseteq A$, $\forall\, B$,
- $A, B \subseteq C \Rightarrow A \cap B \subseteq A \cup B \subseteq C$,
  $(A \subseteq B, A \subseteq C) \Rightarrow A \subseteq B \cap C \subseteq B \cup C$.
- επέκταση ορισμών ένωσης/τομής σε οποιοδήποτε (ακόμη και άπειρο) πλήθος συνόλων, π.χ. $A_i := \{i\}, \bigcup_{i=0}^{\infty} A_i = \mathbb{N}$.

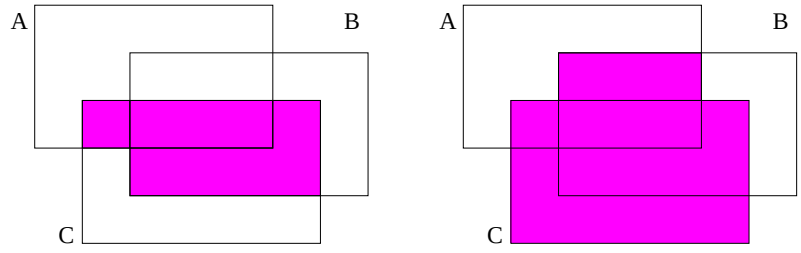
Ιδιότητες ένωσης και τομής συνόλων

Οι πράξεις ένωσης και τομής

- είναι προσεταιριστικές, δηλ.
  $A_1 \cup (A_2 \cup (\cdots (A_{k-1} \cup A_k) \cdots)) = A_1 \cup A_1 \cup \cdots \cup A_k$,
  $A_1 \cap (A_2 \cap (\cdots (A_{k-1} \cap A_k) \cdots)) = A_1 \cap A_1 \cap \cdots \cap A_k$,
- είναι αντιμεταθετικές, δηλ. $A \cup B = B \cup A$, $A \cap B = B \cap A$,
- έχουν ουδέτερο στοιχείο: $A \cup \emptyset = A, A \cap \Omega = A$, όπου το σύμπαν Ω (σύνολο αναφοράς) εξαρτάται από την συγκεκριμένη εφαρμογή,
- είναι επιμεριστική η μία ως προς την άλλη, δηλ.
  $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$,
  $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$.

Επιμεριστικότητα

$(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$, $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$



Διαγράμματα **Venn**.

Απόδειξη $(P \cup Q) \cap R = (P \cap R) \cup (Q \cap R$

Έστωσαν $A := (P \cup Q) \cap R$,
$B_1 := P \cap R, B_2 := Q \cap R, B := B_1 \cup B_2$.
Πρέπει να δείξουμε $A = B$.

Απόδειξη $(P \cup Q) \cap R = (P \cap R) \cup (Q \cap R$

Έστωσαν $A := (P \cup Q) \cap R$,
$B_1 := P \cap R, B_2 := Q \cap R, B := B_1 \cup B_2$.
Πρέπει να δείξουμε $A = B$.

$[B \subseteq A]$
$B_1 \subseteq P \Rightarrow B_1 \subseteq P \cup Q, B_1 \subseteq R$ άρα $B_1 \subseteq A$.
Ομοίως $B_2 \subseteq A$. Συνεπώς $B = B_1 \cup B_2 \subseteq A$.

Απόδειξη $(P \cup Q) \cap R = (P \cap R) \cup (Q \cap R$

Έστωσαν $A := (P \cup Q) \cap R$,
$B_1 := P \cap R, B_2 := Q \cap R, B := B_1 \cup B_2$.
Πρέπει να δείξουμε $A = B$.

$[B \subseteq A]$
$B_1 \subseteq P \Rightarrow B_1 \subseteq P \cup Q, B_1 \subseteq R$ άρα $B_1 \subseteq A$.
Ομοίως $B_2 \subseteq A$. Συνεπώς $B = B_1 \cup B_2 \subseteq A$.

$[A \subseteq B]$
$a \in A \Rightarrow a \in P \cup Q \,\&\, a \in R$.
Αν $a \in P$, επειδή $a \in R$, έπεται $a \in P \cap R$.
Αλλιώς $a \notin P$, κι επειδή $a \in P \cup Q$, $a \in Q$· άρα $a \in Q \cap R$.
Τελικά, $a \in B$ άρα $A \subseteq B$.

Συναρτήσεις [Liu, ενότ.4.1,4.8]

Αλγεβρικές δομές [Liu, ενότ.11-11.2]

Διμελής σχέση

Ορ. Καρτεσιανό γινόμενο δύο συνόλων:

$$A \times B = \{(a, b) : a \in A, b \in B\}.$$

Ορ. Μια διμελής σχέση είναι ένα υποσύνολο του $A \times B$.

Παράδειγμα.
Φοιτητές $\Phi = \{A, B, C\}$, Μαθήματα $M = \{S_1, S_2\}$,

$$\Phi \times M = \{(A, S_1), (A, S_2), (B, S_1), (B, S_2), (C, S_1), (C, S_2)\}.$$

Τα παρακολουθούμενα μαθήματα Π είναι μια διμελής σχέση:

$$\Pi = \{(A, S_2), (B, S_1), (B, S_2), (C, S_2)\}.$$

Συναρτήσεις

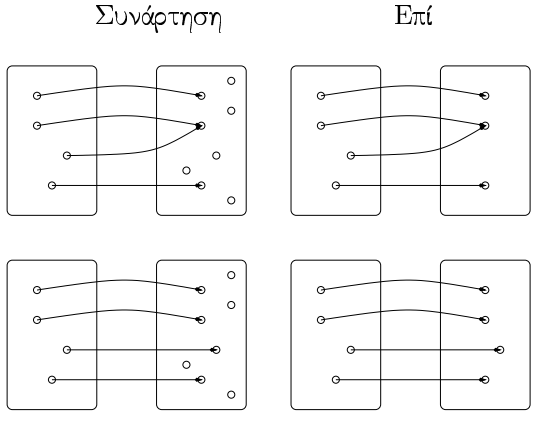
Ορ. Συνάρτηση $A \to B$ καλείται μια διμελής σχέση $D \subseteq A \times B$ αν $\forall a \in A, \exists$ μοναδικό $b \in B : (a, b) \in D$.
Δηλ. πρόκειται για μια μονοσήμαντη απεικόνιση του A στο B.

Η συνάρτηση $f : A \to B$ είναι επί αν $\forall\, b \in B, \exists\, a \in A : (a, b) \in$ σχέση, δηλ. $\forall\, b \in B, \exists\, a \in A :\ f(a) = b$.

Η συνάρτηση $f : A \to B$ είναι 1-1 αν $a \neq a' \in A \Rightarrow f(a) \neq f(a')$

Κάθε συνάρτηση που είναι $1-1$ και επί ονομάζεται και αμφιμονοσήμαντη. Οπότε και ορίζεται η αντίστροφη συνάρτηση στο $f(A)$.

Παραδείγματα συναρτήσεων



Αλγεβρικές Δομές

Ορ. Μία συνάρτηση $f : A \times A \to B$ καλείται διμελής πράξη στο A. Αν $B = A$ τότε η πράξη είναι κλειστή.

Π.χ. Οι πράξεις συνόλων είναι κλειστές (διμελείς) πράξεις.
Π.χ. Η διαίρεση ακεραίων είναι μη κλειστή πράξη, αλλά η διαίρεση ρητών αριθμών είναι κλειστή.

Ορ. Αλγεβρικό σύστημα, ή αλγεβρική δομή είναι ένα σύνολο εφοδιασμένο με μία ή περισσότερες κλειστές πράξεις.

Π.χ. Αλγεβρικές δομές με μία πράξη:
$(\mathbb{N}, +)$, $(\mathbb{Z}, *)$, $(2^\Omega, \cup)$, $2^\Omega := \{$ τα σύνολα με στοιχεία $\in \Omega\}$.

Π.χ. Αλγεβρικές δομές με 2 πράξεις:
$(\mathbb{N}, +, *)$, $(\{\text{Πίνακες } n \times n\}, +, *)$, $(2^\Omega, \cup, \cap)$.

Ημιομάδα, μονοειδές

Ορ. Ημιομάδα = αλγεβρική δομή με μια πράξη, η οποία ικανοποιεί την προσεταιριστική ιδιότητα.
Π.χ. Τα περισσότερα γνωστά παραδείγματα.
Όχι: ύψωση σε δύναμη: $(a \uparrow b) \uparrow \gamma \mapsto (a^b)^\gamma = a^{b\gamma}$, δεν ισούται με: $a \uparrow (b \uparrow \gamma) \mapsto a^{b^\gamma}$.

Ορ. Το αριστερό ουδέτερο στοιχείο $e \in A$ ως προς μια πράξη $\circ$ ικανοποιεί: $\forall\, x \in A,\ e \circ x = x$.
Δεξί ουδέτερο στοιχείο $e \in A$ ως προς $\circ$: $\forall x \in A, x \circ e = x$.
Το ουδέτερο στοιχείο είναι αριστερό και δεξί ουδέτερο στοιχείο.

Ορ. Μονοειδές = ημιομάδα με ουδέτερο στοιχείο.
Π.χ. $(2^\Omega, \cap), (2^\Omega, \cup), (\mathbb{N}, +), (\mathbb{Z}, *)$.
Όχι: ύψωση σε δύναμη: $\nexists e : (\forall a, a \uparrow e = a = e \uparrow a)$.

Ομάδα (**group**)

Ορ. Για κάθε $x \in A$, το συμμετρικό στοιχείο του x ως προς μια πράξη $\circ$ είναι το $x' \in A : x \circ x' = x' \circ x = e$.
Στην πρόσθεση και τον πολλαπλασιασμό, το συμμετρικό καλείται αντίθετο και αντίστροφο, αντίστοιχα.

Ορ. Ομάδα = μονοειδές : υπάρχει το συμμετρικό κάθε στοιχείου.
Π.χ. $(\mathbb{Z}, +)$, $(\mathbb{R} - \{0\}, *)$, (αντιστρέψιμοι πίνακες $n \times n$, $*$).
Όχι: $(2^\Omega, \cup), (2^\Omega, \cap), (\mathbb{N}, +), (\mathbb{Z}, *)$.

Αν ισχύει η αντιμεταθετικότητα, τότε ονομάζεται αντιμεταθετική ή αβελιανή ομάδα (από τον **Abel**).

Δακτύλιος και σώμα

Ορ. Δακτύλιος (**ring**) καλείται κάθε δομή $(A, \oplus, \otimes)$ όπου,
το $(A, \oplus)$ είναι αντιμεταθετική ομάδα,
το $(A, \otimes)$ είναι μονοειδές, και
η πράξη $\otimes$ είναι επιμεριστική ως προς την $\oplus$.
Π.χ. $(\mathbb{Z}, +, *)$, (πίνακες $n \times n, +, *$).

Αν επιπλέον η πράξη $\otimes$ είναι αντιμεταθετική, τότε πρόκειται για αντιμεταθετικό δακτύλιο.

Ορ. Σώμα (**field, corps**) καλείται κάθε αντιμεταθετικός δακτύλιος όπου $\forall a \in A - \{\mathbf{0}\}$ υπάρχει συμμετρικό ως προς την $\otimes$. $\mathbf{0}$ είναι το ουδέτερο στοιχείο της $\oplus$.

Π.χ. $(\mathbb{Q}, +, *), (\mathbb{R}, +, *)$.

Διανυσματικός χώρος

Ορ. Διανυσματικός χώρος επί του σώματος $(A, \oplus, \otimes)$ καλείται κάθε αντιμεταθετική ομάδα $(X, \boxplus)$, όπου έχει οριστεί μια «πράξη»

$$A \times X \to X : (a, x) \mapsto ax,$$

τ.ώ. $\forall a, b \in A, x, y \in X$,

$$a(x \boxplus y) = ax \boxplus ay \quad (1)$$
$$a(bx) = (a \otimes b)x \quad (2)$$
$$(a \oplus b)x = ax \boxplus bx \quad (3)$$
$$1_A x = x \quad (4)$$

Παραδείγματα Διανυσματικών χώρων

Π.χ. $(\mathbb{R}^n, +)$ επί του $(\mathbb{R}, +, *)$.

Π.χ. $(\{$πολυώνυμα $c_0 + c_1 u + \cdots + c_n u^n$, βαθμού n στη μεταβλητή u, όπου $c_i \in \mathbb{R}\}, +)$ επί του $(\mathbb{R}, +, *)$.

Όχι: $(\mathbb{R}, +)$ επί του $(\mathbb{C}, +, *)$ αν σχετίσουμε τα δύο σύνολα με τη συνηθισμένο πολλαπλασιαμό πραγματικού επί μιγαδικό.

Επιπλέον Πράξεις Συνόλων [Liu, ενότ.1.2]

Πληθικοί αριθμοί [Liu, ενότ.1.3]

Διαφορές συνόλων

Διαφορά. $P - Q := \{p \in P : p \notin Q\}$, ή $P \setminus Q$.
Καλείται και συμπλήρωμα του Q ως προς P.
Για το σύμπαν (ή σύνολο αναφοράς) Ω, $\overline{A} := \Omega - A$.
Παρατήρηση. $A - \emptyset = A, A - A = \emptyset$.

Π.χ. $\{a, b\} - \{a, d\} = \{b\}, \{a, b\} - \{a, b, d\} = \emptyset$.

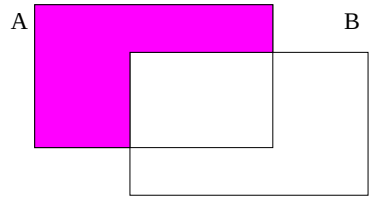
Συμμετρική διαφορά (**xor**). $P \oplus Q := \{p \in P \cup Q : p \notin P \cap Q\}$.
Αντιμεταθετικότητα. $P \oplus Q = Q \oplus P$.

Θεώρ. $P \oplus Q = (P \cup Q) - (P \cap Q) = (P - Q) \cup (Q - P)$.
Π.χ. $\{a, b\} \oplus \{a, d\} = \{b, d\}, \{a, b\} \oplus \{a, b, d\} = \{d\}$.

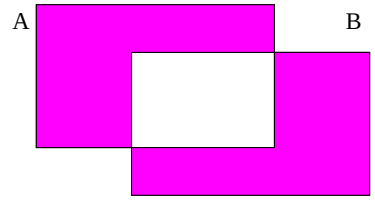
Επέκταση:
$P_1 \oplus \cdots \oplus P_k = \{p \in \bigcup_{i=1}^{k} P_i : p$ ανήκει σε περιττό πλήθος $P_i\}$.

Διαγράμματα **Venn** διαφορών

$A - B$



$A \oplus B$.



Δυναμοσύνολο

Ορ. $P(A) := \{B : B \subseteq A\} = 2^A$.

Π.χ. $P(\emptyset) = \{\emptyset\}$.
Π.χ. $P(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$.

Π.χ. $A = \{a, b, c\} \Rightarrow 2^A = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{c, b\}, \{a, c\}, A\}$.

Π.χ.
$$\begin{aligned} A &= \{1, 2, 3, 4\} \Rightarrow \\ \Rightarrow 2^A &= \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \\ &\quad \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}, \\ &\quad \{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}, A\}. \end{aligned}$$

Πληθικός αριθμός δυναμοσυνόλου

Θεώρημα. $|P(A)| = 2^{|A|}$.
Απόδειξη.
$\forall$ στοιχείο του $P(A)$ αντιστοιχεί σε μια επιλογή στοιχείων του A.
Κάθε επιλογή αντιστοιχεί σε μια συνάρτηση $A \to \{0, 1\}$.
Υπάρχουν $2^{|A|}$ διαφορετικές συναρτήσεις/απεικονίσεις. ΟΕΔ

Γιαυτό χρησιμοποιείται και ο συμβολισμός 2^A.

Πεπερασμένα σύνολα

Ορισμός. Το σύνολο A καλείται πεπερασμένο αν ο πληθικός του αριθμός είναι πεπερασμένος. Αλλιώς καλείται άπειρο.
Π.χ: πεπερασμένο: $\{c, b\}$, άπειρο: $\mathbb{Z}$.

Θεώρ. Το A είναι πεπερασμένο ανν $\exists N' \subseteq \mathbb{N}$ και $\exists$ 1-1 συνάρτηση $f : A \to N' : [\exists\, a \in \mathbb{N} : \forall n \in N',\ n \leq a]$.

Δηλαδή **(i)** υπάρχει 1-1 απεικόνιση από το A σε κάποιο N' και **(ii)** υπάρχει ένας συγκεκριμένος φυσικός a που είναι άνω φράγμα για όλα τα στοιχεία του N'.

Π.χ. $f : \{c, b\} \to \{1, 2, 3, 4\},\ a = 67$.

Γενικά, $a \geq |A|$.

Αριθμήσιμα σύνολα

Ορισμός. Το A είναι αριθμήσιμο αν $\exists$ 1-1 συνάρτηση $f : A \to \mathbb{N}$.
Π.χ. $\{$ περιττοί φυσικοί αριθμοί $\} \to \mathbb{N} : 2k + 1 \mapsto k \geq 0$.

Θεώρ. Το $\mathbb{Z}$ είναι αριθμήσιμο.
Απόδ.
$$f : \mathbb{Z} \to \mathbb{N} : \begin{cases} x \mapsto 2x, & \text{αν } x \geq 0, \\ x \mapsto -2x - 1, & \text{αν } x < 0 \end{cases}$$

Η f είναι συνάρτηση: μονοσήμαντη απεικόνιση στο $\mathbb{N}$.
Είναι 1-1: έστω $x \neq x'$:
- αν $x, x' \geq 0$, έστω $x > x' \Rightarrow 2x > 2x'$,
- αν $x, x' \leq 0$, έστω $x > x' \Rightarrow -2x - 1 < -2x' - 1$,
- αλλιώς $xx' < 0 \Rightarrow f(x), f(x')$ είναι άρτιος και περιττός.

Κατηγορίες συνόλων

Παρατήρ. A πεπερασμένο $\Rightarrow$ αριθμήσιμο.
Το αντίθετο δεν ισχύει, π.χ. $\mathbb{N}$.

Θεώρ. Υπάρχουν μη αριθμήσιμα (άπειρα) σύνολα, π.χ. $\mathbb{R}, [0,1]$.

Κατηγορίες:

- Πεπερασμένα αριθμήσιμα σύνολα, π.χ. $\{a,b\}, \emptyset$.
- Αριθμήσιμα απειροσύνολα, π.χ. $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ (πληθικός αριθμός $\aleph_0$).
- Μη αριθμήσιμα, π.χ. $(0,1), \mathbb{R}, \mathbb{R}^n$ (πληθικός αριθμός $2^{\aleph_0}$).

Υπόθεση του Συνεχούς [**Cantor**] Δεν υπάρχει σύνολο με πληθικό αριθμό ανάμεσα στον πληθικό αριθμό του $\mathbb{N}$ και του $\mathbb{R}$.

Μη αριθμήσιμο σύνολο

Θεωρ. Το $(0,1) \cap \mathbb{R}$ είναι μη αριθμήσιμο· ομοίως το $(0,1) - \mathbb{Q}$.

Απ. Διαγώνιο επιχείρημα (διαγωνιοποίηση), αναγωγή σε άτοπο.
Αριθμήσιμο $\Rightarrow$ τα στοιχεία του $(0,1)$ ταξινομούνται:

$$a_1 = 0, a_{11}a_{12}a_{13}\ldots$$
$$a_2 = 0, a_{21}a_{22}a_{23}\ldots$$
$$a_3 = 0, a_{31}a_{32}a_{33}\ldots$$
$$\vdots$$

χωρίς άπειρη ακολουθία $0: 0,15000\cdots = 0,14999\ldots$
(μπορούμε να εξαιρέσουμε τους ρητούς).

Μη αριθμήσιμο σύνολο

Θεωρ. Το $(0,1) \cap \mathbb{R}$ είναι μη αριθμήσιμο· ομοίως το $(0,1) - \mathbb{Q}$.

Απ. Διαγώνιο επιχείρημα (διαγωνιοποίηση), αναγωγή σε άτοπο.
Αριθμήσιμο $\Rightarrow$ τα στοιχεία του $(0,1)$ ταξινομούνται:

$$a_1 = 0, a_{11}a_{12}a_{13}\ldots$$
$$a_2 = 0, a_{21}a_{22}a_{23}\ldots$$
$$a_3 = 0, a_{31}a_{32}a_{33}\ldots$$
$$\vdots$$

χωρίς άπειρη ακολουθία $0: 0,15000\cdots = 0,14999\ldots$

Θέτω $b_i := \begin{cases} 1, & \text{αν } a_{ii} = 9, \\ 9 - a_{ii}, & \text{αν } a_{ii} \in \{0,1,2,\ldots,8\}. \end{cases} \Rightarrow b_i \neq a_{ii}$

$b := 0, b_1 b_2 b_3 \cdots \in (0,1)$ αλλά $b \neq a_i, \forall\, i$: άτοπο. ΟΕΔ

Επαγωγή [Liu, ενότ.1.5]

Μαθηματική επαγωγή

Μέθοδος απόδειξης μιας μαθηματικής πρότασης $\Pi(n)$, η οποία εξαρτάται από έναν φυσικό $n \in \mathbb{N}$.

Σκοπός είναι να δείξουμε πως η $\Pi(n)$ είναι αληθής, $\forall\, n \geq n_0 \in \mathbb{N}$.

2 στάδια:
- Βάση: δείχνουμε πως η $\Pi(n_0)$ είναι αληθής.
- Βήμα: δείχνουμε πως $\Pi(k) \Rightarrow \Pi(k+1)$, όπου $k \geq n_0$: η $\Pi(k)$ καλείται επαγωγική υπόθεση.

Ισχυρή επαγωγή:
- Βάση: δείχνουμε πως η $\Pi(n_0)$ είναι αληθής.
- Βήμα: δείχνουμε πως $[\Pi(i),\, i = n_0, \ldots, k] \Rightarrow \Pi(k+1)$.

Παράδειγμα επαγωγής

[**Liu**, άσκ. 1.33]. Για $a \neq 1$, $n \in \mathbb{N}$, δείξτε πως

$$\Pi(n) : 1 + a + \cdots + a^n = \frac{a^{n+1} - 1}{a - 1}.$$

Παράδειγμα επαγωγής

[**Liu**, άσκ. 1.33]. Για $a \neq 1$, $n \in \mathbb{N}$, δείξτε πως

$$\Pi(n) : 1 + a + \cdots + a^n = \frac{a^{n+1} - 1}{a - 1}.$$

Λύση.
- Επαγωγική βάση, $\Pi(0)$: $1 = (a-1)/(a-1)$: αληθής.
- Βήμα: $1 + \cdots + a^k + a^{k+1} = (a^{k+2} - 1)/(a-1) \Leftrightarrow$

$$\Leftrightarrow \frac{a^{k+1} - 1}{a - 1} + a^{k+1} = \frac{a^{k+2} - 1}{a - 1} \Leftrightarrow$$

$\Leftrightarrow a^{k+1} - 1 + a^{k+2} - a^{k+1} = a^{k+2} - 1$: αληθής. ΟΕΔ

Πληθικός αριθμός δυναμοσυνόλου

Θεώρημα. $|P(A)| = 2^{|A|}$.

Απόδειξη με επαγωγή ως προς $|A| = n \geq 0$.

Βάση επαγωγής: $|A_0| = 0 \Rightarrow A_0 = \emptyset \Rightarrow |2^{A_0}| = |\{\emptyset\}| = 1$.
$|A_1| = 1 \Rightarrow A_1 = \{a\} \Rightarrow |2^{A_1}| = |\{\emptyset, \{a\}\}| = 2$.

Πληθικός αριθμός δυναμοσυνόλου

Θεώρημα. $|P(A)| = 2^{|A|}$.

Απόδειξη με επαγωγή ως προς $|A| = n \geq 0$.

Βάση επαγωγής: $|A_0| = 0 \Rightarrow A_0 = \emptyset \Rightarrow |2^{A_0}| = |\{\emptyset\}| = 1$.
$|A_1| = 1 \Rightarrow A_1 = \{a\} \Rightarrow |2^{A_1}| = |\{\emptyset, \{a\}\}| = 2$.

Επαγωγικό βήμα: $A_k = A_{k-1} \cup \{a\}$, $|A_k| = k \geq 1$.
Κάθε υποσύνολο του A_k είτε περιέχει το a είτε όχι:

$$\begin{aligned} 2^{A_k} &= 2^{A_{k-1}} \cup \left(\bigcup_{B \subseteq A_{k-1}} \{B \cup \{a\}\}\right) \\ &= 2^{A_{k-1}} \cup \left(\bigcup_{B \in 2^{A_{k-1}}} \{B \cup \{a\}\}\right) \\ \Rightarrow \left|2^{A_k}\right| &= 2 \cdot \left|2^{A_{k-1}}\right| \\ &= 2 \cdot 2^{k-1} = 2^k. \end{aligned}$$

Παράδειγμα ισχυρής επαγωγής

[**Liu**, παράδ. 1.9]:
Κάθε φυσικός $n \geq 2$ είναι είτε πρώτος είτε γινόμενο πρώτων

Βάση: Ο $n = 2$ είναι πρώτος.

Επαγωγική υπόθεση: Η πρόταση ισχύει για $i = 2, \ldots, k$.

Επαγωγικό βήμα:

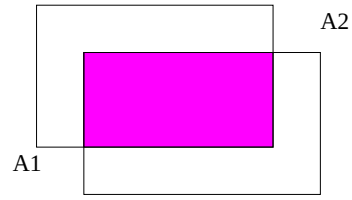
- Αν ο $k+1$ είναι πρώτος, η πρόταση αποδείχθηκε.
- Αλλιώς $\exists\, a, b : 1 < a, b < k+1$ και $k+1 = ab$.
  Υπόθεση $\Rightarrow$ οι a, b είναι είτε πρώτοι είτε γινόμενα πρώτων,

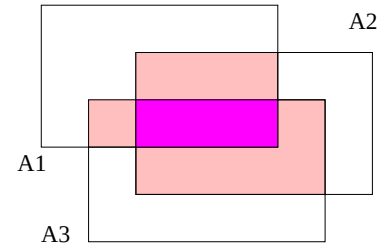
άρα κι ο $k+1$ είναι γινόμενο πρώτων. ΟΕΔ

Αρχή εγκλεισμού-αποκλεισμού [Liu, ενότ.1.6]

Μικρές περιπτώσεις

$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$.





$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_2 \cap A_3| - |A_3 \cap A_1| + |A_1 \cap A_2 \cap A_3|.$$

Απόδειξη για $n = 3$

- $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$.
- $n = 3$

$$\begin{aligned}
|A_1 \cup A_2 \cup A_3| &= |(A_1 \cup A_2) \cup A_3| \\
&= |A_1 \cup A_2| + |A_3| - |(A_1 \cup A_2) \cap A_3| \\
&= |A_1| + |A_2| - |A_1 \cap A_2| + |A_3| \\
&\quad -|(A_1 \cap A_3) \cup (A_2 \cap A_3)| \\
&= |A_1| + |A_2| + |A_3| \\
&\quad -|A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| \\
&\quad + \underbrace{|(A_1 \cap A_3) \cap (A_2 \cap A_3)|}_{|A_1 \cap A_2 \cap A_3|}
\end{aligned}$$

Αρχή εγκλεισμού/αποκλεισμού

$$\begin{aligned}
|A_1 \cup \cdots \cup A_n| &= |A_1| + \cdots + |A_n| \\
&\quad -|A_1 \cap A_2| - |A_1 \cap A_3| - \cdots - |A_{n-1} \cap A_n| \\
&\quad +|A_1 \cap A_2 \cap A_3| + \ldots \\
&\quad \vdots \\
&\quad -(-1)^k \textstyle\sum_{J \in 2^{[n]} \wedge |J| = k} |\cap_{j \in J} A_j| \\
&\quad -(-1)^n |A_1 \cap \cdots \cap A_n| = \\
&= \textstyle\sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \le i_1 < \cdots < i_k \le n} |A_{i_1} \cap \cdots \cap A_{i_k}|
\end{aligned}$$

Σημειώστε πως $J \subseteq [n] := \{1, \ldots, n\}$ & $|J| = k$.

Επαγωγική απόδειξη

Βάση $n = 2$.

Υπόθεση:
$|\bigcup_{i=1}^{n} A_i| = \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \le i_1 < \cdots < i_k \le n} |A_{i_1} \cap \cdots \cap A_{i_k}|$.

Βήμα: $|\bigcup_{i=1}^{n+1} A_i| = |(\bigcup_{i=1}^{n} A_i) \cup A_{n+1}| =$

$$= |\bigcup_{i=1}^{n} A_i| + |A_{n+1}| - |(\bigcup_{i=1}^{n} A_i) \cap A_{n+1}|,$$

εφαρμόζοντας τη βάση. Από επιμεριστικότητα και υπόθεση:

$$|\cdot| = |\bigcup_{i=1}^{n} (A_i \cap A_{n+1})| = \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \le j_1 < \cdots < j_k \le n} |A_{j_1} \cap \cdots \cap A_{j_k} \cap A_{n+1}$$

Παράδειγμα εγκλεισμού/αποκλεισμού

[Liu] 1.14. Πόσοι ακέραιοι $\in [1, 10]$ διαιρούνται από το 2 ή το 3;

$A_2 := \{n \in [1, 10] : 2|n\}, A_3 := \{n \in [1, 10] : 3|n\}$. $|A_2 \cup A_3| = ?$.

Παράδειγμα εγκλεισμού/αποκλεισμού

[Liu] 1.14. Πόσοι ακέραιοι $\in [1, 10]$ διαιρούνται από το 2 ή το 3;

$A_2 := \{n \in [1, 10] : 2|n\}, A_3 := \{n \in [1, 10] : 3|n\}$. $|A_2 \cup A_3| = ?$.

Λήμ.1. Τα πολλαπλάσια του $k \in \mathbb{N}$ στο $[1, M] \subset \mathbb{N}$:

$$|\{n \in [1, M] : k|n\}| = |\{p \geq 1 : pk \leq M\}| = |\{1 \leq p \leq \lfloor \frac{M}{k} \rfloor\}| = \left\lfloor \frac{M}{k} \right\rfloor.$$

Παράδειγμα εγκλεισμού/αποκλεισμού

[Liu] 1.14. Πόσοι ακέραιοι $\in [1, 10]$ διαιρούνται από το 2 ή το 3;

$A_2 := \{n \in [1, 10] : 2|n\}, A_3 := \{n \in [1, 10] : 3|n\}$. $|A_2 \cup A_3| = ?$.

Λήμ.1. Τα πολλαπλάσια του $k \in \mathbb{N}$ στο $[1, M] \subset \mathbb{N}$:

$$|\{n \in [1, M] : k|n\}| = |\{p \geq 1 : pk \leq M\}| = |\{1 \leq p \leq \lfloor \frac{M}{k} \rfloor\}| = \left\lfloor \frac{M}{k} \right\rfloor.$$

Λήμ.2. $2|n,\ 3|n \Leftrightarrow \text{ΕΚΠ}(2, 3)|n$.

Παράδειγμα εγκλεισμού/αποκλεισμού

[Liu] 1.14. Πόσοι ακέραιοι $\in [1, 10]$ διαιρούνται από το 2 ή το 3;

$A_2 := \{n \in [1, 10] : 2|n\}, A_3 := \{n \in [1, 10] : 3|n\}$. $|A_2 \cup A_3| = ?$.

Λήμ.1. Τα πολλαπλάσια του $k \in \mathbb{N}$ στο $[1, M] \subset \mathbb{N}$:

$$|\{n \in [1, M] : k|n\}| = |\{p \geq 1 : pk \leq M\}| = |\{1 \leq p \leq \lfloor \frac{M}{k} \rfloor\}| = \left\lfloor \frac{M}{k} \right\rfloor.$$

Λήμ.2. $2|n,\ 3|n \Leftrightarrow \text{ΕΚΠ}(2, 3)|n$.

Άρα $|A_2| = \lfloor 10/2 \rfloor = 5, |A_3| = \lfloor 10/3 \rfloor = 3$
και $|A_2 \cap A_3| = \lfloor 10/\text{ΕΚΠ}(2, 3) \rfloor = \lfloor 10/6 \rfloor = 1$.
Τελικά $|A_2 \cup A_3| = |A_2| + |A_3| - |A_2 \cap A_3| = 5 + 3 - 1 = 7$.

Παράδειγμα εγκλεισμού/αποκλεισμού

[Liu] 1.14. Πόσοι ακέραιοι $\in [1, 10]$ διαιρούνται από το 2 ή το 3;

$A_2 := \{n \in [1, 10] : 2|n\}, A_3 := \{n \in [1, 10] : 3|n\}$. $|A_2 \cup A_3| = ?$.

Λήμ.1. Τα πολλαπλάσια του $k \in \mathbb{N}$ στο $[1, M] \subset \mathbb{N}$:

$$|\{n \in [1, M] : k|n\}| = |\{p \geq 1 : pk \leq M\}| = |\{1 \leq p \leq \lfloor \frac{M}{k} \rfloor\}| = \left\lfloor \frac{M}{k} \right\rfloor.$$

Λήμ.2. $2|n,\ 3|n \Leftrightarrow \text{ΕΚΠ}(2, 3)|n$. (γιατί χρειάζεται η ισοδυναμία;)

Άρα $|A_2| = \lfloor 10/2 \rfloor = 5, |A_3| = \lfloor 10/3 \rfloor = 3$
και $|A_2 \cap A_3| = \lfloor 10/\text{ΕΚΠ}(2, 3) \rfloor = \lfloor 10/6 \rfloor = 1$.
Τελικά $|A_2 \cup A_3| = |A_2| + |A_3| - |A_2 \cap A_3| = 5 + 3 - 1 = 7$.

Άσκηση

[Liu] 1.62. 75 παιδιά πάνε σε λούνα-παρκ με παιχνίδια Α, Β, Γ:
20 παιδιά και στα 3 παιχνίδια, 55 τουλάχιστον σε 2 παιχνίδια.
$\forall$ παιχνίδι= 50 λεπτά / άτομο· συνολική είσπραξη = 70 ευρώ.
Πόσα παιδιά δεν πήγαν σε κανένα παιχνίδι;

Έστω A, B, Γ το σύνολο παιδιών στο παιχνίδι Α, Β ή Γ.
Ζητείται ο αριθμός $75 - |A \cup B \cup \Gamma|$. Γνωρίζουμε πως
$|A \cup B \cup \Gamma| = |A|+|B|+|\Gamma|-(|A \cap B|+|B \cap \Gamma|+|\Gamma \cap A|)+|A \cap B \cap \Gamma|$.

Άσκηση

[Liu] 1.62. 75 παιδιά πάνε σε λούνα-παρκ με παιχνίδια Α, Β, Γ:
20 παιδιά και στα 3 παιχνίδια, 55 τουλάχιστον σε 2 παιχνίδια.
$\forall$ παιχνίδι= 50 λεπτά / άτομο· συνολική είσπραξη = 70 ευρώ.
Πόσα παιδιά δεν πήγαν σε κανένα παιχνίδι;

Έστω A, B, Γ το σύνολο παιδιών στο παιχνίδι Α, Β ή Γ.
Ζητείται ο αριθμός $75 - |A \cup B \cup \Gamma|$. Γνωρίζουμε πως
$|A \cup B \cup \Gamma| = |A|+|B|+|\Gamma|-(|A \cap B|+|B \cap \Gamma|+|\Gamma \cap A|)+|A \cap B \cap \Gamma|$.

$|A| + |B| + |\Gamma| = 70/0,50 = 140,\ |A \cap B \cap \Gamma| = 20,$
και $55 = |A \cap B| + |B \cap \Gamma| + |\Gamma \cap A| - 2|A \cap B \cap \Gamma|.$

Άρα $|A \cup B \cup \Gamma| = 140 - (55 + 2 \cdot 20) + 20 = 65,$
συνεπώς 10 παιδιά δεν επισκέφτηκαν κανένα παιχνίδι.

Προτάσεις [Liu, ενότ.1.8]

Μαθηματικές / λογικές προτάσεις

Ορ. (Μαθηματική ή λογική) πρόταση είναι μια φράση η οποία είναι είτε αληθής είτε ψευδής, αλλά όχι και τα δύο.

Π.χ. Τώρα βρέχει.

Π.χ. Τα Διακριτά Μαθηματικά είναι μάθημα του πρώτου έτους.

Όχι: Τί ώρα γίνεται το μάθημα των διακριτών;

Όχι: Η ζωή είναι ωραία!

Είδη προτάσεων

Ορ. Ταυτολογία καλείται κάθε πρόταση που είναι πάντα αληθής (συμβολίζεται 1, Α ή Τ).

Ορ. Αντίφαση καλείται κάθε πρόταση που είναι πάντα ψευδής (συμβολίζεται 0, Ψ ή **F**).

Πράξεις και Πίνακες Αληθείας

- άρνηση της p: $\overline{p}$ ή $\neg p$,
- διάζευξη (ή): $p \bigvee q$ αληθής ανν μία ή 2 προτάσεις ισχύουν,
- αποκλειστική διάζευξη (είτε-είτε): $p \underline{\vee} q$ αληθής ανν ακριβώς μία αρχική πρόταση αληθεύει,
- σύζευξη (και): $p \bigwedge q$ αληθής ανν και οι 2 προτάσεις ισχύουν,
- ισοδυναμία: $p \leftrightarrow q$ είναι αληθής ανν οι δυο προτάσεις έχουν τους ίδιους πίνακες αληθείας,

p	q	$p \vee q$	$p \underline{\vee} q$	$p \wedge q$	$p \leftrightarrow q$
F	F	F	F	F	T
F	T	T	T	F	F
T	F	T	T	F	F
T	T	T	F	T	T

Συνεπαγωγή

Αν p τότε q: $p \to q$.

Π.χ. Αν κάποιος είναι επισκέπτης, τότε φοράει κονκάρδα.

p	q	$p \to q$
F	F	T
F	T	T
T	F	F
T	T	T

Π.χ. Αν αντιγράψεις από τον διπλανό σου, τότε μηδενίζεσαι.

Σύνθετες προτάσεις

Οι πράξεις επί ατομικών / απλών προτάσεων ορίζουν σύνθετες λογικές προτάσεις, π.χ. $(p \wedge q)$, $(p \to q)$.

Άσκ. Η σύνθετη πρόταση $(p \leftrightarrow q)$ είναι ισοδύναμη με την σύνθετη πρόταση $[(p \to q) \wedge (q \to p)]$.

Άσκ. Η $(p \leftrightarrow q)$ είναι άρνηση της $(p \underline{\vee} q)$.

Απόδ.

p	q	$p \leftrightarrow q$	$p \to q$	$q \to p$	$[\ldots \wedge \ldots]$	$p \underline{\vee} q$
F	F	T	T	T	T	F
F	T	F	T	F	F	T
T	F	F	F	T	F	T
T	T	T	T	T	T	F

ΟΕΔ

Σύνθετες προτάσεις

Άσκ. Αποδείξτε πως η σύνθετη πρόταση $(p \wedge q) \to (p \vee q)$ είναι ταυτολογία.

Επομένως η $\neg((p \wedge q) \to (p \vee q))$ είναι αντίφαση.

Αντιστοιχίες με πράξεις συνόλων

Θεωρείστε σύνολα που ορίζονται με περιγραφή των στοιχείων τους. Π.χ.

$$A = \{x : p(x)\}.$$

Δηλ. το A περιέχει όλα τα στοιχεία x που ικανοποιούν την ιδιότητα $p(x)$.

Το αποτέλεσμα πράξεων (όπως ένωση, τομή κτλ.) πάνω σε τέτοια σύνολα είναι σύνολο τα στοιχεία του οποίου ικανοποιούν μια λογική πράξη (όπως διάζευξη, σύζευξη κτλ.) των αντίστοιχων ιδιοτήτων.

Αντιστοιχίες με πράξεις συνόλων

$\neq$	$A = \{x : p(x)\}$	$\Leftrightarrow$	$\overline{A} = \{x : \neg p(x)\}$
$\wedge$	$\{x : x \geq 5\} \cap \{x : x < 6\}$	$=$	$\{x : x \geq 5 \wedge x < 6\}$
$\vee$	$\{x : p(x)\} \cup \{x : q(x)\}$	$=$	$\{x : p(x) \vee q(x)\}$
$\underline{\vee}$	$\{x : p(x)\} \oplus \{x : q(x)\}$	$=$	$\{x : p(x) \underline{\vee} q(x)\}$
$\leftrightarrow$	$\{x : p(x)\} = \{x : q(x)\}$	$\Leftrightarrow$	$(p(x) \leftrightarrow q(x))$
$\to$	$\{x : p(x)\} \subseteq \{x : q(x)\}$	$\Leftrightarrow$	$(p(x) \to q(x))$
Απ.	$\{x : p(x)\} \subseteq \{x : q(x)\}$	τότε	$p(x) \to q(x)$
	$\{x : p(x)\} \not\subseteq \{x : q(x)\}$	τότε	$\exists x : p(x)$ αληθής, $q(x)$ ψευδής.

Ιδιότητες **De Morgan**

Να δειχτεί ότι:

- $\overline{p \wedge q} \leftrightarrow \overline{p} \vee \overline{q}$,
- $\overline{p \vee q} \leftrightarrow \overline{p} \wedge \overline{q}$.

Απόδ.

Πίνακες Αληθείας

p	q	$p \wedge q$	$\overline{p} \vee \overline{q}$	$p \vee q$	$\overline{p} \wedge \overline{q}$
0	**0**	**0**	**1**	**0**	**1**
0	**1**	**0**	**1**	**1**	**0**
1	**0**	**0**	**1**	**1**	**0**
1	**1**	**1**	**0**	**1**	**0**

ΟΕΔ

Παράδειγμα

[Liu] σελ.38. Ndó $p \vee q \leftrightarrow (((p \wedge q) \vee (\neg p \wedge \neg q)) \rightarrow p)$.

Απόδ.

p	q	$p \vee q$	$p \wedge q$	$(\neg p \wedge \neg q)$	$\bigvee$	$\bigvee \rightarrow p$
0	**0**	**0**	**0**	**1**	**1**	**0**
0	**1**	**1**	**0**	**0**	**0**	**1**
1	**0**	**1**	**0**	**0**	**0**	**1**
1	**1**	**1**	**1**	**0**	**1**	**1**

ΟΕΔ

Παράδειγμα

[Liu] 1.16. 2 φυλές: η μία λέει πάντα αλήθεια, η άλλη ποτέ.
Ερώτηση: Υπάρχει χρυσός στο νησί;
Απάντηση ιθαγενούς Ι: «Υπάρχει ανν λέω την αλήθεια».

Λύση. Πρόταση A: ο Ι λέει αλήθεια, πρόταση X: ∃ χρυσός.
Δηλ. ο ιθαγενής μας απάντησε «$A \leftrightarrow X$».

A	X	απάντηση $A \leftrightarrow X$	$A \leftrightarrow (A \leftrightarrow X)$
0	0	1	0
0	1	0	1
1	0	0	0
1	1	1	1

Παράδειγμα

[Liu] 1.16. 2 φυλές: η μία λέει πάντα αλήθεια, η άλλη ποτέ.
Ερώτηση: Υπάρχει χρυσός στο νησί;
Απάντηση ιθαγενούς Ι: «Υπάρχει ανν λέω την αλήθεια».

Λύση. Πρόταση A: ο Ι λέει αλήθεια, πρόταση X: ∃ χρυσός.
Δηλ. ο ιθαγενής μας απάντησε «$A \leftrightarrow X$».

A	X	απάντηση $A \leftrightarrow X$	$A \leftrightarrow (A \leftrightarrow X)$
0	0	1	0
0	1	0	1
1	0	0	0
1	1	1	1

Η πρόταση $A \leftrightarrow (A \leftrightarrow X)$ αληθεύει (γιατί;;). Επομένως υπάρχει χρυσός.

Παράδειγμα (συνέχεια)

Πειστήκαμε πως η πρόταση $A \leftrightarrow (A \leftrightarrow X)$ αληθεύει.

Το συμπέρασμα μας πως υπάρχει χρυσός προκύπτει από τον πίνακα αλήθειας.

	A	X	απάντηση $A \leftrightarrow X$	$A \leftrightarrow (A \leftrightarrow X)$	
	0	0	1	0	
▶	0	1	0	1	◀
	1	0	0	0	
▶	1	1	1	1	◀

Το Παράδοξο του **Russell**

Π.χ. Έστω S το σύνολο όλων των συνόλων που δεν ανήκουν στον εαυτό τους. Δηλ. $S = \{x \mid x \notin x\}$.
Το S ανήκει στον εαυτό του; Είτε απαντήσουμε ναι, είτε όχι καταλήγουμε σε αντίφαση.
Άρα το S δεν μπορεί να υπάρχει.

Συμπεραίνουμε πως ό,τι περιγράφουμε με λόγια δεν υφίσταται απαραίτητα ως μαθηματικό αντικείμενο. Ο απλοϊκός ορισμός «σύνολο είναι μια οποιαδήποτε συλλογή αντικειμένων με κάποια κοινή ιδιότητα» είναι επαρκής για το μάθημα μας αλλά όχι γενικότερα.

Στην αξιωματική θεωρία συνόλων **Zermelo-Fraenkel** ένα τέτοιο S δεν μπορεί να οριστεί.

Απόδειξη

Απόδειξη μιας (μαθηματικής) πρότασης P καλείται η τεκμηρίωση της αλήθειας της P.

Μια απόδειξη στηρίζεται σε υποθέσεις Y και χρησιμοποιεί λογικούς συλλογισμούς για να καταδείξει την ισχύ τής P, δηλ. πρόκειται για την τεκμηρίωση της συνεπαγωγής $Y \to P$,

- ευθέως με: $Y \to E \to P$, ή με $P \leftrightarrow Q$, $Y \to Q$.
- επαγωγικά, εφόσον η $P(n)$ είναι συνάρτηση του $n \in \mathbb{N}$.
- με απαγωγή σε άτοπο: $\neg P \to \neg Y$:

Y	P	$Y \to P$	$\neg P \to \neg Y$
0	0	1	1
0	1	1	1
1	0	0	0
1	1	1	1

Απαγωγή σε άτοπο

Έστω θέλουμε να αποδείξουμε ένα θεώρημα της μορφής $Y \to P$. Αρκεί να δείξουμε πως αληθεύει η αντιθετοαντίστροφη πρόταση $\neg P \to \neg Y$.

Γιατί δουλεύει αυτό; Όταν η η υπόθεση Y ψευδής, το θεώρημα ισχύει ούτως ή άλλως. Όταν η υπόθεση Y αληθής, τότε $\neg Y$ ψευδής.

Άρα δείξαμε πως αληθεύει η συνεπαγωγή $\neg P \to$ **False**. Αυτό σημαίνει πως $\neg P$ ψευδής και άρα P αληθής.

Παράδειγμα: Αποδείξτε πως αν ο $3n + 2$ είναι περιττός, τότε ο n είναι περιττός.

Απαγωγή σε άτοπο II

Έστω θέλουμε να αποδείξουμε ένα θεώρημα της μορφής P. Αρκεί να δείξουμε πως αληθεύει η συνεπαγωγή $\neg P \to R$ όπου R μια αντίφαση, δηλ. μια πρόταση που είναι πάντα ψευδής (π.χ. η $r \wedge \neg r$).

Γιατί δουλεύει αυτό; Δείξαμε πως αληθεύει η συνεπαγωγή $\neg P \to$ **False**. Αυτό σημαίνει πως $\neg P$ ψευδής και άρα P αληθής.

Παράδειγμα: Η απόδειξη με διαγωνιοποίηση ότι το $(0, 1)$ δεν είναι αριθμήσιμο.

Προτάσεις με ποσοδείκτες

Υπαρξιακή πρόταση: $\exists\, x$: αν $Y(x)$ ισχύει, τότε ισχύει $P(x)$.

- Αποδεικνύεται αν βρεθεί $x = a : Y(a) \to P(a)$.
  Π.χ. «$\exists\, x : x \notin \mathbb{Q}$» ισχύει για $x = \pi$.
- Καταρρίπτεται αν $\forall x : Y(x)$ ισχύει, η $P(x)$ δεν ισχύει.
  Άρνηση είναι η καθολική «$\forall x : Y(x)$ ισχύει, ισχύει $\neg P(x)$»

Καθολική πρόταση: $\forall\, x$: αν $Y(x)$ ισχύει, τότε ισχύει $P(x)$.

- Αποδεικνύεται αν δειχθεί $Y \to P$.
- Καταρρίπτεται με αντιπαράδειγμα $x = a : Y(a) =$T, $P(a) =$**F**
  Π.χ. «$\forall n \in \mathbb{N}$, ο $n! + 1$ πρώτος» ψευδής: $n = 4$, $4! + 1 = 25$.
  Η άρνηση είναι η υπαρξιακή πρόταση: $\exists x : Y(x)$ και $\neg P(x)$.

Περισσότεροι ποσοδείκτες

Αν μια πρόταση περιέχει ποσοδείκτες και των δύο ειδών, τότε η σειρά τους έχει σημασία.

Π.χ. Έστω $x, y, z \in \mathbb{R}$.
$\forall x, \exists y, z : x = y + z$ αληθής, διότι $z = x - y$.
$\exists y, z : \forall x, x = y + z$ ψευδής, διότι $\forall y, z$, $\exists x = y + z + 1 \neq y + z$

Π.χ. $\forall n \in \mathbb{N}^*, \exists$ πρώτος p, τ.ώ. $n < p \leq n! + 1$.

Απόδ. Αν ο $n! + 1$ είναι πρώτος, η απόδειξη έληξε με $p = n! + 1$.
Αλλιώς, $\exists$ πρώτος $q \,|\, n! + 1$, $2 \leq q < n! + 1$.
Εάν $2 \leq q \leq n$ τότε $q \,|\, n!$, $q \,|\, n! + 1$: άτοπο.
Άρα $q > n$ οπότε θέτω $p = q$. ΟΕΔ

Ψευδές: $\exists$ πρώτος $p : \forall n \in \mathbb{N}^*$, $n < p \leq n! + 1$.