ΠΑΡΑΡΤΗΜΑ

Α ΜΑΘΗΜΑΤΙΚΟ ΥΠΟΒΑΘΡΟ

Α.0. Σύνολα

Μια οποιαδήποτε συλλογή αντικειμένων λέγεται[*] ότι είναι ένα ***σύνολο*** και τα αντικείμενα λέγονται ***στοιχεία*** του συνόλου. Αν με A συμβολίσουμε ένα σύνολο και α είναι ένα αντικείμενο τότε αν το α είναι στοιχείο του A λέμε ότι το *α ανήκει στο A*, συμβολικά $\alpha \in A$, ενώ αν το α δεν είναι στοιχείο του A λέμε ότι το *α δεν ανήκει στο A*, συμβολικά $\alpha \notin A$. Ένα σύνολο πρέπει πάντα να είναι *καλώς ορισμένο*, δηλ. πρέπει πάντα να είναι δυνατός ο προσδιορισμός του αν ένα δοσμένο αντικείμενο ανήκει ή δεν ανήκει στο συγκεκριμένο σύνολο. Ένα σύνολο δίνεται είτε δια περιγραφής, είτε δια αναγραφής των στοιχείων του. Και στις δύο περιπτώσεις χρησιμοποιούμε τις { } για να περικλείουν τις προτάσεις που περιγράφουν τα στοιχεία του συνόλου είτε τα ίδια τα αναγραφόμενα στοιχεία του. Για παράδειγμα,

$A = \{x : x \in \boldsymbol{N}, x \leq 5\}$

$A = \{0, 1, 2, 3, 4, 5\}$

είναι δυο ισοδύναμοι τρόποι να δοθεί το σύνολο με στοιχεία τους αριθμούς 0, 1, 2, 3, 4 και 5. Χρησιμοποιήσαμε το σύμβολο $\boldsymbol{N}$ για το σύνολο των φυσικών αριθμών, δηλ. για το σύνολο {0, 1, 2, …}. Άλλα σύμβολα που χρησιμοποιούνται συχνά είναι:

$\boldsymbol{R}$ για το σύνολο των πραγματικών αριθμών

$\boldsymbol{Z}$ για το σύνολο των ακεραίων, δηλ. για το σύνολο {…, -2, -1, 0, 1, 2, …}

$\boldsymbol{Q}$ για το σύνολο των ρητών

Το σύνολο A λέγεται ***υποσύνολο*** του B, συμβολικά $A \subseteq B$, αν και μόνον αν, κάθε στοιχείο του A είναι στοιχείο του B. Γράφουμε:

---

[*] Οι λέξεις ***σύνολο*** και ***στοιχείο*** είναι οι θεμελιακοί όροι (δεν ορίζονται) της Θεωρίας Συνόλων, όπως είναι και οι λέξεις ***πρόταση***, ***αληθής*** και ***ψευδής*** της Λογικής.

- $A \subseteq B \Leftrightarrow \forall x,$ αν $x \in A$ τότε $x \in B$.

Από τον παραπάνω ορισμό συνεπάγεται ότι ένα σύνολο A δεν είναι υποσύνολο του B, συμβολικά $A \not\subset B$, αν και μόνον αν υπάρχει ένα τουλάχιστον στοιχείο του A που δεν είναι στοιχείο του B. Επίσης εύκολα διαπιστώνουμε ότι για τη σχέση του υποσυνόλου ισχύει η μεταβατική ιδιότητα

- αν $A \subseteq B$ και $B \subseteq \Gamma$, τότε $A \subseteq \Gamma$.

Το σύνολο Α λέγεται ***γνήσιο υποσύνολο*** του Β, συμβολικά Α ⊂ Β, αν και μόνον αν, κάθε στοιχείο του Α είναι στοιχείο του Β αλλά υπάρχει ένα τουλάχιστον στοιχείο του Β που δεν είναι στοιχείο του Α.

Τα σύνολα Α, Β λέγονται ***ίσα***, συμβολικά Α = Β, αν και μόνον αν, κάθε στοιχείο του Α είναι στοιχείο του Β και κάθε στοιχείο του Β είναι στοιχείο του Α. Έτσι έχουμε

- Α = Β $\Leftrightarrow$ Α ⊆ Β και Β ⊆ Α.

Το σύνολο Ω με τα υποσύνολα του οποίου ασχολούμαστε, λέγεται ότι είναι το ***σύνολο αναφοράς*** ή ***καθολικό σύνολο***. Το μοναδικό υποσύνολο του Ω που δεν έχει στοιχεία λέγεται ότι είναι το ***κενό σύνολο*** $\varnothing$ και αποδεικνύεται ότι είναι υποσύνολο κάθε άλλου συνόλου.

Το ***δυναμοσύνολο*** $\wp(A)$ ενός συνόλου A, είναι το σύνολο όλων των υποσυνόλων του A. Για παράδειγμα, αν $A = \{\alpha, \beta\}$ τότε, $\wp(A) = \{\varnothing, \{\alpha\}, \{\beta\}, \{\alpha, \beta\}\}$. Για το δυναμοσύνολο αποδεικνύεται ότι ισχύουν τα παρακάτω:

- Αν $A \subseteq B$ τότε, $\wp(A) \subseteq \wp(B)$.
- Για όλους τους ακέραιους $n \geq 0$, αν ένα σύνολο Α έχει n στοιχεία τότε το $\wp(A)$ έχει 2^n στοιχεία.

Θεωρώντας το σύνολο A υποσύνολο του συνόλου αναφοράς Ω, το ***συμπλήρωμα*** του A, συμβολικά $\boldsymbol{A^c}$, είναι το σύνολο όλων των στοιχείων του Ω που **δεν** είναι στοιχεία του A. Δηλαδή,

- $A^c = \{x \in \Omega : x \notin A\}$

Έστω τώρα A και B δύο υποσύνολα του συνόλου αναφοράς Ω. Η ***ένωση*** των A και B, συμβολικά $\boldsymbol{A \cup B}$, είναι το σύνολο όλων των στοιχείων του Ω που είναι στοιχεία του A **ή** του B. Δηλαδή,

- $A \cup B = \{x \in \Omega : x \in A$ ή $x \in B\}$

Για την ένωση συνόλων ισχύουν οι ιδιότητες:

Ι.1 $A \cup A = A$ (*ανακλαστική*)
Ι.2 $A \cup B = B \cup A$ (*αντιμεταθετική*)
Ι.3 $A \cup (B \cup \Gamma) = (A \cup B) \cup \Gamma$ (*προσεταιριστική*)

Η ***τομή*** των A και B, συμβολικά $\boldsymbol{A \cap B}$, είναι το σύνολο όλων των στοιχείων του Ω που είναι στοιχεία του A **και** του B. Δηλαδή,

- $A \cap B = \{x \in \Omega : x \in A \text{ και } x \in B\}$

Δύο σύνολα λέγονται ξένα, αν και μόνον αν, δεν έχουν κοινά στοιχεία. Έτσι

- Α και Β είναι ξένα $\Leftrightarrow$ $A \cap B = \varnothing$.

Για την τομή συνόλων ισχύουν οι ιδιότητες:

I.4 $A \cap A = A$ (*ανακλαστική*)
I.5 $A \cap B = B \cap A$ (*αντιμεταθετική*)
I.6 $A \cap (B \cap \Gamma) = (A \cap B) \cap \Gamma$ (*προσεταιριστική*)

Επίσης ισχύουν οι ακόλουθες δύο ιδιότητες για την ένωση σε σχέση με την τομή:

I.7 $A \cup (B \cap \Gamma) = (A \cup B) \cap (A \cup \Gamma)$
I.8 $A \cap (B \cup \Gamma) = (A \cap B) \cup (A \cap \Gamma)$

Η ***διαφορά*** $\boldsymbol{A - B}$, είναι το σύνολο όλων των στοιχείων του Ω που είναι στοιχεία του A **και** δεν είναι στοιχεία του B. Δηλαδή,

- $A - B = \{x \in \Omega : x \in A \text{ και } x \notin B\} = A \cap B^c$

Αποδεικνύεται τέλος ότι ισχύουν οι ακόλουθες δύο σημαντικές ιδιότητες, γνωστές ως ***νόμοι de Morgan***

- $(A \cup B)^c = A^c \cap B^c$
- $(A \cap B)^c = A^c \cup B^c$

Ας υποθέσουμε τώρα, ότι σε κάθε στοιχείο i ενός συνόλου I αντιστοιχεί ένα σύνολο A_i. Τότε λέμε ότι έχουμε μια συλλογή ή οικογένεια συνόλων με δείκτες από το σύνολο I και γράφουμε $(A_i)_{i \in I}$. Μπορούμε να γενικεύσουμε τις πράξεις της ένωσης και της τομής δύο συνόλων, για οικογένειες συνόλων. Έτσι, η ένωση των συνόλων μιας οικογένειας $(A_i)_{i \in I}$ είναι το σύνολο των στοιχείων που ανήκουν σ' ένα τουλάχιστον από τα σύνολα A_i

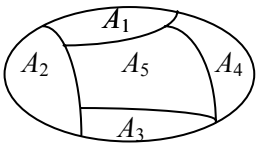
$$\bigcup_{i \in I} A_i = \{x: x \in A_i, \text{ για κάποιο } i \in I\}$$

Ανάλογα, η τομή των συνόλων μιας οικογένειας $(A_i)_{i \in I}$ είναι το σύνολο των στοιχείων που ανήκουν ταυτόχρονα σ' όλα τα σύνολα A_i

$$\bigcap_{i \in I} A_i = \{x: x \in A_i, \text{ για κάθε } i \in I\}.$$

Ονομάζουμε ***διαμέριση*** (ή ***διαμελισμό***) συνόλου A στα μη κενά υποσύνολα $A_1, A_2, \ldots, A_m$ την οικογένεια $(A_i)_{i\in I}$ με $I = \{1, 2, \ldots, m\}$, αυτών των συνόλων, αν και μόνον αν,

- $i \neq j \Rightarrow A_i \cap A_j = \varnothing$,
- $\bigcup_{i\in I} A_i = A$.



Για παράδειγμα, αν $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, η συλλογή των συνόλων A_1, A_2, A_3, A_4, A_5, με $A_1 = \{1, 2\}$, $A_2 = \{3, 4\}$, $A_3 = \{5, 6\}$, $A_4 = \{7\}$, $A_5 = \{8, 9, 10\}$ είναι μια διαμέρισή του.

Το ***καρτεσιανό γινόμενο*** των μη κενών συνόλων A και B είναι το σύνολο,

- $A\times B = \{(\alpha, \beta): \alpha\in A \text{ και } \beta\in B\}$

με τα στοιχεία του (α, β) να λέγονται διατεταγμένα ζεύγη ή διατεταγμένες 2-άδες ορίζοντας:

- $(\alpha, \beta) = (\gamma, \delta) \Leftrightarrow \alpha = \gamma \text{ και } \beta = \delta$

Ο παραπάνω ορισμός γενικεύεται και για περισσότερα από δύο σύνολα :

- $A_1\times A_2\times\ldots\times A_n = \{(\alpha_1, \alpha_2, \ldots, \alpha_n): \alpha_1\in A_1 \text{ και } \alpha_2\in A_2 \text{ και } \ldots \text{ και } \alpha_n\in A_n\}$

όπου, για την ισότητα των ***διατεταγμένων n-άδων*** έχουμε :

- $(\alpha_1, \alpha_2, \ldots, \alpha_n) = (\beta_1, \beta_2, \ldots, \beta_n) \Leftrightarrow \alpha_1 = \beta_1 \text{ και } \alpha_2 = \beta_2 \text{ και } \ldots \text{ και } \alpha_n = \beta_n$

Τα $\alpha_1, \alpha_2, \ldots, \alpha_n$ τα λέμε η 1^{η}, η 2^{η}, …, η n^{η} ***συνιστώσα*** της διατεταγμένης n-άδας. Τέλος, αν $A_1 = A_2 = \ldots = A_n = A$ τότε το $A_1\times A_2\times\ldots\times A_n$ το συμβολίζουμε με A^n, δηλαδή

- $A^n = \{(\alpha_1, \alpha_2, \ldots, \alpha_n): \alpha_i \in A_i, i = 1, 2, \ldots, n\}$

Β.0. Συναρτήσεις

Αν A και B είναι δύο σύνολα, μια ***απεικόνιση*** ή ***συνάρτηση*** f από το A στο B, συμβολικά $f: A \to B$, είναι ένα υποσύνολο του $A\times B$ τ.ώ. για όλα τα $x \in A$, υπάρχει ένα μόνον $y\in B$ με $(x, y)\in f$. Δηλαδή

$$\forall x\in A \Rightarrow \exists y[y\in B \wedge (x, y)\in f]]$$

και

$$[(x, y_1)\in f \wedge (x, y_2)\in f] \Rightarrow y_1 = y_2$$

Λέμε ότι

- A είναι το σύνολο αφετηρίας ή πεδίο ορισμού (π.ο.) (domain)
- B είναι το σύνολο αφίξεως (σ. α.) (codomain)

και αν $(x, y) \in f$, γράφουμε $y = f(x)$ επειδή το y προσδιορίζεται μονοσήμαντα από την επιλογή του x. Η f αντιστοιχεί σε κάθε $x \in A$ ένα και μόνο ένα $y \in B$. Κανένα στοιχείο του A δεν αντιστοιχίζεται σε δύο διαφορετικά στοιχεία του B, αλλά το ίδιο στοιχείο του B μπορεί να αντιστοιχεί σε δύο διαφορετικά στοιχεία του A. Δηλαδή, $\forall x_1, x_2 \in A\ [f(x_1) \neq f(x_2) \Rightarrow x_1 \neq x_2]$. Για παράδειγμα, η

$$f = \{(x, y) : x, y \in \boldsymbol{N} \wedge y = x \bmod 2\}$$

είναι μια συνάρτηση f: $\boldsymbol{N} \rightarrow \{0, 1\}$, επειδή για κάθε φυσικό αριθμό x υπάρχει μια μόνο τιμή y στο $\{0, 1\}$τέτοια ώστε $y = x \bmod 2$, σύμφωνα με τον ορισμό της συνάρτησης mod (βλ. § 2.1). Αντίθετα η

$$g = \{(x, y) : x, y \in \boldsymbol{N} \wedge x + y = \text{περιττός}\}$$

δεν είναι συνάρτηση, επειδή $(1, 2) \in g$ και $(1, 4) \in g$ οπότε για την επιλογή $x = 1$ δεν υπάρχει ένα μόνον y τ. ώ. $(x, y) \in g$.

Δοθείσης μιας συνάρτησης f: $A \rightarrow B$, αν $f(x) = y$, τότε λέμε ότι

- το y είναι η ***εικόνα*** (image) του x μέσω της f
- το x είναι το ***αρχέτυπο*** (preimage) του y

ή ότι

- το x είναι το ***όρισμα*** (argument) της f
- το y είναι η ***τιμή*** (value) της f στο x

Μπορούμε να ορίσουμε μια συνάρτηση καθορίζοντας την τιμή της για κάθε στοιχείο του πεδίου ορισμού της. Για παράδειγμα, θα μπορούσαμε να ορίσουμε $f(n) = 2n + 1$ για $n \in \boldsymbol{N}$, που σημαίνει $\mathrm{f} = \{(n, 2\mathrm{n} + 1) : n \in \boldsymbol{N}\}$.

Δύο συναρτήσεις f και g είναι ***ίσες*** αν έχουν το ίδιο π.ο., το ίδιο σ.α. και αν για όλα τα x του κοινού π.ο., $f(x) = g(x)$.

Ο ***περιορισμός*** μιας συνάρτησης f: $A \rightarrow B$ σε ένα υποσύνολο E του A είναι η συνάρτηση f_r: $E \rightarrow B$ με $f_r(x) = f(x)$, $\forall x \in E$.

Όταν το π.ο. μιας συνάρτησης f είναι ένα Καρτεσιανό γινόμενο, δηλαδή έχουμε f: $A_1 \times A_2 \times \ldots \times A_n \rightarrow B$, συνήθως γράφουμε $y = f(x_1, x_2, \ldots x_n)$ αντί για $y = f((x_1, x_2, \ldots x_n))$ και καλούμε κάθε x_i ένα όρισμα της συνάρτησης f, αν και για την ακρίβεια το μοναδικό όρισμα της f είναι η διατεταγμένη n-άδα $(x_1, x_2, \ldots x_n)$.

Δύο χαρακτηριστικά παραδείγματα συναρτήσεων είναι τα ακόλουθα:

– Η συνάρτηση ***μεγαλύτερος ακέραιος*** ή ***ακέραιο μέρος***, συμβολικά $f(x) = \lfloor x \rfloor$, αντιστοιχεί στον πραγματικό αριθμό x τον μεγαλύτερο ακέραιο που δεν υπερβαίνει τον x.

– Η συνάρτηση ***μικρότερος ακέραιος***, συμβολικά $f(x) = \lceil x \rceil$, αντιστοιχεί στον x τον μικρότερο ακέραιο που δεν είναι μικρότερος από τον x.

Έτσι,

$$\lfloor 3.5 \rfloor = 3,\ \lceil 3.5 \rceil = 4.$$

Χρήσιμες ιδιότητες για τις συναρτήσεις αυτές είναι οι ακόλουθες:

$$\lfloor x \rfloor = n \ \text{ανν}\ n \le x < n + 1,\ n \in \boldsymbol{Z}$$

$$\lceil x \rceil = n \ \text{ανν}\ n - 1 < x \le n,\ n \in \boldsymbol{Z}$$

$$\lfloor x \rfloor = n \ \text{ανν}\ x - 1 < n \le x,\ n \in \boldsymbol{Z}$$

$$\lceil x \rceil = n \ \text{ανν}\ x \le n < x + 1,\ n \in \boldsymbol{Z}$$

$$x - 1 < \lfloor x \rfloor \le x \le \lceil x \rceil < x + 1$$

$$\lfloor -x \rfloor = -\lceil x \rceil$$

$$\lceil -x \rceil = -\lfloor x \rfloor$$

$$\lfloor x + m \rfloor = \lfloor x \rfloor + m,\ m \in \boldsymbol{Z}$$

$$\lceil x + m \rceil = \lceil x \rceil + m,\ m \in \boldsymbol{Z}$$

Μια συνάρτηση με π.ο. το σύνολο $\boldsymbol{N}$ των φυσικών αριθμών και σ.α το σύνολο E είναι μια ***ακολουθία*** στοιχείων του E. Μια ***πεπερασμένη ακολουθία*** μήκους n είναι μια συνάρτηση με π.ο. το σύνολο των n ακεραίων $\{0, 1, 2, \ldots, n - 1\}$. Συχνά σημειώνουμε μια πεπερασμένη ακολουθία παραθέτοντας τις τιμές της: $\langle f(0), f(1), \ldots, f(n - 1)\rangle$.

Ένα ***στρινγκ*** (string) επί ενός πεπερασμένου συνόλου E είναι μια ακολουθία στοιχείων του E. Μερικές φορές καλούμε ***k-στρινγκ*** ένα στρινγκ μήκους k. Ένα ***υποστρινγκ*** h' ενός στρινγκ h είναι μια διατεταγμένη ακολουθία διαδοχικών στοιχείων του h και ένα k-υποστρινγκ ενός στρινγκ είναι ένα υποστρινγκ μήκους k. Για παράδειγμα, 110 είναι ένα 3-υποστρινγκ του δυαδικού στρινγκ 01101000, ενώ το 111 όχι.

Το ***σύνολο τιμών*** (range) της f: $A \to B$ είναι το σύνολο όλων των εικόνων των στοιχείων του A, συμβολικά $f(A)$, και είναι $f(A) \subseteq B$. Για παράδειγμα, το σύνολο τιμών της συνάρτησης f: $\boldsymbol{N} \to \boldsymbol{N}$ η οποία ορίζεται από την $f(n) = 2n + 1$ είναι $f(\boldsymbol{N}) = \{k : k = 2n + 1$ για κάποιο $n \in \boldsymbol{N}\}$. Αν $\Gamma \subseteq A$ τότε η ***εικόνα*** του Γ μέσω της f ορίζεται ως το σύνολο

$$f(\Gamma) = \{y \in B : y = f(\alpha) \text{ για κάποιο } \alpha \in \Gamma\}.$$

Αν κάθε στοιχείο του B είναι μια εικόνα στοιχείου του A, δηλαδή αν $f(A) = B$, τότε λέμε ότι η f είναι μια συνάρτηση ή απεικόνιση του A ***επί*** (onto) του B ή ότι είναι

μια ***επιρριπτική*** (surjective) συνάρτηση του A στο B ή απλά μια ***επίρριψη*** (surjection). Αυτό σημαίνει ότι για κάθε y από το Β πρέπει να υπάρχει x στο A τέτοιο ώστε $f(x) = y$. Για παράδειγμα, η συνάρτηση με τύπο $f(n) = \lfloor n \rfloor$ είναι μια συνάρτηση του $\boldsymbol{N}$ επί του $\boldsymbol{N}$, επειδή κάθε φυσικός αριθμός είναι το ακέραιο μέρος του εαυτού του. Αντίθετα, η συνάρτηση με τύπο $f(n) = 2n + 1$ δεν είναι μια συνάρτηση του $\boldsymbol{N}$ επί του $\boldsymbol{N}$, επειδή δεν υπάρχει όρισμα στην f που να παράγει τιμή 2. Η συνάρτηση όμως αυτή, είναι μια συνάρτηση του $\boldsymbol{N}$ επί του συνόλου των περιττών αριθμών.

Μια συνάρτηση f: $A \rightarrow B$, λέγεται ***συνάρτηση ένα προς ένα (1 – 1)*** ή ***ένριψη*** (*injection*) αν οι εικόνες διαφορετικών στοιχείων του A είναι διαφορετικά στοιχεία του B. Δηλαδή, $\forall x_1,x_2 \in A\ [x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)]$, ή ισοδύναμα, $\forall x_1,x_2 \in A\ [f(x_1) = f(x_2) \Leftrightarrow x_1 = x_2]$. Για παράδειγμα, η συνάρτηση με τύπο $f(n) = 2n$ είναι μια συνάρτηση 1 – 1 από το $\boldsymbol{N}$ στο $\boldsymbol{N}$ επειδή κάθε άρτιος αριθμός m είναι η εικόνα μέσω της f ενός το πολύ στοιχείου του πεδίου ορισμού, του $m/2$. Αντίθετα η συνάρτηση με τύπο $f(n) = \lfloor n/2 \rfloor$ δεν είναι 1 – 1 επειδή η τιμή 2 παράγεται από δύο ορίσματα: 4 και 5.

Μια συνάρτηση f: $A \rightarrow B$, λέγεται ***συνάρτηση 1 – 1 και επί*** ή ότι είναι μια ***αμφίεση*** (*bijection*) αν κάθε στοιχείο του B είναι εικόνα ενός και μόνο στοιχείου του A. Δηλαδή αν είναι, $f(A) = B$ και $\forall x_1,x_2 \in A\ [x_1 \neq x_2 \Leftrightarrow f(x_1) \neq f(x_2)]$. Μια συνάρτηση 1 – 1 και επί συνήθως λέγεται ***1 – 1 αντιστοιχία*** μεταξύ των A και B. Επίσης, αν f: $A \rightarrow A$ είναι μια συνάρτηση 1 – 1 και επί, τότε είναι όπως λέμε μια ***μετάθεση*** των στοιχείων του A ή απλά μια μετάθεση του A.

Οποτεδήποτε υπάρχει μια 1 – 1 αντιστοιχία μεταξύ των A και B, τα δύο σύνολα πρέπει να έχουν τον ίδιο αριθμό στοιχείων ή τον ίδιο πληθάριθμο[†]. Για παράδειγμα, ας θεωρήσουμε το σύνολο E των άρτιων αριθμών, {0, 2, 4, 6, ...}. Υπάρχει μια αμφίεση από το $\boldsymbol{N}$ στο Ε ορισμένη από την $f(n) = 2n$. Έτσι, το σύνολο των άρτιων έχει τον ίδιο πληθάριθμο με το σύνολο των φυσικών.

Έστω f: $A \rightarrow B$ μια συνάρτηση 1 – 1 και επί. Τότε η ***αντίστροφη*** της f, συμβολικά f^{-1}, είναι η συνάρτηση από το B στο A ορισμένη ως

$f^{1}(y) = x$ αν και μόνο αν $f(x) = y$.

Να σημειωθεί ότι αν f είναι μια αμφίεση το ίδιο είναι και η f^{-1}. Στην κρυπτογραφία χρησιμοποιούνται αμφιέσεις ως το εργαλείο κρυπτογράφηση μηνυμάτων και οι αντίστροφοι μετασχηματισμοί χρησιμοποιούνται για αποκρυπτογράφηση. Αν οι μετασχηματισμοί δεν ήταν αμφιέσεις τότε δεν θα ήταν δυνατό να γίνεται πάντα αποκρυπτογράφηση σε ένα μοναδικό μήνυμα.

Έστω g: $A \rightarrow B$, f: $B \rightarrow \Gamma$. Η *σύνθεση* της f με την g, συμβολικά $f \circ g$ είναι μια συνάρτηση από το Α στο Γ ορισμένη από την

$f \circ g\ (x) = f(g(x))$ για όλα τα $x \in A$.

[†] Για την έννοια πληθάριθμος βλ. παρακάτω.

Η σύνθεση μπορεί εύκολα να επεκταθεί σε περισσότερες από δύο συναρτήσεις. Για τις συναρτήσεις $f_1, f_2, \ldots, f_s$, μπορούμε να ορίσουμε την $f_s \circ \ldots \circ f_2 \circ f_1$, αρκεί το (π.ο) της f_s να ισούται με το σύνολο αφίξεως της f_{s-1} και ούτω καθεξής.

Η ***ταυτοτική*** (identity) συνάρτηση επί ενός μη κενού συνόλου A είναι η συνάρτηση $f : A \to A$, τέτοια ώστε $f(x) = x$, για όλα τα $x \in A$. Συχνά η ταυτοτική συνάρτηση επί του A συμβολίζεται με id_A. Αν τώρα $f: A \to B$ είναι μια συνάρτηση 1 – 1 και επί, τότε εύκολα μπορούμε να δούμε ότι

$$f \circ f^{-1} = \mathrm{id}_B \quad \text{και} \quad f^{-1} \circ f = \mathrm{id}_A$$

Οι συναρτήσεις είναι χρήσιμες και σε θέματα απαρίθμησης. Τα σύνολα A και B λέμε ότι έχουν τον ίδιο αριθμό στοιχείων, αν και μόνον αν, υπάρχει μια 1 - 1 αντιστοιχία μεταξύ των A και B. Επίσης, το σύνολο A λέμε ότι είναι ένα ***πεπερασμένο*** σύνολο αν υπάρχει μια 1 - 1 αντιστοιχία μεταξύ του A και του υποσυνόλου $E_n = \{1, 2, 3, \ldots, n\}$ του $\boldsymbol{N}$. Σ' αυτήν την περίπτωση το n θα δηλώνει το πλήθος των στοιχείων του A, δηλαδή $n = |A|$ = ***πληθικός αριθμός*** ή ***πληθάριθμος*** ή ***δύναμη*** (*cardinality*) του A.

Ένα σύνολο A λέμε ότι είναι ***απειροσύνολο*** ή ***μη πεπερασμένο*** όταν υπάρχει μια 1 - 1 αντιστοιχία μεταξύ του A και ενός γνήσιου υποσυνόλου του. Για παράδειγμα, η απεικόνιση $f : f(n) = 2n, \ n \in \boldsymbol{N}$ του $\boldsymbol{N}$ επί του γνήσιου υποσυνόλου του, $M = \{x : x \in \boldsymbol{N}, x \text{ είναι άρτιος}\}$ είναι συγχρόνως 1 - 1 και επί. Άρα, το $\boldsymbol{N}$ είναι ένα μη πεπερασμένο σύνολο. Ένα μη πεπερασμένο σύνολο A λέμε ότι είναι ***μετρήσιμο*** αν υπάρχει μια 1 - 1 αντιστοιχία μεταξύ του A και του συνόλου $\boldsymbol{N}$ των φυσικών αριθμών, διαφορετικά είναι ***μη μετρήσιμο***.

Δύο χρήσιμες αρχές απαρίθμησης είναι οι ακόλουθες:

– Αν Α και Β είναι πεπερασμένα σύνολα με πληθικούς αριθμούς $|A|$ και $|B|$ αντίστοιχα, τότε και το σύνολο $A \cup B$ είναι πεπερασμένο και είναι

$$|A \cup B| = |A| + |B| - |A \cap B|$$

ή γενικότερα,

$$\left|A_1 \cup A_2 \cup \cdots \cup A_s\right| = \sum_{1 \le i \le s} \left|A_i\right| - \sum_{1 \le i < j \le s} \left|A_i \cap A_j\right| + \sum_{1 \le i < j < k \le s} \left|A_i \cap A_j \cap A_k\right| + \cdots + (-1)^{s-1} \left|A_1 \cap A_2 \cap \cdots \cap A_s\right|$$

(***αρχή του εγκλεισμού και του αποκλεισμού***)

– Αν A και B είναι πεπερασμένα σύνολα με πληθικούς αριθμούς $|A|$ και $|B|$ αντίστοιχα, τότε και το σύνολο $A \times B$ είναι πεπερασμένο και είναι,

$$|A \times B| = |A| \cdot |B|$$

ή γενικότερα

$|A_1 \times A_2 \times \ldots \times A_n| = |A_1| \cdot |A_2| \cdot \ldots \cdot |A_n|$

(*αρχή της πολλαπλασιαστικότητας*)

C.0. Διμελείς σχέσεις

Γενικεύοντας την έννοια της συνάρτησης ή απεικόνισης θεωρούμε A και B δύο μη κενά σύνολα. Μια ***διμελής*** ή ***δυαδική*** (binary) ***σχέση*** R από το A στο B είναι ένα υποσύνολο του καρτεσιανού γινομένου $A \times B$.[‡] Δοθέντος ενός (διατεταγμένου) ζεύγους (x, y) από το $A \times B$, το x σχετίζεται με το y δια της R, αν και μόνον αν, το (x, y) ανήκει στο R. Συμβολικά, $x \, R \, y \Leftrightarrow (x, y) \in R$. Ειδική περίπτωση διμελούς σχέσης είναι η συνάρτηση:

- Μια συνάρτηση f: $A \to B$ είναι μια διμελής σχέση από το A στο B τέτοια ώστε, για κάθε $x \in A$, υπάρχει ακριβώς ένα $y \in B$ τέτοιο ώστε $(x, y) \in f$.

Δοθείσης μιας σχέσης R από το A στο B ορίζεται η ***αντίστροφή*** της σχέση R^{-1} ως

$$R^{-1} = \{(y, x) \in B \times A : (x, y) \in R \}$$

Συμβολικά,

$$\forall x \in A, \forall y \in B, \ (y, x) \in R^{-1} \Leftrightarrow (x, y) \in R$$

Η ***σύνθεση*** των σχέσεων $R_1 \subseteq A \times B$ και $R_2 \subseteq B \times \Gamma$ είναι η σχέση

$R_2 \circ R_1 = \{(\alpha, \gamma)$: $\exists \gamma, ((\alpha, \beta) \in R_1) \wedge ((\beta, \gamma) \in R_2\}$.

Είναι εύκολο να δούμε ότι $R_2 \circ R_1 \neq R_1 \circ R_2$. Αποδεικνύεται επίσης ότι

$$R_1 \circ (R_2 \circ R_3) = (R_1 \circ R_2) \circ R_3$$

Η σύνθεση RoR της σχέσης R με τον εαυτό της γράφεται R^2 και γενικότερα, η R^n σημαίνει τη σύνθεση της R με τον εαυτό της n φορές. Επίσης η R^n μπορεί να οριστεί ως $R^{n-1} \circ R$.

Όπως είπαμε, μια διμελής σχέση συνδέει τα στοιχεία δύο συνόλων σε ζεύγη. Μπορούμε ακόμη να ορίσουμε τριμελείς σχέσεις που συνδέουν τα στοιχεία τριών συνόλων σε τριάδες, τετραμελείς σχέσεις που συνδέουν τα στοιχεία τεσσάρων συνόλων σε τετράδες κ.ο.κ. Καταλήγουμε λοιπόν στον ακόλουθο ορισμό.

Έστω τα σύνολα $A_1, A_2, \ldots, A_n$. Μια ***n – μελής σχέση*** (n – ary relation) σ' αυτά τα σύνολα είναι ένα υποσύνολο του καρτεσιανού γινομένου τους $A_1 \times A_2 \times \ldots \times A_n$. Τα σύνολα $A_1, A_2, \ldots, A_n$ λέγονται *πεδία ορισμού* (*domains*) της σχέσης και το n ο *βαθμός* (*degree*) της. Με άλλα λόγια, μια n – μελής σχέση μεταξύ των συνόλων

[‡] Συνήθως χρησιμοποιούμε τον όρο ***σχέση*** αλλά ο όρος διμελής σχέση δηλώνει ακριβέστερα ότι είναι μια σχέση μεταξύ στοιχείων διατεταγμένων ζευγών (από στοιχεία δύο συνόλων).

A_1, A_2, … , A_n είναι ένα σύνολο διατεταγμένων n – άδων στις οποίες το πρώτο στοιχείο είναι στοιχείο του A_1, το δεύτερο στοιχείο είναι στοιχείο του A_2, … , και το n – οστό στοιχείο είναι στοιχείο του A_n.

Ιδιαίτερης σημασίας σχέσεις είναι αυτές που ορίζονται από ένα σύνολο στον εαυτό του. Μια ***διμελής σχέση σε ένα σύνολο*** A είναι μια διμελής σχέση από το Α στο Α. Μια σχέση R σε ένα σύνολο Α λέγεται

- ***ανακλαστική*** αν α R α, $\forall \alpha \in A$, δηλ. αν $(\alpha, \alpha) \in$ R για κάθε στοιχείο του συνόλου Α.
- ***συμμετρική*** αν όποτε είναι α R β, τότε β R α, δηλ. αν όποτε είναι $(\alpha, \beta) \in$ R τότε $(\beta, \alpha) \in$ R.
- ***αντισυμμετρική*** όταν είναι α R β και β R α μόνον αν $\alpha = \beta$, δηλ. όταν είναι $(\alpha, \beta) \in$ R και $(\beta, \alpha) \in$ R, μόνον αν $\alpha = \beta$.
- ***μεταβατική*** αν όποτε είναι α R β και β R γ, τότε α R γ, δηλ. αν όποτε είναι $(\alpha, \beta) \in$ R και $(\beta, \gamma) \in$ R τότε $(\alpha, \gamma) \in$ R.

Χαρακτηριστικό παράδειγμα είναι το ακόλουθο. Αν $\alpha, \beta \in \boldsymbol{Z}$ και $n \in \boldsymbol{N}^*$ τότε με τον ακόλουθο τρόπο

$$\alpha \equiv \beta \pmod{n} \Leftrightarrow \alpha - \beta = k\,n,\ k \in \boldsymbol{Z}$$

ορίζεται μια σχέση "≡ (mod n)" στο σύνολο $\boldsymbol{Z}$ η οποία διαβάζεται "α ισοδύναμο ή ισότιμο με β modulo n". Έτσι $11 \equiv -3 \pmod 7$, αφού $11 - (-3) = 14 = 2\cdot 7$ και $3 \equiv 42 \pmod{13}$, αφού $3 - 42 = -39 = (-3)\cdot 13$. Η σχέση "≡ (mod n)" είναι

- ανακλαστική, γιατί για κάθε $\alpha \in \boldsymbol{Z}$ είναι $\alpha \equiv \alpha \pmod n$, αφού $\alpha - \alpha = 0 = 0\cdot n$
- συμμετρική, γιατί αν $\alpha \equiv \beta \pmod n$, τότε υπάρχει $\kappa \in \boldsymbol{Z}$ με $\alpha - \beta = \kappa\cdot n$, οπότε $\beta - \alpha = (-\kappa)\cdot n$, που σημαίνει ότι $\beta \equiv \alpha \pmod n$, αφού $-\kappa \in \boldsymbol{Z}$
- μεταβατική, γιατί αν $\alpha \equiv \beta \pmod n$ και $\beta \equiv \gamma \pmod n$, τότε υπάρχουν ακέραιοι κ_1 και κ_2 με $\alpha - \beta = \kappa_1\cdot n$ και $\beta - \gamma = \kappa_2\cdot n$, οπότε $\alpha - \gamma = (\alpha - \beta) + (\beta - \gamma) = \kappa_1\cdot n + \kappa_2\cdot n = (\kappa_1 + \kappa_2)\cdot n$ και συνεπώς $\alpha \equiv \gamma \pmod n$, αφού $(\kappa_1 + \kappa_2) \in \boldsymbol{Z}$.

Μια διμελής σχέση R σε ένα σύνολο Α λέγεται ότι είναι μια ***σχέση ισοδυναμίας*** στο Α όταν είναι (i) ανακλαστική, (ii) συμμετρική και (iii) μεταβατική. Μια σχέση ισοδυναμίας συμβολίζεται συνήθως με το σύμβολο ~ ή ≡ που διαβάζεται συνήθως "ισοδύναμο". Δύο στοιχεία που συνδέονται με μια σχέση ισοδυναμίας λέγονται ***ισοδύναμα***. Δηλαδή για μια σχέση ισοδυναμίας στο A ισχύουν:

$$\alpha \sim \alpha,\ \forall \alpha \in A$$
$$\alpha \sim \beta \Rightarrow \beta \sim \alpha$$
$$\alpha \sim \beta \wedge \beta \sim \gamma \Rightarrow \alpha \sim \gamma$$

Για παράδειγμα, σύμφωνα με τον παραπάνω ορισμό, η σχέση "≡ (mod n)" είναι μια σχέση ισοδυναμίας στο σύνολο $\boldsymbol{Z}$.

Αν $\alpha \in A$ και ~ είναι μια σχέση ισοδυναμίας στο Α, το σύνολο όλων των στοιχείων x του A που ικανοποιούν την $x \sim \alpha$ λέγεται ***κλάση ισοδυναμίας*** του α στο A και συμβολίζεται με $[\alpha]$, δηλαδή

$$[\alpha] = \{x: x \in A \text{ με } x \sim \alpha\}$$

Κάθε $x \in [\alpha]$ ονομάζεται ***αντιπρόσωπος*** της κλάσεως ισοδυναμίας $[\alpha]$. Δεν είναι δύσκολο να δειχθεί ότι για τις κλάσεις ισοδυναμίας ισχύουν οι ιδιότητες:

$\alpha \in [\alpha]$

αν $\beta \in [\alpha]$, τότε $[\beta] = [\alpha]$

αν $[\alpha] \cap [\beta] \neq \varnothing$, τότε $[\alpha] = [\beta]$

και το θεώρημα

- Αν ~ είναι μια σχέση ισοδυναμίας σ' ένα σύνολο Α, τότε οι ακόλουθες προτάσεις είναι ισοδύναμες:
  i) $\alpha \sim \beta$
  ii) $[\alpha] = [\beta]$
  iii) $[\alpha] \cap [\beta] \neq \varnothing$

Μπορούμε τώρα να δούμε πως μια σχέση ισοδυναμίας ~ διαμερίζει ένα σύνολο A. Επειδή ένα στοιχείο α του συνόλου A ανήκει στην κλάση ισοδυναμίας του $[\alpha]$, η ένωση όλων των κλάσεων ισοδυναμίας ως προς την ~ είναι το ίδιο το σύνολο A, δηλ. $\bigcup_{\alpha \in A} [\alpha] = A$. Επίσης, από το παραπάνω θεώρημα, προκύπτει ότι αυτές οι κλάσεις ισοδυναμίας είναι είτε ίσες, είτε ξένες μεταξύ τους, δηλ. $[\alpha] \cap [\beta] = \varnothing$ όταν $[\alpha] \neq [\beta]$.

Οι δύο παραπάνω παρατηρήσεις πιστοποιούν ότι οι κλάσεις ισοδυναμίας δημιουργούν μια διαμέριση του συνόλου A. Αντίστροφα τώρα, μια διαμέριση ενός συνόλου A μπορεί να χρησιμοποιηθεί προκειμένου να ορίσουμε μια σχέση ισοδυναμίας. Πράγματι ας υποθέσουμε ότι η οικογένεια $(A_i)_{i \in I}$ είναι μια διαμέριση του A και έστω R μια σχέση στο A που αποτελείται από τα ζεύγη (α, β) όπου τα α και β ανήκουν στο ίδιο υποσύνολο A_i της διαμέρισης. Επειδή το α είναι στο ίδιο υποσύνολο με τον εαυτό του, έχουμε ότι $(\alpha, \beta) \in \mathsf{R}$, $\forall \alpha \in A$. Επομένως η σχέση R είναι ανακλαστική. Η σχέση R είναι συμμετρική γιατί αν $(\alpha, \beta) \in \mathsf{R}$, τότε τα β και α είναι στο ίδιο υποσύνολο της διαμέρισης οπότε θα είναι και $(\beta, \alpha) \in \mathsf{R}$. Αν τώρα $(\alpha, \beta) \in \mathsf{R}$, και $(\beta, \gamma) \in \mathsf{R}$, τότε τα α και β είναι στο ίδιο υποσύνολο, έστω A_k, και τα β και γ είναι στο ίδιο υποσύνολο, έστω A_m, της διαμέρισης. Επειδή όμως τα υποσύνολα μιας διαμέρισης είναι ξένα μεταξύ τους και το β ανήκει στο A_k και στο A_m προκύπτει ότι $A_k = A_m$. Επομένως, τα α και γ ανήκουν στο ίδιο υποσύνολο της διαμέρισης οπότε $(\alpha, \beta) \in \mathsf{R}$. Άρα η R είναι και μεταβατική. Αποδείξαμε λοιπόν ότι η R είναι μια σχέση ισοδυναμίας. Οι κλάσεις ισοδυναμίας της R συνίστανται στα

υποσύνολα του A που περιέχουν συσχετιζόμενα στοιχεία και από τον ορισμό της R αυτά είναι τα υποσύνολα της διαμέρισης. Τα παραπάνω συνοψίζονται στο θεώρημα

- Μια σχέση ισοδυναμίας ~ σ' ένα σύνολο A δημιουργεί μια διαμέριση του A και αντίστροφα, μια διαμέριση του A ορίζει μια σχέση ισοδυναμίας στο A.

Οι κλάσεις ισοδυναμίας ως προς τη σχέση ισοδυναμίας "≡ (mod n)" που ορίσαμε στο παράδειγμα παραπάνω, ονομάζονται ***κλάσεις ισοδυναμίας modulo n*** ή ***κλάσεις υπολοίπου*** ή ***κατάλοιπου modulo n***. Έτσι η κλάση υπολοίπου modulo n του $\alpha \in \boldsymbol{Z}$ περιέχει όλους τους ακέραιους x, για τους οποίους η διαφορά $x - \alpha$ είναι ακέραιο πολλαπλάσιο του n, δηλαδή

$[\alpha]_n = \{x : x = \alpha + k\ \mathrm{n},\ k \in \boldsymbol{Z}\}$

Η σχέση για παράδειγμα "≡ (mod 3)" ορίζει τις ακόλουθες κλάσεις υπολοίπου modulo 3 στο $\boldsymbol{Z}$:

$[0]_3 = \{x : x = 3k,\ k \in \boldsymbol{Z}\}$

$[1]_3 = \{x : x = 3k + 1,\ k \in \boldsymbol{Z}\}$

$[2]_3 = \{x : x = 3k + 2,\ k \in \boldsymbol{Z}\}$

γιατί τα δυνατά υπόλοιπα της διαίρεσης ενός ακέραιου με το 3 είναι 0, 1 και 2. Έτσι ορίζεται και μια διαμέριση του $\boldsymbol{Z}$: $[0]_3$, $[1]_3$, $[2]_3$.

D.0. Εσωτερικές πράξεις

Αν A είναι μη κενό σύνολο, τότε μια απεικόνιση $\varpi : A \times A \to A$ ονομάζεται ***εσωτερική πράξη***[§] στο A. Αν ϖ είναι μια εσωτερική πράξη στο A, τότε λέμε ότι *" το A είναι εφοδιασμένο με την πράξη ϖ "*. Για το συμβολισμό μιας εσωτερικής πράξης συνήθως χρησιμοποιούμε, αντί για το ϖ, ένα από τα σύμβολα $*$, ο, +, ·. Έτσι, χρησιμοποιώντας το σύμβολο $*$, την εικόνα $\varpi((\alpha, \beta))$ του $(\alpha, \beta) \in A \times A$ τη συμβολίζουμε με $\alpha * \beta$ και την ονομάζουμε ***εξαγόμενο*** ή ***αποτέλεσμα*** της εσωτερικής πράξης μεταξύ του α και του β. Με $\alpha_1 * \alpha_2 * \alpha_3$ θα συμβολίζουμε το $(\alpha_1 * \alpha_2) * \alpha_3$ και γενικά με $\alpha_1 * \alpha_2 * \ldots * \alpha_n$ το $(\alpha_1 * \alpha_2 * \ldots * \alpha_{n-1}) * \alpha_n = [\ldots[(\alpha_1 * \alpha_2) * \alpha_3] * \ldots * \alpha_{n-1}] * \alpha_n$. Άμεση συνέπεια του ορισμού μιας εσωτερικής πράξης ως απεικόνισης είναι ότι ισχύουν οι συνεπαγωγές

$$\alpha = \beta \Rightarrow \alpha * \gamma = \beta * \gamma \quad \text{και} \quad \alpha = \beta \Rightarrow \gamma * \alpha = \gamma * \beta.$$

Για παράδειγμα, η ένωση $\cup$ (ή η τομή $\cap$) στο δυναμοσύνολο $\wp(A)$ ενός συνόλου A είναι μια εσωτερική πράξη στο $\wp(A)$. Επίσης η πρόσθεση και ο πολλα-

[§] Όταν δεν έχουμε να κάνουμε με άλλου είδους πράξεις μια εσωτερική πράξη τη λέμε απλά πράξη.

πλασιασμός είναι εσωτερικές πράξεις στο $\boldsymbol{Z}$, γιατί για κάθε $(\alpha, \beta)\in\boldsymbol{Z}\times\boldsymbol{Z}$ τα αποτελέσματα $\alpha + \beta$, $\alpha \cdot \beta$ αυτών των πράξεων είναι ακέραιοι.

Μια πράξη σ' ένα πεπερασμένο σύνολο Σ ορίζεται και με πίνακα διπλής εισόδου ο οποίος λέγεται και πίνακας αποτελεσμάτων της πράξης. Έτσι στο σύνολο $\Sigma = \{1, -1, 2\ -2\}$ ορίζεται η πράξη $*$ με τον ακόλουθο πίνακα

β / α	1	-1	2	-2
1	1	-1	2	-2
-1	-1	1	-2	2
2	2	-2	-1	1
-2	-2	2	1	-1

Σε κάθε ζεύγος (α, β) το α είναι στοιχείο της $1^{ης}$ στήλης και το β της $1^{ης}$ γραμμής. Έτσι είναι $1 * 1 = 1$, $1 * (-1) = -1$, …, $2 * 2 =$ -1, …, $(-2) * (-2) = -1$.

Αν $*$ είναι μια εσωτερική πράξη σε σύνολο Σ και A ένα μη κενό υποσύνολο του Σ, τότε λέμε ότι το A είναι ***κλειστό*** ως προς την πράξη $*$, όταν και μόνον όταν για κάθε $(\alpha, \beta)\in A\times A$ το αποτέλεσμα $\alpha * \beta$ είναι στοιχείο του A.

Για παράδειγμα, στο σύνολο $\boldsymbol{N}$, το υποσύνολο των πολλαπλασίων του 3 είναι κλειστό ως προς την πρόσθεση καθώς και τον πολλαπλασιασμό στο $\boldsymbol{N}$, γιατί $3k + 3m = 3(k + m) \in \boldsymbol{N}$ και $(3k)(3m) = 3(3km) \in \boldsymbol{N}$ για κάθε $k,m \in \boldsymbol{N}$.

Μια πράξη $*$ σε ένα σύνολο Σ ονομάζεται

- ***προσεταιριστική***, αν και μόνον αν,

  $\forall\alpha, \beta, \gamma \in \Sigma, (\alpha * \beta) * \gamma = \alpha * (\beta * \gamma)$

- ***αντιμεταθετική***, αν και μόνον αν,

  $\forall\alpha, \beta \in \Sigma, \alpha * \beta = \beta * \alpha$

Για παράδειγμα**,** η πρόσθεση και ο πολλαπλασιασμός στο $\boldsymbol{R}$ είναι πράξεις προσεταιριστικές και αντιμεταθετικές. Η πρόσθεση στο σύνολο $\boldsymbol{\Pi_n}$ των τετραγωνικών πινάκων είναι πράξη προσεταιριστική και αντιμεταθετική. Ο πολλαπλασιασμός στο ίδιο σύνολο, είναι πράξη προσεταιριστική αλλά δεν είναι αντιμεταθετική, γιατί αν $\boldsymbol{A}$, $\boldsymbol{B}$ είναι δυο $n\times n$ πίνακες δεν είναι πάντα $\boldsymbol{A}\cdot\boldsymbol{B} = \boldsymbol{B}\cdot\boldsymbol{A}$.

Έστω μια πράξη $*$ σε ένα σύνολο Σ. Τότε ένα στοιχείο e του Σ ονομάζεται ***ουδέτερο στοιχείο*** ως προς την πράξη $*$, όταν και μόνον όταν,

$\forall\alpha \in \Sigma, \alpha * e = e * \alpha = \alpha.$

Αν υπάρχει ουδέτερο στοιχείο στο Σ ως προς την πράξη $*$, αποδεικνύεται εύκολα ότι αυτό είναι μοναδικό και γι' αυτό λέμε ότι είναι <u>το</u> ουδέτερο στοιχείο ως προς την πράξη αυτή. Για παράδειγμα, το $\varnothing$ είναι το ουδέτερο στοιχείο του δυναμοσυ-

νόλου $\wp(A)$ ενός συνόλου A ως προς την πράξη της ένωσης $\cup$, αφού για κάθε $X \in \wp(\mathrm{A})$ ισχύει $X \cup \varnothing = X$. Το A είναι το ουδέτερο στοιχείο του $\wp(A)$ ως προς την πράξη της τομής $\cap$, αφού για κάθε $X \in \wp(\mathrm{A})$ ισχύει $X \cap A = X$. Το ουδέτερο στοιχείο ως προς μια πράξη που τη λέμε "πρόσθεση" (+) το συμβολίζουμε με 0, ενώ ως προς μια πράξη που τη λέμε " πολλαπλασιασμό" (·), το συμβολίζουμε με 1 ή Ι.

Αν $*$ είναι μια πράξη σε ένα σύνολο Σ ως προς την οποία υπάρχει ουδέτερο στοιχείο $e \in \Sigma$, δύο στοιχεία α και α' του Σ ονομάζονται ***συμμετρικά*** ως προς την πράξη αυτή, όταν και μόνον όταν ισχύει

$$\alpha * \alpha' = \alpha' * \alpha = e$$

Στην περίπτωση αυτή λέμε ότι το α' είναι το συμμετρικό του α ως προς την πράξη $*$ και αντίστροφα το α συμμετρικό του α' ως προς την $*$. Επίσης, στην περίπτωση μιας πράξης που τη λέμε "πρόσθεση" το συμμετρικό του α το συμβολίζουμε με $-\alpha$ και το λέμε ***αντίθετο*** του α, ενώ στην περίπτωση μιας πράξης που τη λέμε "πολλαπλασιασμό", το συμβολίζουμε με α^{-1} και το λέμε ***αντίστροφο*** του α. Έτσι έχουμε αντιστοίχως

$$\alpha + (-\alpha) = (-\alpha) + \alpha = 0 \quad \text{και} \quad \alpha \cdot \alpha^{-1} = \alpha^{-1} \cdot \alpha = 1$$

Αποδεικνύεται ότι: Έστω $*$ μια πράξη προσεταιριστική στο σύνολο Σ με ουδέτερο στοιχείο e. Αν υπάρχει το συμμετρικό ενός στοιχείου του Σ, τότε αυτό είναι μοναδικό και αν υπάρχουν τα συμμετρικά $\alpha', \beta' \in \Sigma$ των στοιχείων $\alpha, \beta \in \Sigma$, τότε είναι

$$(\alpha * \beta)' = \beta' * \alpha'$$

Η παραπάνω σχέση για πράξεις που σημειώνονται + και · γράφεται αντίστοιχα

$$-(\alpha + \beta) = (-\beta) + (-\alpha) \quad \text{και} \quad (\alpha \cdot \beta)^{-1} = \beta^{-1} \cdot \alpha^{-1}$$

Αν $*$, ο είναι δυο πράξεις σ' ένα σύνολο Σ, τότε λέμε ότι η πράξη $*$ είναι επιμεριστική ως προς την ο, αν και μόνον αν είναι συγχρόνως από αριστερά και από δεξιά επιμεριστική ως προς την ο, δηλαδή αν και μόνον αν

$$\forall \alpha, \beta, \gamma \in \Sigma,\ \alpha * (\beta \circ \gamma) = (\alpha * \beta) \circ (\alpha * \gamma) \quad \text{και} \quad (\beta \circ \gamma) * \alpha = (\beta * \alpha) \circ (\gamma * \alpha)$$

Για παράδειγμα**,** στο δυναμοσύνολο $\wp(A)$ ενός συνόλου A, η τομή $\cap$ είναι επιμεριστική ως προς την ένωση $\cup$ και η ένωση $\cup$ είναι επιμεριστική ως προς την τομή $\cap$.

Ε.0. Εσωτερική πράξη και κλάσεις ισοδυναμίας

Ας θεωρήσουμε αρχικά το σύνολο $M = \{ \frac{\alpha}{\beta} : \alpha, \beta \in \boldsymbol{Z} \text{ με } \beta \neq 0 \}$. Τότε η σχέση που ορίζεται με τον ακόλουθο τρόπο

$$\frac{\alpha}{\beta} \equiv \frac{\gamma}{\delta} \Leftrightarrow \alpha\delta = \beta\gamma$$

είναι μια σχέση ισοδυναμίας στο M και είναι γνωστό ότι η κλάση ισοδυναμίας ενός στοιχείου του M λέγεται ρητός αριθμός. Έτσι τα στοιχεία του συνόλου $\boldsymbol{Q}$ των ρητών αριθμών είναι κλάσεις ισοδυναμίας. Οι εσωτερικές πράξεις που γνωρίσαμε μέχρι τώρα στο $\boldsymbol{Q}$, ήταν στην πραγματικότητα πράξεις μεταξύ κλάσεων ισοδυναμίας. Ας ξαναδούμε την πρόσθεση στο $\boldsymbol{Q}$. Τα κλάσματα $\alpha = 1/3$ και $\beta = 1/5$ δημιουργούν τους ρητούς $[\alpha]$ και $[\beta]$. Αν με τη γνωστή πρόσθεση στο σύνολο M των κλασμάτων προσθέσουμε δύο αντιπρόσωπους των $[\alpha]$ και $[\beta]$, π.χ. τους 1/3 και 1/5, βρίσκουμε άθροισμα $\gamma = 8/15$. Δύο άλλοι αντιπρόσωποι των ρητών $[\alpha]$ και $[\beta]$, π.χ. οι 2/6 και 3/15, δίνουν άθροισμα 16/30, που ανήκει στην κλάση $[\gamma]$, αφού $8/15 \equiv 16/30$. Το ίδιο συμβαίνει και με οποιουσδήποτε αντιπρόσωπους των $[\alpha]$ και $[\beta]$.

Αντιμετωπίζοντας το παραπάνω θέμα γενικά, έστω A ένα σύνολο στο οποίο έχουν οριστεί μια εσωτερική πράξη $*$ και μια σχέση ισοδυναμίας $\sim$. Αν E είναι το σύνολο των κλάσεων ισοδυναμίας των στοιχείων του A (δηλ. η διαμέριση που δημιουργεί η $\sim$ στο A), τότε υπάρχουν διάφοροι τρόποι για να οριστούν εσωτερικές πράξεις στο E. Επειδή κάθε στοιχείο του E αποτελείται από στοιχεία του A, δημιουργείται το ερώτημα αν είναι δυνατό να οριστεί εσωτερική πράξη στο E με τη βοήθεια της πράξης $*$ στο A. Για το σκοπό αυτό σκεπτόμαστε ως εξής. Αν $[\alpha], [\beta] \in E$ και πάρουμε $\alpha_1 \in [\alpha]$ και $\beta_1 \in [\beta]$, τότε το αποτέλεσμα $\alpha_1 * \beta_1$ ανήκει σε μια κλάση ισοδυναμίας, έστω τη $[\gamma]$. Το θέμα τώρα είναι αν δύο άλλοι αντιπρόσωποι α_2, β_2 των κλάσεων $[\alpha]$ και $[\beta]$ αντίστοιχα, δίνουν αποτέλεσμα $\alpha_2 * \beta_2$ το οποίο ανήκει στην κλάση $[\gamma]$. Είναι φανερό ότι για να μπορούμε να ορίσουμε, με τη βοήθεια της πράξης $*$, μια πράξη στο E, που να είναι ανεξάρτητη από την εκλογή των αντιπροσώπων των κλάσεων $[\alpha]$ και $[\beta]$, πρέπει τα αποτελέσματα $\alpha_1 * \beta_1$ και $\alpha_2 * \beta_2$ να ανήκουν πάντα στην ίδια κλάση ισοδυναμίας. Καταλήγουμε λοιπόν στον εξής ορισμό.

Μια σχέση ισοδυναμίας $\sim$ στο σύνολο Α λέγεται ότι είναι ***συμβιβαστή*** με την εσωτερική πράξη $*$ στο Α, όταν ισχύει η

$$\alpha_1 \sim \alpha_2 \text{ και } \beta_1 \sim \beta_2 \Rightarrow (\alpha_1 * \beta_1) \sim (\alpha_2 * \beta_2)$$

Σ' αυτήν την περίπτωση μπορούμε να ορίσουμε μια εσωτερική πράξη στο σύνολο E των κλάσεων ισοδυναμίας των στοιχείων του A, που την συμβολίζουμε επίσης με $*$, με την ισότητα

$$[\alpha] * [\beta] = [\alpha * \beta]$$

Για να ελέγχουμε αν μια σχέση ισοδυναμίας είναι συμβιβαστή με μια πράξη μπορούμε να χρησιμοποιούμε το εξής θεώρημα:

- Μια σχέση ισοδυναμίας $\sim$ σ' ένα σύνολο A είναι συμβιβαστή με μια εσωτερική πράξη $*$ στο A, αν για κάθε $\alpha, \beta, \gamma \in A$ ισχύει

$$\alpha \sim \beta \;\Rightarrow\; (\alpha * \gamma) \sim (\beta * \gamma) \text{ και } (\gamma * \alpha) \sim (\gamma * \beta).$$

Πράγματι, έστω ότι η παραπάνω συνεπαγωγή ισχύει. Αν $\alpha \sim \alpha_1$ και $\beta \sim \beta_1$, τότε έχουμε $(\alpha * \beta) \sim (\alpha_1 * \beta)$ και $(\alpha_1 * \beta\,) \sim (\alpha_1 * \beta_1)$, οπότε αφού η ~ είναι μεταβατική σχέση, έχουμε $(\alpha * \beta) \sim (\alpha_1 * \beta_1)$, δηλαδή η ~ είναι συμβιβαστή με την $*$.

Η σχέση για παράδειγμα, "≡ (mod 3)" ορίζει, όπως έχουμε δει, τις ακόλουθες κλάσεις υπολοίπου modulo 3 στο $\boldsymbol{Z}$:

$$[0] = \{x : x = 3k,\ k \in \boldsymbol{Z}\}$$

$$[1] = \{x : x = 3k + 1,\ k \in \boldsymbol{Z}\}$$

$$[2] = \{x : x = 3k + 2,\ k \in \boldsymbol{Z}\}$$

δηλαδή το σύνολο E είναι το σύνολο $\{[0], [1], [2]\}$. Η παραπάνω σχέση μπορούμε να δούμε εύκολα ότι είναι συμβιβαστή με την πρόσθεση και τον πολλαπλασιασμό στο $\boldsymbol{Z}$, οπότε μπορούμε να ορίσουμε στο E πρόσθεση + και πολλαπλασιασμό · με τις ισότητες

$$[\alpha] + [\beta] = [\alpha + \beta]$$

$$[\alpha] \cdot [\beta] = [\alpha \cdot \beta]$$

και με τους ακόλουθους πίνακες αποτελεσμάτων

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

·	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

Π.χ. είναι

$[2] + [1] = [2 + 1] = [0]$, γιατί αν $\alpha \in [2]$ και $\beta \in [1]$, δηλαδή $\alpha = 3k + 2$ και $\beta = 3m + 1$, τότε $\alpha + \beta = 3(k + m + 1) = 3n$, $(k, m, n \in \boldsymbol{Z})$, δηλαδή $\alpha + \beta \in [0]$.

$[2] \cdot [1] = [2 \cdot 1] = [2]$, γιατί αν $\alpha \in [2]$ και $\beta \in [1]$, δηλαδή $\alpha = 3k + 2$ και $\beta = 3m + 1$, τότε $\alpha \cdot \beta = 3(3km + 2m + k) + 2 = 3n + 2$, $(k, m, n \in \boldsymbol{Z})$, δηλαδή $\alpha \cdot \beta \in [2]$.

F.0. Δομές - Ισομορφισμοί

Όπως είδαμε σ' ένα σύνολο Σ μπορούν να οριστούν διάφορες πράξεις. Τότε το σύνολο Σ μαζί με τις πράξεις αυτές λέμε ότι έχει μια ***αλγεβρική δομή*** ή είναι ένα ***αλγεβρικό σύστημα*** που χαρακτηρίζεται από τις ιδιότητες αυτών των πράξεων. Στην περίπτωση που σε ένα σύνολο Σ έχουν οριστεί μόνο εσωτερικές πράξεις, $*$, ο, …, γράφουμε $(\Sigma, *, \text{ο}, \ldots)$ για να εκφράσουμε την αλγεβρική δομή[**]. Έτσι οι

[**] ή απλά ***δομή***

συμβολισμοί (***N***, +), (***N***, ·), (***R***, +), (***R***, +, ·), εκφράζουν δομές. Οι δομές (***N***, +), (***N***, ·), παρόλο που αναφέρονται στο ίδιο σύνολο ***N***, είναι διαφορετικές γιατί δεν χαρακτηρίζονται από τις ίδιες ιδιότητες. Π.χ. στη δομή (***N***, +) δεν υπάρχει ουδέτερο στοιχείο ως προς την πράξη +, ενώ στη δομή (***N***, ·) υπάρχει και είναι το 1.

Για παράδειγμα, ας θεωρήσουμε τις δομές (A, ο) και (B, ∗) όπου A = {1, 2, 3, 4} και B = {α, β, γ, δ} και οι πράξεις ο, ∗ έχουν τους ακόλουθους πίνακες αποτελεσμάτων

ο	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

∗	α	β	γ	δ
α	β	γ	δ	α
β	γ	δ	α	β
γ	δ	α	β	γ
δ	α	β	γ	δ

Μπορούμε εύκολα να διαπιστώσουμε ότι η απεικόνιση

σ : 1 ↔ δ, 2 ↔ α, 3 ↔ γ, 4 ↔ β

είναι μια 1 – 1 αντιστοιχία μεταξύ των A και B η οποία διατηρεί τις πράξεις με την έννοια ότι όποτε

$A \ni v \leftrightarrow x \in B$ και $A \ni u \leftrightarrow y \in B$

τότε

v ο $u \leftrightarrow x * y$

δηλαδή αν το v από το A αντιστοιχεί στο x από το B και αν το u από το A αντιστοιχεί στο y από το B τότε το v ο u από το A αντιστοιχεί στο $x * y$ από το B. Θεωρώντας ότι τα στοιχεία του A είναι ψηφία και όχι αφηρημένα σύμβολα, είναι εύκολο να πούμε ότι η πράξη ο μπορεί να οριστεί ως εξής: «για κάθε x, $y \in$ Α, το xοy είναι το υπόλοιπο της διαίρεσης (x·y) / 5» (π.χ. 2·4 = 8 = 1·5 + 3 και 2ο4 = 3). Επιπλέον, η δομή (B, ∗) μπορούμε να πούμε ότι είναι μια συγκαλυμμένη ή κωδικοποιημένη εκδοχή της (A, ο) όπου ο κώδικας είναι η αντιστοιχία σ.

Στο παραπάνω παράδειγμα έχουμε μια απεικόνιση που όπως λέμε είναι ένας ***ισομορφισμός*** του A επί του B ή ότι οι δομές είναι ***ισομορφικές***:

Δύο δομές (A, ο) και (B, ∗) λέγονται ισομορφικές όταν

- υπάρχει μια 1 – 1 αντιστοιχία μεταξύ των συνόλων Α και Β, και
- οι πράξεις ο και ∗ διατηρούνται στην αντιστοιχία:

  αν Α ∋ v ↔ x ∈ Β και Α ∋ u ↔ y ∈ Β

  τότε

  v ο u ↔ x ∗ y

Οι ισομορφισμοί μεταξύ δομών χρησιμοποιούνται συνήθως με τους εξής δύο τρόπους:

1) έχοντας ανακαλύψει ορισμένες ιδιότητες μιας δομής μπορούμε, χωρίς καμιά άλλη προσπάθεια, να τις αναγνωρίσουμε ως ιδιότητες οποιασδήποτε άλλης δομής ισομορφικής με αυτή.
2) οποτεδήποτε είναι πιο βολικό, μπορούμε να αντικαταστήσουμε μια δομή με μια άλλη ισομορφική με αυτή.

Έτσι αν εξετάσουμε την δομή (Α, ο) του παραδείγματος, μπορούμε να διαπιστώσουμε ότι

α) η πράξη ο είναι προσεταιριστική γιατί

$1 \circ (1 \circ 1) = 1 \circ 1 = 1 = (1 \circ 1) \circ 1$

$1 \circ (1 \circ 2) = 1 \circ 2 = 2 = (1 \circ 1) \circ 2$

…

$4 \circ (4 \circ 4) = 4 \circ 1 = 4 = (4 \circ 4) \circ 4$

δηλαδή, $\forall\ \alpha, \beta, \gamma \in A,\ \alpha \circ (\beta \circ \gamma) = (\alpha \circ \beta) \circ \gamma$

β) η πράξη ο είναι αντιμεταθετική γιατί [††]

$1 \circ 2 = 2 = 2 \circ 1$

$2 \circ 3 = 1 = 3 \circ 2$

…

$4 \circ 3 = 2 = 3 \circ 4$

δηλαδή, $\forall\ \alpha, \beta \in A,\ \alpha \circ \beta = \beta \circ \alpha$

γ) Το 1 είναι το ουδέτερο στοιχείο του Α ως προς την ο γιατί

$1 \circ 1 = 1$

$1 \circ 2 = 2$

$1 \circ 3 = 3$

$1 \circ 4 = 4$

δηλαδή, $\forall\ \alpha \in A,\ \alpha \circ 1 = \alpha$ [‡‡]

δ) κάθε στοιχείο του Α έχει συμμετρικό γιατί

[††] Μπορούμε να διαπιστώνουμε την αντιμεταθετικότητα μιας πράξης από τον πίνακα αποτελεσμάτων της: ο πίνακας μιας αντιμεταθετικής πράξης είναι συμμετρικός ως προς την κύρια διαγώνιό του.

[‡‡] Αν η πράξη ο είναι αντιμεταθετική, είναι φανερό ότι ένα στοιχείο e του συνόλου Α είναι ουδέτερο στοιχείο ως προς την πράξη αυτή, όταν και μόνον όταν, $\forall\ \alpha \in A,\ \alpha \circ e = \alpha$.

$1 \circ 1 = 1 \Rightarrow 1' = 1$
$2 \circ 3 = 1 \Rightarrow 2' = 3$
$3 \circ 2 = 1 \Rightarrow 3' = 2$
$4 \circ 4 = 1 \Rightarrow 4' = 4$

Σύμφωνα τώρα με όσα είπαμε, τις ίδιες ιδιότητες έχει και η δομή (B, ∗) επειδή είναι όπως είδαμε ισομορφική με την (A, ο). Εννοείται ότι για το ουδέτερο στοιχείο και τα συμμετρικά, θα πρέπει να λάβουμε υπόψη την απεικόνιση (τον ισομορφισμό) σ.

G.0.Μεταθέσεις

Στην § Α.2 είπαμε ότι αν f: $A \to A$ είναι μια συνάρτηση 1 – 1 και επί, τότε είναι μια μετάθεση των στοιχείων του A ή απλά μια μετάθεση του A. Μια βασική ερώτηση που πρέπει να απαντηθεί σε σχέση με τις μεταθέσεις του A είναι: πόσες είναι; Αν το σύνολο A έχει n στοιχεία, τότε όπως θα δούμε στην επόμενη ενότητα, υπάρχουν $n!$ μεταθέσεις του A. Μια άλλη ερώτηση είναι το πόσες φορές μπορεί μια δοσμένη μετάθεση να εφαρμοστεί πριν το κάθε τι επιστρέψει στην αρχική του θέση. Αυτό δεν έχει να κάνει μόνο με το ανακάτεμα της τράπουλας αλλά και με το πρόβλημα της δημιουργίας τυχαίων αριθμών κτλ. Για τη μελέτη των μεταθέσεων, δεν έχει σημασία ποια είναι ακριβώς τα στοιχεία του συνόλου από τη στιγμή που μπορούμε να τα διακρίνουμε, οπότε μπορούμε να αναφερόμαστε στο σύνολο

$\{1, 2, \ldots, n-1, n\}$

ως ένα πρότυπο ενός συνόλου με n στοιχεία.

Ένας στάνταρ τρόπος γραφής των μεταθέσεων f του $\{1, 2, \ldots, n\}$, προκειμένου να περιγράψουμε με λεπτομέρεια το τι κάνει η κάθε μια, είναι με τη μορφή πίνακα

$$f = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ f(1) & f(2) & f(3) & \ldots & f(n) \end{pmatrix}$$

Έτσι, μεταβάλλοντας ελαφρώς το συμβολισμό, η μετάθεση

$$h = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ i_1 & i_2 & i_3 & \ldots & i_n \end{pmatrix}$$

είναι αυτή για την οποία $h(k) = I_k$.

Πάντα υπάρχει η ***τετριμμένη μετάθεση***

$$e = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 1 & 2 & 3 & \ldots & n \end{pmatrix}$$

η οποία δεν ‘‘μετακινεί’’ κάποιο στοιχείο του συνόλου. Δηλαδή, $e(k) = k$ για όλα τα k.

Μια μετάθεση μπορεί να εφαρμοστεί μετά από μια άλλη. Αν f, g είναι δύο μεταθέσεις, γράφουμε $g \circ f$ για τη μετάθεση που προκύπτει εφαρμόζοντας πρώτα την f και μετά την g. Πρόκειται για τη ***σύνθεση*** ή το ***γινόμενο*** των δύο μεταθέσεων. Θα πρέπει να παρατηρήσουμε ότι, γενικά

$$g \circ f \neq f \circ g$$

Της ο συμβολισμός είναι συμβατός με την έννοια και τον συμβολισμό της σύνθεσης συναρτήσεων. Έτσι, για $1 \leq k \leq n$, εξ ορισμού,

$$g \circ f(k) = g(f(k))$$

Συνέπεια του ορισμού των μεταθέσεων ως (1-1 και επί) συναρτήσεων από ένα σύνολο στον εαυτό του, είναι το ότι η σύνθεση μεταθέσεων είναι προσεταιριστική: για της της μεταθέσεις g, h, f της συνόλου,

$$(g \circ h) \circ f = g \circ (h \circ f)$$

Και για κάθε μετάθεση f υπάρχει η ***αντίστροφη*** μετάθεση f^{-1} η οποία έχει ως αποτέλεσμα την αντιστροφή της μετάθεσης που έχει γίνει από την f. Δηλαδή,

$$f \circ f^{-1} = f^{-1} \circ f = e$$

Ο συμβολισμός των μεταθέσεων με πίνακες είναι αρκετά αποτελεσματικός στον υπολογισμό του γινομένου δύο μεταθέσεων. Για να υπολογίσουμε, για παράδειγμα, το

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

βλέπουμε τι κάνει αυτή η σύνθεση σε καθένα από τα 1, 2, 3. Η μετάθεση δεξιά εφαρμόζεται πρώτη. Στέλνει το 1 στο 3, το οποίο στέλνεται στο 1, από τη δεύτερη μετάθεση (αυτή στα αριστερά). Παρόμοια, το 2 στέλνεται στο 2 (από τη μετάθεση στα δεξιά), το οποίο στέλνεται στο 3 (από τη μετάθεση στα αριστερά). Παρόμοια, το 3 στέλνεται στο 1 (από τη μετάθεση στα δεξιά), το οποίο στέλνεται στο 2 (από τη μετάθεση στα αριστερά). Πινακοποιώντας αυτήν την πληροφορία, έχουμε

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Αν πολλαπλασιάσουμε (συνθέσουμε) με αντίθετη σειρά, επαληθεύεται η παρατήρηση που κάναμε παραπάνω ότι η σύνθεση μεταθέσεων δεν είναι αντιμεταθετική:

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Η.0.Συνδυαστική - Πιθανότητες

Ένα σύνολο αντικειμένων τα οποία επιθυμούμε να απαριθμήσουμε μπορεί μερικές φορές να εκφρασθεί σαν μια ένωση ξένων συνόλων ή ως ένα καρτεσιανό γινόμενο συνόλων. Από το γεγονός αυτό απορρέουν δύο βασικές αρχές απαρίθμησης ή κανόνες.

Αν A, B είναι δύο ξένα μεταξύ τους πεπερασμένα σύνολα, ο ***κανόνας του αθροίσματος*** λέει ότι ο αριθμός των τρόπων να επιλεγεί ένα στοιχείο από ένα εκ των δύο αυτών συνόλων είναι το άθροισμα των πληθάριθμων των συνόλων. Δηλαδή,

$$|A \cup B| = |A| + |B|$$

ως άμεση συνέπεια της αρχής του εγκλεισμού και του αποκλεισμού (βλ. § Α.2).

Ο ***κανόνας του γινομένου*** λέει ότι ο αριθμός των τρόπων να επιλεγεί ένα διατεταγμένο ζεύγος είναι ο αριθμός των τρόπων να επιλεγεί το πρώτο στοιχείο επί τον αριθμό των τρόπων να επιλεγεί το δεύτερο στοιχείο. Δηλαδή,

$$|A \times B| = |A| \cdot |B|$$

ως άμεση συνέπεια της αρχή της πολλαπλασιαστικότητας (βλ. § Α.2).

Σε ένα πεπερασμένο σύνολο A με n στοιχεία (n-σύνολο), κάθε διατεταγμένη m-άδα ($m \le n$) της οποίας οι συνιστώσες είναι διαφορετικά ανά δύο στοιχεία του A, λέγεται ***διάταξη m*** στοιχείων του A ή ***m-μετάθεση*** του A. Με άλλα λόγια, μια m-μετάθεση του A είναι μια 1 - 1 συνάρτηση (ένριψη) του συνόλου $\{1, 2, 3,\ldots, m\}$ στο σύνολο A. Ειδικά αν $m = n$, η διάταξη λέγεται ***μετάθεση*** του Α και είναι στην ουσία μια 1 - 1 αντιστοιχία μεταξύ των συνόλων $\{1, 2, 3,\ldots, n\}$ και A.

Το πλήθος των m-μεταθέσεων ενός n-συνόλου, σύμφωνα με τον κανόνα του γινομένου, είναι:

$$P_m^n = n(n-1)(n-2)\ldots(n-m+1)$$

και για $m = n$ έχουμε το πλήθος των μεταθέσεων ενός n-συνόλου

$$P_n = n(n-1)(n-2)\ldots 1 = n!$$

Αν τώρα η διατεταγμένη m-άδα έχει συνιστώσες στοιχεία του A όχι κατ' ανάγκη διαφορετικά μεταξύ τους, τότε λέγεται ***διάταξη με επανάληψη m*** στοιχείων του Α ή ***m-μετάθεση με επανάληψη*** του A και πρόκειται για μια συνάρτηση του συνόλου $\{ 1, 2, \ldots, m \}$ στο A. Το πλήθος των m-μεταθέσεων με επανάληψη ενός n-συνόλου, σύμφωνα με τον κανόνα του γινομένου, είναι

$$PE_m^n = n^{\mathrm{m}}$$

αφού για την επιλογή κάθε συνιστώσας της m-άδας υπάρχουν n δυνατότητες (όσα τα στοιχεία A). Για παράδειγμα, το πλήθος των bit strings μήκους n που σχηματί-

ζονται, είναι $PE_n^2 = 2^n$ επειδή πρόκειται για διατεταγμένες n – άδες από στοιχεία του συνόλου $A = \{0, 1\}$.

Κάθε υποσύνολο με m στοιχεία (m-υποσύνολο) ενός n-συνόλου A λέγεται **συνδυασμός *m*** στοιχείων του A ή ***m*-συνδυασμός** του A. Πρόκειται στην ουσία για τους δυνατούς τρόπους επιλογής m στοιχείων από n χωρίς επανάθεση. Το πλήθος τους το συμβολίζουμε με $\binom{n}{m}$ ή C(n, m) και αποδεικνύεται εύκολα ότι είναι,

$$\binom{n}{m} = \frac{n!}{m!(n-m)!}$$

Επειδή σε κάθε συνδυασμό m στοιχείων του A αντιστοιχούν $m!$ διαφορετικές διατάξεις των m στοιχείων του και το πλήθος των δυνατών m-συνδυασμών του A είναι $\binom{n}{m}$, από τον κανόνα του γινομένου προκύπτει η σχέση ανάμεσα στις διατάξεις, τις μεταθέσεις και τους συνδυασμούς:

$$P_m^n = \binom{n}{m} m! = \binom{n}{m} P_m .$$

Για τους συνδυασμούς, δύο χρήσιμες ιδιότητες είναι οι :

$$\binom{n}{m} = \binom{n}{n-m}$$

$$\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1}$$

Αυτοί οι αριθμοί είναι γνωστοί και ως ***διωνυμικοί συντελεστές*** γιατί εμφανίζονται στο ανάπτυγμα του διωνύμου:

$$(\alpha + \beta)^n = \sum_{m=0}^{n} \binom{n}{m} \alpha^m \beta^{n-m} \qquad (\textbf{\textit{Newton}})$$

Μια ειδική περίπτωση του παραπάνω αναπτύγματος προκύπτει για $\alpha = \beta = 1$:

$$\sum_{m=0}^{n} \binom{n}{m} = 2^n.$$

Ο τύπος αυτός αντιστοιχεί στην απαρίθμηση των υποσυνόλων ενός συνόλου A, με $|A| = n$, με βάση τα στοιχεία που το καθένα περιέχει. Υπάρχουν $\binom{n}{m}$ υποσύνολα με m στοιχεία, επειδή τόσοι είναι οι τρόποι επιλογής m στοιχείων από n.

Ενδεχόμενα

Με τον όρο ***πείραμα τύχης*** (π.τ.) εννοούμε το μηχανισμό που μας επιτρέπει να παρατηρήσουμε ένα τυχαίο φαινόμενο. Σε κάθε πείραμα τύχης αντιστοιχεί ένα ορισμένο σύνολο δυνατών αποτελεσμάτων το οποίο ονομάζουμε ***δειγματικό χώρο*** (δ.χ.) Ω. Για παράδειγμα, στο π.τ. της ρίψης δύο νομισμάτων, μπορούμε να δούμε τον δ.χ. ως το σύνολο όλων των δυνατών 2-στρινγκς επί του συνόλου {Κ, Γ}:

Ω = {ΚΚ, ΚΓ, ΓΚ, ΓΓ}

Ενδεχόμενο ή ***γεγονός*** (event) ενός πειράματος τύχης ονομάζουμε κάθε υποσύνολο του δ.χ. Ω. Όταν ένα ενδεχόμενο περιέχει ένα μόνο στοιχείο του Ω, ονομάζεται ***στοιχειώδες*** ή ***απλό ενδεχόμενο***, ενώ όταν περιέχει δύο ή περισσότερα στοιχεία ονομάζεται ***σύνθετο***.

Επειδή $\Omega \subseteq \Omega$, το Ω είναι ενδεχόμενο του π.τ. και το ονομάζουμε το ***βέβαιο*** ενδεχόμενο, ενώ το $\varnothing$(= κενό σύνολο) το ονομάζουμε το ***αδύνατο*** ενδεχόμενο.

- Αν ο δ. χ. Ω έχει n στοιχεία, τότε το σύνολο όλων των ενδεχομένων είναι το δυναμοσύνολο $\wp(\Omega)$ και έχει 2^n στοιχεία.

Επειδή τα ενδεχόμενα ενός π. τ. είναι υποσύνολα του δ.χ. Ω, μεταφέρονται σ' αυτά οι έννοιες και οι πράξεις που έχουμε ορίσει στα σύνολα, λέμε δε *ότι το ενδεχόμενο Α πραγματοποιείται όταν το αποτέλεσμα του π. τ. είναι στοιχείο του συνόλου Α*.

Έτσι:

- $A \subseteq B \Leftrightarrow (\forall x, x \in \text{A} \Rightarrow x \in \text{B})$

  δηλαδή, *όταν πραγματοποιείται το Α, πραγματοποιείται και το Β*

- $A^c = \{ x \in \Omega: x \notin A \}$ = «**όχι *Α***»

  δηλαδή, *πραγματοποιείται το «όχι Α», όταν δεν πραγματοποιείται το Α*

- $A \cup B = \{ x \in \Omega: x \in A$ ή $x \in B \}$ = «***Α* ή *Β***»

  δηλαδή, *πραγματοποιείται το «Α ή Β»,όταν πραγματοποιείται ένα τουλάχιστον από τα Α, Β*

- $A \cap B = \{ x \in \Omega: x \in A$ και $x \in B\}$ = «***Α* και *Β***»

  δηλαδή, *πραγματοποιείται το «Α και Β», όταν πραγματοποιούνται συγχρόνως τα Α, Β*

- $A - B = \{ x \in \Omega: x \in A \text{ και } x \notin B\} = A \cap B^c =$ «***Α* και όχι *Β***»

  δηλαδή, *πραγματοποιείται το «Α και όχι Β», όταν πραγματοποιείται μόνο το Α*

Αν $A \cap B = \varnothing$ τότε τα σύνολα A, B είναι **ξένα** και λέμε τα ενδεχόμενα A, B ***ασυμβίβαστα*** δηλαδή, *η πραγματοποίηση του ενός αποκλείει την πραγματοποίηση του άλλου.*

Κατανομή Πιθανότητας

Έστω $\Omega \neq \varnothing$ ένας δειγματικός χώρος και $\wp(\Omega)$ το δυναμοσύνολό του. Κατανομή ή μέτρο πιθανότητας, ονομάζουμε την απεικόνιση

$$\Pr\{\} : \wp(\Omega) \to \boldsymbol{R}$$

που είναι τέτοια ώστε για κάθε $A, B \in \Omega$ να είναι:

1. $0 \le \Pr\{A\} \le 1$
2. $\Pr\{\Omega\} = 1$
3. $\Pr\{A \cup B\} = \Pr\{A\} + \Pr\{B\}$ αν $A \cap B = \varnothing$

- Ο αριθμός $\Pr\{A\}$, συμβολικά και $P(A)$, λέγεται ***πιθανότητα του ενδεχομένου*** A.
- Από τον παραπάνω ορισμό προκύπτει ότι:

  i) αν $A_1, A_2, \ldots, A_\kappa$ είναι ανά δύο ασυμβίβαστα ενδεχόμενα, τότε,

  $$\Pr\{A_1 \cup A_2 \cup \ldots \cup A_\kappa\} = \Pr\{A_1\} + \Pr\{A_2\} + \ldots + \Pr\{A_\kappa\}$$

  i) $\Pr\{\varnothing\} = 0$

  ii) αν σ' ένα δ. χ. $\Omega = \{\omega_1, \omega_2, \ldots, \omega_n\}$ τα στοιχειώδη ενδεχόμενα $\{\omega_1\}$, $\{\omega_2\}$, …, $\{\omega_n\}$ είναι ***ισοπίθανα*** (***ισοπίθανος δ.χ.***) τότε,

  $$\Pr\{\omega_i\} = \frac{1}{|\Omega|}, \; i = 1, 2, \ldots, n.$$

  (***ομοιόμορφη κατανομή πιθανότητας***)

  και αν $A = \{\alpha_1, \alpha_2, \ldots, \alpha_\kappa\}$ (α_i = δυνατό αποτέλεσμα του π.τ.), τότε

  $$\Pr\{\mathrm{A}\} = \frac{|A|}{|\Omega|} = \frac{\text{ευνοϊκές περιπτώσεις}}{\text{δυνατές περιπτώσεις}}$$

  (τα στοιχεία του Α τα λέμε *ευνοϊκές περιπτώσεις* για την πραγματοποίηση του ενδεχόμενου Α και τα στοιχεία του Ω *δυνατές περιπτώσεις* του π.τ.). Σε μια τέτοια περίπτωση το π.τ. περιγράφεται συχνά ως ''τυχαία επιλογή ενός στοιχείου του Ω''.

Για παράδειγμα, ας θεωρήσουμε τη ρίψη ενός αμερόληπτου νομίσματος όπου η πιθανότητα να έρθει Κεφαλή είναι η ίδια με την πιθανότητα να έρθει Γράμματα, δηλαδή ίση με 1/2. Αν η ρίψη του νομίσματος γίνει n φορές, έχουμε την ομοιόμορφη κατανομή πιθανότητας ορισμένη επί του δ.χ. $\Omega = \{\text{Κ}, \Gamma\}^n$ με $|\Omega| = 2^n$. Κάθε δυνατό αποτέλεσμα του π.τ. μπορεί να παρασταθεί ως ένα στρινγκ μήκους n επί του {Κ, Γ} και το αντίστοιχο στοιχειώδες ενδεχόμενο πραγματοποιείται με πιθανότητα $1/2^n$. Το ενδεχόμενο

A = {εμφανίζονται ακριβώς m Κεφαλές και $n - m$ Γράμματα}

είναι ένα υποσύνολο του Ω με $|A| = \binom{n}{m}$, γιατί υπάρχουν $\binom{n}{m}$ στρινγκς μήκους n επί του {Κ, Γ} τα οποία περιέχουν ακριβώς m Κ. Επομένως η πιθανότητα του A είναι

$$\Pr\{A\} = \binom{n}{m} \Big/ 2^n \ .$$

Ιδιαίτερα χρήσιμες είναι οι ακόλουθες ιδιότητες:

1. $\Pr\{A^c\} = 1 - \Pr\{A\}$
2. $\Pr\{A \cup B\} = \Pr\{A\} + \Pr\{B\} - \Pr\{A \cap B\}$
1. $\Pr\{A \cup B\} \le \Pr\{A\} + \Pr\{B\}$

Αν για παράδειγμα, θεωρήσουμε το π.τ. της ρίψης δύο αμερόληπτων νομισμάτων, τότε κάθε ένα από τα τέσσερα δυνατά αποτελέσματα έχει πιθανότητα 1/4 και η πιθανότητα να έρθει τουλάχιστον ένα Κ είναι

$$\Pr\{\text{ΚΚ}, \text{ΚΓ}, \text{ΓΚ}\} = \Pr\{\text{ΚΚ}\} + \Pr\{\text{ΚΓ}\} + \Pr\{\text{ΓΚ}\} = 3/4$$

Διαφορετικά, θα μπορούσαμε να χρησιμοποιήσουμε το γεγονός ότι {ΚΚ, ΚΓ, ΓΚ} = {ΓΓ}^{c}, οπότε

$$\Pr\{\text{ΚΚ}, \text{ΚΓ}, \text{ΓΚ}\} = 1 - \Pr\{\Gamma\Gamma\} = 1 - 1/4 = 3/4.$$

Δεσμευμένη ή υπό συνθήκη πιθανότητα

Έστω Ω ένας δ.χ. και A, B δύο ενδεχόμενα με $\Pr\{B\} > 0$. Δεσμευμένη πιθανότητα του A με δεδομένο το B ονομάζουμε τον αριθμό,

$$\Pr\{A \mid B\} = \frac{\Pr\{A \cap B\}}{\Pr\{B\}}$$

ή την πιθανότητα του A με την προϋπόθεση ότι έχει ήδη πραγματοποιηθεί το B.

Αν και $\Pr\{A\} > 0$ τότε ορίζεται και η δεσμευμένη πιθανότητα του B με δεδομένο το A,

$$\Pr\{B \mid A\} = \frac{\Pr\{A \cap B\}}{\Pr\{A\}}$$

Αν θεωρήσουμε το παράδειγμα της ρίψης των δύο αμερόληπτων νομισμάτων και κάποιος μας πει ότι τουλάχιστον το ένα έχει φέρει Κ, τότε ποια είναι η πιθανότητα να έχουν φέρει και τα δύο Κ; Αν θεωρήσουμε ως ενδεχόμενο A να έχουν φέρει και τα δύο Κ και Β το ενδεχόμενο ένα τουλάχιστον έχει φέρει Κ, τότε $\Pr\{A \mid B\} = (1/4)/(3/4) = 1/3$.

- Αν $\Pr\{B\} > 0$, η απεικόνιση $\Pr_B\{\}: \wp(\Omega) \to \boldsymbol{R}$ τέτοια ώστε σε κάθε A του $\wp(\Omega)$ να αντιστοιχίζει τον αριθμό $\Pr_B\{A\} = \Pr\{A \mid B\}$, δηλ. η

  $$\wp(\Omega) \ni A \to \Pr_B\{A\} = \Pr\{A \mid B\}$$

  είναι μια κατανομή πιθανότητας. Πράγματι, είναι προφανές κατ' αρχήν ότι $0 \le \Pr_B\{A\} \le 1$. Επιπλέον,

  $$\Pr\{\Omega \mid B\} = \frac{\Pr\{\Omega \cap B\}}{\Pr\{B\}} = \frac{\Pr\{B\}}{\Pr\{B\}} = 1$$

  οπότε ικανοποιείται και η δεύτερη ιδιότητα/συνθήκη ορισμού της κατανομής πιθανότητας. Στην ουσία, επειδή $\Pr\{B \mid B\} = \Pr\{B\}/\Pr\{B\} = 1$, όλη η υπό συνθήκη πιθανότητα συγκεντρώνεται στο B. Έτσι μπορούμε να παραβλέψουμε όλα τα εκτός του B δυνατά αποτελέσματα και να θεωρήσουμε τις υπό συνθήκες πιθανότητες ως μια κατανομή πιθανότητας ορισμένη στο νέο σύνολο αναφοράς B. Για την τρίτη ιδιότητα/συνθήκη ορισμού, αν A_1, A_2 είναι δύο ασυμβίβαστα ενδεχόμενα, έχουμε

  $$\begin{aligned}
  \Pr\{A_1 \cup A_2\} &= \frac{\Pr\{(A_1 \cup A_2) \cap B\}}{\Pr\{B\}} \\
  &= \frac{\Pr\{(A_1 \cap B) \cup (A_2 \cap B)\}}{\Pr\{B\}} \\
  &= \frac{\Pr\{A_1 \cap B\} + \Pr\{A_2 \cap B\}}{\Pr\{B\}} \\
  &= \frac{\Pr\{A_1 \cap B\}}{\Pr\{B\}} + \frac{\mathrm{P}\{A_2 \cap B\}}{\Pr\{B\}} \\
  &= \Pr\{A_1 / B\} + \mathrm{P}\{A_2 / B\}
  \end{aligned}$$

  Επειδή οι δεσμευμένες πιθανότητες συνιστούν μια κατανομή πιθανότητας, όλες οι ιδιότητες των πιθανοτήτων παραμένουν ισχύουσες. Για παράδειγμα στη θέση της ανισότητας $\Pr\{A_1 \cup A_2\} \le \Pr\{A_1\} + \Pr\{A_2\}$, έχουμε την

$$\Pr\{A_1 \cup A_2/B\} \le \Pr\{A_1/B\} + \Pr\{A_2/B\}$$

- Είναι,

  $$\Pr\{A \cap B\} = \Pr\{A\} \cdot \Pr\{B/A\} = \Pr\{B\} \cdot \Pr\{A/B\}$$
  (***πολλαπλασιαστικός νόμος πιθανοτήτων***)

  όπως προκύπτει εύκολα από τους παραπάνω ορισμούς. Στην πράξη, σε πολλές περιπτώσεις συμβαίνει να ‘‘ξέρουμε’’ την πιθανότητα $\Pr\{B/A\}$ οπότε αν ‘‘ξέρουμε’’ και την πιθανότητα $\Pr\{A\}$, τότε ο παραπάνω τύπος μας δίνει την πιθανότητα $\Pr\{A$ **και** $B\}$.

- Είναι,

  $$\Pr\{A \cap B \cap \Gamma\} = \Pr\{A\} \cdot \Pr\{B/A\} \cdot \Pr\{\Gamma/A \cap B\}$$

  και γενικότερα,

  $$\Pr\{\bigcap_{i=1}^{n} A_i\} = \Pr\{A_1\} \cdot \Pr\{A_2/A_1\} \cdot \Pr\{A_3/A_1 \cap A_2\} \ldots \Pr\{A_n \Big/ \bigcap_{i=1}^{n} A_i\}.$$

- Αν ο δ. χ. Ω είναι ισοπίθανος τότε,

  $$\Pr\{B/A\} = \frac{|A \cap B|}{|A|}$$

- Αν A, B είναι ασυμβίβαστα ενδεχόμενα τότε,

  $$\Pr(B/A) = 0.$$

Ανεξάρτητα ενδεχόμενα

1. Τα ενδεχόμενα A, B του δ. χ. Ω λέγονται ***ανεξάρτητα***, αν και μόνον αν,

   $$\Pr\{A \cap B\} = \Pr\{A\} \cdot \Pr\{B\}$$

2. Ο ορισμός των ανεξάρτητων ενδεχομένων επεκτείνεται σε οσαδήποτε ενδεχόμενα: *n ενδεχόμενα ονομάζονται* ***ανεξάρτητα,*** *αν και μόνον αν, η τομή κάθε k-άδας ενδεχομένων* $(2 \le k \le n)$ *έχει πιθανότητα ίση με το γινόμενο των πιθανοτήτων των k ενδεχομένων*:

   $$\Pr\left\{\bigcap_{k \in S} A_k\right\} = \prod_{k \in S} \Pr\{A_k\} \quad \text{για κάθε υποσύνολο } S \text{ του } E_n = \{1, 2, \ldots, n\}$$

Από τα παραπάνω προκύπτει ότι:

- Αν A, B ανεξάρτητα ενδεχόμενα τότε,

  $\Pr\{A/B\} = \Pr\{A\}$ και $\Pr\{B/A\} = \Pr\{B\}$

  Δηλαδή, η πληροφορία ότι πραγματοποιήθηκε το ένα δεν επηρεάζει την πιθανότητα πραγματοποίησης του άλλου ενδεχομένου.

- Αν A, B ασυμβίβαστα με $\Pr\{A\} \neq 0$ και $\Pr\{B\} \neq 0$ τότε τα A, B δεν είναι ανεξάρτητα.

- Αν A, B ανεξάρτητα ενδεχόμενα τότε,

  i) A, B^c ανεξάρτητα
  ii) A^c, B^c ανεξάρτητα.

Θεώρημα Ολικής Πιθανότητας

Αν $A_1, A_2, \ldots, A_\mu$ είναι μια διαμέριση του δ. χ. Ω και A είναι ένα ενδεχόμενο τότε,

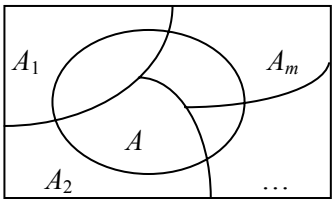
$$\Pr\{A\} = \Pr\{A_1\}\cdot\Pr\{A/A_1\} + \Pr\{A_2\}\cdot\Pr\{A/A_2\} + \ldots + \Pr\{A_m\}\cdot\Pr\{A/A_m\}$$

Πράγματι, επειδή $A_1, A_2, \ldots, A_m$ είναι μια διαμέριση του Ω έχουμε,

$A_i \cap A_j = \varnothing \quad i, j = 1, 2, \ldots, m$

και

$A_1 \cup A_2 \cup \ldots \cup A_m = \Omega$



Είναι τώρα,

$$A = A \cap \Omega = A \cap (A_1 \cup A_2 \cup \ldots \cup A_m) = (A \cap A_1) \cup (A \cap A_2) \cup \ldots \cup (A \cap A_m)$$

αλλά, $A \cap A_1, A \cap A_2, \ldots, A \cap A_m$ είναι ξένα ανά δύο γιατί,

$$(A \cap A_i) \cap (A \cap A_j) = A \cap (A_i \cap A_j) = A \cap \varnothing = \varnothing \quad i,j = 1, 2, \ldots, m$$

οπότε,

$$\Pr\{A\} = \Pr\{A \cap A_1\} + \Pr\{A \cap A_2\} + \ldots + \Pr\{A \cap A_m\}$$
$$= \Pr\{A_1\}\cdot\Pr\{A/A_1\} + \Pr\{A_2\}\cdot\Pr\{A/A_2\} + \ldots + \Pr\{A_m\}\cdot\Pr\{A/A_m\}.$$

- Αν $A_1, A_2, \ldots, A_m$ είναι μια διαμέριση του δ. χ. Ω με $\Pr\{A_k\} > 0$ για όλα τα k με $1 \leq k \leq m$, και A είναι ένα ενδεχόμενο, τότε

$$\Pr(A_k/A) = \frac{\Pr\{A_k\} \cdot \Pr\{A/A_k\}}{\Pr\{A_1\} \cdot \Pr\{A/A_1\} + \Pr\{A_2\} \cdot \Pr\{A/A_2\} + \cdots + \Pr\{A_m\} \cdot \Pr\{A/A_m\}}$$

(***Κανόνας του Bayes***)

Πράγματι είναι,

$$\Pr\{A_k/A\} = \frac{\Pr\{A_k \cap A\}}{\Pr\{A\}}$$

$$= \frac{\Pr\{A_k\} \cdot \Pr\{A/A_k\}}{\Pr\{A_1\} \cdot \Pr\{A/A_1\} + \Pr\{A_2\} \cdot \Pr\{A/A_2\} + \cdots + \Pr\{A_m\} \cdot \Pr\{A/A_m\}}.$$

Ο *κανόνας του Bayes* χρησιμοποιείται συχνά για εξαγωγή συμπεράσματος (inference). Υπάρχει ένας αριθμός ‘‘αιτίων’’ που μπορεί να έχουν ως συνέπεια ένα ‘‘αποτέλεσμα’’. Παρατηρούμε το αποτέλεσμα και θέλουμε να συμπεράνουμε το αίτιο. Τα ενδεχόμενα $A_1, A_2, \ldots, A_m$ συσχετίζονται με τα αίτια και το ενδεχόμενο A αντιπροσωπεύει το αποτέλεσμα. Η πιθανότητα $\Pr\{A/A_k\}$ ότι το αποτέλεσμα θα παρατηρηθεί όταν το αίτιο A_k είναι παρόν ισοδυναμεί με ένα πιθανοτικό μοντέλο της σχέσης αίτιο/αιτιατό. Δοθέντος ότι το ενδεχόμενο Α έχει πραγματοποιηθεί/παρατηρηθεί, θέλουμε να υπολογίσουμε την (υπό συνθήκη) πιθανότητα $\Pr\{A_i/A\}$ ότι το αίτιο A_i είναι παρόν.

Για παράδειγμα, ας υποθέσουμε ότι έχουμε ένα αμερόληπτο νόμισμα και ένα μεροληπτικό το οποίο πάντοτε φέρνει Κ. Εκτελούμε ένα π.τ. ως εξής: επιλέγουμε τυχαία ένα από τα δύο νομίσματα, ρίχνουμε το επιλεγέν νόμισμα μία φορά και στη συνέχεια το ρίχνουμε ξανά. Αν υποτεθεί ότι το επιλεγέν νόμισμα φέρνει και τις δύο φορές Κ, ποια είναι η πιθανότητα να είναι το μεροληπτικό;

Θα χρησιμοποιήσουμε τον κανόνα του Bayes. Έστω A_1 το ενδεχόμενο ότι επιλέγεται το μεροληπτικό νόμισμα και A το ενδεχόμενο ότι το νόμισμα φέρνει Κ δύο φορές. Θέλουμε να υπολογίσουμε την πιθανότητα $\Pr\{A_1/A\}$. Η διαμέριση του δ. χ. Ω που θεωρούμε, αποτελείται από τα A_1, $A_2 = A^c$. Έχουμε $\Pr\{A_1\} = 1/2$, $\Pr\{A/A_1\} = 1$, $\Pr\{A_2\} = 1/2$ και $\Pr\{A/A_2\} = 1/4$. Επομένως,

$$\Pr\{A_1/A\} \quad \frac{(1/2)\cdot 1}{(1/2)\cdot 1 + (1/2)\cdot(1/4)} = \frac{4}{5}.$$

Με αφορμή το τελευταίο παράδειγμα, να πούμε ότι επειδή τα σύνολα A και A^c αποτελούν μια διαμέριση του δ. χ. Ω, μια συνήθης μορφή του κανόνα του Bayes είναι η ακόλουθη (B είναι ένα ενδεχόμενο):

$$\Pr\{A \mid B\} = \frac{\Pr\{A\}\Pr\{B \mid A\}}{\Pr\{A\}\Pr\{B \mid A\} + \Pr\{A^c\}\Pr\{B \mid A^c\}}$$

- Αν $A_1, A_2, \ldots, A_k$ είναι μια διαμέριση του δ. χ. Ω και A ένα ενδεχόμενο τότε,

$$\Pr\{A_1 \cup A_2 \cup \ldots \cup A_k / A\} = \Pr\{A_1/A\} + \Pr\{A_2/A\} + \ldots + \Pr\{A_k/A\}$$

Πράγματι, επειδή

$A_i \cap A_j = \varnothing,\ i,j = 1, 2, \ldots, k \Rightarrow A \cap A_i\ ,\ A \cap A_j$ ασυμβίβαστα, γιατί

$$(A \cap A_i) \cap (A \cap A_j) = A \cap (A_i \cap A_j) = A \cap \varnothing = \varnothing$$

οπότε,

$$\Pr\{A_1 \cup A_2 \cup \ldots \cup A_k / A\} = \frac{\Pr\{(A_1 \cup A_2 \cup \ldots \cup A_\kappa) \cap A\}}{\Pr\{A\}}$$

$$= \frac{\Pr\{(A_1 \cap A) \cup (A_2 \cap A) \cup \cdots \cup (A_k \cap A)\}}{\Pr\{A\}}$$

$$= \frac{\Pr\{A_1 \cap A\} + \Pr\{A_2 \cap A\} + \cdots + \Pr\{A_k \cap A\}}{\Pr\{A\}}$$

$$= \frac{\Pr\{A_1 \cap A\}}{\Pr\{A\}} + \frac{\Pr\{A_2 \cap A\}}{\Pr\{A\}} + \cdots + \frac{\Pr\{A_\kappa \cap A\}}{\Pr\{A\}}$$

$$= \Pr\{A_1 / A\} + \Pr\{A_2 / A\} + \cdots + \Pr\{A_k / A\}.$$

Εφαρμογή Α.1 – Σε ένα πείραμα τύχης τα δυνατά αποτελέσματα είναι δύο. Το ένα ας το ονομάσουμε Ε: «επιτυχία» με πιθανότητα p και το άλλο ας το ονομάσουμε Α: «αποτυχία» με πιθανότητα q. Έστω ότι το πείραμα το επαναλαμβάνουμε n φορές διαδοχικά. Ποια είναι η πιθανότητα, στις n αυτές επαναλήψεις οι επιτυχίες να είναι k ($0 \le k \le n$);

Μια περίπτωση (διάταξη) αυτού του είδους είναι,

$$X: \underbrace{EE\ldots E}_{k}\ \underbrace{AA\ldots A}_{n-k}$$

Η πιθανότητά της, αφού κάθε αποτέλεσμα δεν επηρεάζεται από τα προηγούμενα, είναι:

$$\Pr\{X\} = \underbrace{\Pr\{E\} \cdot \Pr\{E\} \cdot \ldots \cdot \Pr\{E\}}_{k} \cdot \underbrace{\Pr\{A\} \cdot \Pr\{A\} \cdot \cdots \cdot \Pr\{A\}}_{n-k}$$

$$= \underbrace{p \cdot p \cdot \ldots \cdot p}_{k} \cdot \underbrace{q \cdot q \cdot \ldots \cdot q}_{n-k} = p^k \cdot q^{n-k}$$

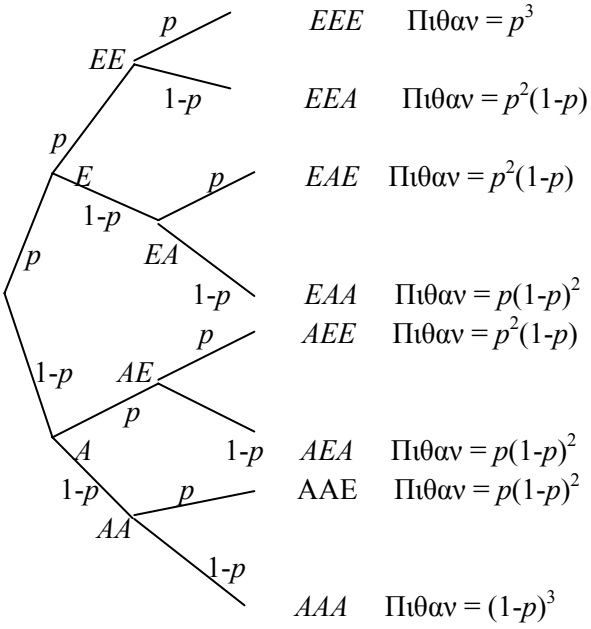
Επειδή όμως το πλήθος των περιπτώσεων (διατάξεων) με k φορές E και n-k φορές A είναι,

$$\binom{n}{k} \cdot \binom{n-k}{n-k} = \binom{n}{k}$$

η ζητούμενη πιθανότητα είναι,

$$\Pr\{n, k, p) = \binom{n}{k} \cdot p^k \cdot q^{n-k}$$

Για μια σειριακή περιγραφή του δ.χ. ενός τέτοιου πειράματος με 3 επαναλήψεις, έχουμε το δένδρο



Οι επαναλήψεις ενός τέτοιου πειράματος με τα δύο αποτελέσματα, «επιτυχία» - «αποτυχία», ονομάζονται ***ανεξάρτητες δοκιμές Bernoulli*** και δείξαμε ότι:

- Στις n ανεξάρτητες δοκιμές του Bernoulli, με πιθανότητα επιτυχίας p και αποτυχίας q, η πιθανότητα να έχουμε k επιτυχίες ($0 \le k \le n$) είναι,

$$\Pr\{n, k, p\} = \binom{n}{k} \cdot p^k \cdot q^{n-k} = \binom{n}{k} \cdot p^k \cdot (1-p)^{n-k}.$$

Την ίδια πιθανότητα έχουμε και στην παρακάτω περίπτωση π.τ. (θα μπορούσαμε να πούμε ότι έχουμε το ίδιο πρόβλημα διατυπωμένο διαφορετικά).

- Έστω $\Omega = \{\omega_1, \omega_2, \ldots, \omega_m\}$ ο δ.χ. ενός π.τ. με κατανομή πιθανότητας $\Pr\{\omega_1\} = p_1$, $\Pr\{\omega_2\} = p_2$, … , $\Pr\{\omega_m\} = p_m$ και $A \subseteq \Omega$ ένα ενδεχόμενο του π.τ. με $\Pr\{A\} = p$. Έστω επίσης οι ακέραιοι $k \le n$ με $k \ge 0$ και $n > 0$. Η πιθανότητα να πραγματοποιηθεί το A σε k ακριβώς από n επαναλήψεις του π.τ. είναι
  $\binom{n}{k} \cdot p^k \cdot q^{n-k}$._

Μια άλλη σημαντική εφαρμογή η οποία εξηγεί γιατί δουλεύουν οι λεγόμενες ***επιθέσεις γενεθλίων*** (birthday attacks) είναι η ακόλουθη.

Εφαρμογή Α.2 – Έστω $\Omega = \{1, 2, \ldots, n\}$ ο δ.χ. ενός π.τ. με ισοπίθανα απλά ενδεχόμενα, δηλ. με ομοιόμορφη κατανομή πιθανότητας

$\Pr\{i\} = 1/n$

Το π.τ. είναι τυχαία επιλογή, με επανάθεση, ενός στοιχείου του Ω και το ερώτημα είναι: ποια είναι η πιθανότητα, μετά από k δοκιμές, δύο τουλάχιστον αποτελέσματα να είναι ίδια; Αποδεικνύεται ότι στην περίπτωση αυτή

- η πιθανότητα, μετά από k δοκιμές, δύο τουλάχιστον αποτελέσματα να είναι ίδια, είναι *τουλάχιστον*

  $1 - e^{-\frac{1}{2}(k-1)k/n}$

  Επομένως, για

  $k > \sqrt{2 \ln 2}\sqrt{n}$

  η πιθανότητα ότι δύο αποτελέσματα θα είναι ίδια, είναι τουλάχιστον 1/2.

Παραλείποντας τις λεπτομέρειες (αφήνονται ως άσκηση), τα βασικά βήματα της απόδειξης των παραπάνω είναι τα ακόλουθα:

- Αν A είναι το ενδεχόμενο ‘‘μετά από k δοκιμές, κανένα αποτέλεσμα ίδιο’’ τότε το ενδεχόμενο ‘‘μετά από k δοκιμές, δύο τουλάχιστον αποτελέσματα ίδια’’ είναι A^c, οπότε $\Pr\{A^c\} = 1 - \Pr\{A\}$.
- $\Pr\{A\} = 1 \cdot \left(1 - \frac{1}{n}\right) \cdot \left(1 - \frac{2}{n}\right) \cdot \left(1 - \frac{3}{n}\right) \cdot \ldots \cdot \left(1 - \frac{k-1}{n}\right)$.

- $\ln(\Pr\{A\}) = \ln\left(1-\frac{1}{n}\right)+\ln\left(1-\frac{2}{n}\right)+\cdots+\ln\left(1-\frac{k-1}{n}\right)$

$$\le -\left(\frac{1}{n}+\frac{2}{n}+\cdots+\frac{k-1}{n}\right)$$

$$= -\left(\frac{\frac{1}{2}(k-1)k}{n}\right).$$

- $\Pr\{A\} \le e^{-\frac{1}{2}(k-1)k/n} \Rightarrow \Pr\{A^c\} \ge 1 - e^{-\frac{1}{2}(k-1)k/n}$.
- Για $k >> 1$, είναι $k(k-1) \approx k^2$, οπότε έχουμε κατά προσέγγιση,

$$\ln(\Pr\{A\}) \le -\frac{k^2}{2n}$$

Η πιθανότητα ότι ‘‘δύο από τα αποτελέσματα θα είναι ίδια’’ είναι μεγαλύτερη ή ίση από 1/2 όταν η πιθανότητα ‘‘όχι δύο είναι ίδια’’ είναι μικρότερη από 1/2. Έτσι, για δοσμένο n λύνουμε για να βρούμε το μικρότερο k τέτοιο ώστε

$$-\frac{k^2}{2n} < \ln\left(\frac{1}{2}\right)$$

και καταλήγουμε ότι, $k > \sqrt{2\ln 2}\sqrt{n}$._

Άσκηση (Birthday paradox): Δείξτε ότι σε μια ομάδα 23 ατόμων, η πιθανότητα τουλάχιστον δύο να έχουν την ίδια ημέρα γενεθλίων, είναι μεγαλύτερη από 1/2.

Τυχαία μεταβλητή

Μια *τυχαία μεταβλητή* (τ.μ.) είναι μια συνάρτηση από το δ. χ. Ω ενός π.τ. στο σύνολο των πραγματικών αριθμών.

ΠΑΡΑΔΕΙΓΜΑ Α.1 – Ρίχνουμε ένα νόμισμα τρεις φορές. Έστω $X(t)$ ο αριθμός των ‘‘Κ’’ (Κ = κεφαλή) που εμφανίζονται όταν το αποτέλεσμα είναι t.

Η τ.μ. παίρνει τις εξής τιμές:

$X(\text{ΚΚΚ}) = 3$
$X(\text{ΚΚΓ}) = X(\text{ΚΓΚ}) = X(\text{ΓΚΚ}) = 2$
$X(\text{ΓΓΚ}) = X(\text{ΓΚΓ}) = X(\text{ΚΓΓ}) = 1$

$X(\Gamma\Gamma\Gamma) = 0$

Να σημειώσουμε ότι η τ.μ. δεν είναι τυχαία και δεν είναι μεταβλητή αλλά συνάρτηση. Συσχετίζει έναν πραγματικό αριθμό με κάθε δυνατό αποτέλεσμα ενός π.τ. γεγονός που μας επιτρέπει να δουλεύουμε με την κατανομή πιθανότητας που προκύπτει στο δημιουργηθέν σύνολο αριθμών.

Για μια τυχαία μεταβλητή X και έναν πραγματικό αριθμό x, ορίζουμε το ενδεχόμενο $X = x$ να είναι το $\{w \in \Omega : X(w) = x\}$. Έτσι,

$$\Pr\{X = x\} = \sum_{\{w \in \Omega : X(w) = x\}} \Pr\{w\}.$$

Η συνάρτηση f με $f(x) = \Pr\{X = x\}$ είναι η ***συνάρτηση πυκνότητας πιθανότητας*** της τ.μ. X και από τις ιδιότητες ορισμού (αξιώματα) της πιθανότητας, είναι

$$\Pr\{\mathrm{X} = \mathrm{x}\} \geq 0 \quad \text{και} \quad \sum_x \Pr\{X = x\} = 1.$$

Είναι σύνηθες να ορίζονται μερικές τυχαίες μεταβλητές στον ίδιο δ.χ. Αν X και Y είναι τυχαίες μεταβλητές, η συνάρτηση f με

$$f(x, y) = \Pr\{X = x \text{ και } Y = y\}$$

είναι η ***από κοινού συνάρτηση πυκνότητας πιθανότητας*** των X και Y. Για μια συγκεκριμένη τιμή y,

$$\Pr\{Y = y\} = \sum_x \Pr\{X = x \text{ και } Y = y\}$$

και παρόμοια, για μια συγκεκριμένη τιμή x,

$$\Pr\{X = x\} = \sum_y \Pr\{X = x \text{ και } Y = y\}.$$

Χρησιμοποιώντας τον ορισμό της δεσμευμένης ή υπό συνθήκη πιθανότητας, έχουμε

$$\Pr\{X = x \mid Y = y\} = \frac{\Pr\{X = x \text{ και } Y = y\}}{\Pr\{Y = y\}}$$

Οι τυχαίες μεταβλητές X και Y σ' ένα δ.χ. Ω είναι ***ανεξάρτητες*** αν για όλους τους πραγματικούς αριθμούς x και y, τα ενδεχόμενα $X = x$ και $Y = y$ είναι ανεξάρτητα ή, ισοδύναμα, αν για όλα τα x και y έχουμε

$$\Pr\{X = x \text{ και } Y = y\} = \Pr\{X = x\} \cdot \Pr\{Y = y\}.$$

Για παράδειγμα, αν X_1 και X_2 είναι οι τυχαίες μεταβλητές στη ρίψη δύο ζαριών, με

$$X_1((i, j)) = i \quad \text{και} \quad X_2((i, j)) = j$$

έτσι ώστε X_1 να είναι η ένδειξη που εμφανίζεται στο πρώτο ζάρι και X_2 να είναι η ένδειξη που εμφανίζεται στο δεύτερο ζάρι, οι τυχαίες μεταβλητές X_1 και X_2 είναι ανεξάρτητες γιατί:

Αν $\Omega = \{1, 2, 3, 4, 5, 6\}$ και $i, j \in \Omega$, επειδή υπάρχουν 36 δυνατά αποτελέσματα (ισοπίθανα), θα έχουμε

$$\Pr\{X_1 = i \text{ και } X_2 = j\} = 1/36$$

Επιπλέον,

$$\Pr\{X_1 = i\} = 1/6 \text{ και } \Pr\{X_2 = j\} = 1/6$$

επειδή η πιθανότητα να εμφανιστεί το i στο πρώτο ζάρι και η πιθανότητα να εμφανιστεί το j στο δεύτερο ζάρι είναι και οι δύο 1/6. Επομένως

$$\Pr\{X_1 = i \text{ και } X_2 = j\} = 1/36 = (1/6)\cdot(1/6) = \Pr\{X_1 = i\} \cdot \Pr\{X_2 = j\}.\_$$

Η ***αναμενόμενη τιμή*** της τ.μ. X στο δ.χ. $\Omega = \{x_1, x_2, \ldots, x_n\}$, είναι

- $E[X] = \sum_x x \Pr\{X = x\}$

Στο παράδειγμα με τις τρεις ρίψεις του νομίσματος, αν X είναι η τ.μ. που αντιστοιχεί τον αριθμό των κεφαλών Κ σ' ένα δυνατό αποτέλεσμα, η αναμενόμενη τιμή θα είναι,

E[X] =

$$\frac{1}{8}\left(X(\text{ΚΚΚ}) + X(\text{ΚΚΓ}) + X(\text{ΚΓΚ}) + X(\text{ΓΚΚ}) + X(\text{ΓΓΚ}) + X(\text{ΓΚΓ}) + X(\text{ΚΓΓ}) + X(\text{ΓΓΓ})\right)$$

$$= \frac{1}{8}(3 + 2 + 2 + 2 + 1 + 1 + 1 + 0) = \frac{12}{8} = \frac{3}{2}$$

ΠΑΡΑΔΕΙΓΜΑ Α.2 – Ας βρούμε την αναμενόμενη τιμή του αθροίσματος των ενδείξεων στη ρίψη των δύο ζαριών.

Η τ.μ. X είναι το άθροισμα των ενδείξεων και είναι:

$X((1,1)) = 2$
$X((1,2)) = X((2,1)) = 3$
$X((1,3)) = X((3,1)) = X((2,2)) = 4$
$X((1,4)) = X((4,1)) = X((2,3)) = X((3,2)) = 5$
$X((1,5)) = X((5,1)) = X((2,4)) = X((4,2)) = X((3,3)) = 6$
$X((1,6)) = X((6,1)) = X((2,5)) = X((5,2)) = X((3,4)) = X((4,3)) = 7$
$X((2,6)) = X((6,2)) = X((3,5)) = X((5,3)) = X((4,4)) = 8$
$X((3,6)) = X((6,3)) = X((4,5)) = X((5,4)) = 9$

$X((4,6)) = X((6,4)) = X((5,5)) = 10$
$X((5,6)) = X((6,5)) = 11$
$X((6,6)) = 12$

Δηλαδή το σύνολο τιμών της X είναι το σύνολο {2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12}. Τώρα έχουμε,

$\Pr\{X = 2\} = \Pr\{X = 12\} = 1/36$
$\Pr\{X = 3\} = \Pr\{X = 11\} = 2/36$
$\Pr\{X = 4\} = \Pr\{X = 10\} = 3/36$
$\Pr\{X = 5\} = \Pr\{X = 9\} = 4/36$
$\Pr\{X = 6\} = \Pr\{X = 8\} = 5/36$
$\Pr\{X = 7\} = 6/36$

οπότε

$$E[X] = 2\cdot(1/36) + 3\cdot(2/36) + 4\cdot(3/36) + 5\cdot(4/36) + 6\cdot(5/36) + 7\cdot(6/36) + 8\cdot(5/36) + 9\cdot(4/36) + 10\cdot(3/36) + 11\cdot(2/36) + 12\cdot(1/36) = 7.\_$$

Αν X είναι μια τ.μ. μια οποιαδήποτε συνάρτηση $g(x)$ ορίζει μια νέα τ.μ. $g(X)$. Αν τώρα ορίζεται η αναμενόμενη τιμή της $g(X)$, τότε

$$E[g(X)] = \sum_x g(x)\Pr\{X = x\}$$

Θέτοντας $g(x) = ax + b$ με $a, b \in \boldsymbol{R}$ έχουμε

$$E[aX] = aE[X] + b$$

Αποδεικνύεται επίσης, ότι αν X και Y είναι τυχαίες μεταβλητές σ' ένα δ.χ. Ω, τότε

$$E[X + Y] = E[X] + E[Y].$$

Επιπλέον, αν X_i, $i = 1, 2, \ldots, n$, $n \in \boldsymbol{N}^*$, είναι τυχαίες μεταβλητές στον δ.χ Ω και $X = X_1 + X_2 + ... + X_n$,τότε

$$E[X] = E[X_1] + E[X_2] + ... + E[X_n]$$

Για παράδειγμα, χρησιμοποιώντας τους παραπάνω τύπους στον υπολογισμό της αναμενόμενης τιμής του αθροίσματος των ενδείξεων που εμφανίζονται στη ρίψη των δύο ζαριών, έχουμε:

$$E[X_1] = E[X_2] = 7/2$$

επειδή και οι δύο είναι ίσες με $(1 + 2 + 3 + 4 + 5 + 6)/6 = 21/6 = 7/2$. Το άθροισμα των δύο αριθμών που εμφανίζονται όταν ρίχνονται τα δύο ζάρια, είναι το άθροισμα $X_1 + X_2$, συνεπώς

$E[X_1 + X_2] = E[X_1 + X_2] = (7/2) + (7/2) = 7$._

Αποδεικνύεται εύκολα ότι αν X και Y είναι ανεξάρτητες μεταβλητές σ' ένα δ.χ. Ω, τότε

$E[XY] = E[X]\cdot E[Y]$.

Διακύμανση

Η αναμενόμενη τιμή μιας τυχαίας μεταβλητής μας λέει για τη μέση της τιμή αλλά δε μας λέει τίποτα για το πως είναι οι τιμές της κατανεμημένες. Η διακύμανση της τ.μ. μας βοηθάει να προσδιορίζουμε πόσο ευρέως διασπαρμένη είναι μια τυχαία μεταβλητή.

Έστω X μια τ.μ. σ' ένα δ.χ. Ω. Η ***διακύμανση*** της X, συμβολικά Var[X], είναι

$$\mathrm{Var}[X] = \sum_x \left(X - E[x]\right)^2 \Pr\{X = x\}$$

και η ***τυπική απόκλιση*** της X, συμβολικά σ_X, είναι $\sqrt{\mathrm{Var}[X]}$.

Αν X είναι μια τ.μ. σ' ένα δ.χ. Ω και $a \in \boldsymbol{R}$, τότε αποδεικνύεται ότι

$\mathrm{Var}[X] = E[X^2] - E[X]^2$

και

$\mathrm{Var}[aX] = a^2\mathrm{Var}[X]$.

Αποδεικνύεται επίσης ότι αν X και Y είναι δύο ανεξάρτητες τ.μ. σ' ένα δ.χ. Ω, τότε $\mathrm{Var}[X + Y] = \mathrm{Var}[X] + \mathrm{Var}[Y]$. Επιπλέον, αν X_i, $i = 1, 2, \ldots, n$, $n \in \boldsymbol{N}^*$, είναι ανά δύο ανεξάρτητες τ.μ. στον Ω, τότε

- $\mathrm{Var}[X_1 + X_2 + \ldots + X_n] = \mathrm{Var}[X_1] + \mathrm{Var}[X_2] + \ldots + \mathrm{Var}[X_n]$.

Ο υπολογισμός της πολυπλοκότητας μέσης περίπτωσης, ενός αλγόριθμου, μπορεί να θεωρηθεί ως υπολογισμός της αναμενόμενης τιμής μιας τυχαίας μεταβλητής. Έστω ο δ.χ ενός π.τ. να είναι το σύνολο εισερχομένων a_j, $j = 1, 2, \ldots, n$ και έστω η τ.μ. X που αναθέτει στην a_j τον αριθμό των πράξεων που έγιναν από τον αλγόριθμο, όταν δίνεται η a_j ως είσοδος. Βασιζόμενοι στη γνώση μας της εισόδου, αναθέτουμε μια πιθανότητα $\Pr\{a_j\}$ σε κάθε δυνατή τιμή εισόδου a_j. Τότε, η πολυπλοκότητα μέσης περίπτωσης, του αλγόριθμου, είναι

$$E(X) = \sum_{j=1}^{n} \Pr\{a_j\}\, X(a_j)$$

που δεν είναι άλλη από την αναμενόμενη τιμή της τ.μ. X.