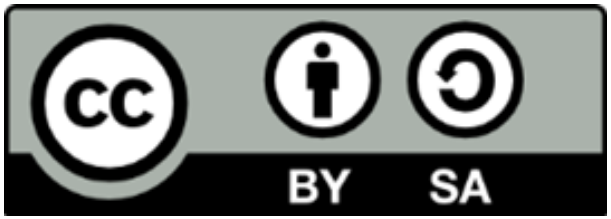
Υπολογιστικά & Διακριτά Μαθηματικά

Ενότητα 9: Εσωτερική πράξη και κλάσεις ισοδυναμίας - Δομές – Ισομορφισμοί

Στεφανίδης Γεώργιος
Τμήμα Εφαρμοσμένης Πληροφορικής

Άδειες Χρήσης

- Το παρόν εκπαιδευτικό υλικό υπόκειται σε άδειες χρήσης Creative Commons.
- Για εκπαιδευτικό υλικό, όπως εικόνες, που υπόκειται σε άλλου τύπου άδειας χρήσης, η άδεια χρήσης αναφέρεται ρητώς.



Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «Ανοικτά Ακαδημαϊκά Μαθήματα στο Πανεπιστήμιο Μακεδονίας» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.

Εσωτερική πράξη και κλάσεις ισοδυναμίας [1]

- Μια σχέση ισοδυναμίας ~ στο σύνολο A λέγεται ότι είναι **συμβιβαστή** με την εσωτερική πράξη $*$ στο A, αν ισχύει

$$a_1 \sim a_2 \text{ και } b_1 \sim b_2 \Rightarrow (a_1 * b_1) \sim (a_2 * b_2)$$

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

$$[a] * [b] = [a * b].$$

- Παράδειγμα:

  Η σχέση "$\equiv \pmod 3$" ορίζει, όπως έχουμε πει, τις ακόλουθες κλάσεις καταλοίπων modulo 3 στο $\mathbb{Z}$:

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

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

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

  δηλαδή το σύνολο E είναι το σύνολο $\mathbb{Z}_3 = \{[0], [1], [2]\}$.

Εσωτερική πράξη και κλάσεις ισοδυναμίας [2]

- Η παραπάνω σχέση μπορούμε να δούμε εύκολα ότι είναι συμβιβαστή με την πρόσθεση και τον πολλαπλασιασμό στο $\mathbb{Z}$, οπότε μπορούμε να ορίσουμε στο $\mathbb{Z}_3$ πρόσθεση + και πολλαπλασιασμό · με τις ισότητες

$$[a] + [b] = [a + b] , \quad [a] \cdot [b] = [a \cdot b]$$

- 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 $a \in [2]$ και $b \in [1]$, δηλαδή $a = 3k + 2$ και $b = 3\ell + 1$, τότε $a + b = 3(k + \ell + 1) = 3m$, $(k, \ell, m \in \mathbb{Z})$, δηλαδή $a + b \in [0]$.

➢ $[2] \cdot [1] = [2 \cdot 1] = [2]$, γιατί αν $a \in [2]$ και $b \in [1]$, δηλαδή $a = 3k + 2$ και $b = 3\ell + 1$, τότε $a \cdot b = 3(3k\ell + 2\ell + k) + 2 = 3m + 2$, $(k, \ell, m \in \mathbb{Z})$, δηλ. $a \cdot b \in [2]$.

Ομάδες [1]

- Ένα σύνολο G εφοδιασμένο με την πράξη $*$ λέγεται **ομάδα**, όταν η πράξη $*$ είναι ***προσεταιριστική***, υπάρχει το ***ουδέτερο στοιχείο*** $e \in G$ ως προς την πράξη $*$ και κάθε στοιχείο του G έχει ***συμμετρικό*** ή *αντίστροφο* στοιχείο.
- Ώστε, η δομή $(G, *)$, είναι ομάδα, όταν:

1) $\forall a, b, c \in G, \quad (a * b) * c = a * (b * c)$
2) $\exists\, e \in G, \forall a \in G, \quad a * e = e * a = a$
3) $\forall a \in G, \exists\, a' \in G, \quad a * a' = a' * a = e$

- Αν επιπλέον η πράξη $*$ είναι αντιμεταθετική, τότε η δομή $(G, *)$ λέγεται *αντιμεταθετική ή* ***αβελιανή ομάδα***, δηλαδή όταν επιπλέον:

4) $\forall a, b \in G, \quad a * b = b * a$

Ομάδες [2]

- Σε μια ομάδα $(G, *)$ αποδεικνύεται ότι ισχύουν οι παρακάτω ιδιότητες:

1. Το ουδέτερο στοιχείο $e \in G$ είναι μοναδικό.
2. Κάθε στοιχείο του συνόλου G έχει ένα μόνο συμμετρικό στοιχείο ως προς την πράξη $*$. Επιπλέον,

$$\forall a, b \in G, (a * b)' = b' * a'$$

3. Κάθε στοιχείο $\alpha \in G$ είναι απλοποιήσιμο, που σημαίνει ότι

$$\forall a, b, c \in G\ ,\ a * b = a * c \Rightarrow b = c \quad \text{και} \quad b * a = c * a \Rightarrow b = c$$

4. Αν $a, b \in G$, τότε η εξίσωση

$$a * x = b$$

έχει μοναδική λύση στο G, την

$$x = a' * b$$

Παράδειγμα [1]

- Στο σύνολο $A = \{x \in \mathbb{R}: -1 < x < 1\}$ ορίζουμε την πράξη $*$ με

$$x * y = \frac{x+y}{1+x\cdot y}$$

- όπου + και · είναι η πρόσθεση και ο πολλαπλασιασμός πραγματικών αριθμών. Μπορούμε να δούμε ότι

i. Η πράξη $*$ είναι εσωτερική στο σύνολο A.

ii. Η δομή $(A, *)$ είναι μια αβελιανή ομάδα.

- Πράγματι: $\left|\frac{x+y}{1+xy}\right| < 1 \Leftrightarrow |x+y| < |1+xy| \Leftrightarrow (x+y)^2 < (1+xy)^2$

i) Είναι,

$$\Leftrightarrow x^2 + y^2 + 2xy < 1 + x^2y^2 + 2xy$$
$$\Leftrightarrow x^2 + y^2 - 1 - x^2y^2 < 0$$
$$\Leftrightarrow \left(x^2 - 1\right)\left(1 - y^2\right) < 0$$

- που ισχύει, διότι

$$|x| < 1 \Leftrightarrow x^2 < 1 \Leftrightarrow x^2 - 1 < 0$$
$$|y| < 1 \Leftrightarrow y^2 < 1 \Leftrightarrow 1 - y^2 > 0$$

Παράδειγμα [2]

- Άρα, για κάθε $x, y \in A$, είναι $x * y \in A$.

ii) Η πράξη $*$ είναι προσεταιριστική, διότι

$$(x * y) * z = \frac{x+y}{1+xy} * z = \frac{\frac{x+y}{1+xy} + z}{1 + \frac{x+y}{1+xy} z} = \frac{x+y+z(1+xy)}{1+xy+(x+y)z} = \frac{x+y+z+xyz}{1+xy+xz+yz}$$

και

$$x * (y * z) = x * \frac{y+z}{1+yz} = \frac{x + \frac{y+z}{1+yz}}{1 + x\frac{y+z}{1+yz}} = \frac{x(1+yz)+y+z}{1+yz+x(y+z)} = \frac{x+y+z+xyz}{1+xy+xz+yz}$$

➢ δηλαδή, $\forall\, x, y, z \in A$ ισχύει, $(x * y) * z = x * (y * z)$

Παράδειγμα [3]

- Η πράξη $*$ είναι αντιμεταθετική, διότι

$$x * y = \frac{x+y}{1+xy} \quad \text{και} \quad y * x = \frac{y+x}{1+yx}$$

➢ δηλαδή, $\forall\, x, y \in A$ ισχύει, $x * y = y * x$.

- Η πράξη $*$ έχει ουδέτερο στοιχείο, διότι

$$\forall\, x \in A,\ x * e = x \Leftrightarrow \frac{x+e}{1+xe} = x \Leftrightarrow x + e = x + x^2 e \Leftrightarrow \left(1 - x^2\right) e = 0 \Leftrightarrow e = 0$$

➢ δηλαδή, το 0 είναι το ουδέτερο στοιχείο της πράξης $*$.

- Κάθε στοιχείο του A έχει συμμετρικό, διότι $x * x' = e \Leftrightarrow \frac{x+x'}{1+xx'} = 0 \Leftrightarrow x + x' = 0 \Leftrightarrow x' = -x$

➢ δηλ., κάθε στοιχείο x του A έχει συμμετρικό στοιχείο το $-x \in A$ ($|-x| = |x| < 1$)

Δακτύλιοι – Σώματα [1]

- Ένα σύνολο R εφοδιασμένο με τις πράξεις + και · λέγεται **δακτύλιος**, όταν η δομή $(R, +)$ είναι αβελιανή προσθετική ομάδα, ο πολλαπλασιασμός είναι προσεταιριστικός και ο πολλαπλασιασμός είναι επιμεριστικός ως προς την πρόσθεση.
- Αν επιπλέον ο πολλαπλασιασμός είναι αντιμεταθετικός, τότε ο δακτύλιος $(R, +, \cdot)$ λέγεται **αντιμεταθετικός δακτύλιος**, και όταν υπάρχει ουδέτερο ή μοναδιαίο στοιχείο ως προς τον πολλαπλασιασμό, τότε λέγεται **δακτύλιος με μοναδιαίο στοιχείο**.
- Ένα σύνολο F εφοδιασμένο με τις πράξεις + και · λέγεται **σώμα**, όταν η δομή $(F, +, \cdot)$ είναι *μη μηδενικός αντιμεταθετικός δακτύλιος*, και η δομή $(F^*, \cdot)$ με $F^* = F - \{0\}$ είναι πολλαπλασιαστική ομάδα.

Δακτύλιοι – Σώματα [2]

- ***Πεπερασμένο σώμα*** είναι ένα σώμα $(F, +, \cdot)$ όπου το F περιέχει ένα πεπερασμένο πλήθος στοιχείων. Το πλήθος των στοιχείων του F είναι η ***τάξη*** του σώματος.
- Το πεπερασμένο σώμα τάξης p^n συμβολίζεται συνήθως με $\mathbb{F}_{p^n}$ ή $GF(p^n)$. Το απλούστερο πεπερασμένο σώμα είναι το $GF(2)$. Οι αριθμητικές πράξεις σ' αυτό συνοψίζονται εύκολα στους ακόλουθους πίνακες

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

a	$-a$	a^{-1}
0	0	–
1	1	1

- Πρέπει να παρατηρήσουμε ότι

✓ η πρόσθεση είναι ισοδύναμη με την πράξη XOR και

✓ ο πολλαπλασιασμός είναι ισοδύναμος με τη λογική (Boolean) πράξη AND.

- Επίσης η πρόσθεση είναι ισοδύναμη με την αφαίρεση, αφού

$$\forall a, b \in GF(2),\ b + a = b + (-a) = b - a.$$

Τέλος Ενότητας

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
ΕΣΠΑ 2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης