

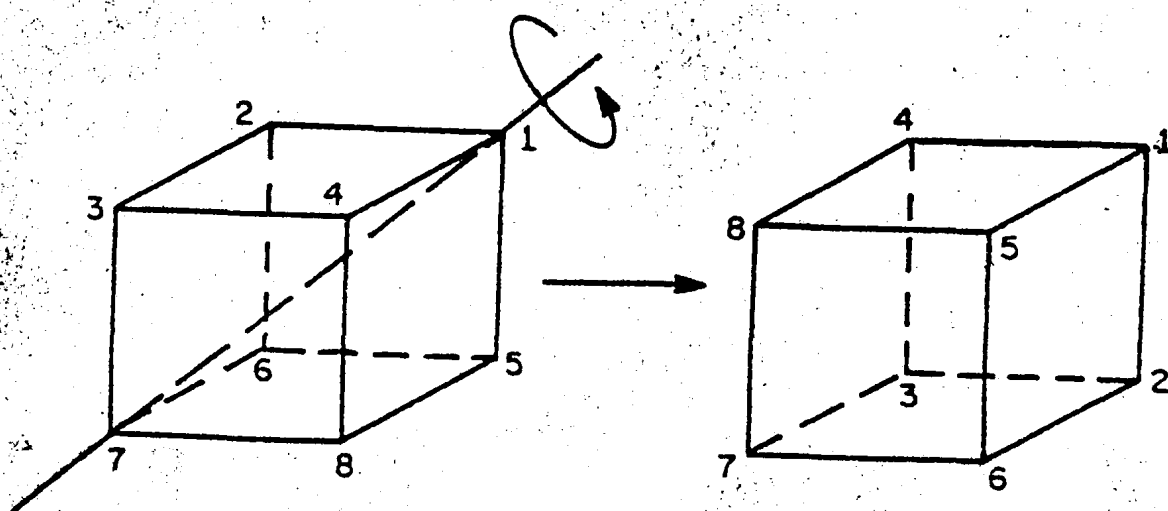
Α. ΦΥΡΑΡΙΔΗ

Επικούρου Καθηγητή

Κ. ΜΕΣΗ

Λέκτορα

αλγεβρικές δομές I



Ιωάννινα 1990



ΒΙΒΛΙΟΘΗΚΗ
ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΙΩΑΝΝΙΝΩΝ

026000028410

207/96



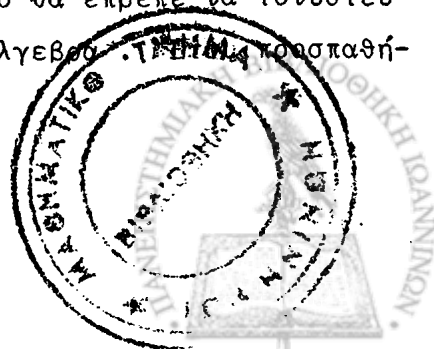
ΠΡΟΛΟΓΟΣ

Με τον όρο "αλγεβρικές δομές" νοούμε σύνολα εφοδιασμένα με πράξεις , ενώ δύο αλγεβρικές δομές A και B του "ίδιου τύπου" καλούνται ισομορφες , αν υπάρχει 1-1 και επί απεικόνιση από το σύνολο A στο B , η οποία διατηρεί τις πράξεις τους (ισομορφισμός) . Έτσι η Άλγεβρα θεωρείται ως η μέλετη εκείνων των ιδιοτήτων των αλγεβρικών δομών οι οποίες παραμένουν αναλλοίωτες υπεράνω των ισομορφισμών (τέτοιες ιδιότητες καλούνται αλγεβρικές) . Από αλγεβρική σκοπιά οι ισομορφες αλγεβρικές δομές μπορούν να θεωρηθούν ίσες ή ίδιες , αφού το μόνο στο οποίο διαφέρουν είναι η φύση των στοιχείων τους . Στην περίπτωση αυτή χρησιμοποιείται η φράση "αυτές είναι ίσες κατά προσέγγιση ισομορφισμού" .

Εξαιρετικό ενδιαφέρον παρουσιάζουν οι αλγεβρικές δομές των οποίων τα στοιχεία , σε σχέση με τις πράξεις , ικανοποιούν ορισμένες ταυτότητες (π.χ. μονοειδή , ομάδες , δακτύλιοι , σώματα , R -μόδουλα κ.λ.π.) . Οι δομές αυτές εμφανίζονται συχνά στην πράξη και έπαιξαν βασικό ρόλο στην ανάπτυξη της Μαθηματικής Επιστήμης .

Εδώ θα αναπτύξουμε τα βασικότερα θέματα της θεωρίας μονοειδών , ομάδων , δακτυλίων και σωμάτων , σύμφωνα με την ύλη που περιέχει το πρόγραμμα σπουδών του Μαθηματικού Τμήματος του Πανεπιστημίου Ιωαννίνων για το μόνο υποχρεωτικό και εισαγωγικό εξαμηνιαίο μάθημα στις αλγεβρικές δομές . Ακολουθώντας το πρόγραμμα σπουδών , προσπαθήσαμε να εφοδιάσουμε τους φοιτητές μ'ένα επαρκές ποσό αποτελεσματικών γνώσεων πάνω στην ύλη αυτή για τις δομές , παρ'όλο ότι υπάρχουν διάφορες απόψεις για το πόσο μπορεί κανείς να προχωρήσει στην ανάπτυξη των αλγεβρικών θεωριών σ'ένα τέτοιο διδακτικό βιβλίο . Πιστεύουμε ότι κάθε περαιτέρω συντόμευση ή θα παρέλειπε πολλά , με αποτέλεσμα επιφανειακή μόνο γνώση του αντικειμένου , ή θα είχε μια πυκνότητα και ψυχρότητα στο ύφος , πράγμα που απωθεί τον αρχάριο φοιτητή και κάνει το αντικείμενο προσιτό μόνο σε λίγους .

Είναι γεγονός ότι οι αφηρημένες έννοιες προκύπτουν όλες από την ανάλυση συγκεκριμένων καταστάσεων . Κρίνουμε ότι το γεγονός αυτό θα έπρεπε να τονιστεί ιδιαίτερα στο εισαγωγικό αυτό βιβλίο στην Αφηρημένη Άλγεβρα .



σαμε να εξηγήσουμε τις διάφορες έννοιες και τα αντικειμενικά κίνητρά τους , παραθέτοντας μετά από κάθε νέο όρο όσο το δυνατό περισσότερα παραδείγματα και παρατηρήσεις .

Στο κεφάλαιο 0 γίνεται μια αναδρομή σε βασικές έννοιες που θα χρειαστούν στα επόμενα και δίνουμε ιδιαίτερη έμφαση στην έννοια της σχέσης ισοδυναμίας , έννοια κεντρικής σημασίας για τα Μαθηματικά .

Στο κεφάλαιο I παρουσιάζονται τα βασικά από τη θεωρία των μονοειδών . Τα μονοειδή είναι η απλούστερη μορφή αλγεβρικής δομής που μελετάμε και αποτελούν ένα εισαγωγικό βήμα για την πληρέστερη κατανόηση των ομάδων . Η μεγάλη σημασία τους όμως διαπιστώθηκε τα τελευταία χρόνια με την ανάπτυξη της Πληροφορικής και αποτέλεσε τη βάση για την αλγεβρική θεμελίωση της θεωρητικής Πληροφορικής . Για το σκοπό αυτό ολόκληρη η §5 είναι αφιερωμένη στις εφαρμογές των μονοειδών στις Γλώσσες και στα Αυτόματα .

Χωρίς να επιχειρείται αξιολόγηση μαθηματικών εννοιών , πιστεύουμε ότι τα μονοειδή και οι ομάδες είναι από τις σημαντικότερες μαθηματικές έννοιες . Σε πολλούς αλγεβριστές έχει ωριμάσει πλέον η ιδέα ότι τα μονοειδή και οι εφαρμογές τους μπορεί και πρέπει να αποτελέσουν ξεχωριστό μάθημα σε κάθε καλό και σύγχρονο πρόγραμμα αλγεβρικών μαθημάτων .

Στο κεφάλαιο II μελετάμε τις ομάδες . Η θεωρία των ομάδων αναπτύχθηκε τα τελευταία 150 χρόνια παρ'όλο ότι παραδείγματα ομάδων συναντά κανείς από την εποχή της αρχικής μελέτης των μαθηματικών .

Από τη σκοπιά της θεωρίας ομάδων :

Οι διάφορες Γεωμετρίες μπορούν να θεωρηθούν ως η μελέτη εκείνων των ιδιοτήτων που παραμένουν αναλλοίωτες υπεράνω των μετασχηματισμών που είναι στοιχεία κατάλληλων ομάδων . Η ταξινόμηση αυτή προτάθηκε από τον Felix Klein (1849-1925) στο ονομαζόμενο "πρόγραμμα του Erlangen" (π.χ. η Ευκλείδεια Γεωμετρία περιγράφεται από την ομάδα των ισομετριών) .



Η ταξινόμηση των διαφορετικών εξισώσεων μέσω της θεωρίας ομάδων είναι δυνατή και προσφέρει νέες μεθόδους λύσεων , όπως έδειξε ο S. Lie (1842-1899) .

Η θεωρία ομάδων έχει εφαρμογές και σε άλλους κλάδους Επιστημών εκτός των Μαθηματικών . Ενδεικτικά αναφέρουμε ότι στη Φυσική και Χημεία έχουμε εφαρμογές σε προβλήματα ατομικής και μοριακής δομής . Για παράδειγμα , οι ομάδες Lorentz παίζουν βασικό ρόλο στη θεωρία σχετικότητας , ενώ στην κρυσταλλογραφία έχουμε όλες τις πιθανές μορφές κρυστάλλων δια μέσου των ομάδων συμμετρίας .

Στο κεφάλαιο III παρουσιάζονται οι δακτύλιοι και τα σώματα . Βασική έννοια στη θεωρία δακτυλίων είναι αυτή του ιδεώδους , που προέκυψε κατά τη θεμελίωση της αλγεβρικής θεωρίας αριθμών . Με τα ιδεώδη εξετάζεται η δομή των δακτυλίων . Από την άλλη μεριά , η θεωρία σωμάτων προέκυψε από την ανάγκη επιλύσεως εξισώσεων . Στη διερεύνηση της ύπαρξης και υπολογισμού των λύσεων εξισώσεως υπάρχει στενή αλληλεπίδραση μεταξύ των θεωριών σωμάτων και ομάδων , γνωστή ως θεωρία Galois (E.Galois (1811-1832)) . Η θεωρία δακτυλίων και σωμάτων έχει πολλές εφαρμογές και σ' άλλους κλάδους των Μαθηματικών .

Κάθε κεφάλαιο χωρίζεται σε παραγράφους . Για τα θεωρήματα , προτάσεις , πορίσματα και τις σχέσεις η αρίθμηση είναι ενιαία για κάθε κεφάλαιο , ενώ η αρίθμηση των παραδειγμάτων είναι ενιαία σε κάθε κεφάλαιο .

Στην αρχή του βιβλίου υπάρχει αναλυτικός πίνακας των περιεχομένων και στις τελευταίες σελίδες του υπάρχει ευρετήριο όρων , πίνακας συμβόλων και βιβλιογραφία , την οποία μπορεί ο αναγνώστης να χρησιμοποιήσει για περαιτέρω μελέτη των αλγεβρικών δομών .

Προσπαθήσαμε οι ατέλειες του συγγράμματος αυτού να περιοριστούν στο ελάχιστο . Γι' αυτό , παρακαλούμε τους αναγνώστες οι οποίοι θα αντιληφθούν τυχόν ατέλειες , παραλείψεις ή σφάλματα να μας τα υποδείξουν ώστε να τα λάβουμε υπόψη .

Τέλος , ευχαριστούμε θερμά τη γραμματέα του Τομέα Άλγεβρας και Γεωμε-



τρίας κ. Αθηναΐδα Δούβλη για την επιμελημένη δακτυλογράφηση του κειμένου .

Α.ΦΥΡΑΡΙΔΗΣ - Κ.ΜΕΕΗΣ

Ιωάννινα 1990



ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Πρόλογος

ΚΕΦΑΛΑΙΟ 0

ΕΙΣΑΓΩΓΗ

§1	Σύνολα	5
§2	Καρτεσιανό γινόμενο συνόλων . Σχέσεις	8
§3	Απεικονίσεις	9
§4	Σχέσεις ισοδυναμίας	17
§5	Πράξεις	27

ΚΕΦΑΛΑΙΟ I

ΜΟΝΟΕΙΔΗ

§1.1	Μονοειδή	34
§1.2	Υπομονοειδή	37
§2	Μονοειδές πηλύκο	39
§3	Ομομορφισμοί μονοειδών	39
§4	Ελεύθερα μονοειδή	46
§5	Εφαρμογές στα αυτόματα και στις γλώσσες	54

ΚΕΦΑΛΑΙΟ II

ΟΜΑΔΕΣ

§1.1	Ομάδες	66
------	--------------	----



§1.2 Στοιχειώδεις ιδιότητες των ομάδων	70
§2.1 Υποομάδες	72
§2.2 Παραγόμενες υποομάδες	79
§2.3 Ομάδα μεταθέτης	82
§3.1 Supremum δύο υποομάδων	83
§4 Ομομορφισμοί ομάδων	87
§5.1 Κυκλικές ομάδες	95
§5.2 Υποομάδες των πεπερασμένων κυκλικών ομάδων	104
§6.1 Ομάδες μεταθέσεων	109
§6.2 Η συμμετρική ομάδα n -βαθμού	111
§6.3 Κύκλοι-μεταβάσεις	118
§6.4 Συστήματα μεταθέσεων που παράγουν την S_n	127
§6.5 Η εναλλάσσουσα ομάδα βαθμού n , A_n	129
§7 Θεώρημα Lagrange	131
§8 Κανονικές υποομάδες	139
§9 Ομάδα πηλίκο	150
§10 Θεωρήματα ισομορφισμών	156

ΚΕΦΑΛΑΙΟ ΙΙΙ

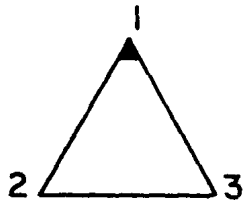
ΔΑΚΤΥΛΙΟΙ-ΣΩΜΑΤΑ

§1.1 Δακτύλιο	170
§1.2 Στοιχειώδεις διδιδιότητες δακτυλίων	174
§2 Σώματα	181
§3 Χαρακτηριστική δακτυλίου	189
§4 Υποδακτύλιοι	193
§5 Υποσώματα	198
§6.1 Ομομορφισμοί δακτυλίων	200
§6.2 Ομομορφισμοί σωμάτων	210
§7 Το σώμα κλασμάτων πεδίου ακεραιότητας	212
§8.1 Ιδεώδη	218
§8.2 Παραγόμενα ιδεώδη	224

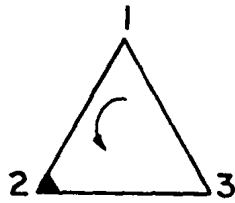


§8.3	Supremum ιδεωδών	228
§8.4	Δακτύλιοι κυρίων ιδεωδών	229
§8.5	Πράξεις επί των ιδεωδών	233
§8.6	Δακτύλιος πηλίκου	236
§8.7	Θεωρήματα ισομορφισμών	241
§8.8	Πρωτοσώματα	248
§8.9	Maximal και πρώτα ιδεώδη	251
Πίνακας Συμβόλων		273
Βιβλιογραφία		277
Ευρετήριο όρων		279

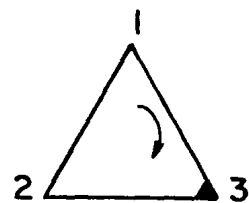




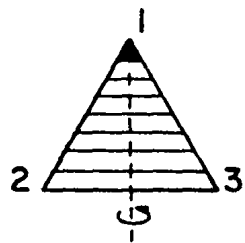
$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = (1) = e$$



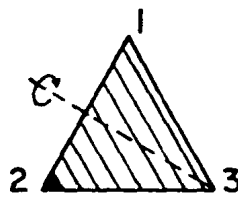
$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3) = g$$



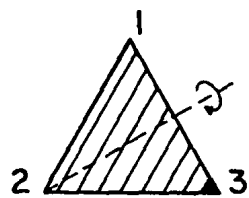
$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\ 3\ 2) = g^2$$



$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2\ 3) = h$$



$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\ 2) = gh$$



$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\ 3) = g^2h$$

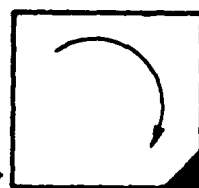
Οι συμμετρίες ενός ισοπλεύρου τριγώνου.



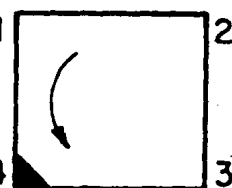
$$(1) = e$$



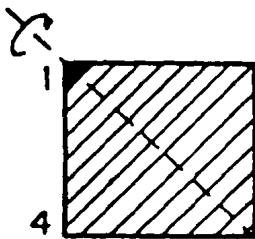
$$(1234) = g$$



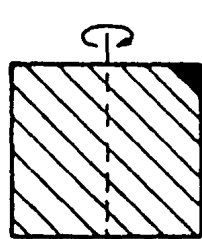
$$(13)(24) = g^2$$



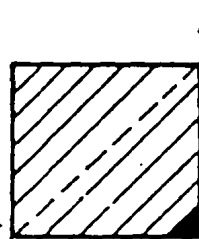
$$(1432) = g^3$$



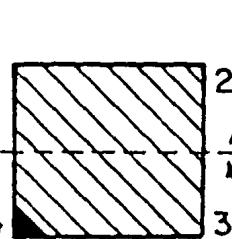
$$(24) = h$$



$$(12)(34) = gh$$



$$(13) = g^2h$$



$$(14)(23) = g^3h$$

Οι συμμετρίες ενός τετραγώνου.



ΚΕΦΑΛΑΙΟ 0

ΕΙΣΑΓΩΓΗ

§ 1. Σύνολα.

Η τόσο βασική έννοια του συνόλου έγινε σήμερα παραδεκτή σαν μια από τις πιο θεμελιακές και χρήσιμες έννοιες στα Μαθηματικά . Δεν υπάρχει Μαθηματικός ορισμός της έννοιας σύνολο , αφού αυτή καθαυτή η έννοια είναι πρωταρχική .

Διαισθητικά :

ένα σύνολο είναι μια συλλογή αντικειμένων * τα αντικείμενα αυτά καλούνται στοιχεία του συνόλου .

Γράφουμε

$$x \in X , \quad x \notin X$$

για να δηλώσουμε ότι το x είναι ή δεν είναι στοιχείο του συνόλου X .

Θα θεωρήσουμε ότι ο αναγνώστης γνωρίζει τις βασικές έννοιες από τη θεωρία συνόλων , όπως της ένωσης , διαχωρίσιμης ένωσης , διαφοράς , δυναμοσυνόλου , ισχύς συνόλου . κ.λ.π.

Θα τονίσουμε όμως , ότι ο ανεπίσημος τρόπος με τον οποίο χρησιμοποιούμε στα μαθηματικά τις ιδιότητες των συνόλων , συχνά σημαίνει ότι γνωρίζουμε καλά κάποια ή τα περισσότερα χρήσιμα αξιώματα της θεωρίας συνόλων , χωρίς αναγκαστικά να έχουμε δει ή μελετήσει τα σύνολα σαν μια αξιωματική θεμελιωμένη θεωρία .



Μια αξιωματική θεμελίωση της θεωρίας Συνόλων είναι χρήσιμη για να ανα-
 ρέσουμε ορισμένα παράδοξα που εμφανίζονται και φέρουν δυσκολίες σε μια μόνο ,
 από τη διαύσθηση προερχόμενη , θεώρηση του αντικειμένου .

Θα υπενθυμίσουμε ότι ένα παράδοξο (αντινομία) απαντάται σ'ένα αξιωματικό
 σύστημα , όταν και τα δύο , ένα δεδομένο και η άρνησή του , συμπεραίνονται
 από τα αξιώματα .

Στη συνέχεια , θα παρουσιάσουμε τη βασική αντινομία που έκανε την αξι-
 ματική θεμελίωση των συνόλων αναγκαία και σύντομα την άρση της σε δύο ενδια-
 φέρουσες τέτοιες θεμελιώσεις .

Ο Georg Cantor , πρώτος το 1870 , ανέπτυξε μια θεωρία συνόλων όχι όμως
 πάνω σε αξιωματικές βάσεις . Στη συνέχεια , ο G.Frege , στις αρχές του αιώνα
 μας , στην προσπάθεια μιας αξιωματικής θεμελίωσης , δέχθηκε τα εξής αξιώματα:

1. Δύο σύνολα είναι ίσα αν-ν έχουν τα ίδια στοιχεία , τυπικά
 $(\forall A)(\forall B)((\forall x)(x \in A \iff x \in B)) \implies A=B$.

2. Για κάθε ιδιότητα π υπάρχει ένα σύνολο
 $A = \{x / \pi(x)\}$,

δηλαδή το A είναι το σύνολο όλων των αντικειμένων x , για καθένα των οποίων
 το $\pi(x)$ γίνεται μια αληθής πρόταση .

Σημειώνουμε ότι η αλήθεια ή το ψεύδος μιας πρότασης γίνεται μέσα σε ορι-
 σμένα πλαίσια κοινής παραδοχής , όπου μια πρόταση αξιολογείται σαν αληθής ή
 ψευδής κατ'αποκλειστικό τρόπο , χωρίς δηλ. να μπορεί να αξιολογηθεί ταυτό-
 χρονα σαν αληθής και ψευδής . Η αποδοχή όμως του 2ου αξιώματος μας επιφέρει
 την αντινομία (παράδοξο) του Russel .

Ο Bertrand Russel , το 1902 , με παράδειγμα απέδειξε ότι:

Το σύνολο όλων των συνόλων δεν έχει σαν στοιχείο τον εαυτό του .

Πραγματικά , το δεδομένο $x \notin x$, δεν είναι παράλογο , αφού πολλά σύνολα το ικα-
 νοποιούν (π.χ. το σύνολο όλων των βιβλίων δεν είναι βιβλίο) .

Αν $\pi(x)$ είναι η ιδιότητα $x \notin x$, τότε από το 2ο αξίωμα μπορούμε να σχη-
 ματίσουμε το σύνολο

$$B = \{x / x \notin x\}$$



απ'όπου συμπεραίνουμε

$$B \notin B \iff B \in B .$$

Εκείνο που σφάλλει εδώ είναι η παραδοχή ότι το B είναι ένα σύνολο .

Για να αποφύγουν αντινομίες , οι E.Zermelo και A.Frankel , το 1920 πα-
ρουσίασαν μια αξιωματική θεωρία συνόλων γνωστή σαν (ZF) σύνολο-θεωρία που
γενικά είναι παραδεκτή σαν θεμελίωση των μαθηματικών .

Το αξιωματικό σχήμα κατασκευής υποσυνόλων της (ZF) συνολοθεωρία μας
λέει ότι :

Για κάθε σύνολο A και κάθε ιδιότητα π , υπάρχει ένα σύνολο B έτσι
ώστε $x \in B$ αν-ν $x \in A$ και έχει την ιδιότητα π .

Αυτό περιορίζει τον τρόπο με τον οποίο μια ιδιότητα μπορεί να χρησιμοποιηθεί
για να σχηματίσουμε ένα σύνολο και έτσι το παράδοξο του Russel αποφεύγεται .

Έδω μπορούμε να σχηματίσουμε το σύνολο

$$B = \{x \in A / x \notin x\}$$

Για να διαπιστώσουμε μια αντινομία που να εμπλέκει τα δεδομένα $B \in B$ και
 $B \notin B$, οφείλουμε να γνωρίζουμε αν $B \in A$. Το $B \in B$ είναι αδύνατο , έτσι
 $B \notin B$ και τότε $B \in A$. Αυτό δε μας οδηγεί σε αντινομία αλλά αντίθετα αποδει-
κνύει ότι για κάθε σύνολο A υπάρχει ένα σύνολο B με $B \notin A$.

Έτσι , δεν υπάρχει το σύνολο όλων των συνόλων . Τα άλλα αξιώματα μας εγγυ-
ώνται την ύπαρξη του κενού συνόλου , του δυναμοσυνόλου κ.λ.π. και την κατα-
σκευή νέων συνόλων από γνωστά σύνολα , ένωση , τομή κ.λ.π.

Μια άλλη αξιωματική θεμελίωση είναι αυτή των Gödel-Bernays-Von-Neumann
που χρησιμοποιείται στη θεωρία κατηγοριών .

Σ'αυτήν , η πρωταρχική έννοια είναι της κλάσης "class" .

Έτσι , μια κλάση A είναι σύνολο αν-ν υπάρχει κλάση B έτσι ώστε
 $A \in B$.

Εδώ μπορούμε να σχηματίσουμε την κλάση όλων των συνόλων ή την κλάση όλων
των ομάδων .

Μ' αυτό τον τρόπο αποφεύγονται δυσκολίες οι οποίες διαφορετικά είναι σύν-
δρομες με το "σύνολο όλων των συνόλων" .



§2 . Καρτεσιανό γινόμενο συνόλων . Σχέσεις.

Θεωρούμε δύο μη-κενά σύνολα A και B . Από τα στοιχεία $a \in A$ και $b \in B$ δημιουργούμε νέα στοιχεία (a,b) . Τα νέα αυτά στοιχεία τα ονομάζουμε διατεταγμένα ζεύγη αν ισχύει

$$(a,b) = (a',b') \iff a = a' \text{ και } b = b' .$$

Καλούμε καρτεσιανό γινόμενο των συνόλων A, B και το συμβολίζουμε $A \times B$ το σύνολο όλων των διατεταγμένων ζευγών (a,b) όπου $a \in A$ και $b \in B$, δηλαδή

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

Αν έχουμε τα σύνολα $A_1, A_2, \dots, A_n$ μπορούμε τότε να γενικεύσουμε την έννοια του διατεταγμένου ζεύγους θεωρώντας την διατεταγμένη n -άδα που κατασκευάζεται ως εξής :

Από τα στοιχεία $a_i \in A_i$ $i=1,2,\dots,n$ δημιουργούμε νέα στοιχεία $(a_1, \dots, a_n)$ τα οποία αποκαλούμε διατεταγμένες n -άδες αν ισχύει

$$(a_1, \dots, a_n) = (a'_1, \dots, a'_n) \iff a_i = a'_i \quad i=1,2,\dots,n .$$

Ονομάζουμε καρτεσιανό γινόμενο των συνόλων $A_1, \dots, A_n$ και το συμβολίζουμε $A_1 \times \dots \times A_n$ το σύνολο όλων των διατεταγμένων n -άδων $(a_1, \dots, a_n)$ όπου $a_i \in A_i$ $i=1,2,\dots,n$, δηλαδή

$$A_1 \times \dots \times A_n = \{(a_1, \dots, a_n) / a_i \in A_i , i=1,2,\dots,n\} .$$

Αν ένα τουλάχιστον από τα σύνολα $A_1, \dots, A_n$ είναι το κενό σύνολο , τότε ορίζουμε σαν καρτεσιανό γινόμενο αυτών το κενό σύνολο .

Ας είναι A και B δύο σύνολα . Κάθε υποσύνολο R του καρτεσιανού γινομένου $A \times B$ καλείται διμελής σχέση στο σύνολο $A \times B$ ή διμελής σχέση μεταξύ των συνόλων A και B .

Αν $A=B$, μια διμελής σχέση στο $A \times A$ ή όπως συνήθως λέμε στο A δεν είναι παρά ένα υποσύνολο R του καρτεσιανού γινομένου $A \times A$.

Συμφωνούμε να γράφουμε $a R b$ για να δηλώσουμε ότι το ζεύγος $(a,b) \in R$.



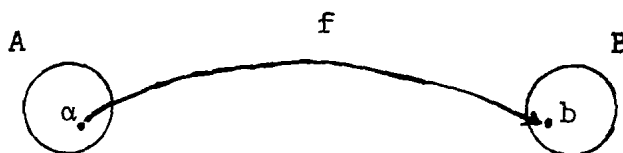
Γενικότερα, μια n -μελής σχέση μεταξύ των συνόλων $A_1, \dots, A_n$, είναι ένα υποσύνολο R του καρτεσιανού γινομένου $A_1 \times \dots \times A_n$.

Μια διμελής σχέση R στο σύνολο A καλείται :

- i) Ανακλαστική (reflexive): $\forall a \in A$ ισχύει $a R a$
- ii) Συμμετρική (symmetric): $\forall a R b \implies b R a$
- iii) Αντισυμμετρική (anti-symmetric): $\forall a R b$ και $b R a \implies a = b$
- iv) Μεταβατική (transitive): $\forall a R b$ και $a R c \implies a R c$

§3 . Απεικονίσεις.

Μία απεικόνιση ενός συνόλου A σ'ένα σύνολο B , είναι ένας μηχανισμός f , που σε κάθε στοιχείο a του A αντιστοιχεί ένα μοναδικό στοιχείο b του B . το b καλείται εικόνα του a μέσω της f .



Το A ονομάζεται σύνολο αφετηρίας της f ενώ το B σύνολο άφιξης της f .

Συμβολίζουμε

$$f : A \rightarrow B \quad \text{ή} \quad A \xrightarrow{f} B$$

μια απεικόνιση από το A στο B , ενώ για να δείξουμε ότι η απεικόνιση $f : A \rightarrow B$ στέλνει το στοιχείο a του A στο στοιχείο b του B γράφουμε

$$b = f(a) \quad \text{ή} \quad a \xrightarrow{f} f(a)$$

Ισότητα απεικονίσεων . Δύο απεικονίσεις

$$f, g : A \rightarrow B$$

είναι ίσες, αν-ν

$$f(a) = g(a), \quad \forall a \in A$$



Η απεικόνιση $g: \Gamma \rightarrow \Delta$ καλείται περιορισμός της απεικόνισης $f: A \rightarrow B$ ή ισοδύναμα η f καλείται επέκταση της g , αν ισχύει

$$\Gamma \subseteq A, \Delta \subseteq B \text{ και } f(c) = g(c) \quad \forall c \in \Gamma.$$

Παρατήρηση .

Μια απεικόνιση $f: A \rightarrow B$ δεν είναι παρά μια σχέση f μεταξύ των συνόλων A και B τέτοια ώστε

i) $\forall a \in A, a f b$ για κάποιο $b \in B$.

ii) Αν $a f b$ και $a f b' \Rightarrow b = b'$.

Σύνθεση απεικονίσεων .

Θεωρούμε τις απεικονίσεις

$$A \xrightarrow{f} B \xrightarrow{g} C.$$

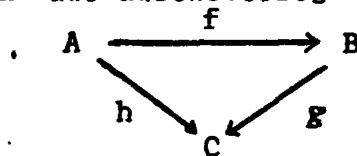
Η σύνθεση των απεικονίσεων f και g είναι μια απεικόνιση

$$g \circ f: A \rightarrow C$$

που ορίζεται ως εξής :

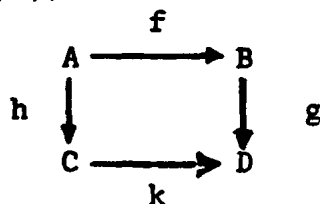
$$(g \circ f)(a) = g(f(a)), \quad \forall a \in A.$$

Ένα διάγραμμα από απεικονίσεις



λέγεται αντιμεταθετικό όταν $g \circ f = h$.

Όμοια το διάγραμμα



είναι αντιμεταθετικό αν $g \circ f = k \circ h$

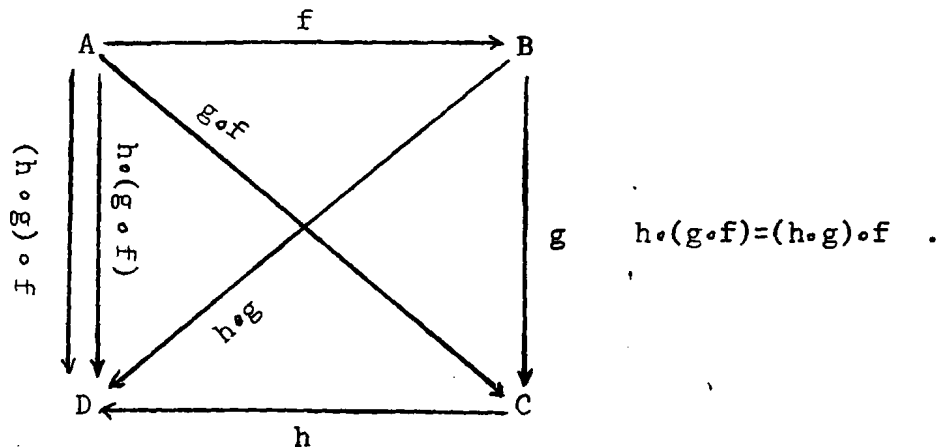


Τώρα , αν $h : C \rightarrow D$ είναι μια τρίτη απεικόνιση είναι εύκολο να αποδείξουμε ότι

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

δηλαδή , η σύνθεση απεικονίσεων έχει την προσεταιριστική ιδιότητα .

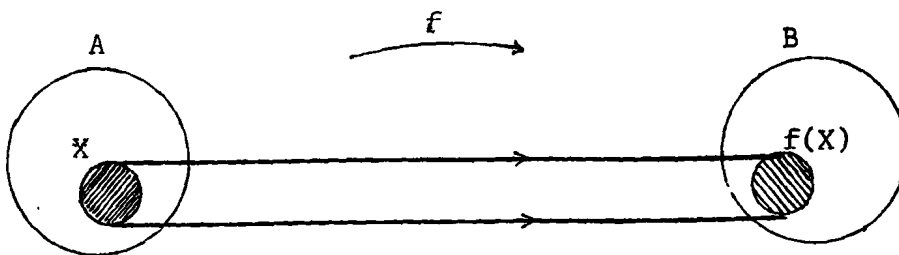
Διαγραμματικά για την προσεταιριστική ιδιότητα έχουμε



Ας είναι τώρα $f : A \rightarrow B$ μια απεικόνιση .

Αν $X \subseteq A$, ονομάζουμε εικόνα του X μέσω της f - συμβολισμός $f(X)$ - το σύνολο

$$f(X) = \{b \in B / b = f(a) \text{ για κάποιο } a \in X\} = \{f(a) / a \in X\}$$



Έτσι , κάθε απεικόνιση $f : A \rightarrow B$ ορίζει μια απεικόνιση

$$\mathcal{P}(A) \rightarrow \mathcal{P}(B) , \quad X \mapsto f(X)$$

($\mathcal{P}(A)$ συμβολίζει το δυναμοσύνολο του A) .



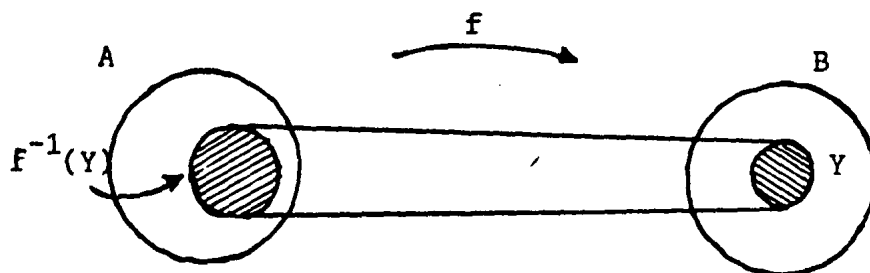
Η παραπάνω απεικόνιση έχει τις επόμενες ιδιότητες :

Για $X_1, X_2 \in \mathcal{P}(A)$ ισχύουν :

- i) $X_1 \subseteq X_2 \implies f(X_1) \subseteq f(X_2)$
- ii) $f(X_1 \cup X_2) = f(X_1) \cup f(X_2)$
- iii) $f(X_1 \cap X_2) \subseteq f(X_1) \cap f(X_2)$.

Αν $Y \subseteq B$ ονομάζουμε αντίστροφη εικόνα του Y μέσω της f -συμβολισμός $f^{-1}(Y)$ -το σύνολο

$$f^{-1}(Y) = \{a \in A / f(a) \in Y\} \text{ .}$$



Η f και εδώ ορίζει μια απεικόνιση

$$\mathcal{P}(B) \longrightarrow \mathcal{P}(A) \text{ , } Y \longmapsto f^{-1}(Y)$$

η οποία διατηρεί τα σύμβολα $\subseteq, \cap, \cup$, δηλαδή για $Y_1, Y_2 \in \mathcal{P}(B)$ ισχύουν :

- i) $Y_1 \subseteq Y_2 \implies f^{-1}(Y_1) \subseteq f^{-1}(Y_2)$
- ii) $f^{-1}(Y_1 \cup Y_2) = f^{-1}(Y_1) \cup f^{-1}(Y_2)$
- iii) $f^{-1}(Y_1 \cap Y_2) = f^{-1}(Y_1) \cap f^{-1}(Y_2)$.

Τέλος , για απεικονίσεις $A \xrightarrow{f} B \xrightarrow{g} C$ και για $X \subseteq A$, $Y \subseteq B$ έχουμε :

- i) $(g \circ f)(X) = g(f(X))$
- ii) $(g \circ f)^{-1}(Y) = f^{-1}(g^{-1}(Y))$.



Είδη απεικονίσεων .

■ Μια απεικόνιση $f : A \rightarrow B$ ονομάζεται ένα προς ένα (1-1) ή ένεση (injective) αν για κάθε $\alpha_1, \alpha_2 \in A$

$$\alpha_1 \neq \alpha_2 \implies f(\alpha_1) \neq f(\alpha_2) .$$

Ισοδύναμα , η $f : A \rightarrow B$ είναι 1-1 , αν-ν για κάθε $\alpha_1, \alpha_2 \in A$.

$$f(\alpha_1) = f(\alpha_2) \implies \alpha_1 = \alpha_2 .$$

■ Η απεικόνιση $f : A \rightarrow B$ ονομάζεται επί ή έφεση (surjection) αν-ν $f(A) = B$.

Μ'άλλα λόγια , η $f : A \rightarrow B$ είναι επί αν-ν για κάθε $b \in B$, $b = f(\alpha)$ για κάποιο $\alpha \in A$.

■ Μια απεικόνιση $f : A \rightarrow B$ ονομάζεται ένα προς ένα και επί ή αμφίεση (bijective) όταν ταυτόχρονα είναι 1-1 και επί .

Για παράδειγμα , η ταυτοτική απεικόνιση

$$I_A : A \rightarrow A , \quad I_A(\alpha) = \alpha , \quad \forall \alpha \in A$$

είναι 1-1 και επί .

Εύκολα αποδεικνύεται ότι για απεικονίσεις $A \xrightarrow{f} B \xrightarrow{g} C$ έχουμε :

- i) Αν οι f, g είναι 1-1 απεικονίσεις τότε η $g \circ f$ είναι 1-1 .
- ii) Αν οι f, g είναι επί απεικονίσεις τότε η $g \circ f$ είναι επί .
- iii) Αν η $g \circ f$ είναι 1-1 απεικόνιση τότε η f είναι 1-1 .
- iv) Αν η $g \circ f$ είναι επί απεικόνιση τότε η g είναι επί .

Αντιστρέψιμες απεικονίσεις .

Ας είναι $f : A \rightarrow B$ μια απεικόνιση 1-1 και επί . Για κάθε στοιχείο $b \in B$ υπάρχει ένα και μόνο ένα στοιχείο $\alpha \in A$, τέτοιο ώστε $b = f(\alpha)$.

Πραγματικά , αφού η f είναι επί , θα υπάρχει $\alpha \in A$ με $b = f(\alpha)$ και μάλιστα μοναδικό γιατί , αν $b = f(\alpha')$ τότε

$$f(\alpha) = f(\alpha') \implies \alpha = \alpha'$$

αφού η f είναι 1-1 .



Αν λοιπόν σε κάθε στοιχείο b του B αντιστοιχίσουμε το μοναδικό $a \in A$ για το οποίο ισχύει $f(a) = b$, ορίζουμε έτσι μια απεικόνιση

$$f^{-1} : B \rightarrow A$$

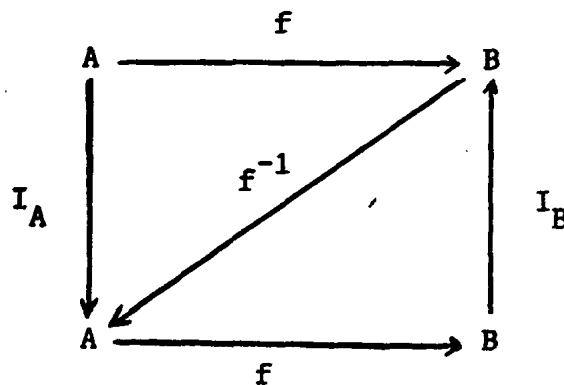
δηλαδή

$$(f^{-1}(b) = a) \iff (f(a) = b) \quad (1)$$

Η απεικόνιση f^{-1} ονομάζεται αντίστροφη της f και ικανοποιεί τις σχέσεις

$$f^{-1} \circ f = I_A \quad \text{και} \quad f \circ f^{-1} = I_B \quad (2)$$

Διαγραμματικά δηλαδή έχουμε



ΘΕΩΡΗΜΑ 1. Ας είναι $f : A \rightarrow B$ μια απεικόνιση. Αν υπάρχει απεικόνιση $g : B \rightarrow A$ τέτοια ώστε

$$g \circ f = I_A \quad \text{και} \quad f \circ g = I_B \quad (3)$$

τότε η f είναι 1-1 και επί και μάλιστα η αντίστροφός της είναι η g .

Απόδειξη.

Ένα προς ένα.

$$\begin{aligned} f(\alpha_1) = f(\alpha_2) &\implies g(f(\alpha_1)) = g(f(\alpha_2)) \implies (g \circ f)(\alpha_1) = \\ &= (g \circ f)(\alpha_2) \stackrel{(3)}{\implies} I_A(\alpha_1) = I_A(\alpha_2) \implies \alpha_1 = \alpha_2. \end{aligned}$$

Επί.

Για κάθε $b \in B$, το στοιχείο $a = g(b) \in A$ απεικονίζεται από την f στο στοιχείο b , αφού



$$f(a) = f(g(b)) = (f \circ g)(b) \stackrel{(3)}{=} I_B(b) = b .$$

Η f είναι λοιπόν 1-1 και επί και μάλιστα

$$f^{-1} = g .$$

Πραγματικά ,

$$g = I_A \circ g \stackrel{(3)}{=} (f^{-1} \circ f) , g = f^{-1} \circ (f \circ g) \stackrel{(3)}{=} f^{-1} \circ I_B = f^{-1} . \blacksquare$$

ΠΟΡΙΣΜΑ 1 . Η σύνθεση $g \circ f$ δύο 1-1 και επί απεικονίσεων f και g είναι 1-1 και επί , της οποίας η αντίστροφη απεικόνιση είναι η $f^{-1} \circ g^{-1}$.

ΠΟΡΙΣΜΑ 2 . Η αντίστροφη απεικόνιση f^{-1} μιας 1-1 και επί απεικόνισης f είναι και αυτή 1-1 και επί και μάλιστα

$$(f^{-1})^{-1} = f . \blacksquare$$

Η απαλλαγή των ορισμών της 1-1 απεικόνισης και επί απεικόνισης από σχέσεις που εμπλέκουν στοιχεία και ο εντοπισμός ιδιοτήτων που εμπλέκουν μόνο ισοτήτες μεταξύ απεικονίσεων και σύνθεσης απεικονίσεων , επέφερε τις επόμενες δύο προτάσεις που έπαιξαν βασικό ρόλο στους ορισμούς επιμορφισμού και μονομορφισμού σε μια τυχούσα κατηγορία .

ΠΡΟΤΑΣΗ 1 . Μια απεικόνιση $f : A \rightarrow B$ είναι επί αν-ν για κάθε σύνολο C και για κάθε ζεύγος απεικονίσεων $B \xrightleftharpoons[h]{g} C$ με $g \circ f = h \circ f$ ισχύει $g = h$.

Απόδειξη .

Ας υποθέσουμε ότι η f είναι επί . Αν οι απεικονίσεις $B \xrightleftharpoons[h]{g} C$ πληρούν τη σχέση $g \circ f = h \circ f$, τότε , επειδή η f είναι επί , για κάθε $b \in B$ υπάρχει $a \in A$ με $f(a) = b$. Άρα

$$g(b) = g(f(a)) = h(f(a)) = h(b) , \quad \forall b \in B$$

δηλαδή $g = h$.

Αντίστροφα . Αν υποθέσουμε ότι η $f : A \rightarrow B$ δεν είναι επί και κατασκευάσουμε απεικονίσεις $g, h : B \rightarrow C$ με $g \circ f = h \circ f$ αλλά $g \neq h$, τότε προφανώς θα έχουμε αποδείξει το αντίστροφο .

Αφού η f δεν είναι επί θα υπάρχει κάποιο $b_1 \in B$ που δεν είναι εικόνα



$f(a)$ κάποιου $a \in A$.

Εκλέγουμε ένα $b_2 \neq b_1$ (αυτό είναι δυνατό, αφού η f δεν είναι επί και ορίζουμε δύο απεικονίσεις :

$$g : B \rightarrow B \quad \text{με} \quad g = I_B$$

και

$$h : B \rightarrow B \quad \text{με} \quad h(b) = \begin{cases} b & \text{αν } b \neq b_1 \\ b_2 & \text{αν } b = b_1 \end{cases}.$$

Είναι $h \neq g$, επειδή $h(b_1) \neq g(b_1)$.

Επιπλέον :

$$(g \circ f)(a) = g(f(a)) = I_B(f(a)) = f(a), \quad \forall a \in A$$

και ακόμη, επειδή $f(a) \neq b_1$, για κάθε $a \in A$, έχουμε $(h \circ f)(a) = h(f(a)) = f(a)$ συνεπώς $g \circ f = h \circ f$. ■

ΠΡΟΤΑΣΗ 2. Μια απεικόνιση $f : B \rightarrow A$ είναι 1-1, αν-ν για κάθε σύνολο C και κάθε ζεύγος απεικονίσεων $C \xrightarrow[g]{h} B$ με $f \circ g = f \circ h$ ισχύει $g = h$.

Απόδειξη. Υποθέσουμε ότι η $f : B \rightarrow A$ είναι 1-1 και ας είναι $g, h : C \rightarrow B$ απεικονίσεις τέτοιες ώστε $f(g(c)) = f(h(c)) \quad \forall c \in C$. Αφού η f είναι 1-1 $g(c) = h(c) \quad \forall c \in C$ δηλαδή $g = h$.

Θα αποδείξουμε το αντίστροφο αποδεικνύοντας ότι, αν η $f : B \rightarrow A$ δεν είναι 1-1, μπορούμε να κατασκευάσουμε απεικονίσεις $g, h : B \rightarrow B$ έτσι ώστε $g \neq h$ και $f \circ g = f \circ h$.

Πραγματικά, επειδή η f δεν είναι 1-1, μπορούμε να βρούμε δύο διακεκριμένα στοιχεία b_1 και b_2 του B με $f(b_1) = f(b_2)$.

Παίρνουμε $g : B \rightarrow B$ να είναι $g = I_B$ και ορίζουμε την $h : B \rightarrow B$ από

$$h(b) = \begin{cases} b & \text{αν } b \neq b_1 \\ b_2 & \text{αν } b = b_1 \end{cases}.$$

Είναι $g \neq h$, αφού $g(b_1) \neq h(b_1)$ και επιπλέον

$$(f \circ g)(b) = f(g(b)) = f(b), \quad \forall b \in B,$$

ενώ



$$(f \circ h)(b) = f(h(b)) = \begin{cases} f(b) & \text{αν } b \neq b_1 \\ f(b_2) = f(b_1) & \text{αν } b = b_1 \end{cases}$$

δηλαδή $f \circ g = f \circ h$. ■

§4. Σχέσεις ισοδυναμίας .

Ας είναι X ένα μη-κενό σύνολο . Μία σχέση R στο X καλείται σχέση ισοδυναμίας στο X αν είναι ανακλαστική, συμμετρική και μεταβατική .

Αν για τα στοιχεία $x, y \in X$ συμβαίνει $x R y$ δηλαδή $(x, y) \in R$, τότε γράφουμε $x \equiv y(R)$

και λέμε ότι το " x είναι ισοδύναμο με το y κατά μέτρο R ."

Με το νέο συμβολισμό η σχέση R στο σύνολο X είναι σχέση ισοδυναμίας, όταν

- 1) $x \equiv x(R)$, $\forall x \in X$.
- 2) Αν $x \equiv y(R) \implies y \equiv x(R)$.
- 3) Αν $x \equiv y(R)$ και $y \equiv z(R) \implies x \equiv z(R)$.

Αν $x \in X$, ονομάζουμε κλάση ισοδυναμίας του x και την συμβολίζουμε $[x]$ ή $R(x)$ το σύνολο όλων των στοιχείων του X που είναι ισοδύναμα με το x κατά μέτρο R :

$$[x] = \{y / y \in X \text{ και } y \equiv x(R)\} .$$

Είναι αναγκαίο να γνωρίζουμε τότε δύο κλάσεις ισοδυναμίας είναι ίσες . Παρατηρούμε ότι :

$$[x] = [y] \iff x \equiv y(R) \tag{4}$$

Πραγματικά , αν $[x] = [y]$, επειδή $x \equiv x(R)$, τότε $x \in [x]$. άρα $x \in [y]$, δηλαδή $x \equiv y(R)$. Αντίστροφα , αν $x \equiv y(R)$, τότε , αν $z \in [x]$, έχουμε $z \equiv x(R)$. Αλλά :

$z \equiv x(R)$ και $x \equiv y(R) \implies z \equiv y(R)$ δηλαδή $z \in [y]$ και έτσι $[x] \subseteq [y]$. Όμοια αποδεικνύεται ότι $[y] \subseteq [x]$. Επομένως $[x] = [y]$.

Ένα οποιοδήποτε στοιχείο y της κλάσης ισοδυναμίας $[x]$ το λέμε αντιπρόσωπο της κλάσης $[x]$.



Στη συνέχεια θα δείξουμε ότι δύο κλάσεις ισοδυναμίας ή είναι ξένες μεταξύ τους ή ταυτίζονται :

$$\forall x, y \in X \quad [x] \cap [y] = \emptyset \quad \text{ή} \quad [x] = [y] \quad (5)$$

Πραγματικά, αν $[x] \cap [y] \neq \emptyset$, τότε υπάρχει $z \in [x] \cap [y]$. Επομένως $z \in [x]$ και $z \in [y]$, δηλαδή $x \equiv z(R)$ και $z \equiv y(R)$ και τελικά $x \equiv y(R)$. Σύμφωνα με την (4) έχουμε $[x] = [y]$.

Θα τονίσουμε εδώ ότι για κάθε $x \in X$ είναι $x \equiv x(R)$ δηλαδή $x \in [x]$ και επομένως

$$[x] \neq \emptyset \quad \text{για κάθε} \quad x \in X \quad (6)$$

Αν R είναι μια σχέση ισοδυναμίας στο X τότε το σύνολο όλων των κλάσεων ισοδυναμίας στο X το συμβολίζουμε X/R και το καλούμε σύνολο πηλίκου του συνόλου X με την σχέση R , δηλαδή

$$X/R = \{A/A \subset X \text{ με } A = [x] \text{ για κάποιο } x \in X\}.$$

Τέλος, παρατηρούμε ότι

$$X = \bigcup_{x \in X} [x] = \bigcup_{[x] \in X/R} [x]. \quad (7)$$

Υπενθυμίζουμε ότι μια οικογένεια υποσυνόλων $(A_i)_{i \in I}$ ενός συνόλου X αποτελεί ένα διαμελισμό ή διαμερισμό (partition) του X όταν

- i) $A_i \neq \emptyset, \forall i \in I$
- ii) $\bigcup_{i \in I} A_i = X$
- iii) $A_i \cap A_j = \emptyset$ για κάθε $i \neq j \in I$.

Στην περίπτωση αυτή γράφουμε $X = \sum_{i \in I} A_i$.

Αν R είναι μία σχέση ισοδυναμίας στο X τότε από τις σχέσεις (5), (6), (7) παίρνουμε ότι, οι διακεκριμένες κλάσεις ισοδυναμίας δηλαδή τα στοιχεία του συνόλου πηλίκου X/R αποτελούν ένα διαμελισμό του X . Έτσι



Κάθε σχέση ισοδυναμίας R σ' ένα σύνολο X ορίζει ένα διαμελισμό του συνόλου X .

Αλλά και αντίστροφα ,

"κάθε διαμελισμός" $S = (A_i)_{i \in I}$ του X ορίζει μια σχέση ισοδυναμίας R_S στο X , της οποίας ο αντίστοιχος διαμελισμός συμπίπτει με τον S .

Πραγματικά , η σχέση R_S που ορίζεται ως εξής :

$x \equiv y(R_S)$ εάν-ν $x \in A_i$, $y \in A_i$ για κάποιο (μοναδικό) $i \in I$ είναι μία σχέση ισοδυναμίας στο X .

Η κλάση ισοδυναμίας $R_S(x)$ του τυχόντος στοιχείου $x \in X$ ως προς την σχέση R_S είναι το στοιχείο $A_i \in S$ που περιέχει το x , αφού

$$\begin{aligned} R_S(x) &= \{y/y \in X, y \equiv x(R_S)\} \\ &= \{y/y \in X, y \in A_i\} = A_i. \end{aligned}$$

Έτσι ο διαμελισμός που ορίζει η σχέση R_S δεν είναι παρά ο αρχικός διαμελισμός S .

Αν λοιπόν $E(X)$ είναι το σύνολο όλων των σχέσεων ισοδυναμίας στο X και $Q(X)$ το σύνολο όλων των διαμελισμών του X τότε η απεικόνιση

$$f : E(X) \rightarrow Q(X), \quad R \mapsto X/R$$

που στέλνει δηλαδή κάθε σχέση ισοδυναμίας R στον αντίστοιχο διαμελισμό X/R που αυτή ορίζει στο X είναι 1-1 και επί .

Πραγματικά , ορίζοντας την απεικόνιση

$$g : Q(X) \rightarrow E(X), \quad S \mapsto R_S$$

αποδεικνύεται εύκολα ότι

$$g \circ f = I_{E(X)} \quad \text{και} \quad f \circ g = I_{Q(X)}.$$

Δηλαδή τα σύνολα $E(X)$ και $Q(X)$ είναι ισοδύναμα .

Μ' άλλα λόγια

Υπάρχουν τόσες σχέσεις ισοδυναμίας σ' ένα σύνολο X όσοι είναι και οι διαμελισμοί του συνόλου X .



Παράδειγμα . Να βρεθούν όλες οι σχέσεις ισοδυναμίας πάνω στο σύνολο $\{x, y, z\}$.

Οι δυνατοί διαμελισμοί του συνόλου $\{x, y, z\}$ είναι οι παρακάτω

$\{x, y, z\}$

$\{x, y\}$, $\{z\}$

$\{x, z\}$, $\{y\}$

$\{y, z\}$, $\{x\}$

$\{x\}$, $\{y\}$, $\{z\}$

οπότε πέντε σχέσεις ισοδυναμίας μπορούμε να ορίσουμε στο σύνολο $\{x, y, z\}$.

Για παράδειγμα η ισοδυναμία που ορίζει ο διαμελισμός

$\{y, z\}$, $\{x\}$

είναι η

$$R = \{(x, x), (y, y), (z, z), (y, z), (z, y)\} .$$

Εύκολα τώρα διαπιστώνεται ότι :

Αν R_1 και R_2 είναι δύο σχέσεις ισοδυναμίας στο σύνολο X , τότε η τομή τους $R_1 \cap R_2$ είναι σχέση ισοδυναμίας στο X . (Άσκηση)

Γενικώτερα , αν $\{R_i\}_{i \in I}$ είναι μια οικογένεια σχέσεων ισοδυναμίας σ' ένα σύνολο X τότε και η τομή τους

$$\bigcap_{i \in I} R_i$$

είναι μία σχέση ισοδυναμίας στο σύνολο X . (Άσκηση) .

Παραδείγματα σχέσεων ισοδυναμίας .

α. Αριθμητικές ισοδυναμίες .

Ας είναι m ένας θετικός ακέραιος . Στο σύνολο Z των ακεραίων ορίζουμε σχέση R_m ως εξής

$$x \equiv y (R_m) \iff x - y = km , \quad k \in Z .$$

Η R_m είναι μία σχέση ισοδυναμίας στο Z . Πραγματικά ,



i) Η R_m είναι ανακλαστική
 $\forall x \in \mathbb{Z} \quad x-x=0m \implies x \equiv x(R_m)$.

ii) Η R_m είναι συμμετρική
 Αν $x \equiv y(R_m) \implies x-y=km$, επομένως $y-x=(-k)m \implies y \equiv x(R_m)$.

iii) Η R_m είναι μεταβατική :
 Αν $x \equiv y(R_m)$ και $y \equiv z(R_m)$, τότε
 $x-y=k_1m$ και $y-z=k_2m$,

οπότε

$$x-z=(k_1+k_2)m \implies x \equiv z(R_m) .$$

θα δείξουμε στη συνέχεια ότι :

$x \equiv y(R_m)$ αν-ν $x=am+r$ και $y=bm+r$, $0 \leq r < m$ δηλαδή , $x \equiv y(R_m)$ αν-ν
 οι x, y είναι ισοϋπόλοιποι διαιρούμενοι με τον m .

Πραγματικά , αν $x=am+r$ και $y=bm+r$ τότε $x-y=(a-b)m$ άρα
 $x \equiv y(R_m)$.

Αντίστροφα , αν $x \equiv y(R_m)$ θα είναι

$$x-y=q \cdot m , \quad q \in \mathbb{Z} .$$

Ατ' την Ευκλείδεια διαίρεση έχουμε

$$y=bm+r , \quad 0 \leq r < m$$

οπότε

$$x=y+q \cdot m=bm+r+qm=(b+q)m+r \quad \text{με} \quad 0 \leq r < m$$

πράγμα που επιθυμούσαμε .

ΑΣ είναι τώρα

$$\dots [-2], [-1], [0], [1], [2] \dots \quad (*)$$

οι κλάσεις των στοιχείων του $\mathbb{Z}$.

Παρατηρούμε ότι για κάθε ακέραιο x η κλάση $[x]$ ταυτίζεται με την κλάση $[r]$, όπου r είναι το υπόλοιπο της διαίρεσης του x με τον m , δηλαδή

$$[x] = [r] , \quad x=am+r , \quad 0 \leq r < m .$$

Πραγματικά , από την $x=am+r$ παίρνουμε $x-r=am$, δηλαδή

$$x \equiv r(R_m) \quad \text{οπότε} \quad [x] = [r] .$$



Οι διακεκριμένες λοιπόν κλάσεις ισοδυναμίας που εμφανίζονται στην (*) είναι οι

$$[0], \dots, [m-1] \quad (**)$$

που αντιστοιχούν σ' όλα τα δυνατά υπόλοιπα της διαίρεσης ενός ακεραίου x με τον m .

Τις κλάσεις (**) τις καλούμε ακεραίους κατά μέτρο m και τους συμβολίζουμε

$$\bar{0}, \bar{1}, \dots, \overline{m-1}.$$

Το σύνολο πηλίκων $\mathbb{Z}/R_m$ το γράφουμε $\mathbb{Z}_m$ δηλαδή

$$\mathbb{Z}_m = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}.$$

όπου

$$\bar{0} = \{km / k \in \mathbb{Z}\}$$

$$\bar{1} = \{km+1 / k \in \mathbb{Z}\}$$

$$\vdots$$

$$\overline{m-1} = \{km+(m-1) / k \in \mathbb{Z}\}.$$

β. Αν R_1 και R_2 είναι δύο σχέσεις ισοδυναμίας στο σύνολο X , θα λέμε ότι η R_1 είναι λεπτότερη από τη R_2 (συμβολίζουμε $R_1 \prec R_2$) όταν

$$x \equiv y(R_1) \implies x \equiv y(R_2).$$

θα παρατηρήσουμε ότι αν $R_1 \prec R_2$, τότε ο διαμελισμός του X που αντιστοιχεί στην R_1 είναι "λεπτότερος" από τον διαμελισμό του X που αντιστοιχεί στη R_2 .

γ. Κάθε σχέση ισοδυναμίας R σε ένα σύνολο X ορίζει, με φυσικό τρόπο μια απεικόνιση επί

$$p: X \longrightarrow X/R, \quad x \longmapsto [x]$$

που την καλούμε κανονική προβολή.

Αλλά και η αντίστροφη κατάσταση πληρούται, δηλαδή: Κάθε απεικόνιση $f: X \longrightarrow Y$ ορίζει μια σχέση ισοδυναμίας R_f στο X ως εξής:

$$x \equiv y(R_f) \iff f(x) = f(y) \quad (\text{Άσκηση}).$$

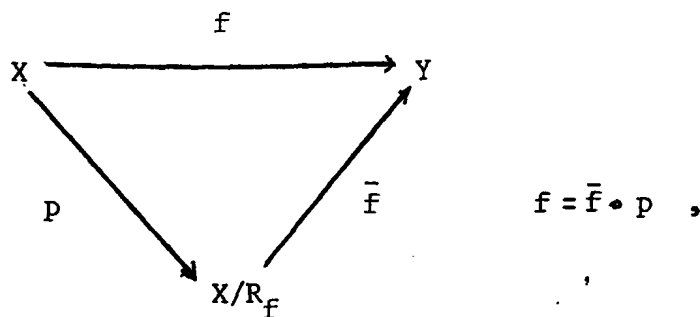
Η R_f καλείται πυρηνική ισοδυναμία της f .



Θα δούμε τώρα ένα θεώρημα που μας λέει πως μπορούμε να αναλύσουμε μια απεικόνιση σε σύνθεση δύο απλούστερων απεικονίσεων .

ΘΕΩΡΗΜΑ 2 .

Κάθε απεικόνιση $f: X \rightarrow Y$ μπορεί να εκφραστεί σαν σύνθεση $\bar{f} \circ p$ δύο απεικονίσεων , μιας επί απεικόνισης p και μιας 1-1 απεικόνισης $\bar{f}$



όπου R_f είναι η πυρηνική ισοδυναμία της f και

$$p(x) = [x] \quad , \quad \forall x \in X$$

$$\bar{f}([x]) = f(x) \quad , \quad \forall [x] \in X/R_f$$

Απόδειξη .

Η p είναι φανερά μία επί απεικόνιση , ενώ η $\bar{f}$ είναι καλά ορισμένη. Πραγματικά ,

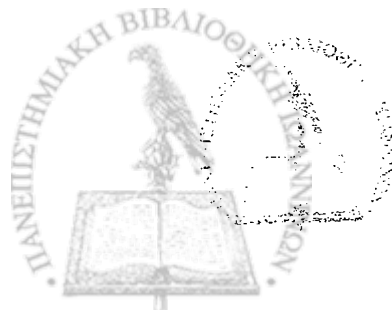
$$\begin{aligned}
 [x] = [y] &\implies x \equiv y (R_f) \\
 &\implies f(x) = f(y) \\
 &\implies \bar{f}([x]) = \bar{f}([y]) \quad .
 \end{aligned}$$

Από τον παραπάνω συλλογισμό , ακολουθώντας την αντίθετη πορεία , συμπεραίνουμε ότι η $\bar{f}$ είναι 1-1 . Το ότι $f = \bar{f} \circ p$ είναι τετριμμένο .

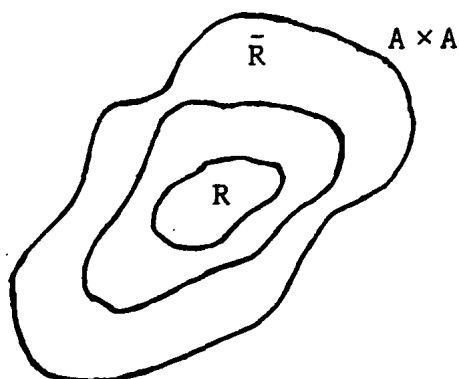
δ. Η παραγόμενη σχέση ισοδυναμίας .

Ας είναι R ένα υποσύνολο του $A \times A$.

Ορίζουμε τη σχέση ισοδυναμίας που παράγεται από το R και τη συμβολίζουμε με $\bar{R}$, να είναι η τομή όλων των σχέσεων ισοδυναμίας στο σύνολο A που περιέχουν το R .



Δηλαδή



$$\bar{R} = \bigcup_{s \in \mathcal{C}} S$$

όπου $\mathcal{C}$ η οικογένεια όλων των σχέσεων ισοδυναμίας S στο σύνολο A με $S \supseteq R$.

Η παραγόμενη σχέση ισοδυναμίας $\bar{R}$ είναι φανερά η μικρότερη σχέση ισοδυναμίας στο σύνολο A που περιέχει το R .

Η επόμενη πρόταση περιγράφει την παραγόμενη σχέση ισοδυναμίας $\bar{R}$.

ΠΡΟΤΑΣΗ 3 .

Δύο στοιχεία a και b του A είναι ισοδύναμα κατά μέτρο $\bar{R}$ δηλαδή $(a,b) \in \bar{R}$ εάν-ν $a=b$ ή υπάρχει φυσικός n και στοιχεία $a_1, \dots, a_{n+1} \in A$ με $a=a_1$, $b=a_{n+1}$ και για κάθε k , $1 \leq k \leq n$ να είναι $(a_k, a_{k+1}) \in R$ ή $(a_{k+1}, a_k) \in R$.

Απόδειξη .

1. Η $\bar{R}$ είναι μια σχέση ισοδυναμίας που περιέχει το R .

i) Ανακλαστική .

Για κάθε $a \in A$ έχουμε $(a,a) \in \bar{R}$ από τον ορισμό της $\bar{R}$.

ii) Συμμετρική .

Έστω $(a,b) \in \bar{R}$.

Αν $a=b$ τότε $(b,a) \in \bar{R}$.

Αν $a \neq b$ τότε υπάρχουν στοιχεία $a_1, \dots, a_{n+1} \in A$ με $a=a_1$, $b=a_{n+1}$

έτσι ώστε

$$(a_k, a_{k+1}) \in R \text{ ή } (a_{k+1}, a_k) \in R, \quad 1 \leq k \leq n.$$

$$\text{Θέτουμε, } b=a_{n+1}=\beta_1, \quad a_n=\beta_2, \dots, a_2=\beta_n, \quad a_1=\beta_{n+1}$$

και έχουμε



$(\beta_k, \beta_{k+1}) \in R$ ή $(\beta_{k+1}, \beta_k) \in R$, $1 \leq k \leq n$
που σημαίνει ότι $(b, a) \in \bar{R}$.

iii) Μεταβατική .

Έστω $(a, b) \in \bar{R}$ και $(b, c) \in \bar{R}$. Θα δείξουμε ότι $(a, c) \in \bar{R}$.

Αν $a=b$ ή $b=c$ τότε $(a, c) \in \bar{R}$. Διαφορετικά , αφού $(a, b) \in \bar{R}$ θα υπάρχουν στοιχεία του A

$$a = \alpha_1, \dots, \alpha_{n+1} = b$$

έτσι ώστε για κάθε k , $1 \leq k \leq n$ να είναι

$$(\alpha_k, \alpha_{k+1}) \in R \text{ ή } (\alpha_{k+1}, \alpha_k) \in R \quad (1)$$

Όμοια αφού $(b, c) \in \bar{R}$ θα υπάρχουν στοιχεία του A ,

$$b = \beta_1, \beta_2, \dots, \beta_{\lambda+1} = c$$

έτσι ώστε για κάθε v , $1 \leq v < \lambda$ να είναι

$$(\beta_v, \beta_{v+1}) \in R \text{ ή } (\beta_{v+1}, \beta_v) \in R \quad (2)$$

Παίρνουμε τώρα

$$a = \alpha_1, \alpha_2, \dots, \alpha_{n+1} = b = \beta_1, \beta_2, \dots, \beta_{\lambda+1} = c$$

δηλαδή $n+\lambda+1$ στοιχεία του A και από τις σχέσεις (1), (2) έχουμε

$$\left. \begin{array}{l} (\alpha_1, \alpha_2) \in R \text{ ή } (\alpha_2, \alpha_1) \in R \\ \vdots \\ (\alpha_n, \alpha_{n+1}) \in R \text{ ή } (\alpha_{n+1}, \alpha_n) \in R \\ (\alpha_{n+1}, \beta_2) \in R \text{ ή } (\beta_2, \alpha_{n+1}) \in R \\ (\beta_2, \beta_3) \in R \text{ ή } (\beta_3, \alpha_2) \in R \\ \vdots \\ (\beta_\lambda, \beta_{\lambda+1}) \in R \text{ ή } (\beta_{\lambda+1}, \beta_\lambda) \in R \end{array} \right\} \quad (3)$$

Οι σχέσεις (3) μας εξασφαλίζουν ότι $(a, c) \in \bar{R}$, δηλαδή η $\bar{R}$ είναι και μεταβατική , άρα είναι σχέση ισοδυναμίας .

Από τον ορισμό της $\bar{R}$ έχουμε ότι :

$$(a, b) \in R \implies (a, b) \in \bar{R}$$



δηλαδή $R \subseteq \bar{R}$.

2. Η $\bar{R}$ είναι η μικρότερη σχέση ισοδυναμίας που περιέχει το R .
θα δείξουμε ότι αν S είναι μία ισοδυναμία που περιέχει το R , πράγμα που σημαίνει ότι

$$(\alpha, \beta) \in R \implies (\alpha, \beta) \in S \quad (4)$$

τότε η S θα περιέχει και την $\bar{R}$ δηλαδή

$$(\alpha, \beta) \in R \implies (\alpha, \beta) \in S.$$

Πραγματικά, έστω ότι $(\alpha, \beta) \in \bar{R}$.

Αν $\alpha = \beta$ τότε $(\alpha, \beta) \in S$. Αν $\alpha \neq \beta$ θα υπάρχουν στοιχεία του A

$$\alpha = \alpha_1, \alpha_2, \dots, \alpha_{n+1} = \beta$$

έτσι ώστε

$$(\alpha_k, \alpha_{k+1}) \in R \quad \text{ή} \quad (\alpha_{k+1}, \alpha_k) \in R, \quad 1 \leq k \leq n,$$

οπότε σε συνδυασμό με την (4) έχουμε

$$(\alpha_k, \alpha_{k+1}) \in S \quad \text{ή} \quad (\alpha_{k+1}, \alpha_k) \in S, \quad 1 \leq k \leq n.$$

Η συμμετρικότητα και η μεταβατικότητα της S δίνουν τελικά $(\alpha, \beta) \in S$. ■

Παράδειγμα.

Θεωρούμε το σύνολο $X = \{1, 2, 3, 4, 5, 6, 7, 8\}$ και το ακόλουθο υποσύνολο R του $X \times X$

$$R = \{(1, 1), (1, 2), (5, 8), (7, 4)\}.$$

θα βρούμε την σχέση ισοδυναμίας $\bar{R}$ που παράγεται από το R .

α) Η $\bar{R}$ είναι η μικρότερη σχέση ισοδυναμίας στο X που περιέχει το R , άρα

$$(1, 1), (1, 2), (5, 8), (7, 4) \in \bar{R}$$

β) Η $\bar{R}$ είναι ανακλαστική, άρα

$$(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6), (7, 7), (8, 8) \in \bar{R}$$

γ) Η $\bar{R}$ είναι συμμετρική, επομένως

$$(2, 1), (8, 5), (4, 7) \in \bar{R}$$

Από τα α), β), γ) και τη συμμετρικότητα της σχέσης $\bar{R}$ συμπεραίνουμε ότι



$$\bar{R} = \{(1,1), (2,2), (3,3), (4,4), (5,5), (6,6), (7,7), (8,8), (1,2), (2,1), (8,5), (5,8), (7,4), (4,7)\} .$$

§5. Πράξεις .

Μια πράξη (διμελής) στο σύνολο X δεν είναι παρά μία απεικόνιση

$$* : X \times X \longrightarrow X , \quad (x,y) \longmapsto x * y .$$

Σ'ένα σύνολο μπορούν γενικά να ορισθούν πολλές πράξεις . Για να διακρίνουμε τις διάφορες πράξεις χρησιμοποιούμε γενικά διάφορα σύμβολα όπως $*$, $\cdot$, $\circ$, $\square$, $\blacksquare$, $+$.

Η πράξη $*$ καλείται αντιμεταθετική , αν συμβαίνει

$$x * y = y * x \quad \forall x, y \in X$$

και προσεταιριστική όταν :

$$x * (y * z) = (x * y) * z \quad \forall x, y, z \in X .$$

Παραδείγματα :

1) Στο σύνολο των φυσικών αριθμών $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ η συνηθισμένη πρόσθεση , ο συνηθισμένος πολ/σμός , καθώς και η απεικόνιση Ε.Κ.Π

$$[,] : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} , \quad (m, n) \longmapsto [m, n]$$

είναι διμελείς πράξεις .

2) Στο δυναμοσύνολο $\mathcal{P}(A)$ ενός συνόλου A , οι απεικονίσεις

$$\cup : \mathcal{P}(A) \times \mathcal{P}(A) \longrightarrow \mathcal{P}(A) \quad (X, Z) \longmapsto X \cup Z$$

$$\cap : \mathcal{P}(A) \times \mathcal{P}(A) \longrightarrow \mathcal{P}(A) \quad (X, Z) \longmapsto X \cap Z$$

είναι διμελείς πράξεις .

Ας είναι $A \neq \emptyset$ ένα υποσύνολο του X . Θα λέμε ότι το A είναι κλειστό ως προς την πράξη $* : X \times X \longrightarrow X$, αν

$$\forall a, b \in A \quad \text{το} \quad a * b \in A .$$

Για παράδειγμα το σύνολο των άρτιων φυσικών $2\mathbb{N} \subseteq \mathbb{N}$ είναι κλειστό ως προς την πρόσθεση και τον πολ/σμό .



Προσεταιριστικές πράξεις .

Ας είναι $*$: $X \times X \longrightarrow X$ μια προσεταιριστική πράξη .

Το κοινό αποτέλεσμα $(x_1 * x_2) * x_3 = x_1 * (x_2 * x_3)$ θα το καλούμε γινόμενο των στοιχείων x, x_2, x_3 , μ' αυτή την τάξη, και θα το συμβολίζουμε απλά $x_1 * x_2 * x_3$.

Γενικότερα θα συμβολίζουμε με

$$x = x_1 * x_2 * \dots * x_n$$

το παρακάτω γινόμενο των n στοιχείων $x_1, \dots, x_n$ του X

$$x = (((\dots(((x_1 * x_2) * x_3) * x_4) x_5 \dots) * x_{n+1}) * x_n) .$$

ΠΡΟΤΑΣΗ 4 . (Γενικευμένος προσεταιριστικός νόμος) .

Ένα γινόμενο n στοιχείων $x_1, x_2, \dots, x_n$ μπορεί να εξαρτάται από την πράξη των στοιχείων αυτών, δεν εξαρτάται όμως από τη διάταξη των πράξεων . Με άλλα λόγια, κάθε άλλο γινόμενο x' των στοιχείων $x_1, \dots, x_n$, παρμένα με αυτή την τάξη, είναι ίσο με το x .

Απόδειξη.

Η πρόταση αληθεύει για $n=3$. Ας υποθέσουμε ότι αληθεύει για k στοιχεία, για όλα τα $k < n$.

Αν x' είναι ένα γινόμενο των $x_1, \dots, x_n$, μ' αυτή την τάξη, τότε $x' = x'_1 * x'_2$, όπου x'_1, x'_2 είναι οι όροι της τελικής πράξης που γίνεται για να υπολογίσουμε το x' .

Το x'_1 σχηματίζεται από τα στοιχεία $x_1, x_2, \dots, x_r$ και το x'_2 από τα $x_{r+1}, \dots, x_n$, ($1 \leq r \leq n-1$) .

Στην περίπτωση $r=n-1$ έχουμε $x'_2 = x_n$ και το x'_1 είναι ένα γινόμενο των $x_1, \dots, x_{n-1}$ και, σύμφωνα με την υπόθεση, $x'_1 = x_1 * \dots * x_{n-1}$, οπότε

$$x' = (x_1 * \dots * x_{n-1}) * x_n = x_1 * \dots * x_n = x .$$

Αν $1 \leq r \leq n-2$, σύμφωνα με την υπόθεση είναι :

$$x'_1 = x_1 * \dots * x_r \quad \text{και} \quad x'_2 = x_{r+1} * \dots * x_n ,$$

οπότε



$$\begin{aligned}
 x' &= (x_1 * \dots * x_r) * (x_{r+1} * \dots * x_n) \\
 &= (x_1 * \dots * x_r) * [(x_{r+1} * \dots * x_{n-1}) * x_n] = \\
 &= [(x_1 * \dots * x_{n-1}) * (x_{r+1} * \dots * x_{n-1})] * x_n = \\
 &= (x_1 * \dots * x_{n-1}) * x_n = x \quad . \blacksquare
 \end{aligned}$$

Ο γενικευμένος προσεταιριστικός νόμος μας επιτρέπει να μιλάμε για δυνάμεις (αντιστ. πολ/σια) ενός στοιχείου $x \in X$ αν η πράξη σημειώνεται πολλαπλασιαστικά (αντιστ. προσθετικά) .

Έτσι

Πολλαπλασιαστικά

$$x^1 = x$$

$$x^m = x^{m-1} \cdot x, \quad m \in \mathbb{N}^*, \quad m > 1$$

Προσθετικά

$$1x = x$$

$$mx = (m-1)x + x, \quad m \in \mathbb{N}^*, \quad m > 1$$

Επομένως $\forall m, n \in \mathbb{N}^*$ έχουμε

$$x^m \cdot x^n = x^{m+n}$$

$$(x^m)^n = x^{mn}$$

$$mx + nx = (m+n)x$$

$$m(nx) = (mn)x$$

Ουδέτερο στοιχείο για μία πράξη.

Ας είναι $* : X \times X \rightarrow X$ μια πράξη στο X . Ένα στοιχείο $e \in X$ καλείται δεξιό ουδέτερο (αντιστ. αριστερό ουδέτερο) για την πράξη $*$ αν

$$x * e = x \quad (\text{αντιστ. } e * x = x), \quad \forall x \in X$$

Αν το στοιχείο e είναι ταυτόχρονα δεξιό και αριστερό ουδέτερο για την πράξη $*$ δηλαδή

$$x * e = x = e * x, \quad \forall x \in X$$

τότε καλείται ουδέτερο για την πράξη $*$.

Αν υπάρχουν δεξιά ουδέτερα και αριστερά ουδέτερα στοιχεία για την πράξη $*$, τότε υπάρχει ένα μόνο , που είναι ουδέτερο στοιχείο για την πράξη $*$.

Πραγματικά , έστω e ένα δεξιό ουδέτερο και e' ένα αριστερό ουδέτερο . Τότε



$$e = e' * e = e' .$$

Έτσι :

Αν υπάρχει ουδέτερο στοιχείο για μία πράξη , αυτό είναι μοναδικό και μιλάμε για το ουδέτερο στοιχείο μίας τέτοιας πράξης .

Συμμετρικά στοιχεία για μία πράξη .

Ας είναι $* : X \times X \rightarrow X$ μία πράξη με ουδέτερο στοιχείο e .

Ένα στοιχείο x' (αντιστ. x'') καλείται δεξιό συμμετρικό (αντιστ. αριστερό συμμετρικό) ενός στοιχείου $x \in X$ ως προς την πράξη $*$ αν

$$x * x' = e \quad (\text{αντιστ. } x'' * x = e) .$$

Αν ένα στοιχείο x' είναι ταυτόχρονα και δεξιό και αριστερό συμμετρικό του στοιχείου x δηλαδή αν ικανοποιεί την σχέση

$$x * x' = e = x' * x$$

τότε λέγεται συμμετρικό του x .

Αν η πράξη είναι προσεταιριστική και υπάρχουν δεξιά και αριστερά συμμετρικά ενός στοιχείου x , τότε υπάρχει μόνο ένα , που είναι συμμετρικό του x .

Παραγματικά , αν x' είναι ένα δεξιό και x'' είναι ένα αριστερό συμμετρικό του x τότε

$$x * x' = e \quad \text{και} \quad x'' * x = e .$$

επομένως

$$x'' = x'' * e = x'' * (x * x') = (x'' * x) * x' = e * x' = x' .$$

Έτσι

Για μία προσεταιριστική πράξη με ουδέτερο στοιχείο το συμμετρικό (αν υπάρχει) ενός στοιχείου x είναι μοναδικό .

Στην περίπτωση που έχουμε ένα πεπερασμένο σύνολο $E = \{x, y, z, w, k\}$ μπορούμε να ορίσουμε μία πράξη $*$ με τη βοήθεια ενός τετραγώνου πίνακα , αν γράψουμε π.χ. το στοιχείο $w * z$ στη διασταύρωση της γραμμής που βρίσκεται το w και της στήλης του z (σχ.1) .



*	x	y	z	w	k
x					
y					
z					
w				$w*z$	
k					

(σχ.1)

Σε τέτοιους πίνακες μπορούμε να ελέγξουμε αν η πράξη έχει ουδέτερο στοιχείο e ή αν είναι αντιμεταθετική.

Πραγματικά, το e είναι ουδέτερο στοιχείο, αν η γραμμή και η στήλη που έχουν το e στην κορυφή είναι οι ίδιες με την αρχική γραμμή και στήλη, αντίστοιχα (σχ.2)

*	x	y	...	e	...	k
x						
y						
...						
e	x	y	...	e	...	k
...						
k						

(σχ.2)

και η πράξη είναι αντιμεταθετική αν ο πίνακας είναι συμμετρικός ως προς τη διαγώνιο του (σχ.3)

*	...	x	...	y
...				
x				
...				
y				

$x*y$

$y*x$

(σχ.3)



Σχέση ισοδυναμίας συμβιβαστή με πράξη .

Ας είναι R μία σχέση ισοδυναμίας στο σύνολο X και $* : X \times X \longrightarrow X$ μία πράξη σ' αυτό .

Θα λέμε ότι η σχέση ισοδυναμίας R συμβιβάζεται με την πράξη $*$ αν-ν

$$\left. \begin{array}{l} x \equiv y(R) \\ x' \equiv y'(R) \end{array} \right\} \implies x * x' \equiv y * y'(R) .$$

Για μία τέτοια συμβιβαστή σχέση R μπορούμε , με τη βοήθεια της πράξης $*$, να ορίσουμε μία νέα "πράξη" $\hat{*}$ στο σύνολο πηλύκο X/R ως εξής

$$\hat{*} : X/R \times X/R \longrightarrow X/R , \quad [x] \hat{*} [x'] = [x * x'] .$$

Εδώ θα πρέπει να εξετάσουμε αν η αντιστοιχία αυτή είναι μία απεικόνιση μ' άλλα λόγια , αν η "πράξη" $\hat{*}$ είναι καλά ορισμένη , δηλαδή αν

$$([x], [x']) = ([y], [y']) \text{ τότε } [x] \hat{*} [x'] = [y] \hat{*} [y'] .$$

Πραγματικά ,

$$\begin{aligned} ([x], [x']) = ([y], [y']) &\implies [x] = [y] \text{ και } [x'] = [y'] \\ &\implies x \equiv y(R) \text{ και } x' \equiv y'(R) \\ &\implies x * x' \equiv y * y'(R) . \end{aligned}$$

(αφού η R είναι συμβιβαστή με την πράξη $*$)

$$\implies [x] \hat{*} [x'] = [y] \hat{*} [y']$$

όπως το θέλαμε .

Παράδειγμα .

Στο σύνολο $\mathbb{Z}$ των ακεραίων η αριθμητική ισοδυναμία R_m είναι συμβιβαστή με την πρόσθεση και με τον πολ/σμό του $\mathbb{Z}$.

Πραγματικά , έχουμε :

$$\left. \begin{array}{l} x \equiv y(R_m) \\ x' \equiv y'(R_m) \end{array} \right\} \iff \left\{ \begin{array}{l} x - y = km \\ x' - y' = k'm \end{array} \right. \quad (1)$$



Προσθέτοντας τις σχέσεις (1) κατά μέλη , παίρνουμε :

$$(x+x')-(y+y') = (k+k')m \quad , \quad \text{δηλαδή}$$

$$x+x' \equiv y+y' \pmod{m} \quad .$$

Αν πολ/σουμε την πρώτη των (1) με x' και τη δεύτερη με y και τις προσθέ-
σουμε , έχουμε :

$$xx' - yy' = (kx' + x'y)m \quad \text{δηλαδή}$$

$$xx' \equiv yy' \pmod{m} \quad .$$

Έτσι μπορούμε να ορίσουμε στο σύνολο $Z_m = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$ δύο νέες πράξεις

$$+ : Z_m \times Z_m \longrightarrow Z_m \quad , \quad \bar{a} + \bar{b} = \overline{a+b} \quad , \quad \forall \bar{a}, \bar{b} \in Z_m$$

$$\cdot : Z_m \times Z_m \longrightarrow Z_m \quad , \quad \bar{a} \cdot \bar{b} = \overline{a \cdot b} \quad , \quad \forall \bar{a}, \bar{b} \in Z_m \quad .$$

που εύκολα διαπιστώνουμε ότι είναι αντιμεταθετικές και προσεταιριστικές .

Έτσι , οι πίνακες πρόσθεσης και πολ/σμού στο Z_6 είναι οι εξής :

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

.	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

ΟΡΙΣΜΟΣ .

Μία σχέση ισοδυναμίας R σ'ένα σύνολο X , λέμε ότι έχει πεπερασμένο δείκτη , αν το σύνολο πηλίκο X/R είναι πεπερασμένο .

Για παράδειγμα , η αριθμητική ισοδυναμία R_m στο Z έχει πεπερασμένο δείκτη , αφού

$$Z_m = Z/R_m = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\} \quad .$$



ΚΕΦΑΛΑΙΟ I

ΜΟΝΟΕΙΔΗ

§1.1 Μονοειδή

ΟΡΙΣΜΟΣ. Ένα μονοειδές $(M, *)$ είναι ένα ζεύγος που σχηματίζεται από ένα σύνολο M και μια διμελή πράξη

$$*: M \times M \longrightarrow M, \quad (x, y) \longmapsto x * y$$

που είναι

i) προσεταιριστική : $x * (y * z) = (x * y) * z \quad \forall x, y, z \in M$

ii) έχει ουδέτερο στοιχείο, δηλαδή υπάρχει $e \in M$ τέτοιο ώστε

$$x * e = x = e * x \quad \forall x \in M.$$

θα λέμε το μονοειδές $(M, *)$ αντιμεταθετικό όταν

$$x * y = y * x, \quad \forall x, y \in M.$$

Παρατηρήσεις.

1) Σ' ένα μονοειδές $(M, *)$, το ουδέτερο στοιχείο e είναι μοναδικό. Έτσι θα το συμβολίζουμε με 1 (αντ. 0) αν η πράξη $*$ σημειώνεται πολλαπλασιαστικά (αντ. προσθετικά).

2) Το $M \neq \emptyset$ αφού $e \in M$.

3) Ισχύει ο γενικευμένος προσεταιριστικός νόμος.



Ορίζοντας λοιπόν

$$x^0 = e \quad \forall x \in M$$

μπορούμε να μιλάμε για τις φυσικές δυνάμεις ενός στοιχείου $x \in E$.

Έτσι έχουμε

Πολλαπλασιαστικά

$$x^0 = 1$$

$$x^1 = x$$

$$x^m = x^{m-1}x, \quad \forall m \in \mathbb{N}, m > 1$$

Προσθετικά

$$0x = 0$$

$$1x = x$$

$$mx = (m-1)x + x \quad \forall m \in \mathbb{N}, m > 1.$$

Παραδείγματα.

1) Τα σύνολα $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ των φυσικών, ακεραίων, ρητών, πραγματικών και μιγαδικών αντίστοιχα, με πράξη τη συνηθισμένη πρόσθεση, είναι αντιμεταθετικά μονοειδή.

2) Για ένα σύνολο $A \neq \emptyset$, το σύνολο

$$\text{Hom}(A, A) = \{f: A \longrightarrow A / f \text{ απεικόνιση}\}$$

με πράξη τη σύνθεση απεικονίσεων

$$(f, h) \longmapsto h \circ f$$

είναι μονοειδές, με ουδέτερο στοιχείο την ταυτοτική απεικόνιση

$I_A: A \longrightarrow A$. Το μονοειδές αυτό είναι γενικά μη-αντιμεταθετικό.

3) Το σύνολο $P(E)$ όλων των υποσυνόλων ενός συνόλου E γίνεται μονοειδές.

i) με πράξη την τομή " $\cap$ " και ουδέτερο στοιχείο το E

ii) με πράξη την ένωση " $\cup$ " και ουδέτερο στοιχείο το $\emptyset$.

4) Υπενθυμίζουμε ότι μια αριθμητική συνάρτηση f είναι μια απεικόνιση $f: \mathbb{N}^* \longrightarrow \mathbb{C}$.

Στο σύνολο $\mathcal{A}$ των αριθμητικών συναρτήσεων ορίζουμε μια πράξη (ενελικτικό γινόμενο)

$$*: \mathcal{A} \times \mathcal{A} \longrightarrow \mathcal{A}, \quad (f, g) \longmapsto f * g$$



όπου, $f * g$ είναι η αριθμητική συνάρτηση που ορίζεται από τη σχέση

$$(f * g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right) = \sum_{st=n} f(s)g(t) \quad , \quad \forall n \in \mathbb{N}^* .$$

(Το πρώτο άθροισμα εκτείνεται πάνω σ' όλους τους φυσικούς διαιρέτες του n , ενώ το δεύτερο πάνω σ' όλα τα διατεταγμένα ζεύγη (s, t) φυσικών αριθμών με $st = n$).

Το ζεύγος $(\mathcal{A}, *)$ είναι ένα αντιμεταθετικό μονοειδές.

Για κάθε $f, g, h \in \mathcal{A}$ έχουμε $(f * (g * h)) = ((f * g) * h)$

Πραγματικά, $\forall n \in \mathbb{N}$ είναι

$$\begin{aligned} (f * (g * h))(n) &= \sum_{st=n} f(s)(g * h)(t) = \sum_{st=n} f(s) \left(\sum_{rp=t} g(r)h(p) \right) = \\ &= \sum_{srp=n} f(s)g(r)h(p) . \end{aligned}$$

Όμοια

$$\begin{aligned} ((f * g) * h)(n) &= \sum_{kp=n} (f * g)(k)h(p) = \sum_{kp=n} \left(\sum_{sr=k} f(s)g(r) \right) h(p) = \\ &= \sum_{srp=n} f(s)g(r)h(p) . \end{aligned}$$

Η αριθμητική συνάρτηση $\varepsilon: \mathbb{N}^* \longrightarrow \mathbb{C}$ που ορίζεται από

$$\varepsilon(n) = \begin{cases} 1 & \text{όταν } n=1 \\ 0 & \text{όταν } n>1 \end{cases}$$

είναι το ουδέτερο στοιχείο. Θα δείξουμε ότι

$$\varepsilon * f = f = f * \varepsilon \quad \forall f \in \mathcal{A} .$$

Πραγματικά, $\forall n \in \mathbb{N}^*$ είναι

$$(\varepsilon * f)(n) = \sum_{st=n} \varepsilon(s)f(t) = \varepsilon(1)f(n) = f(n)$$

και όμοια



$$(f * e)(n) = f(n) \quad .$$

Τέλος , εύκολα αποδεικνύεται ότι η πράξη $*$ είναι αντιμεταθετική .

Θα σημειώσουμε εδώ ότι ο ρόλος του μονοειδούς $(\mathbb{Z}, +)$ στη θεωρία Αριθμών είναι βασικός .

§1.2. Υπομονοειδή

ΟΡΙΣΜΟΣ. Ένα υποσύνολο S ενός μονοειδούς $(M, *)$, που είναι κλειστό ως προς την πράξη $*$ και περιέχει το ουδέτερο στοιχείο του M , το καλούμε υπομονοειδές του M , δηλαδή αν

$$i) \forall x, y \in S \implies x * y \in S$$

$$ii) e \in S \quad .$$

Το υπομονοειδές S είναι φανερά και αυτό ένα μονοειδές ως προς την πράξη $*$. Για παράδειγμα , το σύνολο των άρτιων ακεραίων $2\mathbb{Z} = \{2k/k \in \mathbb{Z}\}$ είναι υπομονοειδές του $(\mathbb{Z}, +)$ αφού

$$\forall 2k_1, 2k_2 \in 2\mathbb{Z} \implies 2k_1 + 2k_2 = 2(k_1 + k_2) \in 2\mathbb{Z}$$

και $0 \in 2\mathbb{Z}$, ενώ το $2\mathbb{Z}$ δεν είναι υπομονοειδές του $(\mathbb{Z}, -)$ αφού το $1 \notin 2\mathbb{Z}$.

Και το κλασσικό αποτέλεσμα .

ΠΡΟΤΑΣΗ 1. Αν A και B είναι υπομονοειδή του μονοειδούς $(M, *)$, τότε και η τομή τους $A \cap B$ είναι υπομονοειδές του M .

Απόδειξη.

Αν e είναι το ουδέτερο στοιχείο του M , τότε

$$e \in A \cap B \quad , \text{ αφού } e \in A \text{ και } e \in B \quad .$$

Μένει να δείξουμε ότι αν $x, y \in A \cap B$ τότε $x * y \in A \cap B$. Πραγματικά , αν $x, y \in A \cap B$ τότε $x, y \in A$ και $x, y \in B$, οπότε $x * y \in A$, $x * y \in B$ άρα $x * y \in A \cap B$.

Με τον ίδιο τρόπο αποδεικνύεται ότι , αν $\{A_i\}_{i \in I}$ είναι μια οικογένεια υπομονοειδών ενός μονοειδούς $(M, *)$ και η τομή τους



$\bigcap_{i \in I} A_i$ είναι ένα υπομονοειδές του M .

Ας είναι S ένα υποσύνολο ενός μονοειδούς $(M, *)$. Από τα προηγούμενα συμπεραίνουμε ότι :

"η τομή όλων των υπομονοειδών του M που περιέχουν το S είναι υπομονοειδές του M , συμβολισμός $\langle S \rangle$ " και είναι το $\langle S \rangle$ φανερά το "μικρότερο" υπομονοειδές του M που περιέχει το S (με την έννοια ότι περιέχεται σε κάθε υπομονοειδές που περιέχει το S) .

Καλούμε το $\langle S \rangle$ υπομονοειδές που παράγεται από το σύνολο S .

Έτσι, για παράδειγμα, αν $S = \emptyset$ τότε $\langle \emptyset \rangle$ είναι το υπομονοειδές $\{e\}$, ενώ, αν το S είναι υπομονοειδές, τότε $\langle S \rangle = S$.

Το $\langle S \rangle$ περιγράφεται από την επόμενη πρόταση.

ΠΡΟΤΑΣΗ 2. Ας είναι $(M, *)$ ένα μονοειδές με ουδέτερο στοιχείο e και S ένα υποσύνολο του M με $e \in S$.

Τότε το $\langle S \rangle$ είναι το σύνολο όλων των πεπερασμένων γινομένων από στοιχεία του S , δηλ.

$$\langle S \rangle = \{s_1 * \dots * s_n / n \in \mathbb{Z}^+, s_i \in S, i=1, \dots, n\}$$

Απόδειξη.

Το $\langle S \rangle$ είναι υπομονοειδές του M .

Πραγματικά, $\forall s_1 * \dots * s_k, s'_1 * \dots * s'_l \in \langle S \rangle$ είναι

$$(s_1 * \dots * s_k) * (s'_1 * \dots * s'_l) = s_1 * \dots * s'_l \in \langle S \rangle \text{ και } e \in \langle S \rangle \text{ αφού } e \in S.$$

Από τον ορισμό του, το $\langle S \rangle$ περιέχει το S .

Μένει να δείξουμε ότι είναι το μικρότερο υπομονοειδές του M που περιέχει το S .

Ας είναι F ένα άλλο υπομονοειδές του M που περιέχει το S . Αν $s_1, \dots, s_k \in S$, τότε, επειδή $S \subseteq F$ και το F υπομονοειδές, έχουμε $s_1 * \dots * s_k \in F$, δηλ. το τυχόν $s_1 * \dots * s_k \in \langle S \rangle$ ανήκει και στο



F , άρα $\langle S \rangle \subseteq F$.

Παρατήρηση.

Αν το $e \notin S$, τότε παίρνουμε το σύνολο $S \cup \{e\}$ και πέφτουμε στην προηγούμενη περίπτωση.

§2. Μονοειδές πηλίκο.

Ας είναι $(M, *)$ ένα μονοειδές και R μια σχέση ισοδυναμίας στο M συμβιβαστή με την πράξη $*$. Στο σύνολο πηλίκο M/R ορίζεται τότε μια πράξη $\hat{*}$ ως εξής (βλέπε Κεφ. 0, §5)

$$\forall [x], [y] \in M/R, [x] \hat{*} [y] = [x * y].$$

Το M/R εφοδιασμένο με την πράξη $\hat{*}$ γίνεται μονοειδές, που ονομάζεται **μονοειδές πηλίκο**.

Πραγματικά, η προσεταιριστικότητα της πράξης συμπεραίνεται απλά από την προσεταιριστικότητα της $*$, ενώ το ουδέτερο στοιχείο είναι η κλάση $[e]$, αφού $\forall [x] \in M/R$ έχουμε,

$$[x] \hat{*} [e] = [x * e] = [x] = [e * x] = [e] \hat{*} [x].$$

Παράδειγμα 1.

Στα μονοειδή $(\mathbb{Z}, +)$ και $(\mathbb{Z}, \cdot)$ η σχέση ισοδυναμίας R_m συμβιβάζεται και με την πρόσθεση και τον πολ/σμό. (βλέπε Κεφ. 0, §5). Έτσι έχουμε τα μονοειδή.

α) $(\mathbb{Z}_m, +)$ με ουδέτερο στοιχείο την κλάση $\bar{0}$

β) $(\mathbb{Z}_m, \cdot)$ με ουδέτερο στοιχείο την κλάση $\bar{1}$

όπου

$$\begin{cases} \bar{a} + \bar{b} = \overline{a+b} \\ \bar{a} \cdot \bar{b} = \overline{a \cdot b} \end{cases} \quad \forall \bar{a}, \bar{b} \in \mathbb{Z}_m.$$

§3. Ομομορφισμοί Μονοειδών.

Ας είναι $(M, *)$ και $(N, *)$ δύο μονοειδή.

Μια απεικόνιση

$$f: M \longrightarrow N$$



ονομάζεται ομομορφισμός μονοειδών όταν

$$0_1) f(x*y) = f(x)*f(y) \quad \forall x, y \in M$$

$$0_2) f(e_M) = e_N$$

όπου e_M και e_N τα ουδέτερα στοιχεία των M και N αντίστοιχα .

Ένας ομομορφισμός $f: M \longrightarrow N$ καλείται :

επιμορφισμός , αν η f είναι επί .

μονομορφισμός , αν η f είναι 1-1 .

ισομορφισμός , αν η f είναι 1-1 και επί . Στην περίπτωση αυτή καλούμε τα μονοειδή $(M, *)$ και $(N, *)$ ισομορφα και το συμβολίζουμε

$$M \cong N .$$

Είναι φανερό ότι :

Αν $f: M \longrightarrow M'$ είναι ένας ομομορφισμός μονοειδών , τότε ο f είναι ισομορφισμός , εάν και μόνο εάν υπάρχει ομομορφισμός $g: M' \longrightarrow M$ έτσι ώστε $g \circ f = I_M$ και $f \circ g = I_{M'}$.

Παραδείγματα

1) Η απεικόνιση $f: (P(E), \cup) \longrightarrow (P(E), \cap)$ που ορίζεται από

$$f(X) = C_E X \quad , \quad \forall X \in P(E)$$

είναι ένας ομομορφισμός μονοειδών , αφού

$$0_1) \quad \forall X, Y \in P(E) \quad \text{είναι}$$

$$f(X \cup Y) = C_E (X \cup Y) = C_E X \cap C_E Y = f(X) \cap f(Y)$$

και

$$0_2) f(\emptyset) = C_E \emptyset = E .$$

Η f είναι επιπλέον και 1-1 και επί .

Πραγματικά , αν $f(X) = f(Y)$, δηλ. $C_E X = C_E Y$, τότε $X = Y$ (Η f είναι 1-1) .

Τέλος, για κάθε $X \in P(E)$, υπάρχει το $C_E X$ με

$$f(C_E X) = C_E (C_E X) = X \quad (\text{Η } f \text{ είναι επί}) .$$



Έτσι η f είναι ισομορφισμός, οπότε

$$(P(E), \cup) \cong (P(E), \cap) .$$

2) Αν R είναι μια σχέση ισοδυναμίας συμβιβαστή με την πράξη του μονοειδούς, τότε η κανονική προβολή

$$p: (M, *) \longrightarrow (M/R, \hat{*}) , \quad p(m) = [m] , \quad \forall m \in M$$

είναι ένας επιμορφισμός, αφού

$$0_1) \quad \forall m, n \in M , \quad p(m * n) = [m * n] = [m] \hat{*} [n] = p(m) \hat{*} p(n)$$

$$0_2) \quad p(e_M) = [e_M]$$

και η p είναι φανερά επί.

3) Αν f, g είναι ομομορφισμοί μονοειδών

$$(M, *) \xrightarrow{f} (N, *) \xrightarrow{g} (A, *)$$

τότε και η σύνθεσή τους

$$g \circ f: (M, *) \longrightarrow (A, *)$$

είναι ένας ομομορφισμός μονοειδών. (Άσκηση).

ΠΡΟΤΑΣΗ 3. Ας είναι $f: (M, *) \longrightarrow (N, *)$ ένας ομομορφισμός μονοειδών.

α) Αν A είναι ένα υπομονοειδές του M , τότε και η εικόνα του $f(A)$ είναι υπομονοειδές του N .

β) Αν B είναι ένα υπομονοειδές του N , τότε και η αντίστροφη εικόνα του $f^{-1}(B)$ είναι υπομονοειδές του M .

Απόδειξη.

α) Έχουμε $f(A) = \{y/y \in N \text{ και } \exists x \in A, \text{ έτσι ώστε } f(x) = y\}$.
Αν $y_1, y_2 \in f(A)$, τότε υπάρχουν $x_1, x_2 \in A$ με

$$f(x_1) = y_1 \text{ και } f(x_2) = y_2$$

οπότε



$$y_1 * y_2 = f(x_1) * f(x_2) \stackrel{f \text{ ομομ.}}{=} f(x_1 * x_2)$$

με το $x_1 * x_2 \in A$ αφού το A υπομονοειδές .

Έτσι $\forall y_1, y_2 \in f(A) \Rightarrow y_1 * y_2 \in f(A)$.

Επιπλέον , επειδή $e_M \in A$ και $f(e_M) = e_N$, έχουμε $e_N \in f(A)$.

β) Είναι $f^{-1}(B) = \{x/x \in M \text{ και } f(x) \in B\}$.

Το $e_M \in f^{-1}(B)$, αφού $f(e_M) = e_N \in B$.

Αν τώρα $x, y \in f^{-1}(B)$, τότε $f(x) , f(y) \in B$

οπότε $f(x * y) = f(x) * f(y) \in B$ δηλ. $x * y \in f^{-1}(B)$.■

Ας είναι τώρα $f: M \longrightarrow N$ ένας ομομορφισμός μονοειδών . Η πυρηνική ισοδυναμία R_f στο M

$$a = a'(R_f) \iff f(a) = f(a')$$

είναι συμβιβαστή με την πράξη του M .

Πραγματικά

$$\left. \begin{array}{l} a = a'(R_f) \\ b = b'(R_f) \end{array} \right\} \iff \begin{array}{l} f(a) = f(a') \\ f(b) = f(b') \end{array}$$

επομένως

$$f(a * b) = f(a) * f(b) = f(a') * f(b') = f(a' * b')$$

δηλαδή $a * b \equiv a' * b'(R_f)$.

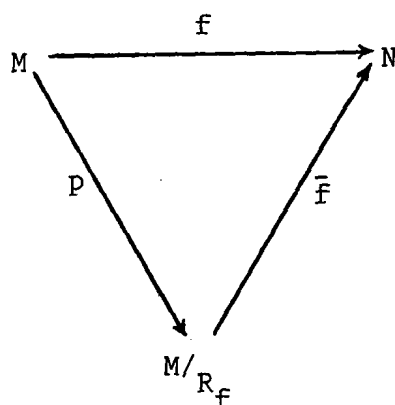
Η R_f λοιπόν δομεί το σύνολο πηλύκο M/R_f σε μονοειδές $(M/R_f, \hat{*})$, όπου

$$\forall [a], [b] \in M/R_f, [a] \hat{*} [b] = [a * b] .$$

Θα παρατηρήσουμε , στη συνέχεια , (βλέπε θεωρ.2, Κεφ.0, §4) ότι η απεικόνιση $f: M \longrightarrow N$ γράφεται σαν σύνθεση μιας επί p και μιας 1-1 $\bar{f}$ όπου p είναι η κανονική προβολή (επιμορφισμός)



$$p(x) = [x] \quad \text{και} \quad \bar{f}([x]) = f(x) \quad .$$



Ο $\bar{f}$ είναι ομομορφισμός . Πραγματικά , $\forall [x], [y] \in M/R_f$ έχουμε

$$\begin{aligned} \bar{f}([x] * [y]) &= \bar{f}([x*y]) = f(x*y) = f(x) * f(y) \\ &= \bar{f}([x]) * \bar{f}([y]) \quad . \end{aligned}$$

και

$$\bar{f}([e_M]) = f(e_M) = e_N \quad .$$

Έτσι κάθε ομομορφισμός μονοειδών $f : (M, *) \rightarrow (N, *)$ γράφεται σαν σύνθεση

$$f = \bar{f} \circ p$$

ενός επιμορφισμού και ενός μονομορφισμού .

Ας παρατηρήσουμε ότι για τις εικόνες έχουμε

$$\bar{f}(M/R_f) = f(M) \quad .$$

Θεωρώντας τον μονομορφισμό $\bar{f}$ σαν απεικόνιση

$$\bar{f} : M/R_f \longrightarrow f(M)$$

ο $\bar{f}$ είναι ένας ισομορφισμός μονοειδών , οπότε

$$M/R_f \simeq f(M) \quad .$$

Δείξαμε λοιπόν .



ΘΕΩΡΗΜΑ 1. (Ομομορφισμού) Ας είναι R_f η κυρηνική ισοδυναμία που ορίζει ένας ομομορφισμός μονοειδών $f: (M, *) \longrightarrow (N, *)$. Το μονοειδές πηλύκο $(M/R_f, *)$ είναι ισομορφο με την εικόνα $f(M)$ του μονοειδούς M , δηλ.

$$M/R_f \cong f(M) \quad . \blacksquare$$

Παράδειγμα 1. θεωρήστε τα μονοειδή $(M, *)$ και $(M', *)$ με πίνακες πολ/σμού αντίστοιχα τους : (1) και (2)

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	b	b	b
c	c	c	c	c

(1)

$*$	$\bar{e}$	γ
$\bar{e}$	$\bar{e}$	γ
γ	γ	γ

(2)

Η απεικόνιση $f: M \longrightarrow M'$ με

$$f(e) = \bar{e}, \quad f(a) = \bar{e}, \quad f(b) = \gamma, \quad f(c) = \gamma$$

είναι ένας επιμορφισμός μονοειδών, οπότε $f(M) = M'$.

Για την κυρηνική ισοδυναμία R_f ισχύει $R_f(e) = R_f(a)$ και $R_f(b) = R_f(c)$ έτσι

$$M/R_f = \{R_f(e), R_f(b)\},$$

Η απεικόνιση $\bar{f}: M/R_f \longrightarrow M'$ με

$$\bar{f}(R_f(e)) = \bar{e} \quad \text{και} \quad \bar{f}(R_f(b)) = \gamma$$

είναι ισομορφισμός, οπότε $M/R_f \cong M'$.

Ας είναι $(X, *)$ ένα μονοειδές με ουδέτερο στοιχείο e και $\text{Hom}(X, X)$ το μονοειδές όλων των απεικονίσεων του X στο X με πράξη τη σύνθεση απεικονίσεων.

ΘΕΩΡΗΜΑ 2. (Gayley). Κάθε μονοειδές $(X, *)$ είναι ισομορφο με ένα υπομονοειδές του $\text{Hom}(X, X)$.



Απόδειξη. θεωρούμε την απεικόνιση $f: X \longrightarrow \text{Hom}(X, X)$, $x \longmapsto f_x$

όπου η απεικόνιση $f_x: X \longrightarrow X$ ορίζεται ως εξής :

$$f_x(z) = x * z \quad \forall z \in X .$$

Η f είναι 1-1 . Πραγματικά , αν $f_x = f_y$, τότε $f_x(e) = f_y(e)$,
δηλ. $x * e = y * e \implies x = y$.

Η f είναι ομομορφισμός· αρκεί να δείξουμε

$$\alpha) f_{x_1 * x_2} = f_{x_1} \circ f_{x_2} , \quad \forall x_1, x_2 \in X$$

$$\beta) f_e = I_X .$$

Για το α) έχουμε : $\forall z \in X$, $f_{x_1 * x_2}(z) = (x_1 * x_2) * z$. Απ' την άλλη μεριά

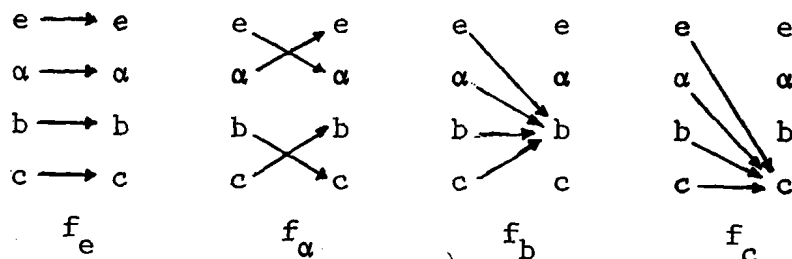
$$\begin{aligned} (f_{x_1} \circ f_{x_2})(z) &= f_{x_1}(f_{x_2}(z)) = f_{x_1}(x_2 * z) = \\ &= x_1 * (x_2 * z) = (x_1 * x_2) * z \end{aligned}$$

όπως το επιθυμούσαμε .

Για το β) παρατηρούμε ότι $\forall z \in X$ είναι $f_e(z) = e * z = z = I_X(z)$.

Η f είναι λοιπόν μονομορφισμός , και αν την θεωρήσουμε σαν απεικόνιση $X \longrightarrow f(X)$ είναι ισομορφισμός . Άρα $X \cong f(X)$. ■

Παράδειγμα 2. Ας είναι $(M, *)$ το μονοειδές του προηγούμενου παραδείγματος . Εδώ έχουμε τις απεικονίσεις f_e, f_a, f_b, f_c , όπως αυτές δίνονται από το επόμενο σχήμα



Έτσι , για τον ομομορφισμό $f: M \longrightarrow \text{Hom}(M, M)$ έχουμε ότι

$$f(M) = \{f_e, f_a, f_b, f_c\}$$



που είναι υπομονοειδές του $\text{Hom}(M, M)$ με πίνακα πολ/σμού

$\circ$	f_e	f_a	f_b	f_c
f_e	f_e	f_a	f_b	f_c
f_a	f_a	f_e	f_c	f_b
f_b	f_b	f_b	f_b	f_b
f_c	f_c	f_c	f_c	f_c

Ο ομομορφισμός $M \longrightarrow f(M)$ με $e \longmapsto f_e$, $a \longmapsto f_a$, $b \longmapsto f_b$, $c \longmapsto f_c$ είναι ισομορφισμός, οπότε

$$M \simeq f(M).$$

§4. Ελεύθερα μονοειδή.

Ας είναι X ένα σύνολο, το αλφάβητο μας, τα στοιχεία του οποίου θα τα καλούμε γράμματα.

Μια λέξη w με μήκος $\ell(w) = n \geq 1$, από το αλφάβητο X , είναι ένα στοιχείο του συνόλου $X^n = \underbrace{X \times \dots \times X}_{n\text{-φορές}}$ δηλαδή

$$w = (x_1, \dots, x_n), \text{ όπου } x_i \in X \text{ για κάθε } 1 \leq i \leq n$$

που στη συνέχεια θα σημειώνουμε :

$$w = x_1 \dots x_n.$$

Έτσι τα στοιχεία του X είναι λέξεις με μήκος 1, του X^2 με μήκος 2 κ.ο.κ.

θα συμβολίζουμε με Λ τη λέξη χωρίς γράμματα και θα την καλούμε κενή λέξη. Το μήκος της είναι $\ell(\Lambda) = 0$.

Το σύνολο όλων των λέξεων w , με μήκος ≥ 0 , που παράγονται από το αλφάβητο X , το σημειώνουμε X^* δηλ.

$$X^* = \{w/w \text{ λέξη από το } X \text{ με } \ell(w) \geq 0\}.$$



$$\begin{aligned} &= x_1 \dots x_n y_1 \dots y_k z_1 \dots z_l = (x_1 \dots x_n y_1 \dots y_k) \cdot (z_1 \dots z_l) = \\ &= [(x_1 \dots x_n) \cdot (y_1 \dots y_k)] \cdot (z_1 \dots z_l) . \end{aligned}$$

Για την κενή λέξη Λ έχουμε ,

$$\Lambda \cdot w = w = w \cdot \Lambda , \quad \forall w \in X^*$$

Το σύνολο λοιπόν X^* με την παραπάνω πράξη δομείται σε μονοειδές με ουδέτερο στοιχείο την κενή λέξη Λ . Το μονοειδές αυτό $(X^*, \cdot)$ καλείται Ελεύθερο μονοειδές που παράγεται από το σύνολο X .

Παρατήρηση.

Η πράξη " $\cdot$ " δεν είναι γενικά αντιμεταθετική , ενώ κάθε λέξη $x_1 \dots x_n \in X^*$, με μήκος n , μπορούμε να την γράψουμε σαν γινόμενο λέξεων μήκους 1 ως εξής :

$$x_1 \dots x_n = x_1 \cdot \dots \cdot x_n .$$

Παράδειγμα 2. Αν $X = \{0,1\}$ τότε $X^* = \{\Lambda, 0, 1, 00, 01, 10, 11, 000, 001, \dots\}$ και

$$01 \cdot 101 = 01101$$

$$101 \cdot 01 = 10101$$

$$01 \cdot \Lambda = 01 = \Lambda \cdot 01 .$$

Παράδειγμα 3 . Η 1-1 και επί απεικόνιση $h : \mathbb{N} \rightarrow \{x\}^*$ του παραδείγματος 1 είναι ένας ισομορφισμός του προσθετικού μονοειδούς $(\mathbb{N}, +)$ στο μονοειδές $(\{x\}^*, \cdot)$.

Η h είναι ομομορφισμός . Πραγματικά , $\forall m, n \in \mathbb{N}$ έχουμε

$$h(m+n) = \underbrace{x \dots x}_{m+n \text{ φορές}} = \underbrace{(x \dots x)}_{m \text{ φορές}} \cdot \underbrace{(x \dots x)}_{n \text{ φορές}} = h(m) \cdot h(n)$$

και $h(0) = \Lambda$. Έτσι



$$(N, +) \simeq (\{x\}^*, -)$$

Υπάρχει ένα σπουδαίο θεώρημα που μας χαρακτηρίζει τα ελεύθερα μονοειδή .

ΘΕΩΡΗΜΑ 3. Το ελεύθερο μονοειδές $(X^*, -)$ έχει την εξής χαρακτηριστική ιδιότητα . Για κάθε άλλο μονοειδές $(M, *)$, και για οποιαδήποτε απεικόνιση $\varphi: X \longrightarrow M$, υπάρχει μοναδικός ομομορφισμός

$$\hat{\varphi}: (X^*, -) \longrightarrow (M, *)$$

που προεκτείνει την φ , που κάνει δηλ. το επόμενο διάγραμμα αντιμεταθετικό

$$(3) \quad \begin{array}{ccc} X & \xrightarrow{i} & X^* \\ & \searrow \varphi & \downarrow \hat{\varphi} \\ & & M \end{array} \quad \varphi = \hat{\varphi} \circ i$$

όπου η απεικόνιση i ορίζεται από $i(x) = x$, $\forall x \in X$.

Απόδειξη. Ας είναι $\varphi: X \longrightarrow M$ μια τυχούσα απεικόνιση . Ορίζουμε την απεικόνιση

$$\hat{\varphi}: X^* \longrightarrow M$$

ως εξής

$$\left. \begin{array}{l} \hat{\varphi}(\Lambda) = e_M \\ \text{Για κάθε λέξη } x_1 \dots x_n \in X^* , \text{ με μήκος } n , \text{ να είναι} \\ \hat{\varphi}(x_1 \dots x_n) = \varphi(x_1) * \varphi(x_2) * \dots * \varphi(x_n) \end{array} \right\} \quad (4)$$

Η $\hat{\varphi}$ είναι ομομορφισμός μονοειδών τέτοιος ώστε $\varphi = \hat{\varphi} \circ i$.

Πραγματικά , $\hat{\varphi}(\Lambda) = e_M$ και για κάθε $x_1 \dots x_n , y_1 \dots y_k \in X^*$, με μήκη



αντίστοιχα v και k ισχύει

$$\begin{aligned}\hat{\varphi}((x_1 \dots x_v) \cdot (y_1 \dots y_k)) &= \hat{\varphi}(x_1 \dots x_v y_1 \dots y_k) = \\ &= \varphi(x_1) * \dots * \varphi(x_v) * \varphi(y_1) * \dots * \varphi(y_k) \\ &= \hat{\varphi}(x_1 \dots x_v) * \hat{\varphi}(y_1 \dots y_k) .\end{aligned}$$

Επιπλέον

$$(\hat{\varphi} \circ i)(x) = \hat{\varphi}(i(x)) = \hat{\varphi}(x) = \varphi(x) \quad \forall x \in X .$$

Η μοναδικότητα του $\hat{\varphi}$. Ας υποθέσουμε ότι υπάρχει και άλλος ομομορφισμός

$$h: X^* \longrightarrow M \quad \text{με} \quad h \circ i = \varphi \quad (5)$$

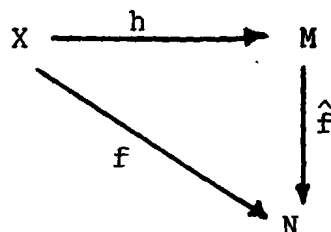
Τότε $h(\Lambda) = e_M = \hat{\varphi}(\Lambda)$, και για κάθε $x_1 \dots x_v \in X^*$ με μήκος v έχουμε

$$\begin{aligned}(4) \quad \hat{\varphi}(x_1 \dots x_v) &= \varphi(x_1) * \dots * \varphi(x_v) = (5) \\ &= (h \circ i)(x_1) * \dots * (h \circ i)(x_v) \\ &= h(i(x_1)) * \dots * h(i(x_v)) = h(x_1) * \dots * h(x_v) \\ &\stackrel{\text{h ομομ}}{=} h(x_1 \dots x_v) = h(x_1 \dots x_v) .\end{aligned}$$

Άρα $\hat{\varphi} = h$, όπως επιθυμούσαμε. ■

Θεωρούμε ένα (μη κενό) σύνολο X

Θεώρημα 4. (Μοναδικότητας). Αν $(M, \cdot)$ είναι ένα μονοειδές και $h: X \longrightarrow M$ μια απεικόνιση τέτοια ώστε, κάθε άλλο μονοειδές $(N, \cdot)$ και κάθε απεικόνιση $f: X \longrightarrow N$ να ορίζουν μοναδικό ομομορφισμό μονοειδών $\hat{f}: (M, \cdot) \longrightarrow (N, \cdot)$ που να κάνει αντιμεταθετικό το διάγραμμα



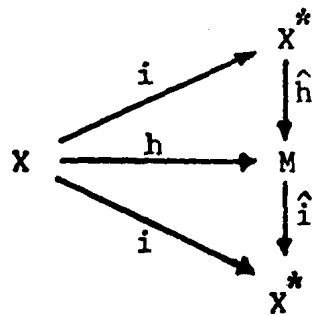
$$f = \hat{f} \circ h$$



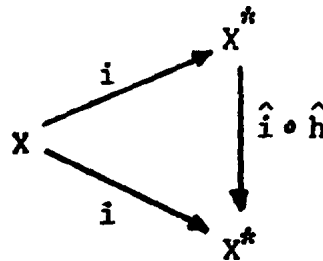
Τότε τα μονοειδή $(M, -)$ και X^* είναι ισομορφα δηλαδή $(M, -) \simeq X^*$.

Απόδειξη. Σύμφωνα με το θεώρημα 3 η απεικόνιση $h: X \longrightarrow M$ ορίζει ένα ομομορφισμό $\hat{h}: X^* \longrightarrow M$ τέτοιο ώστε $\hat{h} \circ i = h$.

Με την σειρά της η απεικόνιση $i: X \longrightarrow X^*$ ορίζει σύμφωνα με την υπόθεση μας ένα ομομορφισμό $\hat{i}: M \longrightarrow X^*$ τέτοιο ώστε $\hat{i} \circ h = i$.

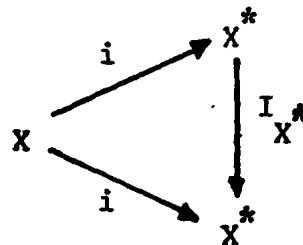


Έτσι η σύνθεση $\hat{i} \circ \hat{h}$ κάνει αντιμεταθετικό το διάγραμμα



αφού $\hat{i} \circ \hat{h} \circ i = \hat{i} \circ h = i$.

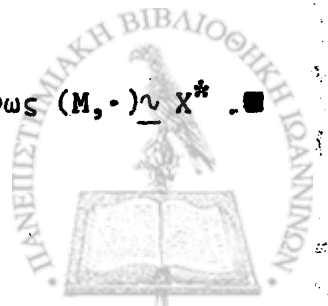
Αλλά και ο ταυτοτικός ομομορφισμός I_{X^*} κάνει αντιμεταθετικό το διάγραμμα



Από το θεώρημα 3 παίρνουμε

$$\hat{i} \circ \hat{h} = I_{X^*}.$$

Με τον ίδιο τρόπο δείχνουμε ότι $\hat{h} \circ \hat{i} = I_M$ και επομένως $(M, -) \simeq X^*$.



Πρόταση 4. Κάθε πεπερασμένο παραγόμενο μονοειδές $(M, *)$ είναι η ομόμορφη εικόνα ενός ελεύθερου μονοειδούς .

Απόδειξη. Υποθέτουμε ότι το M παράγεται από το πεπερασμένο υποσύνολο του

$$A = \{m_1, \dots, m_n\} \subseteq M$$

Αν τώρα πάρουμε το αλφάβητο $X = \{x_1, \dots, x_n\}$ με n στοιχεία και ορίσουμε την απεικόνιση

$$\varphi: X \longrightarrow M \quad \text{με} \quad \varphi(x_i) = m_i \quad \forall i=1, 2, \dots, n$$

η φ προεκτείνεται (θεωρ. 3) σ' ένα ομομορφισμό μονοειδών $\hat{\varphi}: X^* \longrightarrow M$.

Ο $\hat{\varphi}$ είναι επιμορφισμός . Πραγματικά , κάθε $y \in M$ γράφεται

$$y = m_{i_1} * m_{i_2} * \dots * m_{i_k}, \quad m_{i_\lambda} \in A, \quad \forall \lambda \in \{1, \dots, k\},$$

επειδή το A παράγει το M .

Το y είναι η εικόνα της λέξης $x_{i_1} x_{i_2} \dots x_{i_k}$ με μήκος k αφού

$$\hat{\varphi}(x_{i_1} \dots x_{i_k}) = \varphi(x_{i_1}) * \dots * \varphi(x_{i_k}) = m_{i_1} * \dots * m_{i_k} = y$$

Έτσι $M = \hat{\varphi}(X^*)$. ■

ΠΟΡΙΣΜΑ 1. Κάθε πεπερασμένο μονοειδές είναι η ομόμορφη εικόνα ενός ελεύθερου μονοειδούς . ■

Παράδειγμα 4. Ας είναι $(M, *)$ το μονοειδές του παραδείγματος 1, §3 .

Το M παράγεται από το σύνολο $A = \{a, b\}$, αφού

$$a * b = c \quad \text{και} \quad a * a = e \tag{6}$$

θεωρούμε το αλφάβητο $X = \{x, y\}$ και ορίζουμε την απεικόνιση

$$\varphi: X \longrightarrow M, \quad \text{με} \quad \varphi(x) = a \quad \text{και} \quad \varphi(y) = b \tag{7}$$

Ο φ επεκτείνεται μοναδικά σ' ένα ομομορφισμό



$$\hat{\varphi}: X^* \longrightarrow M$$

που είναι επιμορφισμός, αφού

$$\begin{aligned} e &= \varphi(\Lambda) \quad , \quad \alpha \stackrel{(7)}{=} \varphi(x) = \hat{\varphi}(x) \quad , \quad b \stackrel{(7)}{=} \varphi(y) = \hat{\varphi}(y) \\ c &\stackrel{(6)}{=} a * b \stackrel{(7)}{=} \varphi(x) * \varphi(y) = \hat{\varphi}(xy) \quad . \end{aligned}$$

Άρα $M = \hat{\varphi}(X^*)$.

55. Εφαρμογές στα αυτόματα και στις γλώσσες

Οι θεωρίες των αυτομάτων και τυπικών γλωσσών εμφανίστηκαν στη δεκαετία του 50. Συγκεκριμένα, το 1956 ο Norm Chomsky πρώτος όρισε τις τυπικές γλώσσες σαν υποσύνολα ελεύθερων μονοειδών, οι δε M. Rabin και D. Scott το 1959 έκαναν την πρώτη συστηματική παρουσίαση της τυπικής θεωρίας των αυτομάτων.

Η σχέση μεταξύ της θεωρίας γλωσσών και της θεωρίας αυτομάτων είναι πολύ ενδιαφέρουσα. Καθεμιά χρησιμοποιείται σαν εργαλείο ή αιτία προβλημάτων για την άλλη. Τα τελευταία 20 χρόνια είχαμε μια δραστήρια ανάπτυξη των δύο θεωριών, που οδήγησε σε μια σαφή μαθηματική παρουσίασή τους, χρησιμοποιώντας θεωρήματα και μεθόδους απόδειξης οι οποίες είναι στην ουσία αλγεβρικές.

Πολλά από τα αποτελέσματα που δημοσιεύτηκαν παρουσιάζουν μεγάλο ενδιαφέρον στη Λογική, Γλωσσολογία, προγραμματισμό, ηλεκτρονικά κυκλώματα, στα φαινόμενα αναπαραγωγής κυττάρων κ.λ.κ.

ΓΛΩΣΣΕΣ.

Ας είναι X ένα πεπερασμένο σύνολο το αλφάβητό μας.

Μία γλώσσα πάνω στο X είναι ένα υποσύνολο L του ελεύθερου μονοειδούς X^* .

Έτσι, το σύνολο των Ελληνικών λέξεων είναι μία γλώσσα πάνω στο αλφάβητο $X = \{\alpha, \beta, \gamma, \dots, \omega\}$.

Όμοια, το σύνολο $L = \{a^n b^n \mid n \geq 0\}$, που περιέχει σαν στοιχεία λέξεις με μόνο a ακολουθούμενες από λέξεις με μόνο b , που έχουν όμως το ίδιο μήκος, είναι μία γλώσσα πάνω στο $X = \{a, b\}$.



Πράξεις πάνω στις γλώσσες από το αλφάβητο X .

Αν $L_1 \subseteq X^*$ και $L_2 \subseteq X^*$ είναι δύο γλώσσες πάνω στο ίδιο αλφάβητο X , τότε μπορούμε να ορίσουμε τις επόμενες βασικές πράξεις.

■ Ένωση $L_1 \cup L_2 = \{w \mid w \in L_1 \text{ ή } w \in L_2\}$

■ Τομή $L_1 \cap L_2 = \{w \mid w \in L_1 \text{ και } w \in L_2\}$

■ Παράθεση (ή γινόμενο) $L_1 L_2 = \{wv \mid w \in L_1 \text{ και } v \in L_2\}$

δηλαδή ονομάζουμε παράθεση των γλωσσών L_1 και L_2 τη γλώσσα που σχηματίζεται αν παραθέσουμε κάθε λέξη της L_1 δίπλα σε κάθε λέξη της L_2 . Για παράδειγμα, αν $X = \{a, b, c\}$ και θεωρήσουμε της γλώσσες $L_1 = \{ab, ba\}$, $L_2 = \{ac, c\}$ τότε

$$L_1 L_2 = \{abac, abc, baac, bac\}.$$

Η παράθεση λέξεων είναι πράξη προσεταιριστική, δηλαδή αν $L_1 \subseteq X^*$, $L_2 \subseteq X^*$, $L_3 \subseteq X^*$ είναι τρεις οποιοσδήποτε γλώσσες, τότε

$$L_1(L_2 L_3) = (L_1 L_2)L_3.$$

Πραγματικά,

$$\begin{aligned} L_1(L_2 L_3) &= \{v(wu) \mid v \in L_1, w \in L_2, u \in L_3\} = \\ &= \{(vw)u \mid v \in L_1, w \in L_2, u \in L_3\} = (L_1 L_2)L_3. \end{aligned}$$

■ Θήκη Μπορούμε επαγωγικά να ορίσουμε την n -στη δύναμη μιας γλώσσας $L \subseteq X^*$ ως εξής:

$$L^0 = \{\Lambda\}$$

$$L^1 = L$$

$$L^2 = LL$$

$\vdots$

$$L^{v+1} = L^v L$$

Θέτουμε

$$L^* = \{\Lambda\} \cup L \cup L^2 \cup \dots = \bigcup_{k=0}^{\infty} L^k.$$



Η γλώσσα $L^* \subseteq X^*$, που ορίστηκε με τον παραπάνω τρόπο ονομάζεται θήκη της γλώσσας L . Δηλαδή η θήκη L^* μιας γλώσσας L περιέχει όλες τις λέξεις που σχηματίζονται, αν παραθέσουμε οποιονδήποτε αριθμό λέξεων της L .

Για παράδειγμα, αν $X = \{a, b, c\}$ και $L = \{bc\}$ θα έχουμε

$$L^0 = \{\Lambda\}$$

$$L^1 = L = \{bc\}$$

$$L^2 = LL = \{bcbc\}$$

$$L^3 = L^2L = \{bcbc bc\}$$

$\vdots$

Έτσι $L^* = \{bc\}^* = \{\Lambda, bc, bc bc, bc bc bc, \dots\}$.

Συντακτική ισοδυναμία της γλώσσας L .

Ας είναι $L \subseteq X^*$ μία γλώσσα. Για κάθε λέξη $u \in X^*$ ορίζουμε το σύνολο

$$L_u = \{(t, s) \mid tus \in L, t, s \in X^*\}.$$

Στο X^* ορίζουμε μία σχέση R_L ως εξής:

$$u_1 = u_2(R_L) \text{ αν-ν } L_{u_1} = L_{u_2}.$$

Θα δείξουμε ότι η R_L είναι μία σχέση ισοδυναμίας στο ελεύθερο μονοειδές X^* συμβιβαστή με την πράξη του.

Είναι φανερό ότι η R_L είναι σχέση ισοδυναμίας. Ας υποθέσουμε ότι

$$u_1 \equiv u_2(R_L) \text{ και } w_1 \equiv w_2(R_L)$$

τότε

$$L_{u_1} = L_{u_2} \text{ και } L_{w_1} = L_{w_2}.$$

Θα δείξουμε ότι

$$L_{u_1 w_1} = L_{u_2 w_2}. \quad (8)$$

Πραγματικά,

$$(t, s) \in L_{u_1 w_1} \iff t u_1 w_1 s \in L \iff (t, w_1 s) \in L_{u_1} = L_{u_2} \iff$$



$$\begin{aligned} \Leftrightarrow tu_2w_1s \in L_1 &\Leftrightarrow (tu_2, s) \in L_{w_1} = L_{w_2} \Leftrightarrow \\ \Leftrightarrow tu_2w_2s \in L &\Leftrightarrow (t, s) \in L_{u_2w_2} \end{aligned}$$

και η (8) ισχύει .

Οπότε

$$u_1w_1 = u_2w_2(R_L) .$$

Η R_L καλείται συντακτική ισοδυναμία της γλώσσας L , ενώ το μονοειδές πηλύκο

$$X^*/R_L$$

καλείται συντακτικό μονοειδές της γλώσσας L .

Η επόμενη πρόταση μας περιγράφει μία βασική ιδιότητα της συντακτικής ισοδυναμίας .

ΠΡΟΤΑΣΗ 5 .

Θεωρούμε τη γλώσσα $L \subseteq X^*$ και την συντακτική ισοδυναμία της R_L .

Τότε ,

$$\alpha) u \equiv w(R_L) \text{ και } u \in L \implies w \in L .$$

β) Για κάθε σχέση ισοδυναμίας S στο X^* συμβιβαστή με την πράξη του τέτοια ώστε

$$u \equiv w(S) \text{ και } u \in L \implies w \in L \quad (9)$$

ισχύει

$$v_1 \equiv v_2(S) \implies v_1 \equiv v_2(R_L)$$

δηλαδή η $S \prec R_L$.

Απόδειξη .

$$\alpha) \text{ Αφού } u \equiv w(R_L) \implies L_u = L_w \quad (10)$$

Αλλά $(\Lambda, \Lambda) \in L_u$ επειδή $\Lambda u \Lambda = u \in L$, έτσι από την (10) έχουμε $(\Lambda, \Lambda) \in L_w$, δηλαδή $w = \Lambda w \Lambda \in L$.

β) Η σχέση

$$v_1 \equiv v_2(S) \implies v_1 \equiv v_2(R_L)$$



είναι ισοδύναμη με την

$$v_1 \equiv v_2(S) \implies L_{v_1} = L_{v_2} \implies L_{v_1} \cap L_{v_2} = L_{v_1} \cap L_{v_2} \implies L_{v_1} \cap L_{v_2} = L_{v_1} \cap L_{v_2}$$

Έστω $(s,t) \in L_{v_1}$. Αφού η S είναι σύμβαστη, θα έχουμε

$$\left. \begin{array}{l} v_1 \equiv v_2(S) \\ s \equiv s(S) \\ t \equiv t(S) \end{array} \right\} \implies sv_1t \equiv sv_2t(S) \quad \text{οπότε} \quad sv_1t \in L_{v_2}$$

Αλλά τότε $sv_1t \in L_{v_2}$ και $sv_1t \in L_{v_1} \implies sv_2t \in L_{v_1}$

οπότε $(s,t) \in L_{v_2}$ και έτσι

$$L_{v_1} \subseteq L_{v_2}$$

Όμοια αποδεικνύεται ότι και

$$L_{v_2} \subseteq L_{v_1}$$

οπότε $L_{v_1} = L_{v_2}$.

Ένας τρόπος για να εντοκίσουμε γλώσσες είναι μέσω των αυτομάτων.

ΑΥΤΟΜΑΤΑ

Ας είναι X ένα αλφάβητο. Μπορούμε να φανταστούμε ένα αυτόματο σαν ένα "μαύρο κουτί" που, όταν το τροφοδοτήσουμε με μια λέξη $x_1 \dots x_n \in X^*$, αυτό την αποδέχεται ή όχι.



(01) Ένα πεπερασμένο αυτόματο είναι μια 5-αδα

$$M = (S, X, \delta, s_0, F)$$

όπου

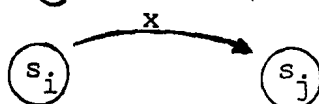
■ S, X, F είναι πεπερασμένα σύνολα

(S είναι το σύνολο των εσωτερικών καταστάσεων, X το αλφάβητο ει-

σόδου και $F \subseteq S$ ένα σύνολο από εσωτερικές καταστάσεις που ονομάζονται τελικές).

- s_0 μια διακεκριμένη αρχική εσωτερική κατάσταση .
- $\delta: S \times X \longrightarrow S$ μια απεικόνιση που ονομάζεται απεικόνιση μετάβασης και μας περιγράφει τη λειτουργία του αυτόματου , δηλ. , αν το αυτόματο βρίσκεται στην εσωτερική κατάσταση s και το τροφοδοτήσουμε με το γράμμα $x \in X$, θα πάει στην εσωτερική κατάσταση $\delta(s,x)$.

Ένα αυτόματο $\mathcal{A}$ μπορεί να παρασταθεί από το διάγραμμα καταστάσεων με κορυφές $\odot$ τις εσωτερικές του καταστάσεις και βέλη



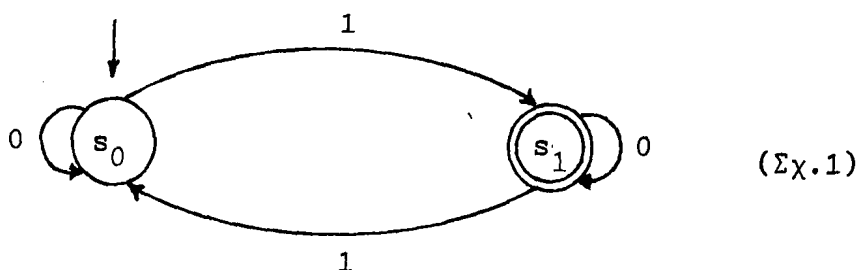
για κάθε γράμμα $x \in X$ τέτοιο ώστε $\delta(s_i, x) = s_j$.

Σε μια τέτοια παράσταση , ο συμβολισμός $\odot$ δηλώνει ότι η εσωτερική κατάσταση s είναι τελική , ενώ ο συμβολισμός $\rightarrow \odot$ σημαίνει ότι η s είναι η αρχική του κατάσταση .

Παράδειγμα 1. Το αυτόματο $\mathcal{A} = (S, X, \delta, s_0, F)$ με $S = \{s_0, s_1\}$, $X = \{0, 1\}$, $F = \{s_1\}$ και απεικόνιση μετάβασης δ που δίνεται από τον παρακάτω πίνακα

δ	0	1
s_0	s_0	s_1
s_1	s_1	s_0

μπορεί να παρασταθεί με το επόμενο διάγραμμα καταστάσεων .



Ας δούμε τώρα πως μεταβάλλονται οι εσωτερικές καταστάσεις ενός αυτόματου $\mathcal{A}$.

Η δ επεκτείνεται επαγωγικά σε μια απεικόνιση

$$\delta^* : S \times X^* \longrightarrow S$$

ως εξής:

- i) Βασικό βήμα : $\delta^*(s, \Lambda) = s \quad \forall s \in S$
- ii) Επαγωγικό βήμα : $\delta^*(s, wx) = \delta(\delta^*(s, w), x), \forall s \in S, w \in X^*, x \in X$ } (11)

Μ' άλλα λόγια, αν το αυτόματο βρίσκεται στην εσωτερική κατάσταση s , αυτή δεν μεταβάλλεται όταν το αυτόματο δεν δε χθεί καμιά λέξη (Βασικό βήμα). αν όμως στην εσωτερική κατάσταση s δεχθεί τη λέξη wx , μας μεταφέρει σε μια νέα εσωτερική κατάσταση $\delta(\delta^*(s, w), x)$ που προκύπτει, δίνοντας πρώτα τη λέξη w (μεταφορά στην εσωτερική κατάσταση $\delta^*(s, w)$), και στη συνέχεια το γράμμα x .

Στη συνέχεια, θα παρατηρήσουμε ότι, για κάθε $s \in S$ και $w, v \in X^*$, έχουμε

$$\delta^*(s, wv) = \delta^*(\delta^*(s, w), v) \quad (12)$$

Για την απόδειξη εργαζόμαστε επαγωγικά πάνω στο μήκος της λέξης v .

Αν $v = \Lambda$, τότε,

$$\delta^*(\delta^*(s, w), \Lambda) \stackrel{(11.i)}{=} \delta^*(s, w) = \delta^*(s, w\Lambda).$$

Υποθέτουμε, στη συνέχεια, ότι η (12) ισχύει για όλες τις λέξεις v με μήκος k ($k \geq 0$), και ας είναι z μια λέξη με μήκος $k+1$. Τότε:

$$z = xv$$

όπου $x \in X$ και $v \in X^*$ με μήκος k . Έτσι

$$\delta^*(s, wz) = \delta^*(s, wxv) \stackrel{\text{υποθ.}}{=} \delta^*(\delta^*(s, wx), v)$$

$$\stackrel{(11.ii)}{=} \delta^*(\delta(\delta^*(s, w), x), v) \stackrel{\text{υποθ.}}{=} \delta^*(\delta^*(s, w), xv) =$$



$$= \delta^*(\delta^*(s, w), z)$$

όπως το επιθυμούσαμε . ■

Ας υποθέσουμε ότι το αυτόματο

$$\mathcal{A} = (S, X, \delta, s_0, F)$$

βρίσκεται στην αρχική εσωτερική κατάσταση s_0 και ας το τροφοδοτήσουμε με την λέξη $w \in X^*$, τότε το $\mathcal{A}$ θα πάει στην εσωτερική κατάσταση $\delta^*(s_0, w)$.

Αν συμβεί η $\delta^*(s_0, w)$ να είναι τελική, δηλαδή $\delta^*(s_0, w) \in F$, τότε λέμε ότι το αυτόματο $\mathcal{A}$ αναγνωρίζει τη λέξη w .

Το σύνολο όλων των λέξεων που αναγνωρίζει το αυτόματο $\mathcal{A}$, ονομάζεται συμπεριφορά του και συμβολίζεται $|\mathcal{A}|$, δηλαδή

$$|\mathcal{A}| = \{w \mid w \in X^* \text{ και } \delta^*(s_0, w) \in F\}.$$

Μία γλώσσα $L \subseteq X^*$ τη λέμε αναγνωρίσιμη αν υπάρχει αυτόματο

$$\mathcal{A} = (S, X, \delta, s_0, F)$$

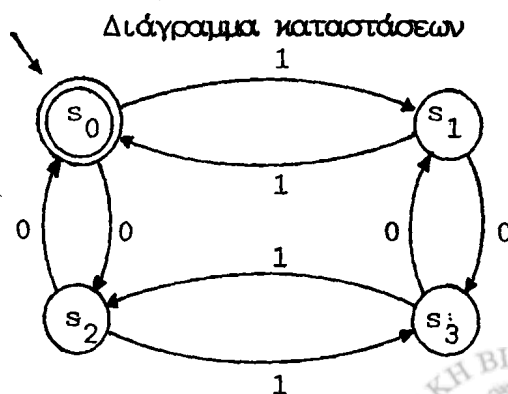
τέτοιο ώστε

$$|\mathcal{A}| = L.$$

Με άλλα λόγια, οι αναγνωρίσιμες γλώσσες είναι όλες εκείνες οι γλώσσες που προκύπτουν σαν συμπεριφορά κάποιου αυτόματου.

Παράδειγμα 2. θεωρούμε το πεπερασμένο αυτόματο $\mathcal{A} = (S, X, \delta, s_0, F)$ όπου $S = \{s_0, s_1, s_2, s_3\}$, $X = \{0, 1\}$, $F = \{s_0\}$ και η δ ορίζεται από τον παρακάτω πίνακα

δ	0	1
s_0	s_2	s_1
s_1	s_3	s_0
s_2	s_0	s_3
s_3	s_1	s_2



Το $\mathcal{A}$ αναγνωρίζει τη λέξη 110101 . Πραγματικά , $\delta(s_0,1) = s_1$ και $\delta(s_1,1) = s_0$, οπότε

$$\delta^*(s_0,11) \stackrel{(11_{ii})}{=} \delta(\delta(s_0,1),1) = \delta(s_1,1) = s_0 \quad (13)$$

οπότε

$$\delta^*(s_0,110) \stackrel{(11_{ii})}{=} \delta(\delta^*(s_0,11),0) \stackrel{(13)}{=} \delta(s_0,0) = s_2$$

Συνεχίζοντας , μ' αυτό τον τρόπο βρίσκουμε

$$\begin{aligned} \delta(s_0,1101) &= s_3 , \delta(s_0,11010) = s_1 \quad \text{και τελικά} \\ \delta(s_0,110101) &= s_0 \in F . \end{aligned}$$

Διατρέχοντας το διάγραμμα καταστάσεων , παρατηρούμε ότι η γλώσσα L , που αναγνωρίζει το $\mathcal{A}$, είναι το σύνολο όλων των λέξεων που περιέχουν άρτιο αριθμό 0 και άρτιο αριθμό 1 .

Παράδειγμα 3 . Για το αυτόματο $\mathcal{A}$ του παραδείγματος 1 παρατηρούμε ότι $\forall w \in \{0,1\}^*$ έχουμε

$$\delta^*(s_0,w) = \begin{cases} s_0 & \text{αν η } w \text{ περιέχει άρτιο αριθμό 1} \\ s_1 & \text{αν η } w \text{ περιέχει περιττό αριθμό 1 .} \end{cases}$$

Έτσι , η γλώσσα L που αναγνωρίζει το αυτόματο αυτό , είναι το σύνολο όλων των λέξεων $w \in \{0,1\}^*$ που έχουν περιττό αριθμό 1.

Υπάρχουν και γλώσσες που δεν αναγνωρίζονται από αυτόματα . Για παράδειγμα , θεωρούμε το αλφάβητο $X = \{a,b\}$ και την γλώσσα

$$L = \{a^n b^n / n \geq 0\} .$$

Η L δεν είναι αναγνωρίσιμη . Πραγματικά , ας υποθέσουμε ότι η L είναι αναγνωρίσιμη δηλαδή , υπάρχει αυτόματο

$$\mathcal{A} = (S, X, \delta, s_0, F)$$

έτσι ώστε

$$|\mathcal{A}| = L = \{a^n b^n \mid n \geq 0\} .$$



Αυτό σημαίνει ότι για κάθε $n \geq 0$ έχουμε

$$\delta^*(s_0, a^n b^n) \in F \quad (14)$$

Αλλά οι εσωτερικές καταστάσεις

$$\delta^*(s_0, a), \delta^*(s_0, a^2), \delta^*(s_0, a^3), \dots$$

δεν μπορεί να είναι όλες διαφορετικές μεταξύ τους γιατί το σύνολο S είναι πεπερασμένο. Έτσι θα έχουμε

$$\delta^*(s_0, a^k) = \delta^*(s_0, a^l) \quad (15)$$

για κάποιους φυσικούς k και l με $k < l$. Αλλά τότε

$$\begin{aligned} \delta^*(s_0, a^k b^l) &= \delta^*(\delta^*(s_0, a^k), b^l) \xrightarrow{(15)} \delta^*(\delta^*(s_0, a^l), b^l) = \\ &= \delta^*(s_0, a^l b^l) \in F \end{aligned}$$

δηλαδή

$$a^k b^l \in |L|$$

πράγμα άτοπο (αφού $k < l$). Στο άτοπο αυτό οδηγηθήκαμε γιατί υποθέσαμε ότι η γλώσσα L ήταν αναγνωρίσιμη.

Θα δώσουμε στην συνέχεια ένα κριτήριο αναγνωρισιμότητας μιας γλώσσας L με την βοήθεια της συντακτικής ισοδυναμίας R_L .

ΠΡΟΤΑΣΗ 6. Ας είναι $L \subseteq X^*$ μία γλώσσα και R_L η συντακτική της ισοδυναμία. Αν η R_L έχει πεπερασμένο δείκτη, τότε η L είναι αναγνωρίσιμη.

Για την απόδειξη της θα χρειασθούμε το επόμενο Λήμμα.

ΛΗΜΜΑ. Αν $L \subseteq X^*$ είναι μία γλώσσα και υποθέσουμε ότι υπάρχει ένα πεπερασμένο μονοειδές $(M, *)$, ένας ομομορφισμός $\varphi: X^* \rightarrow M$ και ένα υποσύνολο $B \subseteq M$ τέτοιο ώστε $\varphi^{-1}(B) = L$ τότε η L είναι αναγνωρίσιμη.

Απόδειξη.

Παίρνουμε το αυτόματο

$$\mathcal{A} = (M, X, \delta, e, B)$$

με αρχική εσωτερική κατάσταση το ουδέτερο στοιχείο e του M . Η απεικόνιση μετάβασης

$$\delta: M \times X \rightarrow M$$



ορίζεται από

$$\delta(m, x) = m * \varphi(x) \quad \forall m \in M, \quad x \in X.$$

Επαγωγικά πάνω στο μήκος της λέξης $w \in X^*$ αποδεικνύεται εύκολα ότι

$$\delta^*(m, w) = m * \varphi(w) \quad (16)$$

οπότε

$$\begin{aligned} w \in |\mathcal{L}| &\iff \delta^*(e, w) \in B \stackrel{(16)}{\iff} e * \varphi(w) \in B \\ &\iff \varphi(w) \in B \iff w \in \varphi^{-1}(B) \iff w \in L. \end{aligned}$$

Έτσι $|\mathcal{L}| = L$ που σημαίνει ότι η L είναι αναγνωρίσιμη.

Απόδειξη πρότασης 6.

Η συντακτική ισοδυναμία R_L έχει σύμφωνα με την πρόταση 5 την ιδιότητα

$$u \equiv v(R_L) \quad \text{και} \quad u \in L \implies v \in L. \quad (17)$$

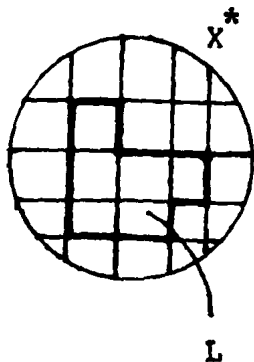
Αυτό σημαίνει ότι αν μία κλάση ισοδυναμίας $R_L(w)$ τέμνει την L , τότε περιέχεται ολόκληρη στην L .

Παραγωγικά, ας υποθέσουμε ότι $R_L(w) \cap L \neq \emptyset$ και ας είναι $t \in R_L(w)$ και $t \in L$, δηλαδή $t \equiv w(R_L)$ και $t \in L$

τότε σύμφωνα με την (17) και $w \in L$.

Για να δείξουμε ότι $R_L(w) \subseteq L$, παίρνουμε μία τυχούσα λέξη $s \in R_L(w)$, τότε $s \equiv w(R_L)$ και, καθώς $w \in L$, θα έχουμε και $s \in L$.

Η L λοιπόν γράφεται σαν ένωση κάποιων κλάσεων ισοδυναμίας, και ας υποθέσουμε ότι



$$L = \cup R_L(w) \quad (18)$$



θεωρούμε το συντακτικό μονοειδές X^* / R_L και την κανονική προβολή

$$P : X^* \longrightarrow X^* / R_L, \quad p(w) = R_L(w)$$

που στέλνει κάθε λέξη $w \in X^*$ στην κλάση της και παίρνουμε για B το σύνολο όλων εκείνων των κλάσεων $R_L(w)$ που περιέχονται στην L , τότε, λόγω της (18), θα έχουμε

$$P^{-1}(B) = L.$$

Αφού το συντακτικό μονοειδές είναι πεπερασμένο, σύμφωνα με το Λήμμα η L είναι αναγνωρίσιμη.

Σχόλια : θα μπορούσε κανείς να επεκταθεί και σε άλλα ενδιαφέροντα θέματα όπως :

■ Στην μελέτη των ιδιοτήτων που έχουν οι αναγνωρίσιμες γλώσσες π.χ. η κλάση των αναγνωρίσιμων γλωσσών είναι κλειστή ως προς την ένωση, την τομή, το συμπλήρωμα και τις κωδικοποιήσεις (Άλγεβρα των αναγνωρίσιμων γλωσσών).

■ Στην ελαχιστοποίηση των πεπερασμένων αυτομάτων.

■ Στις αλγεβρικές γραμματικές που ορίζουν τις αλγεβρικές γλώσσες. Οι περισσότερες τεχνητές γλώσσες είναι αλγεβρικές και αυτό υπογραμμίζει τη σημασία των γλωσσών αυτών. Σημειώνουμε ότι η κλάση των αλγεβρικών γλωσσών είναι ευρύτερη εκείνης των αναγνωρίσιμων γλωσσών.

■ Στις αλγεβρικές μηχανές που αναγνωρίζουν τις αλγεβρικές γλώσσες.

Η ανάπτυξη όμως των παραπάνω θεμάτων θα ξεφευγε από το σκοπό αυτού του κεφαλαίου.



ΚΕΦΑΛΑΙΟ II

ΟΜΑΔΕΣ

§1.1. Ομάδες

Ορισμός. Μια ομάδα $(G, *)$ είναι ένα ζεύγος που σχηματίζεται από ένα σύνολο G και μια πράξη $* : G \times G \longrightarrow G$, $(x, y) \longmapsto x * y$ που έχει τις επόμενες ιδιότητες :

O_1) Είναι προσεταιριστική : $x*(y*z) = (x*y)*z$, $\forall x, y, z \in G$.

O_2) Υπάρχει ουδέτερο στοιχείο $e \in G$, δηλαδή $x*e = x = e*x$, $\forall x \in G$.

O_3) Για κάθε στοιχείο $x \in G$ υπάρχει το συμμετρικό του $x' \in G$ έτσι ώστε $x*x' = e = x'*x$.

Μ' άλλα λόγια, μια ομάδα $(G, *)$ είναι ένα μονοειδές που ικανοποιεί τη συνθήκη O_3).

Η ομάδα $(G, *)$ λέγεται αβελιανή (προς τιμή του Νορβηγού Μαθηματικού Niels-Henrik Abel (1802-1829)), όταν η πράξη $*$ είναι αντιμεταθετική, δηλαδή όταν $x*y = y*x$ $\forall x, y \in G$.

Θα παρατηρήσουμε εδώ ότι σε μια ομάδα G

1) Το ουδέτερο στοιχείο e είναι μοναδικό - μοναδικό επίσης είναι και το συμμετρικό x' του στοιχείου $x \in G$ (βλ. Κεφ. 0, §5).



Στην περίπτωση που η πράξη σημειώνεται πολ/κά (αντιστ. προσθετικά) συμβολίζουμε με x^{-1} (αντιστ. $-x$) το συμμετρικό του στοιχείου x και το καλούμε αντίστροφο του x (αντιστ. αντίθετο του x), οπότε

$$x \cdot x^{-1} = 1 = x^{-1} \cdot x \quad (\text{αντιστ. } x + (-x) = 0 = (-x) + x) .$$

2) Ισχύει ο γενικευμένος προσεταιριστικός νόμος . Έτσι , αν η ομάδα G είναι πολ/κή (αντιστ. προσθετική) , μπορούμε να μιλάμε για φυσικές δυνάμεις (αντιστ. φυσικά πολ/σια) των στοιχείων της , όπως ακριβώς και στα μονοειδή . (Βλ. Κεφ. I)

Στη γενική μελέτη των ομάδων (αβελιανών και όχι) συμφωνούμε να σημειώνουμε την πράξη πολ/κά $((x,y) \longmapsto xy)$. Προσθετικά σημειώνεται μια ομάδα ιδιαίτερα στη μελέτη των αβελιανών ομάδων .

Τέλος , ονομάζουμε τάξη της ομάδας G τον πληθικό αριθμό $|G|$ του συνόλου G . Η ομάδα G λέγεται πεπερασμένης τάξης , αν ο $|G|$ είναι πεπερασμένος αριθμός , και άπειρης τάξης αν ο $|G|$ είναι άπειρο .

Παράδειγμα 1.

i) Τα σύνολα $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ των ακεραίων , ρητών , πραγματικών και μιγαδικών αριθμών αντίστοιχα , εφοδιασμένα με τη συνηθισμένη πρόσθεση , αποτελούν αβελιανές ομάδες . εφοδιασμένα όμως με το γνωστό μας πολ/σμό δεν αποτελούν ομάδες .

ii) Τα σύνολα $\mathbb{Q}^* = \mathbb{Q} - \{0\}$, $\mathbb{R}^* = \mathbb{R} - \{0\}$, $\mathbb{C}^* = \mathbb{C} - \{0\}$, εφοδιασμένα με το συνηθισμένο πολ/σμό , αποτελούν αβελιανές ομάδες .

iii) Τα σύνολα $\mathbb{Q}^+$, $\mathbb{R}^+$ των θετικών ρητών και θετικών πραγματικών αριθμών αντίστοιχα , εφοδιασμένα με το γνωστό μας πολ/μό , αποτελούν αβελιανές ομάδες .

iv) Το σύνολο $\mathbb{Q}^+$ εφοδιασμένο με την παρακάτω πράξη " $\ast$ "

$$a \ast b = \frac{ab}{2} \quad \forall a, b \in \mathbb{Q}^+$$



δομείται σε αβελιανή ομάδα · το ουδέτερο στοιχείο είναι το 2 , ενώ το συμμετρικό του στοιχείου α είναι το $\alpha' = 4/\alpha$.

Παράδειγμα 2.

Το σύνολο $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$ των ακεραίων modulo m εφοδιασμένο με την πράξη πρόσθεσης κλάσεων

$$\bar{a} + \bar{b} = \overline{a+b} \quad , \quad \forall \bar{a}, \bar{b} \in \mathbb{Z}_m \quad (\text{βλέπε Κεφ. 0, §4})$$

δομείται σε αβελιανή ομάδα · το ουδέτερο στοιχείο της είναι η κλάση $\bar{0}$, ενώ η αντίθετη της κλάσης $\bar{a}$ είναι η κλάση $\overline{m-a}$:

$$\bar{a} + (\overline{m-a}) = \overline{a+m-a} = \bar{m} = \bar{0} \quad .$$

Η ομάδα $(\mathbb{Z}_m, +)$ είναι ένα κλασσικό παράδειγμα ομάδας πεπερασμένης τάξης .

Παράδειγμα 3.

Το σύνολο $M_{m \times n}(\mathbb{C})$ όλων των $m \times n$ πινάκων , με στοιχεία μιγαδικούς αριθμούς , εφοδιασμένο με τη γνωστή μας πρόσθεση πινάκων , δομείται σε αβελιανή ομάδα .

Παράδειγμα 4.

Το σύνολο $GL_n(\mathbb{R})$ όλων των αντιστρέψιμων $n \times n$ πινάκων με στοιχεία πραγματικούς αριθμούς , δηλαδή

$$GL_n(\mathbb{R}) = \{A/A \in M_{n \times n}(\mathbb{R}) \quad \text{και} \quad \det A \neq 0\}$$

εφοδιασμένο με το γνωστό πολ/σμό πινάκων , δομείται σε ομάδα (μη-αβελιανή για $n > 1$) · εδώ , το ρόλο του ουδέτερου στοιχείου παίζει ο μοναδιαίος $n \times n$ πίνακας I_n . Η $GL_n(\mathbb{R})$ καλείται γενική γραμμική ομάδα βαθμού n στο $\mathbb{R}$. Η $GL_n(F)$ ορίζεται όμοια πάνω σε οποιοδήποτε σώμα F .

Παράδειγμα 5.



Το πεπερασμένο σύνολο $V = \{e, a, b, c\}$ εφοδιασμένο με την πράξη " $*$ "

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

δομείται σε αβελιανή ομάδα που καλείται **τετραδική ομάδα του Klein** (προς τιμή του Γερμανού Μαθηματικού Felix Klein: 1849-1925) .

Παράδειγμα 6.

Το σύνολο όλων των ακολουθιών πραγματικών αριθμών εφοδιασμένο με την πράξη πρόσθεσης

$$(x_0, x_1, \dots, x_n, \dots) + (y_0, y_1, \dots, y_n, \dots) = (x_0 + y_0, x_1 + y_1, \dots, x_n + y_n, \dots)$$

δομείται σε αβελιανή ομάδα * το μηδενικό στοιχείο είναι η μηδενική ακολουθία $(0, 0, \dots, 0, \dots)$, ενώ η αντίθετη της ακολουθίας $(x_0, x_1, \dots, x_n, \dots)$ είναι η ακολουθία $(-x_0, -x_1, \dots, -x_n, \dots)$.

Παράδειγμα 7. (ευθύ γινόμενο ομάδων)

Έστω $n \in \mathbb{Z}^+$ και $G_1, G_2, \dots, G_n$ πολ/κές ομάδες (όχι αναγκαία διακεκριμένες) . Το σύνολο

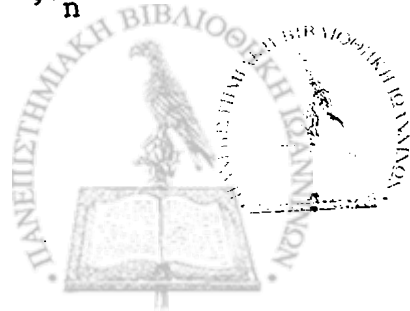
$$G_1 \times \dots \times G_n = \prod_{i=1}^n G_i = \{(g_1, g_2, \dots, g_n) / g_i \in G_i \quad i=1, 2, \dots, n\}$$

εφοδιασμένο με την πράξη "πολ/σμός συνιστώσα με συνιστώσα"

$$(g_1, \dots, g_n) \cdot (g'_1, \dots, g'_n) = (g_1 g'_1, \dots, g_n g'_n)$$

αποτελεί ομάδα με μοναδιαίο στοιχείο την n -αδα $(1, 1, \dots, 1)$ και αντίστροφο του στοιχείου $(g_1, \dots, g_n)$ την n -αδα $(g_1^{-1}, \dots, g_n^{-1})$.

Την ομάδα αυτή την καλούμε **ευθύ γινόμενο** των $G_1, \dots, G_n$ που γενικά δεν είναι αβελιανή ομάδα εκτός και αν όλες οι ομάδες $G_1, \dots, G_n$ είναι



αβελιανές .

§1.2.Στοιχειώδεις ιδιότητες των ομάδων

Πρόταση 1.

Σε μια πολ/κή ομάδα G ισχύουν τα επόμενα .

i) Αν $c \in G$ και $cc = c$ τότε $c = 1$.

ii) Για κάθε $a, b, x \in G$

$$\left. \begin{array}{l} ax = bx \implies a = b \\ xa = xb \implies a = b \end{array} \right\} \quad (\text{Νόμοι απλοποίησης})$$

iii) $(a^{-1})^{-1} = a$ για κάθε $a \in G$

iv) $(ab)^{-1} = b^{-1}a^{-1}$ για κάθε $a, b \in G$

v) Για κάθε $a, b \in G$, οι εξισώσεις $ax = b$ και $ya = b$ έχουν μοναδικές λύσεις στην G , τις $x = a^{-1}b$ και $y = ba^{-1}$ αντίστοιχα .

Απόδειξη.

i) $cc = c \implies c^{-1}(cc) = c^{-1}c$ οπότε $(c^{-1}c)c = 1$ δηλαδή $1c = 1$
άρα $c = 1$.

ii) Πολλ/ζοντας την $ax = bx$, από δεξιά με x^{-1} , έχουμε
 $(ax)x^{-1} = (bx)x^{-1} \implies a(xx^{-1}) = b(xx^{-1})$ άρα $a1 = b1 \implies a = b$. Όμοια εργαζόμαστε και για την άλλη .

iii) Η σχέση $aa^{-1} = 1 = a^{-1}a \quad \forall a \in G$ και η μοναδικότητα του αντίστροφου στοιχείου μας βεβαιώνουν ότι $(a^{-1})^{-1} = a$, $\forall a \in G$.

iv) Έχουμε

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a \cdot 1 \cdot a^{-1} = aa^{-1} = 1 .$$

Όμοια $(b^{-1}a^{-1})(ab) = 1$. Το στοιχείο $b^{-1}a^{-1}$ είναι αντίστροφο του ab και από τη μοναδικότητα του αντίστροφου έχουμε $(ab)^{-1} = b^{-1}a^{-1}$.

v) Το $a^{-1}b$ είναι λύση της εξίσωσης $ax = b$. Πραγματικά ,

$$a(a^{-1}b) = (aa^{-1})b = 1b = b .$$

Ας είναι τώρα $x \in G$ μια άλλη λύση της επομένως $ax = b$.



Πολ/ζουμε από αριστερα με a^{-1} , οπότε

$$a^{-1}(ax) = a^{-1}b \implies (a^{-1}a)x = a^{-1}b \implies 1x = a^{-1}b,$$

δηλαδή $x = a^{-1}b$, όπως το επιθυμούσαμε.

Με τον ίδιο τρόπο δείχνουμε ότι το $y = b^{-1}a$ είναι η μοναδική λύση της $ya = b$. ■

Παρατήρηση.

Ανάλογα αποτελέσματα έχουμε και στην περίπτωση που η G είναι προσθετική ομάδα. Στην περίπτωση αυτή π.χ. έχουμε

$$-(a+b) = -b + (-a) \quad \forall a, b \in G.$$

Ας είναι τώρα G μια πολ/κή ομάδα. Για κάθε $a_1, \dots, a_m \in G$ έχουμε

$$(a_1 a_2 \dots a_m)^{-1} = a_m^{-1} \dots a_2^{-1} a_1^{-1} \quad (1)$$

Εργαζόμαστε επαγωγικά. Πραγματικά, για $m=1$ δεν έχουμε να δείξουμε τίποτα, ενώ για $m=2$ ισχύει (πρόταση 1, iv).

Υποθέτουμε ότι ισχύει για όλα τα γινόμενα στοιχείων της G , με πλήθος στοιχείων $< m$, ($m \geq 2$). Τότε

$$\begin{aligned} (a_1 \dots a_m)^{-1} &= ((a_1 \dots a_{m-1}) a_m)^{-1} = a_m^{-1} (a_1 \dots a_{m-1})^{-1} \\ &\stackrel{\text{υποθ.}}{=} a_m^{-1} a_{m-1}^{-1} \dots a_1^{-1}. \end{aligned}$$

Παρατήρηση

Στην περίπτωση που η G είναι προσθετική, για κάθε $a_1, \dots, a_m \in G$ έχουμε

$$-(a_1 + \dots + a_m) = (-a_m) + \dots + (-a_1) \quad (1')$$

θέτοντας $a_1 = \dots = a_m = a$ στις (1) και (1') παίρνουμε

Πολ/κή $(a^m)^{-1} = (a^{-1})^m, \quad \forall m \in \mathbb{Z}^+ \quad (2)$		Προσθετικά $-(ma) = m(-a), \quad \forall m \in \mathbb{Z}^+ \quad (2')$
---	--	--



Βέβαια σε μια πολ/κή ομάδα G (αντιστ. προσθετική) έχει νόημα το a^{-1} (αντιστ. το $-a$) και είναι φυσικό να ορίσουμε

Πολ/κή		Προσθετικά
$a^{-m} = (a^{-1})^m \stackrel{(2)}{=} (a^m)^{-1}$		$(-m)a = m(-a) \stackrel{(2')}{=} -(ma)$

Έτσι μπορούμε να μιλάμε για ανέραιες δυνάμεις στοιχείων μιας πολ/κής ομάδας και ανέραια πολ/σια στοιχείων μιας προσθετικής ομάδας .

Τέλος, για κάθε στοιχείο a μιας ομάδας G και $\forall m, n \in \mathbb{Z}$ έχουμε

Πολ/κή		Προσθετικά
i) $a^m a^n = a^{m+n}$		i) $ma + na = (m+n)a$
ii) $(a^m)^n = a^{mn}$		ii) $m(na) = (mn)a$

§2.1 Υποομάδες.

ΟΡΙΣΜΟΣ.

Ένα μη κενό υποσύνολο H μιας ομάδας G ονομάζεται υποομάδα της G , αν ισχύουν :

- i) Για κάθε $x, y \in H \implies xy \in H$
- ii) Για κάθε $x \in H \implies x^{-1} \in H$.

Είναι φανερό ότι κάθε υποομάδα H της G μπορεί να θεωρηθεί σαν ομάδα, με πολ/σμό τον περιορισμό του πολ/σμού της G στο H . Δύο παραδείγματα υποομάδων μιας ομάδας G είναι η ίδια η G και η τετριμμένη υποομάδα $\{1\}$ που περιέχει μόνο το μοναδιαίο στοιχείο . Κάθε υποομάδα H της G τέτοια ώστε $H \neq G$ και $H \neq \{1\}$, θα την καλούμε γνήσια υποομάδα .

Τέλος , θα γράφουμε $H \leq G$, για να δηλώνουμε ότι η H είναι υποομάδα της G , $H \not\leq G$ αν δεν είναι και $H < G$ αν H είναι γνήσια υποομάδα .



Παρατήρηση.

Η σχέση " $\leq$ " στο σύνολο $\mathcal{L}(G)$ όλων των υποομάδων μιας ομάδας G είναι μια μερική διάταξη (partial order), δηλαδή είναι :

α) Ανακλαστική : $H \leq H$ για κάθε $H \in \mathcal{L}(G)$

β) Αντισυμμετρική : Αν $H_1 \leq H_2$ και $H_2 \leq H_1$, τότε $H_1 = H_2$

γ) Μεταβατική : Αν $H_1 \leq H_2$ και $H_2 \leq H_3$, τότε $H_1 \leq H_3$.

Η επόμενη πρόταση μας δίνει ένα απλούστερο κριτήριο για να διαπιστώνουμε αν ένα υποσύνολο μιας ομάδας G είναι υποομάδα της .

ΠΡΟΤΑΣΗ 2.

Ένα μη κενό υποσύνολο H μιας ομάδας G είναι υποομάδα της , εάν και μόνο εάν ισχύει :

$$\text{iii) Για κάθε } x, y \in H \implies xy^{-1} \in H .$$

Απόδειξη.

Αν $H \leq G$, τότε φανερά ισχύει η iii) . Αντίστροφα, αφού $H \neq \emptyset$ υπάρχουν $x \in H$. επομένως από την υπόθεση μας , το στοιχείο $xx^{-1} = 1 \in H$, έτσι $\forall x \in H$ θα έχουμε $1 \cdot x^{-1} = x^{-1} \in H$. Αν τώρα $x, y \in H$, τότε το $y^{-1} \in H$, οπότε , από την υπόθεση μας , και το στοιχείο $x \cdot (y^{-1})^{-1} = xy \in H$, όπως το επιθυμούσαμε . ■

Παρατήρηση

Αν η ομάδα G είναι προσθετική , οι συνθήκες i) και ii) γράφονται :

$$\text{i')} \text{ Για κάθε } x, y \in H \implies x+y \in H$$

$$\text{ii')} \text{ Για κάθε } x \in H \implies -x \in H$$

ενώ η iii) γράφεται



iii') Για κάθε $x, y \in H \implies x-y \in H$
(όπου $x-y = x+(-y)$).

Τα πράγματα, στην περίπτωση πεπερασμένων υποσυνόλων μιας ομάδας G απλουστεύονται περισσότερο. Έτσι

ΠΡΟΤΑΣΗ 3.

Ένα μη-κενό πεπερασμένο υποσύνολο H μιας ομάδας G είναι υποομάδα της εάν και μόνο εάν

v) Για κάθε $x, y \in H \implies xy \in H$.

Απόδειξη.

Το $H \neq \emptyset$ και πεπερασμένο, επομένως $\forall x \in H$ τα στοιχεία του H

$$x, x^2, x^3, \dots$$

δεν είναι όλα διακεκριμένα. Υποθέτουμε ότι $x^r = x^s$, με $r > s$,
έτσι $x^{r-s} = 1$ ή $x(x^{r-s-1}) = 1$. επομένως, $x^{-1} = x^{(r-s)-1} \in H$, όπως
επιθυμούσαμε.

Το αντίστροφο είναι φανερό. ■

Παράδειγμα 1.

$H (\mathbb{Q}^*, \cdot)$ είναι υποομάδα της $(\mathbb{R}^*, \cdot)$ και αυτή της $(\mathbb{C}^*, \cdot)$.

$H (\mathbb{Q}^+, \cdot)$ είναι υποομάδα της $(\mathbb{R}^+, \cdot)$.

Παράδειγμα 2.

Το σύνολο $G = \{1, -1, i, -i\}$ είναι υποομάδα της $(\mathbb{C}^*, \cdot)$. Το G
λοιπόν είναι και αυτό μια ομάδα με πίνακα πολ/σμού



.	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

Παράδειγμα 3.

Το σύνολο των n -στών ριζών της μονάδας ($n \in \mathbb{Z}^+$)

$$G_n = \{z/z \in \mathbb{C}^* \text{ και } z^n = 1\}$$

είναι υποομάδα της $(\mathbb{C}^*, \cdot)$.

Πραγματικά, $G_n \neq \emptyset$, αφού $1 \in G_n$. Αν τώρα $z, v \in G_n$, τότε $zv^{-1} = \frac{z}{v} \in G_n$, αφού $(\frac{z}{v})^n = \frac{z^n}{v^n} = 1$.

Παράδειγμα 4.

Μια ενδιαφέρουσα υποομάδα της γενικής γραμμικής ομάδας βαθμού n $GL_n(\mathbb{R})$, είναι η υποομάδα $O_n(\mathbb{R})$ των ορθογωνίων πινάκων βαθμού n πάνω στο $\mathbb{R}$.

$$O_n(\mathbb{R}) = \{A/A \in GL_n(\mathbb{R}) \text{ και } A^{-1} = {}^t A\}$$

(όπου ${}^t A$ παριστάνει τον ανάστροφο του A).

Πραγματικά, $O_n(\mathbb{R}) \neq \emptyset$, αφού $I_n \in O_n(\mathbb{R})$. Επίσης, αν $A, B \in O_n(\mathbb{R})$, τότε και $AB^{-1} \in O_n(\mathbb{R})$, αφού

$$(AB^{-1})^{-1} = (B^{-1})^{-1} \cdot A^{-1} = ({}^t B)^{-1} \cdot {}^t A = {}^t (B^{-1}) \cdot {}^t A = {}^t (AB^{-1})$$

(Υπενθυμίζουμε ότι αν $A \in O_n(\mathbb{R})$, τότε $\det A = \pm 1$).

Όμοια, για οποιοδήποτε σώμα F , μπορούμε να ορίσουμε την υποομάδα $O_n(F)$ των ορθογωνίων πινάκων, βαθμού n , πάνω στο F .

Παράδειγμα 5.



Μια υποομάδα της $GL_n(\mathbb{R})$ είναι η $SL_n(\mathbb{R})$, όπου

$$SL_n(\mathbb{R}) = \{A/A \in GL_n(\mathbb{R}), \text{ με } \det A = 1\}$$

Πραγματικά, αν $A, B \in SL_n(\mathbb{R})$, τότε και ο $AB^{-1} \in SL_n(\mathbb{R})$, αφού $\det(AB^{-1}) = \det A \cdot \det B^{-1} = \det A \cdot (\det B)^{-1} = 1 \cdot 1 = 1$.

Την $SL_n(\mathbb{R})$ την ονομάζουμε ειδική γραμμική ομάδα βαθμού n πάνω στο $\mathbb{R}$.

Η $SL_n(F)$ ορίζεται όμοια πάνω σε οποιοδήποτε σώμα F .

Παράδειγμα 6.

Η προσθετική ομάδα $\mathbb{R}$ των ακολουθιών πραγματικών αριθμών έχει δύο ενδιαφέρουσες υποομάδες:

α) Την υποομάδα S των συγκλινουσών ακολουθιών.

Πραγματικά, αν $(x_n), (y_n) \in S$, τότε και $(x_n) - (y_n) = (x_n - y_n) \in S$, αφού $\lim_{n \rightarrow \infty} (x_n - y_n) = \lim_{n \rightarrow \infty} x_n - \lim_{n \rightarrow \infty} y_n$.

β) Την υποομάδα S_0 των μηδενικών ακολουθιών.

Αν $(x_n), (y_n) \in S_0$, οπότε $\lim_{n \rightarrow \infty} x_n = 0$ και $\lim_{n \rightarrow \infty} y_n = 0$, τότε

$(x_n) - (y_n) = (x_n - y_n) \in S_0$, αφού $\lim_{n \rightarrow \infty} (x_n - y_n) = \lim_{n \rightarrow \infty} x_n - \lim_{n \rightarrow \infty} y_n = 0 - 0 = 0$.

Παράδειγμα 7.

Τα σύνολα $\{\bar{0}, \bar{2}, \bar{4}\}$ και $\{\bar{0}, \bar{3}\}$ είναι υποομάδες της προσθετικής ομάδας $(\mathbb{Z}_6, +)$.

Παράδειγμα 8.

Τα υποσύνολα $\{e, a\}$, $\{e, b\}$, $\{e, c\}$ είναι οι μόνες γνήσιες υποομάδες της τετραδικής ομάδας του Klein (βλέπε, Κεφ. II, §1.1, παραδ. 5).

Παράδειγμα 9.

Δύο ενδιαφέρουσες υποομάδες του ευθέως γινομένου $G_1 \times G_2$ δύο



ομάδων G_1 και G_2 είναι οι επόμενες

$$\{1\} \times G_2 = \{(1, g) / g \in G_2\} \text{ και } G_1 \times \{1\} = \{(g', 1) / g' \in G_1\} .$$

Παράδειγμα 10. (Κέντρο ομάδας)

Το κέντρο $Z(G)$ μιας ομάδας G είναι το σύνολο όλων εκείνων των στοιχείων της G που αντιμετατίθεται με όλα τα στοιχεία της G , δηλαδή

$$Z(G) = \{z / z \in G \text{ και } zx = xz, \forall x \in G\} .$$

Είναι $Z(G) \leq G$. Πραγματικά, $Z(G) \neq \emptyset$, αφού $1 \in Z(G)$. Επίσης $\forall z_1, z_2 \in Z(G) \implies z_1 z_2 \in Z(G)$, αφού $\forall x \in G$, έχουμε

$$x(z_1 z_2) = (x z_1) z_2 = (z_1 x) z_2 = z_1 (x z_2) = z_1 (z_2 x) = (z_1 z_2) x$$

και επιπλέον $\forall z \in Z(G) \implies z^{-1} \in Z(G)$. αφού $\forall x \in G$ έχουμε

$$zx = xz \implies x = z^{-1} x z \implies x z^{-1} = z^{-1} x .$$

Θα παρατηρήσουμε εδώ ότι, αν η G είναι αβελιανή, τότε $Z(G) = G$.

Από τη Γραμμική Άλγεβρα έχουμε ότι για σώμα $F = \mathbb{R}$ ή $\mathbb{C}$ αν ο πίνακας $A \in SL_n(F)$ αντιμετατίθεται μ' όλους τους πίνακες του $SL_n(F)$ τότε ο A είναι βαθμωτός δηλαδή $A = aI_n$, $a \in F$.

Έτσι

$$Z(SL_n(F)) = \{aI_n / a \in F \text{ και } a^n = 1\} .$$

Αν H_1, H_2 είναι δύο υποομάδες μιας ομάδας G , η τετριμμένη υποομάδα περιέχεται και στις δύο. Είναι φυσικό λοιπόν, το ερώτημα ποιά είναι η μεγαλύτερη υποομάδα της G , που περιέχεται και στις δύο.

ΠΡΟΤΑΣΗ 4.

Αν H_1, H_2 είναι δύο υποομάδες μιας ομάδας G , τότε και η τομή τους $H_1 \cap H_2$ είναι υποομάδα της G .



Απόδειξη

Η $H_1 \cap H_2 \neq \emptyset$ αφού $1 \in H_1 \cap H_2$.

Για κάθε $x, y \in H_1 \cap H_2$, έχουμε $x, y \in H_1$ και $x, y \in H_2$, επομένως $xy^{-1} \in H_1$ και $xy^{-1} \in H_2$ οπότε $xy^{-1} \in H_1 \cap H_2$. ■

Έτσι, η τομή $H_1 \cap H_2$ είναι η μεγαλύτερη υποομάδα της G που περιέχεται στις H_1 και H_2 .

Γενικότερα.

Αν $(H_i)_{i \in I}$ είναι μια μη-κενή οικογένεια υποομάδων μιας ομάδας G , τότε και η τομή $\bigcap_{i \in I} H_i$ είναι υποομάδα της G .

Παράδειγμα 11.

Ας είναι G μια ομάδα και $x \in G$. Ονομάζουμε κεντροποιούσα του x στην G , το σύνολο όλων των στοιχείων της G που αντιμετατίθενται με το x .

$$C_G(x) = \{z/z \in G \text{ με } xz = zx\}.$$

Με απόδειξη όμοια με εκείνη του παραδείγματος 10, έχουμε ότι η $C_G(x)$ είναι υποομάδα της G .

Η τομή της οικογένειας $(C_G(x))_{x \in G}$ είναι το κέντρο $Z(G)$ της G . Πραγματικά,

$$\bigcap_{x \in G} C_G(x) = \{z/z \in G \text{ με } zx = xz \quad \forall x \in G\} = Z(G).$$

Παράδειγμα 12.

Η τομή των υποομάδων $SL_n(\mathbb{R})$ και $O_n(\mathbb{R})$ της ομάδας $GL_n(\mathbb{R})$ ονομάζεται ειδική ορθογώνια ομάδα βαθμού n στο $\mathbb{R}$ και συμβολίζεται $SO_n(\mathbb{R})$

$$SO_n(\mathbb{R}) = \{A/A \in O_n(\mathbb{R}) \text{ με } \det A = 1\}.$$



§2.2 Παραγόμενες υποομάδες.

Έστω X ένα υποσύνολο μιας ομάδας G . Η τομή όλων των υποομάδων της G που περιέχουν το X καλείται υποομάδα παραγόμενη από το X και συμβολίζεται $\langle X \rangle$. Αυτή είναι η "μικρότερη" υποομάδα της G που περιέχει το X , με την εξής έννοια :

αν $X \subseteq H \leq G$, τότε $\langle X \rangle \leq H$.

Έτσι για παράδειγμα, αν $X = \emptyset$, τότε $\langle \emptyset \rangle = \{1\}$, ενώ, αν το X είναι υποομάδα της G , τότε $\langle X \rangle = X$. Αν το $X \neq \emptyset$ είναι περασμένο υποσύνολο της G , δηλαδή αν $X = \{x_1, \dots, x_n\}$, τότε γράφουμε $\langle x_1, \dots, x_n \rangle$ και όχι $\langle \{x_1, \dots, x_n\} \rangle$, για την υποομάδα που παράγεται από το X .

Είναι εύκολο να περιγράψουμε τα στοιχεία του $\langle X \rangle$ με εκφράσεις από στοιχεία του X .

ΠΡΟΤΑΣΗ 5.

Αν X είναι ένα μη-κενό υποσύνολο μιας ομάδας G , τότε

$$\langle X \rangle = \{x_1^{\alpha_1} \dots x_n^{\alpha_n} / n \in \mathbb{Z}^+, x_i \in X, \alpha_i \in \mathbb{Z}, i=1,2,\dots,n\}$$

Απόδειξη

i) Το σύνολο $H = \{x_1^{\alpha_1} \dots x_n^{\alpha_n} / n \in \mathbb{Z}^+, x_i \in X, \alpha_i \in \mathbb{Z}, i=1,\dots,n\}$ είναι υποομάδα της G . Πραγματικά, για κάθε $x = x_1^{\alpha_1} \dots x_n^{\alpha_n}$ και $y = y_1^{\beta_1} \dots y_m^{\beta_m}$ στοιχεία του H είναι

$$xy^{-1} = x_1^{\alpha_1} \dots x_n^{\alpha_n} (y_1^{\beta_1} \dots y_m^{\beta_m})^{-1} = x_1^{\alpha_1} \dots x_n^{\alpha_n} y_m^{-\beta_m} \dots y_1^{-\beta_1} \in H$$

Επιπλέον, $\forall x \in X$ είναι $x = x^1$, σχέση που δείχνει ότι $X \subseteq H$.

ii) Η H είναι η μικρότερη υποομάδα της G που περιέχει το X .

Πραγματικά, αν $B \leq G$, με $X \subseteq B$, τότε, για κάθε $x_1^{\alpha_1} \dots x_n^{\alpha_n}$ της



$$B = \langle k \rangle = \left\{ k, k^2, k^3, k^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} \quad \text{ενώ}$$

$$A \cap B = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}.$$

Ας είναι τώρα S μια υποομάδα της G .

Αν $X \subseteq S$ και $\langle X \rangle = S$, θα λέμε ότι το X είναι ένα σύνολο γεννητόρων της S . Για παράδειγμα, το σύνολο S είναι ένα σύνολο γεννητόρων της υποομάδας S .

Είναι δυνατόν όμως η υποομάδα S να παράγεται και από άλλα υποσύνολά της, δηλαδή είναι δυνατόν $S = \langle X \rangle = \langle Y \rangle$ $X, Y \subseteq S$ με $X \neq Y$. Για παράδειγμα, η ομάδα $(\mathbb{Z}, +)$ παράγεται από τα υποσύνολα $\{1\}$ $\{-1\}$ και $\{1, 2, \dots, n, \dots\}$.

Στην περίπτωση που υπάρχει ένα πεπερασμένο σύνολο γεννητόρων X της S , θα λέμε την S πεπερασμένα παραγόμενη.

Είναι φυσικό λοιπόν να μας ενδιαφέρουν τα "μικρότερα" σύνολα γεννητόρων. Έτσι :

Ονομάζουμε ανάγωγο γενετικό σύστημα μιας υποομάδας S , ένα υποσύνολο $X \subseteq S$, τέτοιο ώστε $\forall X'$ με $X' \subset X$ να έχουμε $\langle X' \rangle \subset \langle X \rangle = S$.

Έτσι, τα $\{1\}$ και $\{-1\}$ είναι ανάγωγα γενετικά συστήματα της $(\mathbb{Z}, +)$, ενώ το $\{1, 2, \dots, n, \dots\}$ δεν είναι, αφού το $\{1\} \subset \{1, 2, \dots, n, \dots\}$ και $\langle 1 \rangle = (\mathbb{Z}, +)$.

Τέλος, αν $X = \{a\}$, η υποομάδα $\langle a \rangle$ που παράγεται από το a καλείται κυκλική ή μονογενής υποομάδα. Έτσι

Αν η G είναι πολ/κή : $\langle a \rangle = \{a^n / n \in \mathbb{Z}\}$

Αν η G είναι προσθετική : $\langle a \rangle = \{na / n \in \mathbb{Z}\}$.

Παράδειγμα 14.

α) Η πολ/κή ομάδα $G = \{1, -1, i, -i\}$ του παραδείγματος 2 είναι κυκλική, αφού $\langle i \rangle = G$.

β) Η προσθετική ομάδα $\mathbb{Z}_m$ είναι κυκλική, αφού $\langle \bar{1} \rangle = \mathbb{Z}_m$.



§2.3. Ομάδα μεταθέτης

ΟΡΙΣΜΟΣ. Ο μεταθέτης (commutator) $[x, y]$ δύο στοιχείων x και y μιας ομάδας G είναι το στοιχείο

$$[x, y] = xyx^{-1}y^{-1}.$$

(Η σχέση $[x, y]yx = xy$ δικαιολογεί την ονομασία μεταθέτης).
Σημειώνουμε ότι, αν $x, y \in G$, τότε

α) $[x, y] = [y, x]^{-1}$

β) $[x, y] = 1$ εάν και μόνο εάν $xy = yx$.

Πραγματικά

α) $[y, x]^{-1} = (yxy^{-1}x^{-1})^{-1} = (x^{-1})^{-1}(y^{-1})^{-1}x^{-1}y^{-1} = xyx^{-1}y^{-1} = [x, y]$

β) Αν $[x, y] = 1 \implies xyx^{-1}y^{-1} = 1$. Πολ/ζοντας από δεξιά, πρώτα με y και μετά με x , παίρνουμε $xy = yx$. Αντίστροφα :
Αν $xy = yx$, πολ/ντας και τα δύο μέλη από δεξιά, πρώτα με x^{-1} και μετά με y^{-1} , έχουμε $xyx^{-1}y^{-1} = 1$, δηλαδή $[x, y] = 1$.

Θα παρατηρήσουμε, τέλος, ότι το γινόμενο δύο μεταθετών δεν είναι γενικά ένας μεταθέτης, δηλαδή το σύνολο των μεταθετών μιας ομάδας G δεν είναι γενικά υποομάδα της.

Η υποομάδα της G , που παράγεται από τους μεταθέτες $[x, y]$ όλων των στοιχείων x, y της G , ονομάζεται ομάδα μεταθέτης της G και συμβολίζεται $[G, G]$ ή G' :

$$[G, G] = \langle \{ [x, y] / x, y \in G \} \rangle =$$

$$= \{ [x_1, y_1]^{a_1} \dots [x_n, y_n]^{a_n} / n \in \mathbb{Z}^+, x_i, y_i \in G, a_i \in \mathbb{Z} \}.$$

Παρατηρούμε ότι, αν κάποιος από τους εκθέτες a_i είναι αρνητικός $a_i = -\beta_i$ ($\beta_i \geq 0$), τότε



$$[x_i, y_i]^{\alpha_i} = [x_i, y_i]^{-\beta_i} = ([x_i, y_i]^{-1})^{\beta_i} = [y_i, x_i]^{\beta_i} .$$

Επομένως

$$[G, G] = \{ [x_1, y_1] \dots [x_k, y_k] / k \in \mathbb{Z}^+, x_i, y_i \in G \} .$$

Είναι φανερό ότι μια ομάδα G είναι αβελιανή εάν-ν $[G, G] = \{1\}$.
Με κάποια έννοια , η $[G, G]$ μας παρέχει ένα μέτρο για το πόσο η ομάδα G διαφέρει από μια αβελιανή ομάδα .■

§3.1. Supremum δύο υποομάδων.

Ας είναι G μια ομάδα και δύο υποομάδες της H και K . Είναι φανερό ότι η G είναι η μεγαλύτερη υποομάδα που περιέχει τις H και K . Φυσικό είναι λοιπόν, να αναρωτηθούμε ποιά είναι η μικρότερη υποομάδα της G που περιέχει και την H και την K . Βέβαια , μια τέτοια υποομάδα θα περιέχει το σύνολο $H \cup K$ και η απάντηση σ' αυτό το ερώτημα θα ήταν απλή , αν το σύνολο $H \cup K$ ήταν υποομάδα της G . Ατυχώς όμως , αυτό δε συμβαίνει γενικά .

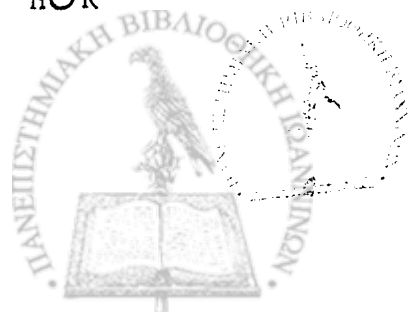
Για παράδειγμα , η ένωση $\{e, a\} \cup \{e, b\} = \{e, a, b\}$ των υποομάδων $\{e, a\}$ και $\{e, b\}$ της ομάδας V του Klein , δεν είναι υποομάδα της, αφού $ab = c \notin \{e, a, b\}$, όπως επίσης και η ένωση των υποομάδων $\mathbb{Z} \times \{0\}$ και $\{0\} \times \mathbb{Z}$ της προσθετικής ομάδας $\mathbb{Z} \times \mathbb{Z}$ δεν είναι υποομάδα της , αφού $(1, 0) + (0, 1) = (1, 1) \notin (\mathbb{Z} \times \{0\}) \cup (\{0\} \times \mathbb{Z})$.
Πιο συγκεκριμένα .

ΠΡΟΤΑΣΗ 6.

Η ένωση $H \cup K$ δύο υποομάδων μιας ομάδας G είναι υποομάδα της, εάν και μόνο εάν $H \leq K$ ή $K \leq H$.

Απόδειξη.

Αν $H \leq K$ ή $K \leq H$, τότε $H \cup K = K$ ή $H \cup K = H$. Αντίστροφα , υποθέτοντας ότι $H \not\leq K$ και $K \not\leq H$, θα δείξουμε ότι η ένωση $H \cup K$



δεν είναι υποομάδα της G .

Υπάρχει στοιχείο $h \in H$ με $h \notin K$ και στοιχείο $k \in K$ με $k \notin H$. Θα δείξουμε ότι το $hK \notin H \cup K$, δηλαδή ότι το $H \cup K$ δεν είναι κλειστό ως προς την πράξη.

Αν $hk \in H$, τότε $h^{-1}(hk) = k \in H$ άτοπο, άρα $hk \notin H$. Όμοια, το $hk \notin K$, δηλαδή $hk \notin H \cup K$. ■

ΟΡΙΣΜΟΣ. Ονομάζουμε **supremum** δύο υποομάδων H και K μιας ομάδας G , και το συμβολίζουμε $H \vee K$, την υποομάδα που παράγεται από την ένωση $H \cup K$, δηλαδή

$$H \vee K = \langle H \cup K \rangle.$$

Έτσι, $H \vee K = \bigcap \{T / T \leq G, \text{ με } H \cup K \subseteq T\}$. Επομένως, το **supremum** $H \vee K$ είναι η μικρότερη υποομάδα της G που περιέχει και την H και την K .

Μπορούμε λοιπόν να περιγράψουμε τα στοιχεία της ομάδας $H \vee K$ αυτά είναι της μορφής

$$h_1^{\alpha_1} k_1^{\beta_1} h_2^{\alpha_2} k_2^{\beta_2} \dots h_n^{\alpha_n} k_n^{\beta_n}, n \in \mathbb{Z}^+, h_i \in H, k_i \in K \text{ και } \alpha_i, \beta_i \in \mathbb{Z}.$$

Επειδή οι H και K είναι υποομάδες, αυτά είναι της μορφής $h_1 k_1 h_2 k_2 \dots h_n k_n, n \in \mathbb{Z}^+, h_i \in H, k_i \in K$.

Επομένως

$$H \vee K = \{h_1 k_1 \dots h_n k_n / n \in \mathbb{Z}^+, h_i \in H, k_i \in K, i=1, \dots, n\}$$

Παράδειγμα 1.

α) Στην ομάδα V του Klein έχουμε

$$\{e, a\} \vee \{e, b\} = V$$



β) Στην προσθετική ομάδα $\mathbb{Z} \times \mathbb{Z}$ έχουμε

$$(\{0\} \times \mathbb{Z}) \vee (\mathbb{Z} \times \{0\}) = \mathbb{Z} \times \mathbb{Z} \quad . \blacksquare$$

Τα στοιχεία της $H \vee K$ έχουν απλούστερη μορφή στην περίπτωση που οι ομάδες H και K αντιμετατίθενται .

ΟΡΙΣΜΟΣ. Αν X και Y είναι δύο μη-κενά υποσύνολα μιας ομάδας G ορίζουμε το γινόμενο τους XY να είναι το σύνολο

$$XY = \{xy / x \in X \text{ και } y \in Y\} \quad .$$

Ο ορισμός ισχύει και στην περίπτωση που τα X, Y είναι υποομάδες της G .

Αν $X = \{x\}$, τότε συμβολίζουμε xY το γινόμενο $\{x\} \cdot Y$, δηλαδή

$$xY = \{xy / y \in Y\}$$

και όμοια , αν $Y = \{y\}$, γράφουμε

$$Xy = \{xy / x \in X\} \quad .$$

Παρατήρηση.

Στην περίπτωση που η ομάδα G είναι προσθετική , έχουμε

$$x + Y = \{x+y / y \in Y\} \text{ και } X+y = \{x+y / x \in X\} \quad .$$

Ορίζουμε έτσι μια πράξη "γινόμενο" μέσα στο σύνολο των μη-κενών υποσυνόλων της ομάδας G , η οποία είναι προσεταιριστική , δηλαδή , αν X, Y, Z είναι μη-κενά υποσύνολα της G , έχουμε

$$X(YZ) = \{x(yz) / x \in X , y \in Y , z \in Z\} = (XY)Z \quad ,$$

ενώ γενικά , δεν είναι αντιμεταθετική .

Αν τώρα οι υποομάδες H και K αντιμετατίθενται , δηλαδή

$$HK = KH \quad ,$$



για κάθε $hk \in HK$ υπάρχει $k'h' \in KH$, έτσι ώστε

$$hk = k'h'.$$

Επομένως, για το γινόμενο $h_1k_1h_2k_2$ έχουμε

$$\begin{aligned} h_1k_1h_2k_2 &= h_1k_1k'_2h'_2 & (h_2k_2 &= k'_2h'_2) \\ &= h_1k'h'_2 & (k_1k'_2 &= k') \\ &= h_1h'k & (k'h'_2 &= h'k) \\ &= hk & (h'_1h' &= h) \end{aligned}$$

Γενικότερα,

$$h_1k_1 \cdot h_2k_2 \cdot \dots \cdot h_nk_n = hk \quad \text{για κάποια } h \in H \text{ και } k \in K$$

Έτσι, αν $HK = KH$, τότε

$$HVK = \{hk / h \in H \text{ και } k \in K\} = HK = KH.$$

Η σχέση " $\leq$ " είναι μια μερική διάταξη στο σύνολο $\mathcal{L}(G)$ όλων των υποομάδων μιας ομάδας G . Το ζεύγος, λοιπόν, $(\mathcal{L}(G), \leq)$ είναι ένα μερικά διατεταγμένο σύνολο (poset) τέτοιο ώστε, αν $H, K \in \mathcal{L}(G)$, τότε :

α) Υπάρχει το κάτω πέρασ (meet) $H \wedge K$ των H και K , που είναι η τομή τους $H \cap K$.

β) Υπάρχει το άνω πέρασ (join) $H \vee K$ των H και K , που είναι το supremum HVK .

Το μερικά διατεταγμένο σύνολο $(\mathcal{L}(G), \leq)$ είναι ένα δίκτυο (lattice).

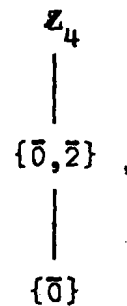
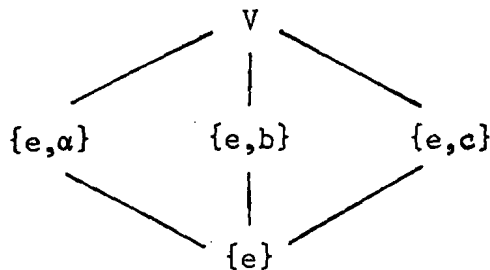
Είναι χρήσιμο να γράφουμε το διάγραμμα δικτύου, για τις υποομάδες μιας ομάδας G . Σ'ένα τέτοιο διάγραμμα, μια ευθεία γραμμή,



H
|
K

που γράφεται από την υποομάδα H στην K, θα δηλώνει ότι $K < H$, και ότι δεν υπάρχει υποομάδα A με $K < A < H$. Τη μεγαλύτερη υποομάδα θα τη βάζουμε στην κορυφή του διαγράμματος.

Έτσι, τα διαγράμματα δικτύων των υποομάδων της ομάδας του Klein V και της προσθετικής ομάδας Z_4 είναι τα επόμενα



§4. Ομομορφισμοί Ομάδων.

ΟΡΙΣΜΟΣ.

Ας είναι G και G' δύο ομάδες. Μια απεικόνιση $f: G \longrightarrow G'$ θα λέγεται ομομορφισμός από την ομάδα G στην G', όταν

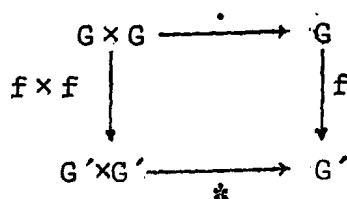
$$i) f(xy) = f(x)f(y) \quad \forall x, y \in G$$

Στην περίπτωση που συμβολίζουμε τις πράξεις των ομάδων διαφορετικά, δηλαδή, αν έχουμε τις ομάδες $(G, \cdot)$ και $(G', *)$, τότε η σχέση

i) γράφεται

$$i') f(x \cdot y) = f(x) * f(y) \quad \forall x, y \in G.$$

Μ'άλλα λόγια η απεικόνιση $f: G \longrightarrow G'$ είναι ομομορφισμός ομάδων, όταν το επόμενο διάγραμμα είναι αντιμεταθετικό



(Η απεικόνιση $f \times f$ ορίζεται ως εξής : $(f \times f)(x, y) = (f(x), f(y))$

$\forall (x, y) \in G \times G$. Ένας ομομορφισμός ομάδων $f : G \longrightarrow G'$ καλείται

Επιμορφισμός , όταν η απεικόνιση f είναι επί .

Μονομορφισμός , όταν η απεικόνιση f είναι 1-1 .

Ισομορφισμός , όταν η απεικόνιση f είναι 1-1 και επί δηλαδή όταν ο f είναι ταυτόχρονα επιμορφισμός και μονομορφισμός . Στην περίπτωση αυτή θα λέμε ότι οι ομάδες G και G' είναι ισομορφες και θα το συμβολίσουμε $G \cong G'$.

Παραδείγματα.

1) Για τυχούσες ομάδες G και G' , υπάρχει πάντα ένας ομομορφισμός από τη G στην G' , ο τετριμμένος ομομορφισμός

$$f : G \longrightarrow G' , f(x) = 1_{G'} , \quad \forall x \in G .$$

2) Για κάθε ομάδα G , η ταυτοτική απεικόνιση $I_G : G \longrightarrow G$ είναι ένας ομομορφισμός , αφού $I_G(xy) = xy = I_G(x)I_G(y)$, $\forall x, y \in G$. Ο I_G είναι φανερά ένας ισομορφισμός .

3) Η απεικόνιση $f : \mathbb{Z} \longrightarrow \mathbb{Z}$, $f(n) = 2n$ $\forall n \in \mathbb{Z}$ είναι φανερά ένας ομομορφισμός της ομάδας $(\mathbb{Z}, +)$ στον εαυτό της . Η f είναι ένας μονομορφισμός , ενώ δεν είναι επιμορφισμός .

4) Η κανονική προβολή $p : \mathbb{Z} \longrightarrow \mathbb{Z}_m$, $p(n) = \bar{n}$, $\forall n \in \mathbb{Z}$ είναι ένας ομομορφισμός της ομάδας $(\mathbb{Z}, +)$ στην $(\mathbb{Z}_m, +)$, αφού $p(k+n) = \overline{k+n} = \bar{k} + \bar{n} = p(k) + p(n)$, $\forall k, n \in \mathbb{Z}$.

Η p είναι φανερά ένας επιμορφισμός , ενώ δεν είναι μονομορφισμός .

5) Ας είναι $V = \{e, a, b, c\}$ η ομάδα του Klein . Η απεικόνιση $\varphi : V \longrightarrow V$, με $\varphi(e) = \varphi(a) = e$ και $\varphi(b) = \varphi(c) = a$, είναι ένας ομομορφισμός (για παράδειγμα $\varphi(ab) = \varphi(c) = a = ea = \varphi(a)\varphi(b)$) . Η φ όμως δεν είναι ούτε επιμορφισμός ούτε και μονομορφισμός .

6) Αν G και H είναι δύο ομάδες , τότε οι απεικονίσεις

$$G \xrightleftharpoons[\pi_1]{i_1} G \times H \xrightleftharpoons[\pi_2]{i_2} H$$



όπου

$$\pi_1(g, h) = g, \quad \forall (g, h) \in G \times H$$

$$\pi_2(g, h) = h, \quad \forall (g, h) \in G \times H$$

$$i_1(g) = (g, 1_H), \quad \forall g \in G$$

$$i_2(h) = (1_G, h), \quad \forall h \in G$$

είναι ομομορφισμοί ομάδων. Ιδιαίτερα οι π_1, π_2 είναι επιμορφισμοί, ενώ οι i_1, i_2 είναι μονομορφισμοί.

Ας είναι τώρα $f: G \longrightarrow H$ ένας ομομορφισμός ομάδων. Τότε,

$$\alpha) f(1_G) = 1_H$$

$$\beta) f(x^{-1}) = (f(x))^{-1} \quad \forall x \in G.$$

Πραγματικά,

$$f(1_G) \cdot f(1_G) = f(1_G \cdot 1_G) = f(1_G) = 1_H f(1_G) \implies 1_H = f(1_G).$$

Για το $\beta)$ αρκεί να δείξουμε ότι $f(x^{-1}) \cdot f(x) = 1_H = f(x) f(x^{-1})$.

Είναι $f(x^{-1}) \cdot f(x) \stackrel{\text{f ομομ}}{=} f(x^{-1}x) = f(1_G) = 1_H$. Όμοια

$f(x) \cdot f(x^{-1}) = 1_H$, όπως το επιθυμούσαμε.

Ας δούμε όμως τι συμβαίνει με τη σύνθεση ομομορφισμών:

Αν $f: G \longrightarrow H$ και $g: H \longrightarrow K$ είναι ομομορφισμοί ομάδων, τότε και η σύνθεσή του

$$g \circ f: G \longrightarrow K$$

είναι ομομορφισμός. Πραγματικά, $\forall x, y \in G$ έχουμε

$$(g \circ f)(xy) = g(f(xy)) \stackrel{\text{f ομομ}}{=} g(f(x) \cdot f(y)) =$$

$$\stackrel{\text{g ομομ}}{=} g(f(x)) \cdot g(f(y)) = (g \circ f)(x) \cdot (g \circ f)(y).$$



Ένας ομομορφισμός $f: G \longrightarrow G$ μιας ομάδας G στον εαυτό της, καλείται ενδομορφισμός της G .

Το σύνολο $\text{End}(G)$ όλων των ενδομορφισμών της ομάδας G , με πράξη τη σύνθεση απεικονίσεων, αποτελεί φανερά ένα μονοειδές.

Ένας ισομορφισμός $f: G \longrightarrow G$, μιας ομάδας G στον εαυτό της, ονομάζεται αυτομορφισμός της ομάδας G .

Εύκολα διαπιστώνεται ότι το σύνολο όλων των αυτομορφισμών μιας ομάδας G , με πράξη τη σύνθεση απεικονίσεων, είναι ομάδα που θα την παριστάνουμε $\text{Aut}(G)$.

ΟΡΙΣΜΟΣ. Ας είναι $f: G \longrightarrow H$ ένας ομομορφισμός ομάδων. Ονομάζουμε πυρήνα (kernel) του f , και το συμβολίζουμε $\text{Ker}(f)$, το σύνολο όλων των στοιχείων της G που η f απεικονίζει στο μοναδιαίο στοιχείο της H , δηλαδή

$$\text{Ker}(f) = \{x / x \in G \text{ και } f(x) = 1_H\}.$$

Το $\text{Ker}(f)$ είναι υποομάδα της G .

Πραγματικά, $\text{Ker}(f) \neq \emptyset$ το $1_G \in \text{Ker}(f)$, αφού $f(1_G) = 1_H$. Επιπλέον, αν $x, y \in \text{Ker}(f)$, δηλαδή, αν $f(x) = f(y) = 1_H$, τότε και $xy^{-1} \in \text{Ker}(f)$, αφού

$$f(xy^{-1}) \stackrel{f \text{ ομομ}}{=} f(x)f(y^{-1}) = f(x)[f(y)]^{-1} = 1_H \cdot 1_H^{-1} = 1_H.$$

Μπορούμε να δούμε αν ένας ομομορφισμός είναι μονομορφισμός, εξετάζοντας τον πυρήνα. Έχουμε το επόμενο κριτήριο

$\text{Ο ομομορφισμός } f: G \longrightarrow H \text{ είναι μονομορφισμός} \iff \text{Ker}(f) = \{1_G\}$
--

Πραγματικά, ας υποθέσουμε ότι $\text{Ker}(f) = \{1_G\}$. Αν τώρα $f(x) = f(y)$, τότε

$$[f(y)]^{-1} \cdot f(x) = [f(y)]^{-1} \cdot f(y), \text{ οπότε}$$



$$f(y^{-1})f(x) = 1_H \quad \text{συνεπώς}$$

$$f(y^{-1}x) = 1_H, \quad \text{δηλαδή } y^{-1}x = 1_G \implies y = x.$$

Αντίστροφα, ας είναι ο f ένας μονομορφισμός.

Αν $x \in \text{Ker}(f)$, τότε $f(x) = 1_H$ αλλά και $f(1_G) = 1_H$ έτσι $f(x) = f(1_G)$,
οπότε $x = 1_G$ (ο f μονομορφισμός). Συνεπώς $\text{Ker}(f) = \{1_G\}$.

ΠΡΟΤΑΣΗ 7.

Ας είναι $f: G \longrightarrow G'$ ένας ομομορφισμός ομάδων. Ισχύουν τα
επόμενα

- i) Αν $H \leq G$, τότε και η εικόνα $f(H)$ είναι υποομάδα της G' .
- ii) Αν $K \leq G'$, τότε και η αντίστροφη εικόνα $f^{-1}(K)$ είναι υποομάδα της G .

Απόδειξη.

Η απόδειξη είναι περίπου όμοια, όπως και στα μονοειδή (βλέπε
Κεφ. I, § 3, προτ. 3)

$$\text{i)} \text{ Μένει να δείξουμε ότι } \forall z \in f(H) \implies z^{-1} \in f(H).$$

Αν $z \in f(H)$, τότε υπάρχει $x \in H$ ώστε $f(x) = z$. Αλλά και το $x^{-1} \in H$,
αφού η H υποομάδα, επομένως

$$f(x^{-1}) = [f(x)]^{-1} = z^{-1} \implies z^{-1} \in f(H).$$

$$\text{ii)} \text{ Μένει να δείξουμε ότι, αν } x \in f^{-1}(K) \implies x^{-1} \in f^{-1}(K).$$

Αν $x \in f^{-1}(K) \implies f(x) \in K$, επομένως $[f(x)]^{-1} \in K$, αφού $K \leq G'$,
και έτσι $f(x^{-1}) \in K$, δηλαδή $x^{-1} \in f^{-1}(K)$. ■

Ονομάζουμε εικόνα (image) του ομομορφισμού $f: G \longrightarrow G'$, και
γράφουμε $\text{Im}(f)$, την υποομάδα $f(G)$ της G' .

$$\text{Im}(f) = f(G).$$



Έτσι, ο ομομορφισμός f είναι επιμορφισμός, εάν-ν $\text{Im}(f) = G'$, ενώ ο f είναι ισομορφισμός, εάν-ν $\text{Ker}(f) = \{1\}$ και $\text{Im}(f) = G'$.

Είναι φανερό τώρα ότι ο ομομορφισμός $f: G \longrightarrow G'$ είναι ένας επιμορφισμός της ομάδας G στην ομάδα $\text{Im}(f)$, ενώ ο μονομορφισμός $f: G \longrightarrow G'$ είναι ένας ισομορφισμός της ομάδας G στην ομάδα $\text{Im}(f)$.

ΟΡΙΣΜΟΣ. Θα λέμε ότι η ομάδα G εμφυτεύεται στην ομάδα G' , αν υπάρχει ένας μονομορφισμός $\varphi: G \longrightarrow G'$.

Στην περίπτωση αυτή, $G \cong \text{Im}(\varphi)$, αλλά και αντίστροφα, αν η ομάδα G είναι ισομορφή με μια υποομάδα K της G' , δηλαδή υπάρχει ισομορφισμός $\varphi: G \longrightarrow K$, τότε η απεικόνιση

$$\begin{aligned} G &\longrightarrow G' \\ x &\longmapsto \varphi(x) \end{aligned}$$

είναι ένας μονομορφισμός, δηλαδή η G εμφυτεύεται στην G' .

Αν τώρα $f: G \longrightarrow G'$ ένας ισομορφισμός ομάδων, τότε και η αντίστροφη απεικόνιση $f^{-1}: G' \longrightarrow G$ είναι ομομορφισμός ομάδων.

Αρκεί να δείξουμε ότι, για κάθε $x, y \in G'$, έχουμε

$$f^{-1}(xy) = f^{-1}(x)f^{-1}(y).$$

Επειδή η παραπάνω ιδιότητα αφορά στοιχεία της G και η f είναι 1-1, αρκεί να δείξουμε ότι

$$f(f^{-1}(xy)) = f(f^{-1}(x)f^{-1}(y)).$$

Αλλά $f(f^{-1}(xy)) = xy$ και $f(f^{-1}(x)f^{-1}(y)) = f(f^{-1}(x)) \cdot f(f^{-1}(y)) = xy$ όπως το επιθυμούσαμε.

Όπως και στα μονοειδή έτσι και στις ομάδες, αν $f: G \longrightarrow G'$



είναι ομομορφισμός ομάδων , τότε ο f είναι ισομορφισμός , εάν και μόνο εάν υπάρχει ομομορφισμός $g: G' \longrightarrow G$ έτσι ώστε

$$g \circ f = I_G \quad \text{και} \quad f \circ g = I_{G'} .$$

Παρατήρηση .

Θα παρατηρήσουμε εδώ ότι ισομόρφες ομάδες έχουν τις ίδιες αλγεβρικές ιδιότητες , αφού οι ιδιότητες της μιας μεταφέρονται και στην άλλη από τον ισομορφισμό . Γενικά , στην Άλγεβρα ταυτίζουμε τις ισομόρφες δομές , αφού μας ενδιαφέρουν οι ιδιότητες τους και όχι η φύση των στοιχείων τους . Η μελέτη λοιπόν των ομάδων απλοποιείται σημαντικά , γιατί , από τη στιγμή που ξέρουμε ότι πολλές ομάδες είναι ισομόρφες , αρκεί να μελετήσουμε μια από αυτές .

Παράδειγμα 1.

Η απεικόνιση $\log: \mathbb{R}^+ \longrightarrow \mathbb{R}$, $x \longmapsto \log x$ (όπου $\log x$ δηλώνει τον φυσικό λογάριθμο του x) είναι ένας ομομορφισμός ομάδων

$$\log: (\mathbb{R}^+, \cdot) \longrightarrow (\mathbb{R}, +) .$$

Πραγματικά , $\forall x, y \in \mathbb{R}^+$ είναι $\log(xy) = \log x + \log y$. Επίσης η απεικόνιση $e: \mathbb{R} \longrightarrow \mathbb{R}^+$, $x \longmapsto e^x$ είναι ένας ομομορφισμός ομάδων

$$e: (\mathbb{R}, +) \longrightarrow (\mathbb{R}^+, \cdot) ,$$

αφού για $\forall x, y \in \mathbb{R}$ έχουμε $e^{x+y} = e^x \cdot e^y$.

Η σύνθεση $\log \circ e: (\mathbb{R}, +) \longrightarrow (\mathbb{R}, +)$ είναι ταυτοτικός ομομορφισμός , αφού

$$[\log \circ e](x) = \log(e^x) = x \quad \forall x \in \mathbb{R} .$$

Και η σύνθεση $e \circ \log: (\mathbb{R}^+, \cdot) \longrightarrow (\mathbb{R}^+, \cdot)$ είναι ο ταυτοτικός ομομορφισμός , αφού $\forall x \in \mathbb{R}^+$ έχουμε

$$[e \circ \log](x) = e^{\log x} = x .$$

Δηλαδή , ο $\log$ είναι ένας ισομορφισμός της ομάδας $(\mathbb{R}^+, \cdot)$ στην



ομάδα $(\mathbb{R}, +)$ με αντίστροφο τον e :

$$(\mathbb{R}^+, \cdot) \cong (\mathbb{R}, +) .$$

Παράδειγμα 2 .

Η απεικόνιση $\det : GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^*$, $A \longmapsto \det A$ είναι ένας ομομορφισμός της πολ/κής ομάδας $GL_n(\mathbb{R})$ στην ομάδα $(\mathbb{R}^*, \cdot)$. Πραγματικά , αν $A, B \in GL_n(\mathbb{R})$ είναι $\det(AB) = \det A \cdot \det B$.

Ο $\det$ είναι επιμορφισμός , αφού για κάθε $\alpha \in \mathbb{R}^*$ υπάρχει πίνακας $A \in GL_n(\mathbb{R})$ π.χ. ο πίνακας $A = (\alpha_{ij})$ με $\alpha_{ij} = 0$, όταν $i \neq j$, $\alpha_{11} = \alpha$ και $\alpha_{22} = \dots = \alpha_{nn} = 1$, έτσι ώστε $\det A = \alpha$. Άρα $\text{Im}(\det) = \mathbb{R}^*$.

Ο πυρήνας του ομομορφισμού $\det$ είναι

$$\text{Ker}(\det) = \{A/A \in GL_n(\mathbb{R}) \text{ με } \det A = 1\} = SL_n(\mathbb{R}) .$$

Παράδειγμα 3 . (Εσωτερικοί αυτομορφισμοί ομάδας G) .

Ας είναι G μια ομάδα . Σε κάθε στοιχείο $g \in G$ αντιστοιχούμε ένα αυτομορφισμό τ_g της G , ως εξής :

$$\tau_g : G \longrightarrow G , \quad \tau_g(x) = g x g^{-1} \quad \forall x \in G .$$

(το στοιχείο $g x g^{-1}$ καλείται συζυγές του x από το g) .

Πραγματικά , έχουμε :

$$\tau_g(xy) = g x y g^{-1} = g x g^{-1} g y g^{-1} = \tau_g(x) \cdot \tau_g(y) \quad x, y \in G ,$$

δηλαδή ο τ_g είναι ομομορφισμός της G .

Επιπλέον , αν $g_1, g_2 \in G$, τότε $\tau_{g_1 g_2} = \tau_{g_1} \circ \tau_{g_2}$. Πραγματικά ,

$\forall x \in G$ έχουμε

$$\begin{aligned} \tau_{g_1 g_2}(x) &= g_1 g_2 x (g_1 g_2)^{-1} = g_1 g_2 x g_2^{-1} g_1^{-1} = \tau_{g_1}(\tau_{g_2}(x)) = \\ &= (\tau_{g_1} \circ \tau_{g_2})(x) . \end{aligned}$$



Ιδιαίτερα, επειδή $\tau_{1_G} = I_G$ είναι $\tau_g \circ \tau_{g^{-1}} = \tau_{1_G} = \tau_{g^{-1}} \circ \tau_g$.

Επομένως, ο τ_g είναι αντιστρέψιμος, έτσι ο $\tau_g \in \text{Aut}(G)$. Ο αυτομορφισμός τ_g ονομάζεται εσωτερικός αυτομορφισμός της G , που αντιστοιχεί στο στοιχείο g . Κάθε άλλος αυτομορφισμός της G καλείται εξωτερικός αυτομορφισμός.

Είναι φανερό τώρα ότι το σύνολο όλων των εσωτερικών αυτομορφισμών της G , με πράξη τη σύνθεση απεικονίσεων, αποτελεί ομάδα που την συμβολίζουμε $\text{Inn}(G)$ και μάλιστα $\text{Inn}(G) \leq \text{Aut}(G)$.

§5.1. Κυκλικές ομάδες.

ΟΡΙΣΜΟΣ. Μια ομάδα G καλείται κυκλική, αν υπάρχει στοιχείο $x \in G$ που να την παράγει, δηλαδή αν

$$G = \langle x \rangle = \{x^n / n \in \mathbb{Z}\}.$$

Στην περίπτωση αυτή, το στοιχείο x καλείται γεννήτορας της G .

Παρατηρήσεις.

1. Αν η G είναι προσθετική, η G είναι κυκλική με γεννήτορα το στοιχείο x , όταν

$$G = \langle x \rangle = \{nx / n \in \mathbb{Z}\}.$$

2. Είναι δυνατόν μια κυκλική ομάδα $G = \langle x \rangle$ να έχει και άλλο γεννήτορα $y \in G$, δηλαδή $G = \langle y \rangle$. Για παράδειγμα, η προσθετική ομάδα των ακεραίων $\mathbb{Z}$ είναι κυκλική, $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$ και μάλιστα τα στοιχεία της 1 και -1 είναι οι μόνοι γεννήτορές της.

Παράδειγμα 1. Η προσθετική ομάδα $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$ είναι κυκλική με γεννήτορα την κλάση $\bar{1}$, δηλαδή

$$\mathbb{Z}_m = \langle \bar{1} \rangle.$$

(Για την $\mathbb{Z}_4$ π.χ. έχουμε $\mathbb{Z}_4 = \langle \bar{1} \rangle = \langle \bar{3} \rangle$).



Παράδειγμα 2 . Η ομάδα $G_n = \{z/z \in \mathbb{C}, \text{ και } z^n = 1\}$ των n -στων ριζών της μονάδας είναι κυκλική . Πραγματικά, οι n -στες ρίζες της μονάδας είναι οι n σε πλήθος μιγαδικοί αριθμοί

$$z_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n} = e^{i \frac{2k\pi}{n}} \quad k=0,1,2,\dots,n-1$$

($e^{ix} = \cos x + i \sin x$ και $e^{-ix} = \cos x - i \sin x$, ταυτότητες Euler) .

Η G_n είναι λοιπόν πεπερασμένης τάξης n , δηλαδή

$$G_n = \{z_0 = 1, z_1, z_2, \dots, z_{n-1}\}$$

Κάνοντας χρήση του τύπου του De Moivre

$$(\cos \theta + i \sin \theta)^k = \cos(k\theta) + i \sin(k\theta)$$

παρατηρούμε ότι

$$z_1^0 = 1 = z_0$$

$$z_1^1 = z_1$$

$$z_1^2 = (\cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n})^2 = z_2$$

⋮

$$z_1^{n-1} = (\cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n})^{n-1} = z_{n-1}$$

$$\text{Επομένως } G_n = \langle z_1 \rangle = \{1, z_1, z_1^2, \dots, z_1^{n-1}\}$$

Υπάρχουν βέβαια ομάδες που δεν είναι κυκλικές .

Παράδειγμα 3 .

α) Η ομάδα $V = \{e, a, b, c\}$ του Klein δεν είναι κυκλική , αφού οι υποομάδες της

$$\langle e \rangle = \{e\}, \langle a \rangle = \{e, a\}, \langle b \rangle = \{e, b\}, \langle c \rangle = \{e, c\}$$

είναι διαφορετικές από τη V .



β) Η ομάδα $(\mathbb{Q}, +)$ δεν είναι κυκλική, αφού $\langle 0 \rangle = \{0\}$ και για κάθε ρητό $q \neq 0$ η $\langle q \rangle = \{nq / n \in \mathbb{Z}\}$ είναι γνήσια υποομάδα της, αφού υπάρχουν ρητού π.χ. ο $9/2 \notin \langle q \rangle$.

Συνεχίζοντας, θα παρατηρήσουμε ότι :

Κάθε κυκλική ομάδα είναι αβελιανή.

Πραγματικά, αν $G = \langle a \rangle = \{a^n / n \in \mathbb{Z}\}$ και a^r, a^s είναι δύο τυχόντα στοιχεία της, τότε

$$a^r \cdot a^s = a^{r+s} = a^{s+r} = a^s \cdot a^r.$$

Το αντίστροφο δεν ισχύει. Για παράδειγμα, οι αβελιανές ομάδες V του Klein και $(\mathbb{Q}, +)$ δεν είναι κυκλικές.

ΘΕΩΡΗΜΑ 1. Κάθε υποομάδα μιας κυκλικής ομάδας είναι κυκλική. Ιδιαίτερα αν H είναι μια μη-τετριμμένη υποομάδα της $G = \langle a \rangle$ και m είναι ο ελάχιστος θετικός ακέραιος έτσι ώστε $a^m \in H$, τότε $H = \langle a^m \rangle = \{a^{mk} / k \in \mathbb{Z}\}$.

Απόδειξη.

Έστω η κυκλική ομάδα $G = \langle a \rangle = \{a^n / n \in \mathbb{Z}\}$ και H μια υποομάδα της. Αν $H = \{1\}$, τότε φανερά η H είναι κυκλική. Αν $H \neq \{1\}$, τότε, αν $a^m \in H$, και το $a^{-m} \in H$ (η H υποομάδα), που σημαίνει ότι υπάρχουν θετικού ακέραιου n έτσι ώστε $a^n \in H$. Ας είναι m ο ελάχιστος θετικός ακέραιος έτσι ώστε $a^m \in H$. Το στοιχείο a^m παράγει την H , δηλαδή $H = \langle a^m \rangle = \{a^{mk} / k \in \mathbb{Z}\}$. Πραγματικά, είναι φανερό ότι $\langle a^m \rangle \leq H$.

Μένει να δείξουμε ότι $H \leq \langle a^m \rangle$, δηλαδή ότι κάθε στοιχείο $b \in H$ είναι όσο $b = a^{mq}$, για κάποιο ακέραιο q .

Επειδή $b \in H$ και $H \leq G$, θα έχουμε $b = a^n$ για κάποιο ακέραιο n . Από τον Αλγόριθμο του Ευκλείδη παίρνουμε

$$n = mq + r \quad \text{με} \quad 0 \leq r < m.$$



Τότε

$$a^n = a^{mq+r} = (a^m)^q \cdot a^r \implies (a^m)^{-q} a^n = a^r .$$

Επειδή $a^m, a^n \in H$ και η H υποομάδα και το $(a^m)^{-q} \cdot a^n \in H$, δηλαδή $a^r \in H$ που σημαίνει ότι το $r=0$, αφού έχουμε εκλέξει τον m σαν τον ελάχιστο θετικό ακέραιο για τον οποίο $a^m \in H$. Έτσι $n=mq$ οπότε $b=a^n=a^{mq}$, όπως επιθυμούσαμε. ■

Για παράδειγμα, στην ομάδα $(\mathbb{Z}, +)$, που είναι κυκλική $\mathbb{Z} = \langle 1 \rangle$, κάθε υποομάδα της $\neq \{0\}$ είναι της μορφής

$$\langle m \rangle = \{mk / k \in \mathbb{Z}\} = m\mathbb{Z}$$

για κάποιο φυσικό $m \geq 1$.

Επομένως, όλες οι υποομάδες της $(\mathbb{Z}, +)$ είναι οι

$$\{0\}, \langle 1 \rangle, \langle 2 \rangle, \langle 3 \rangle, \dots$$

δηλαδή οι

$$\{0\}, \mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z}, \dots$$

ΠΡΟΤΑΣΗ 8. Ας είναι $f: G \longrightarrow H$ ένας ομομορφισμός από την κυκλική ομάδα $G = \langle a \rangle$ στην ομάδα H . Τότε και η εικόνα $\text{Im}(f)$ είναι κυκλική και μάλιστα $\text{Im}(f) = \langle f(a) \rangle$.

Απόδειξη.

Παρατηρούμε ότι, για κάθε ακέραιο n , έχουμε

$$[f(a)]^n \xrightarrow{f \text{ ομομ}} f(a^n) \in \text{Im}(f),$$

συνεπώς $\langle f(a) \rangle \leq \text{Im}(f)$.

Αντίστροφα, αν $z \in \text{Im}(f)$, τότε $z = f(a^k)$ για κάποιο ακέραιο k ,

δηλαδή $z = [f(a)]^k$ άρα $z \in \langle f(a) \rangle$ και τελικά $\text{Im}(f) \leq \langle f(a) \rangle$.

Έτσι $\text{Im}(f) = \langle f(a) \rangle$. ■



Ας είναι τώρα $G = \langle a \rangle = \{a^n / n \in \mathbb{Z}\}$ μια κυκλική ομάδα .

A) . Αν για κάθε ζεύγος ακεραίων (k, λ) με $k \neq \lambda$ συμβαίνει $a^k \neq a^\lambda$, τότε η G είναι μια κυκλική ομάδα άπειρης τάξης .

B) . Αν υπάρχει ζεύγος ακεραίων (k, λ) με $k \neq \lambda$ ώστε να ισχύει $a^k = a^\lambda$, θα έχουμε

$$a^h = 1 \quad , \quad h > 0 \quad .$$

($h = k - \lambda$ αν $k > \lambda$ και $h = \lambda - k$ αν $\lambda > k$) .

Ας είναι τώρα m ο ελάχιστος θετικός ακέραιος για τον οποίο ισχύει

$$a^m = 1 \quad \text{και} \quad a^k \neq 1 \quad \text{για κάθε} \quad k \quad \text{με} \quad 0 < k < m \quad .$$

Τα στοιχεία της $1, a, a^2, \dots, a^{m-1}$ είναι διαφορετικά μεταξύ τους , ενώ κάθε άλλο στοιχείο $a^\lambda \in G$ με $\lambda > m$ ταυτίζεται με ένα από αυτά .
πραγματικά , από τον αλγόριθμο του Ευκλείδη παίρνουμε

$$\lambda = mq + r \quad 0 \leq r < m$$

οπότε ,

$$a^\lambda = a^{mq+r} = (a^m)^q \cdot a^r = 1 \cdot a^r = a^r \quad .$$

Συνεπώς ,

$$G = \{1, a, \dots, a^{m-1}\}$$

δηλαδή η G είναι μια κυκλική ομάδα πεπερασμένης τάξης m .

ΟΡΙΣΜΟΣ . Καλείται **τάξη** του στοιχείου a μιας ομάδας G , η τάξη της κυκλικής υποομάδας $\langle a \rangle$ που παράγει το στοιχείο a .

Επομένως

i) Το στοιχείο a έχει **τάξη** n , αν η υποομάδα $\langle a \rangle$ είναι τάξης n .

ii) Το στοιχείο a θα λέμε ότι έχει **άπειρη τάξη** , αν η υποομά-



δα $\langle a \rangle$ είναι άπειρη .

Με άλλα λόγια , η τάξη του στοιχείου a είναι ο ελάχιστος θετικός ακέραιος n (αν υπάρχει τέτοιος) για τον οποίο

α) $a^n = 1$, αν η ομάδα είναι πολ/κή

β) $na = 0$, αν η ομάδα είναι προσθετική .

Αν τέτοιος θετικός ακέραιος δεν υπάρχει , δηλαδή όταν

$$a^n = 1 \iff n = 0$$

θα λέμε ότι το στοιχείο a έχει άπειρη τάξη .

Θα παρατηρήσουμε εδώ ότι , τα στοιχεία x και x^{-1} μιας ομάδας G έχουν την ίδια τάξη . Πραγματικά ,

$$\langle x \rangle = \{x^n / n \in \mathbb{Z}\} = \{x^{-n} / n \in \mathbb{Z}\} = \langle x^{-1} \rangle .$$

Παραδείγματα .

1) Στην προσθετική ομάδα $\mathbb{Z}$ των ακεραίων κάθε μη-μηδενικό στοιχείο έχει άπειρη τάξη .

2) Στην ομάδα V του Klein τα στοιχεία a, b, c έχουν τάξη 2 , αφού $\langle a \rangle = \{e, a\}$, $\langle b \rangle = \{e, b\}$, $\langle c \rangle = \{e, c\}$.

3) Στην προσθετική ομάδα $\mathbb{Z}_4$ τα στοιχεία $\bar{0}, \bar{1}, \bar{2}, \bar{3}$ έχουν τάξη 1, 4, 2, 4 αντίστοιχα, αφού είναι οι μικρότεροι θετικοί ακέραιοι για τους οποίους ισχύει

$$1 \cdot \bar{0} = \bar{0} \quad , \quad 4 \cdot \bar{1} = \bar{4} = \bar{0} \quad , \quad 2 \cdot \bar{2} = \bar{4} = \bar{0} \quad , \quad 4 \cdot \bar{3} = \bar{12} = \bar{0} .$$

4) Στην ομάδα των κουατερνιών (βλέπε Κεφ. II, §2.2, παράδ. 13) οι πίνακες j , k έχουν τάξη 4 , αφού

$$\langle j \rangle = \{j, j^2, j^3, I_2\} \quad , \quad \langle k \rangle = \{k, k^2, k^3, I_2\} .$$

ΠΡΟΤΑΣΗ 9.

Έστω $\varphi : G \longrightarrow H$ ένας μονομορφισμός από την G στην H . Τότε,



για κάθε $x \in G$, τα στοιχεία x και $\varphi(x)$ έχουν την ίδια τάξη.

Απόδειξη.

Αν $\varphi' = \varphi|_{\langle x \rangle}$, τότε από την πρόταση 8 θα έχουμε

$$\langle x \rangle \cong \text{Im} \varphi' = \langle \varphi(x) \rangle.$$

Οι υποομάδες λοιπόν $\langle x \rangle$, $\langle \varphi(x) \rangle$ έχουν την ίδια τάξη που σημαίνει ότι τα στοιχεία x και $\varphi(x)$ έχουν την ίδια τάξη. ■

Παρατηρήσεις

1) Μια ομάδα G καλείται περιοδική (periodic), αν κάθε στοιχείο της έχει πεπερασμένη τάξη.

Κάθε ομάδα πεπερασμένης τάξης είναι περιοδική, αφού τα στοιχεία της έχουν πεπερασμένη τάξη (οι αντίστοιχες κυκλικές ομάδες που παράγουν είναι πεπερασμένες).

Υπάρχουν όμως και άπειρες περιοδικές ομάδες. Ένα παράδειγμα είναι η ομάδα των ρητών modulo 1 $\mathbb{Q}/\mathbb{Z}$, την οποία θα μελετήσουμε παρακάτω.

2) Μια ομάδα G ονομάζεται ελεύθερα στρέψης (torsion-free), αν κάθε στοιχείο της διαφορετικό από το ουδέτερο έχει άπειρη τάξη. Για παράδειγμα οι ομάδες

$$(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{Q}^+, \cdot), (\mathbb{R}^+, \cdot)$$

3) Γενικά, μια άπειρη ομάδα μπορεί να έχει στοιχεία διάφορα του ουδέτερου πεπερασμένης τάξης και επίσης στοιχεία άπειρης τάξης. Τέτοιες ομάδες ονομάζονται μικτές (mixed).

Για παράδειγμα, στην πολ/κή ομάδα $(\mathbb{C}^*, \cdot)$, το στοιχείο

$$z_1 = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n} \quad \text{έχει τάξη } n, \text{ αφού}$$

$$G_n = \langle z_1 \rangle \quad (\text{βλέπε παραδ. 2}),$$

ενώ το στοιχείο 3 έχει άπειρη τάξη. Άρα η $(\mathbb{C}^*, \cdot)$ είναι μικτή.



ΠΡΟΤΑΣΗ 10.

Ας είναι G μια ομάδα και a ένα στοιχείο της με πεπερασμένη τάξη m . Τότε

$$i) a^k = 1 \iff m \mid k$$

$$ii) a^r = a^s \iff r \equiv s \pmod{m}$$

iii) Για κάθε θετικό ακέραιο k με $k \mid m$ έχουμε ότι η τάξη του στοιχείου a^k είναι ίση με $\frac{m}{k}$.

Απόδειξη.

$$i) (\Leftarrow) \text{ Αν } k = m \cdot \lambda, \text{ τότε } a^k = a^{m\lambda} = (a^m)^\lambda = 1^\lambda = 1.$$

$$(\Rightarrow) \text{ Αν } k = mq + r, \text{ με } 0 \leq r < m, \text{ τότε}$$

$a^k = a^{mq+r} = (a^m)^q \cdot a^r = 1 \cdot a^r = a^r$ και επειδή $a^k = 1$, έχουμε $a^r = 1$ με $0 \leq r < m$. Ο m όμως είναι ο ελάχιστος θετικός ακέραιος με $a^m = 1$, οπότε $r = 0$. Έτσι, $k = mq$, δηλαδή $m \mid k$.

$$ii) a^r = a^s \iff a^{r-s} = 1 \stackrel{(i)}{\iff} m \mid r-s \iff r \equiv s \pmod{m}$$

$$iii) \text{ Είναι } (a^k)^{\frac{m}{k}} = a^m = 1 \text{ και } (a^k)^r \neq 1, \text{ με}$$

$0 < r < \frac{m}{k}$, γιατί, αν $a^{kr} = 1$ με $0 < r < \frac{m}{k}$, θα είχαμε $kr < \frac{m}{k}k = m$, δηλαδή $a^{kr} = 1$ με $kr < m$ άτοπο, αφού ο m είναι ο ελάχιστος θετικός ακέραιος με $a^m = 1$. ■

Στη συνέχεια, θα δείξουμε ότι όλες οι άπειρες κυκλικές ομάδες είναι ισομόρφες με την $(\mathbb{Z}, +)$ ενώ όλες οι κυκλικές ομάδες τάξης m είναι ισομόρφες με την $(\mathbb{Z}_m, +)$.

ΘΕΩΡΗΜΑ 2.

Κάθε άπειρη κυκλική ομάδα είναι ισομόρφη με την προσθετική ομάδα $\mathbb{Z}$.



Απόδειξη.

Έστω $G = \langle \alpha \rangle$ μια άπειρη κυκλική ομάδα . θεωρούμε την απεικόνιση

$$i: \mathbb{Z} \longrightarrow G, \quad i(k) = \alpha^k \quad \forall k \in \mathbb{Z}.$$

Η απεικόνιση i είναι ομομορφισμός . Πραγματικά

$$i(k+\lambda) = \alpha^{k+\lambda} = \alpha^k \cdot \alpha^\lambda = i(k) \cdot i(\lambda) \quad \forall k, \lambda \in \mathbb{Z}.$$

Η i είναι επιμορφισμός , αφού για κάθε $\alpha^k \in \langle \alpha \rangle$ υπάρχει το στοιχείο $k \in \mathbb{Z}$, με $i(k) = \alpha^k$. Τέλος , είναι και μονομορφισμός , γιατί αν $k \neq \lambda$, τότε $\alpha^k \neq \alpha^\lambda$, αφού η G είναι άπειρη κυκλική ομάδα .

Έτσι $(\mathbb{Z}, +) \cong G$. ■

ΠΟΡΙΣΜΑ 1.

Αν $G = \langle \alpha \rangle$ είναι μια άπειρη κυκλική ομάδα , τότε

- i) Τα στοιχεία α και α^{-1} είναι οι μόνοι γεννήτορες της G .
- ii) Οι διακεκριμένες υποομάδες της είναι οι

$$\{1\}, \langle \alpha \rangle, \langle \alpha^2 \rangle, \langle \alpha^3 \rangle, \dots$$

Απόδειξη.

- i) Αν η G είχε και άλλο γεννήτορα α^k , με $k \neq 1, -1$ δηλαδή $G = \langle \alpha^k \rangle$, από τον ισομορφισμό $f: G \longrightarrow \mathbb{Z}$, $f(\alpha^n) = n$, $\forall \alpha^n \in G$, έχουμε

$$\begin{aligned} \text{Im}(f) &= \mathbb{Z} = \langle f(\alpha^k) \rangle && (\text{Πρόταση 8}) \\ &= \langle k \rangle \end{aligned}$$

δηλαδή $\mathbb{Z} = \langle k \rangle$ με $k \neq 1, -1$ άτοπο .

- ii) Εδώ η εργασία είναι ανάλογη παρατηρώντας μόνο ότι οι διακεκριμένες υποομάδες της $\mathbb{Z}$ είναι οι

$$\{0\}, \langle 1 \rangle, \langle 2 \rangle, \langle 3 \rangle, \dots \quad \blacksquare$$



ΘΕΩΡΗΜΑ 3 .

Κάθε πεπερασμένη κυκλική ομάδα τάξης m είναι ισομορφή με την προσθετική ομάδα $\mathbb{Z}_m$.

Απόδειξη.

Έστω $G = \{1, \alpha, \alpha^2, \dots, \alpha^{m-1}\}$ μια κυκλική ομάδα τάξης m . Παρατηρούμε ότι

$$\bar{r}, \bar{s} \in \mathbb{Z}_m \text{ και } \bar{r} = \bar{s} \text{ , τότε } r \equiv s \pmod{m} \text{ , οπότε}$$

$$\alpha^r = \alpha^s \text{ , σύμφωνα με πρόταση 10 .}$$

Η απεικόνιση επομένως

$$\beta: \mathbb{Z}_m \longrightarrow G \text{ , } \beta(\bar{k}) = \alpha^k \text{ , } \forall k \in \mathbb{Z}_m$$

είναι καλά ορισμένη .

Η β είναι ένας ομομορφισμός . Πραγματικά , για κάθε $\bar{k}, \bar{l} \in \mathbb{Z}_m$, έχουμε

$$\beta(\overline{k+l}) = \beta(\overline{k+l}) = \alpha^{k+l} = \alpha^k \cdot \alpha^l = \beta(\bar{k}) \cdot \beta(\bar{l}) \text{ .}$$

Η β είναι φανερά ένας επιμορφισμός . Τέλος , η β είναι και μονομορφισμός . αν $\beta(\bar{k}) = \beta(\bar{l})$, δηλαδή αν $\alpha^k = \alpha^l$, τότε $k \equiv l \pmod{m}$, σύμφωνα με την πρόταση 10 δηλαδή $\bar{k} = \bar{l}$. Έτσι $(\mathbb{Z}_m, +) \cong G$. ■

Άρα η μελέτη των άπειρων κυκλικών ομάδων και των πεπερασμένων κυκλικών ομάδων τάξης m , ανάγεται στην μελέτη των ομάδων $(\mathbb{Z}, +)$ και $(\mathbb{Z}_m, +)$ αντίστοιχα .

55.2. Υποομάδες των πεπερασμένων κυκλικών ομάδων.

Θεωρούμε την πεπερασμένη κυκλική ομάδα

$$G = \langle \alpha \rangle = \{1, \alpha, \alpha^2, \dots, \alpha^{m-1}\} \text{ .}$$

Αν H είναι μια υποομάδα της , τότε η H είναι κυκλική (θεώρημα 1) θα υπάρξει λοιπόν στοιχείο $b = \alpha^n \in G$ ώστε $H = \langle \alpha^n \rangle$.



ΠΡΟΤΑΣΗ 11 .

Η υποομάδα $\langle \alpha^n \rangle$ της G συμπίπτει με την υποομάδα $\langle \alpha^d \rangle$,
όπου d είναι ο μ.κ.δ των n και m δηλαδή

$$\langle \alpha^n \rangle = \langle \alpha^d \rangle \quad \text{με} \quad d = (n, m)$$

και περιέχει $\frac{m}{d}$ στοιχεία .

Απόδειξη.

Αφού $d = (n, m)$, τότε $n = dn'$, $n' \in \mathbb{Z}$. Επομένως , $\alpha^n = \alpha^{dn'} = (\alpha^d)^{n'}$,
δηλαδή $\alpha^n \in \langle \alpha^d \rangle$, που σημαίνει ότι $\langle \alpha^n \rangle \subseteq \langle \alpha^d \rangle$.

Αντίθετα , αφού $d = (n, m)$, έχουμε $d = nx + my$, $x, y \in \mathbb{Z}$, οπότε

$$\alpha^d = \alpha^{nx+my} = (\alpha^n)^x \cdot (\alpha^m)^y = (\alpha^n)^x \cdot 1 = (\alpha^n)^x ,$$

δηλαδή $\alpha^d \in \langle \alpha^n \rangle$, επομένως $\langle \alpha^d \rangle \subseteq \langle \alpha^n \rangle$.

Άρα $\langle \alpha^n \rangle = \langle \alpha^d \rangle$.

Ο d είναι διαιρέτης m , επομένως η τάξη του α^d είναι $\frac{m}{d}$
(Πρόταση 10) , δηλαδή η ομάδα $\langle \alpha^d \rangle$ περιέχει ακριβώς $\frac{m}{d}$ στοιχεία . ■

ΠΟΡΙΣΜΑ 2.

Αν σε μια τυχούσα ομάδα G το στοιχείο α έχει τάξη m και
 $d = (n, m)$, τότε τα στοιχεία της α^n και α^d έχουν την ίδια τάξη $\frac{m}{d}$. ■

Παράδειγμα 4.

Στην προσθετική ομάδα $\mathbb{Z}_{12} = \{\bar{0}, \bar{1}, \dots, \bar{11}\} = \langle \bar{1} \rangle$ ας πάρουμε την
κλάση $\bar{8}$. Επειδή $(8, 12) = 4$, η κλάση $\bar{8}$ παράγει μια υποομάδα με
 $\frac{12}{4} = 3$ στοιχεία , την

$$\langle \bar{8} \rangle = \langle \bar{4} \rangle = \{\bar{0}, \bar{4}, \bar{8}\} .$$

Έτσι οι κλάσεις $\bar{8}, \bar{4} \in \mathbb{Z}_{12}$ έχουν τάξη 3 .



ΠΡΟΤΑΣΗ 12 .

Αν $G = \{1, \alpha, \dots, \alpha^{m-1}\}$ είναι μια κυκλική ομάδα τάξης m , τότε τα στοιχεία α^r και α^s παράγουν την ίδια υποομάδα της, δηλαδή $\langle \alpha^r \rangle = \langle \alpha^s \rangle$, εάν και μόνο εάν $(r, m) = (s, m)$.

Απόδειξη .

Αν $\langle \alpha^r \rangle = \langle \alpha^s \rangle$ τότε $|\langle \alpha^r \rangle| = |\langle \alpha^s \rangle|$. Αν τώρα $d = (r, m)$ και $d' = (s, m)$ τότε από την πρόταση 11 θα έχουμε

$$i) \langle \alpha^r \rangle = \langle \alpha^d \rangle \quad \text{οπότε} \quad |\langle \alpha^r \rangle| = \frac{m}{d}$$

$$ii) \langle \alpha^s \rangle = \langle \alpha^{d'} \rangle \quad \text{οπότε} \quad |\langle \alpha^s \rangle| = \frac{m}{d'}$$

Έτσι $\frac{m}{d} = \frac{m}{d'}$, οπότε $d = d'$.

Αντίστροφα, αν $d = (r, m) = (s, m)$ τότε σύμφωνα με την πρόταση 11 $\langle \alpha^r \rangle = \langle \alpha^d \rangle = \langle \alpha^s \rangle$. ■

Για παράδειγμα, οι κλάσεις $\bar{2}, \bar{10} \in \mathbb{Z}_{12}$ παράγουν την ίδια υποομάδα

$$\langle \bar{2} \rangle = \langle \bar{10} \rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\},$$

αφού

$$(2, 12) = (10, 12) = 2. \quad \blacksquare$$

ΠΟΡΙΣΜΑ 3 .

Αν $G = \{1, \alpha, \dots, \alpha^{m-1}\}$ είναι μια κυκλική ομάδα τάξης m , το στοιχείο α^n παράγει την G , εάν και μόνο εάν οι m, n είναι πρώτοι μεταξύ του, δηλαδή

$$G = \langle \alpha^n \rangle = \langle \alpha \rangle \iff (m, n) = 1. \quad \blacksquare$$

Έτσι, τα διαφορετικά στοιχεία α^n της $G = \{1, \dots, \alpha^{m-1}\}$ που



παράγουν την G είναι τόσα όσοι είναι οι φυσικοί αριθμοί k ($0 < k < m$) οι πρώτοι προς τον m , δηλαδή το πλήθος τους είναι ίσο με $\varphi(m)$, όπου φ η συνάρτηση του Euler.

Παράδειγμα 5 .

Στην κυκλική ομάδα $Z_{18} = \{\bar{0}, \bar{1}, \dots, \bar{17}\} = \langle \bar{1} \rangle$, έχουμε

$$Z_{18} = \langle \bar{1} \rangle = \langle \bar{5} \rangle = \langle \bar{7} \rangle = \langle \bar{11} \rangle = \langle \bar{13} \rangle = \langle \bar{17} \rangle ,$$

αφού οι $1, 5, 7, 11, 13, 17$ είναι πρώτοι με τον 18 .

Η εύρεση των υποομάδων μιας ομάδας είναι μια εργασία αρκετά επίπονη. Στην περίπτωση όμως των κυκλικών ομάδων τα πράγματα απλουστεύονται. Έτσι, αν $G = \langle \alpha \rangle$ είναι μια άπειρη κυκλική ομάδα, όλες οι υποομάδες της είναι οι $\{1\}, \langle \alpha \rangle, \langle \alpha^2 \rangle, \dots$ (Πόρισμα 1).

Ας δούμε τι συμβαίνει στις πεπερασμένες κυκλικές ομάδες.

ΘΕΩΡΗΜΑ 4 .

Αν $G = \langle \alpha \rangle$ είναι μια κυκλική ομάδα τάξης m , τότε

i) Για κάθε θετικό ακέραιο n η G έχει μια υποομάδα τάξης n εάν και μόνο εάν $n \mid m$.

ii) Εάν $n \mid m$, τότε η G έχει μια μοναδική υποομάδα τάξης n .

Απόδειξη .

i) Αν $n \mid m$, τότε, αφού $\frac{m}{n} \mid m$, το $\alpha^{\frac{m}{n}}$ έχει τάξη $\frac{m}{m/n} = n$ (Προτ. 10)

δηλαδή η $\langle \alpha^{\frac{m}{n}} \rangle$ έχει τάξη n .

Αντίστροφα .

Ας είναι H μια υποομάδα της G με τάξη n . Επειδή $H = \langle \alpha^k \rangle$,

η H θα έχει τάξη $\frac{m}{(k, m)}$, οπότε



$$\frac{m}{(m,k)} = n \implies m = n(k,m) , \text{ δηλαδή } n|m .$$

ii) Έστω H_1, H_2 υποομάδες της G τάξης n με $n|m$.

$$\text{Αλλά } H_1 = \langle \alpha^{k_1} \rangle \text{ και } H_2 = \langle \alpha^{k_2} \rangle .$$

Παρατηρούμε ότι :

$$\text{Η τάξη της } H_1 \text{ θα είναι } \frac{m}{(k_1,m)} = n$$

και

$$\text{η τάξη της } H_2 \text{ θα είναι } \frac{m}{(k_2,m)} = n , \text{ οπότε } (k_1,m) = (k_2,m) . \text{ Από την}$$

$$\text{πρόταση 12 όμως έχουμε } \langle \alpha^{k_1} \rangle = \langle \alpha^{k_2} \rangle , \text{ δηλαδή } H_1 = H_2 . \blacksquare$$

Από τα i) και ii) του προηγούμενου θεωρήματος συμπεραίνουμε ότι μια κυκλική ομάδα τάξης m έχει ακριβώς $\tau(m)$ σε πλήθος υποομάδες , (όπου $\tau(m)$ είναι το πλήθος των θετικών διαιρετών του m) .

ΠΟΡΙΣΜΑ 4 .

Αν η ομάδα $G = \langle \alpha \rangle$ είναι κυκλική τάξης m και $d_1, \dots, d_{\tau(m)}$ είναι όλοι θετικοί διαιρέτες του m , τότε οι

$$\langle \alpha^{d_1} \rangle , \dots , \langle \alpha^{d_{\tau(m)}} \rangle$$

είναι όλες οι διακεκριμένες υποομάδες της G .

Απόδειξη .

Παρατηρούμε ότι , επειδή κάθε d_i διαιρεί τον m , έχουμε $(d_i, m) = d_i$. επομένως , αν $d_i \neq d_j$, τότε $(d_i, m) \neq (d_j, m)$ και επομένως $\langle \alpha^{d_i} \rangle \neq \langle \alpha^{d_j} \rangle$. Έτσι , οι $\tau(m)$ σε πλήθος υποομάδες

$$\langle \alpha^{d_1} \rangle , \dots , \langle \alpha^{d_{\tau(m)}} \rangle$$

είναι όλες διακεκριμένες . $\blacksquare$



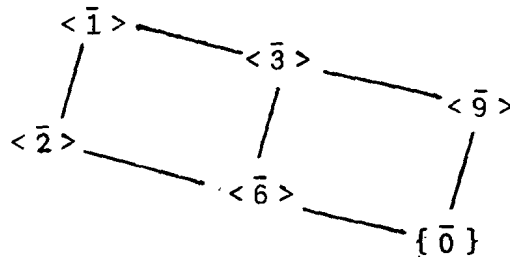
Παράδειγμα 6 .

Οι υποομάδες της $\mathbb{Z}_{18}$ είναι οι

$$\langle \bar{1} \rangle = \mathbb{Z}_{18} , \quad \langle \bar{2} \rangle = \{ \bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}, \bar{12}, \bar{14}, \bar{16} \} ,$$

$$\langle \bar{3} \rangle = \{ \bar{0}, \bar{3}, \bar{6}, \bar{9}, \bar{12}, \bar{15} \} , \quad \langle \bar{6} \rangle = \{ \bar{0}, \bar{6}, \bar{12} \} , \quad \langle \bar{9} \rangle = \{ \bar{0}, \bar{9} \}$$

και η $\langle \bar{18} \rangle = \{ \bar{0} \}$, αφού οι 1,2,3,6,9,18 είναι όλοι οι φυσικοί διαιρέτες του 18 . Το διάγραμμα δίκτυο της $\mathbb{Z}_{18}$ είναι



§6.1. Ομάδες μεταθέσεων.

Μια μετάθεση ενός μη κενού συνόλου X είναι μία 1-1 και επί απεικόνιση του X στον εαυτό του

$$\sigma : X \longrightarrow X$$

Συμβολίζουμε με $S(X)$ το σύνολο των μεταθέσεων του συνόλου X . Αφού η σύνθεση δύο 1-1 και επί απεικονίσεων είναι 1-1 και επί , το σύνολο $S(X)$ δομείται με πράξη τη σύνθεση απεικονίσεων σε ομάδα .

Το ουδέτερο στοιχείο της είναι η ταυτοτική μετάθεση I_X , ενώ το συμμετρικό του στοιχείο $\sigma \in S(X)$ είναι η 1-1 και επί σ^{-1} . Η ομάδα $(S(X), \circ)$ καλείται ομάδα μεταθέσεων επί του X .

Θα σημειώσουμε ότι το $S(X)$ είναι ένα υπομονοειδές του μονοειδούς $\text{Hom}(X, X)$ (Βλέπε, Κεφ. I) .

ΘΕΩΡΗΜΑ 5. (Gayley)

Κάθε ομάδα X είναι ισόμορφη με μια υποομάδα της ομάδας $S(X)$



των μεταθέσεων επί του X .

Απόδειξη

Για κάθε $x \in X$, η απεικόνιση

$$f_x : X \longrightarrow X, \quad f_x(z) = x \cdot z, \quad \forall z \in X$$

είναι 1-1 και επί. Πραγματικά, αν $f_x(z_1) = f_x(z_2)$, δηλαδή αν

$$xz_1 = xz_2, \quad \text{τότε } z_1 = z_2, \quad \text{αφού η } X \text{ είναι ομάδα.}$$

Επιπλέον, $\forall z \in X$ υπάρχει το στοιχείο $x^{-1}z \in X$ τέτοιο ώστε $f_x(x^{-1}z) = x(x^{-1}z) = z$.

Η απεικόνιση τώρα $f : X \longrightarrow S(X)$

$$x \longmapsto f_x$$

είναι μονομορφισμός ομάδων, δηλαδή

$$\alpha) f_{x_1 x_2} = f_{x_1} \circ f_{x_2} \quad \forall x_1, x_2 \in X$$

$$\beta) \text{ Αν } f_{x_1} = f_{x_2} \text{ τότε } x_1 = x_2.$$

Η απόδειξη του είναι η ίδια με εκείνη που κάναμε στο αντίστοιχο θεώρημα για μονοειδή. (Βλέπε Θεωρ. 2, Κεφ. I).

Επομένως, η ομάδα X εμφυτεύεται στην $S(X)$ και έτσι η $X \cong f(X)$. ■

Η μελέτη λοιπόν όλων των ομάδων ανάγεται στη μελέτη όλων των υποομάδων των ομάδων μεταθέσεων.

Τέλος, θα παρατηρήσουμε ότι, κατά προσέγγιση ισομορφισμού, η ομάδα $S(X)$ δεν εξαρτάται από το σύνολο X αλλά από τον πληθικό του αριθμό $|X|$.

Πραγματικά, αν X και Y είναι δύο σύνολα με $|X| = |Y|$, τότε υπάρχει μία 1-1 και επί $\varphi : X \longrightarrow Y$ και η απεικόνιση $h : S(X) \longrightarrow S(Y)$, $h(\sigma) = \varphi \circ \sigma \circ \varphi^{-1}$, $\forall \sigma \in S(X)$ είναι ένας ισομορφισμός ομάδων. (Άσκηση).



§6.2. Η συμμετρική ομάδα n -βαθμού.

Ενδιαφέρον παρουσιάζουν οι ομάδες μεταθέσεων $S(X)$, όπου X είναι ένα πεπερασμένο σύνολο, δηλαδή $|X| = n$, $n > 0$.

Απ' όλα τα ισοδύναμα σύνολα με πληθικό αριθμό n , εκλέγουμε το σύνολο

$$I_n = \{1, 2, \dots, n\},$$

και συμβολίζουμε S_n την ομάδα μεταθέσεων επί του I_n .

Η S_n καλείται **συμμετρική ομάδα n -βαθμού**.

Μια μετάθεση $\sigma \in S_n$, $\sigma = \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$ μπορεί να γραφεί

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma_1 & \sigma_2 & \dots & \sigma_n \end{pmatrix} \quad (*)$$

όπου $\sigma_i = \sigma(i)$, $i = 1, 2, \dots, n$.

Στη γραφή (*) τα $\sigma_1, \sigma_2, \dots, \sigma_n$ δεν είναι παρά τα $1, 2, \dots, n$ γραμμένα με διαφορετική ενδεχομένως τάξη.

Παρατηρούμε τώρα ότι, αν $i_1, i_2, \dots, i_n$ είναι μια τυχούσα διάταξη των $1, 2, \dots, n$, τότε

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma_1 & \sigma_2 & \dots & \sigma_n \end{pmatrix} = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ \sigma_{i_1} & \sigma_{i_2} & \dots & \sigma_{i_n} \end{pmatrix},$$

όπου $\sigma_{i_k} = \sigma(i_k)$, $k = 1, 2, \dots, n$.

Μ' άλλα λόγια, δεν έχει σημασία η διάταξη των αριθμών της πάνω γραμμής, αρκεί βέβαια κάτω από κάθε αριθμό να γράφουμε την εικόνα του μέσω της σ .

Η παρατήρηση αυτή μας διευκολύνει στον υπολογισμό του "γινομένου" $\sigma \circ \tau$ δύο μεταθέσεων $\sigma, \tau \in S_n$, που θα το συμβολίζουμε απλούστερα $\sigma \tau$. Έτσι,



$$\sigma \tau = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma_1 & \sigma_2 & \dots & \sigma_n \end{pmatrix} \begin{pmatrix} 1 & 2 & \dots & n \\ \tau_1 & \tau_2 & \dots & \tau_n \end{pmatrix} = \begin{pmatrix} \tau_1 & \tau_2 & \dots & \tau_n \\ \sigma_{\tau_1} & \sigma_{\tau_2} & \dots & \sigma_{\tau_n} \end{pmatrix} = \begin{pmatrix} 1 & 2 & \dots & n \\ \tau_1 & \tau_2 & \dots & \tau_n \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma_{\tau_1} & \sigma_{\tau_2} & \dots & \sigma_{\tau_n} \end{pmatrix} .$$

Η αντίστροφη της μετάθεσης σ είναι η

$$\sigma^{-1} = \begin{pmatrix} \sigma_1 & \sigma_2 & \dots & \sigma_n \\ 1 & 2 & \dots & n \end{pmatrix}$$

αφού $\sigma \sigma^{-1} = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix} = \sigma^{-1} \sigma .$

Στο εξής θα συμβολίζουμε (1) την ταυτοτική μετάθεση .

Παράδειγμα 1.

Θεωρούμε τις μεταθέσεις $\sigma, \tau \in S_4$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} .$$

Τότε ,

$$\sigma \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$

και

$$\sigma^{-1} = \begin{pmatrix} 2 & 4 & 1 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} .$$



Για να ορίσουμε τώρα μια μετάθεση $\sigma \in S_n$, μπορούμε με n τρόπους να εκλέξουμε το $\sigma(1)$, αφού αυτό θα είναι κάποιο από τα $1, 2, \dots, n$. Από τη στιγμή που ορίζεται το $\sigma(1)$, υπάρχουν μόνο $n-1$ τρόποι για να εκλέξουμε το $\sigma(2)$, αφού το $\sigma(2)$ το εκλέγουμε από το σύνολο $\{1, 2, \dots, n\} - \{\sigma(1)\}$. Έτσι, υπάρχουν $n(n-1)$ τρόποι για να εκλεγούν τα $\sigma(1), \sigma(2)$.

Συνεχίζοντας μ' αυτό τον τρόπο, βρίσκουμε ότι η σ μπορεί να οριστεί με $n(n-1) \dots 2 \cdot 1 = n!$ τρόπους. Έτσι, η S_n περιέχει $n!$ σε πλήθος μεταθέσεις, δηλαδή

$$|S_n| = n!$$

Παράδειγμα 2.

Η S_3 έχει $3! = 6$ μεταθέσεις τις επόμενες

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

και πίνακα πολ/σμού τον επόμενο

	e	ρ_1	ρ_2	μ_1	μ_2	μ_3
e	e	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	e	μ_3	μ_1	μ_2
ρ_2	ρ_2	e	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	e	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	e	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	e

Ο παραπάνω πίνακας δεν είναι συμμετρικός ως προς τη διαγώνιό του,



πράγμα που σημαίνει ότι η S_3 δεν είναι αβελιανή ομάδα .

Γενικότερα , η ομάδα S_n $n \geq 3$ δεν είναι αβελιανή .
 Η S_3 δεν είναι αβελιανή . Αν $n > 3$ για τις μεταθέσεις

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \dots & n \\ 1 & 3 & 2 & 4 & 5 & \dots & n \end{pmatrix} \text{ και } \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \dots & n \\ 3 & 2 & 1 & 4 & 5 & \dots & n \end{pmatrix}$$

έχουμε $\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \dots & n \\ 3 & 1 & 2 & 4 & 5 & \dots & n \end{pmatrix}$ και $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \dots & n \\ 2 & 3 & 1 & 4 & 5 & \dots & n \end{pmatrix}$

δηλαδή $\tau\sigma \neq \sigma\tau$.

Οι ομάδες S_1 και S_2 είναι φανερά αβελιανές .

ΟΡΙΣΜΟΣ . Ονομάζουμε πρόσημο μια μετάθεσης $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma_1 & \sigma_2 & \dots & \sigma_n \end{pmatrix}$,

και το συμβολίζουμε $\varepsilon(\sigma)$, τον αριθμό

$$\prod_{i < j} \frac{\sigma_i - \sigma_j}{i - j} ,$$

όπου το γινόμενο εκτείνεται στα $\frac{n(n-1)}{2}$ σε πλήθος ζεύγη

$$\begin{aligned} &(1,2), (1,3), \dots, (1,n) \\ &\quad (2,3), \dots, (2,n) \\ &\quad \dots\dots\dots \\ &\quad (n-1,n) \end{aligned}$$

ΠΡΟΤΑΣΗ 13 .

Το πρόσημο κάθε μετάθεσης $\sigma \in S_n$ είναι ίσο με $+1$ ή -1 ,
 δηλαδή $\varepsilon(\sigma) = \pm 1$.

Απόδειξη .

Για κάθε παράγοντα $i-j$ του παρανομαστή θα βρούμε ένα παράγοντα



του αριθμητή όσο με $i-j$ ή $-(i-j)$.

Πραγματικά, αφού η σ είναι 1-1 και επί, υπάρχουν μοναδικός φυσικός ℓ και m από τους $1, 2, \dots, n$, έτσι ώστε $\sigma_\ell = i$ και $\sigma_m = j$. Αν $\ell < m$, ο παράγων $\sigma_\ell - \sigma_m = i-j$ εμφανίζεται στον αριθμητή, ενώ, αν $\ell > m$, θα έχουμε στον αριθμητή τον παράγοντα $\sigma_m - \sigma_\ell = -(i-j)$. Έτσι

$$\frac{\sigma_\ell - \sigma_m}{i-j} = 1 \quad \text{ή} \quad \frac{\sigma_m - \sigma_\ell}{i-j} = -1.$$

Παρατηρούμε όμως ότι, διακεκριμένοι παράγοντες $i-j$ και $i'-j'$ του παρανομαστή, αντιστοιχούν, με τον παραπάνω τρόπο, σε διακεκριμένους παράγοντες $\pm(\sigma_\ell - \sigma_m)$, $\pm(\sigma_{\ell'} - \sigma_{m'})$ του αριθμητή, γιατί, αν $\ell = \ell'$ και $m = m'$, τότε $i = i'$ και $j = j'$ άτοπο. Έτσι $\epsilon(\sigma) = \pm 1$.

Παράδειγμα 3.

$$\text{Για τις μεταθέσεις της } S_3, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \text{ και } \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

έχουμε

$$\epsilon(\sigma) = \prod_{i < j} \frac{\sigma_i - \sigma_j}{i-j} = \frac{\sigma_1 - \sigma_2}{1-2} \cdot \frac{\sigma_1 - \sigma_3}{1-3} \cdot \frac{\sigma_2 - \sigma_3}{2-3} = \frac{2-3}{1-2} \cdot \frac{2-1}{1-3} \cdot \frac{3-1}{2-3} = 1$$

$$\epsilon(\tau) = \prod_{i < j} \frac{\tau_i - \tau_j}{i-j} = \frac{\tau_1 - \tau_2}{1-2} \cdot \frac{\tau_1 - \tau_3}{1-3} \cdot \frac{\tau_2 - \tau_3}{2-3} = \frac{3-2}{1-2} \cdot \frac{3-1}{1-3} \cdot \frac{2-1}{2-3} = -1.$$

Μια μετάθεση $\sigma \in S_n$ θα λέγεται άρτια αν $\epsilon(\sigma) = 1$ και περιττή αν $\epsilon(\sigma) = -1$.

Έτσι στο προηγούμενο παράδειγμα, η σ είναι άρτια και η τ περιττή.



Παράδειγμα 4 .

Στην S_n , η μετάθεση $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 1 & 3 & 4 & \dots & n \end{pmatrix}$ είναι περιττή.

Πραγματικά ,

$$\varepsilon(\sigma) = \prod_{i < j} \frac{\sigma_i - \sigma_j}{i - j} = \frac{2-1}{1-2} \cdot \frac{2-3}{1-3} \cdot \frac{2-4}{1-4} \cdots \frac{2-n}{1-n} \cdot \frac{1-3}{2-3} \cdot \frac{1-4}{2-4} \cdots \frac{1-n}{2-n}$$

$\vdots$

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

Ας δούμε όμως τώρα τι ισχύει για το πρόσημο του γινομένου $\sigma\tau$ δύο μεταθέσεων $\sigma, \tau \in S_n$.

$$\begin{aligned} \varepsilon(\sigma\tau) &= \prod_{i < j} \frac{(\sigma\tau)_i - (\sigma\tau)_j}{i - j} = \prod_{i < j} \frac{\sigma_{\tau_i} - \sigma_{\tau_j}}{i - j} = \\ &= \prod_{i < j} \frac{\sigma_{\tau_i} - \sigma_{\tau_j}}{i - j} \cdot \frac{\tau_i - \tau_j}{\tau_i - \tau_j} = \prod_{i < j} \frac{\sigma_{\tau_i} - \sigma_{\tau_j}}{\tau_i - \tau_j} \cdot \prod_{i < j} \frac{\tau_i - \tau_j}{i - j} = \\ &= \prod_{i < j} \frac{\sigma_{\tau_i} - \sigma_{\tau_j}}{\tau_i - \tau_j} \cdot \varepsilon(\tau) \end{aligned} \quad (1)$$

Αλλά

$$\prod_{i < j} \frac{\sigma_{\tau_i} - \sigma_{\tau_j}}{\tau_i - \tau_j} = \prod_{k < m} \frac{\sigma_k - \sigma_m}{k - m} \quad (2)$$

Πραγματικά , ας πάρουμε ένα παράγοντα $\frac{\sigma_k - \sigma_m}{k - m}$ $k < m$ του 2^{ου} μέλους της (2) .

Υπάρχουν p, q έτσι ώστε $\tau_p = k$, $\tau_q = m$.



Αν $p < q$, τότε ο παραγοντας $\frac{\sigma_{\tau_p} - \sigma_{\tau_q}}{\tau_p - \tau_q}$ του $1^{\text{ου}}$ μέλους της (2)

αντιστοιχεί στον $\frac{\sigma_k - \sigma_m}{k-m}$.

Αν $p > q$, τότε $\frac{\sigma_{\tau_q} - \sigma_{\tau_p}}{\tau_q - \tau_p} = \frac{\sigma_{\tau_p} - \sigma_{\tau_q}}{\tau_p - \tau_q} = \frac{\sigma_k - \sigma_m}{k-m}$

Αντίστροφα, έστω $\frac{\sigma_{\tau_i} - \sigma_{\tau_j}}{\tau_i - \tau_j}$, $i < j$ ένας παράγοντας, του $1^{\text{ου}}$ μέλους της (2) τότε $\tau_i = k$, $\tau_j = m$.

Αν $k < m$, έχουμε $\frac{\sigma_{\tau_i} - \sigma_{\tau_j}}{\tau_i - \tau_j} = \frac{\sigma_k - \sigma_m}{k-m} \in 2^{\text{o}}$ μέλος

αν $k > m$, τότε $\frac{\sigma_{\tau_i} - \sigma_{\tau_j}}{\tau_i - \tau_j} = \frac{\sigma_{\tau_j} - \sigma_{\tau_i}}{\tau_j - \tau_i} = \frac{\sigma_m - \sigma_k}{m-k} \in 2^{\text{o}}$ μέλος.

Οι σχέσεις (1) και (2) μας δίνουν τελικά ότι

$$\varepsilon(\sigma\tau) = \varepsilon(\sigma) \cdot \varepsilon(\tau)$$

Απο τα παραπάνω συμπεραίνουμε ότι το πρόσημο μετάθεσης είναι ένας ομομορφισμός της S_n πολ/κή ομάδα $\{+1, -1\}$

$$\varepsilon : S_n \longrightarrow \{+1, -1\}$$

Ο πυρήνας $\text{Ker}(\varepsilon)$ του ε είναι το σύνολο όλων των άρτιων μεταθέσεων. Οι άρτιες μεταθέσεις της S_n αποτελούν λοιπόν μια υποομάδα της S_n , που την ονομάζουμε εναλλάσσουσα ομάδα βαθμού n και τη συμβολίζουμε A_n .

Εύκολα διαπιστώνεται ότι :



α) Το γινόμενο δύο άρτιων ή περιττών μεταθέσεων είναι άρτια μετάθεση .

β) Το γινόμενο μιας άρτιας με μια περιττή μετάθεση είναι περιττή μετάθεση .

γ) Η αντίστροφη μιας άρτιας (αντισ. περιττής) μετάθεσης είναι άρτια (αντισ. περιττή) μετάθεση .

§ 6.3. Κύκλοι - Μεταβάσεις .

ΟΡΙΣΜΟΣ . Έστω $x_1, x_2, \dots, x_k$ ($k \leq n$) k διακεκριμένα στοιχεία του συνόλου $I_n = \{1, 2, \dots, n\}$. Συμβολίζουμε $(x_1 x_2 \dots x_k)$ τη μετάθεση του S_n που απεικονίζει

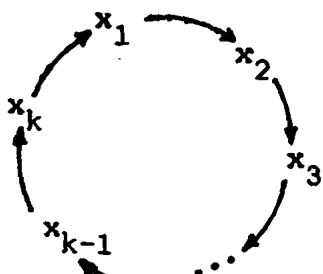
$$x_1 \mapsto x_2, x_2 \mapsto x_3, \dots, x_{k-1} \mapsto x_k \text{ και } x_k \mapsto x_1$$

και αφήνει αμετάβλητα τα υπόλοιπα $n-k$ στοιχεία του συνόλου I_n .
δηλαδή

$$(x_1 x_2 \dots x_k) = \begin{pmatrix} x_1 & x_2 & \dots & x_n & x_{k+1} & \dots & x_n \\ x_2 & x_3 & \dots & x_1 & x_{k+1} & \dots & x_n \end{pmatrix} .$$

Η $(x_1 x_2 \dots x_k)$ καλείται ένας κύκλος μήκους k ή ένας k -κύκλος .

Ένας κύκλος $(x_1 x_2 \dots x_k)$ λοιπόν μας μεταθέτει κυκλικά τα στοι-



χεία $x_1, \dots, x_k$ του I_n και αφήνει αμετάβλητα τα υπόλοιπα . Μπορεί επομένως να περιγραφεί με περισσότερους από ένα τρόπους , έτσι

$$(x_1 x_2 \dots x_k) = (x_2 x_3 \dots x_k x_1) = \dots = (x_k x_1 \dots x_{k-1}) .$$

Για παράδειγμα , στην S_4 η μετάθεση

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = (1 \ 4 \ 3 \ 2) = (4 \ 3 \ 2 \ 1) = (3 \ 2 \ 1 \ 4) = (2 \ 1 \ 4 \ 3)$$



είναι ένας κύκλος μήκους 4 .

Παρατηρήσεις .

α) Επειδή οι κύκλοι είναι μεταθέσεις , μπορούν να πολ/σθούν όπως ακριβώς οι μεταθέσεις . Το γινόμενο όμως δύο κύκλων δεν είναι απαραίτητα ένας κύκλος . Πραγματικά , στην S_6 , για τους κύκλους (1 4 5 6) και (2 1 5) , έχουμε

$$(1\ 4\ 5\ 6)(2\ 1\ 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 5 & 2 & 1 \end{pmatrix} ,$$

που δεν είναι ένας κύκλος .

Εκείνο όμως που ισχύει και θα το δούμε παρακάτω , είναι ότι κάθε μετάθεση της S_n μπορεί να γραφεί σαν γινόμενο κύκλων .

β) Κάθε κύκλος μήκους 1 στην S_n είναι η ταυτοτική μετάθεση $(1) = (2) = \dots = (n)$.

γ) Κάθε k -κύκλος $\sigma = (\sigma_1 \sigma_2 \dots \sigma_k)$ στην ομάδα S_n ($k \leq n$) έχει τάξη k , αφού

$$\sigma^k = \sigma \sigma \dots \sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix} = (1) ,$$

ενώ για κάθε $x \in \{\sigma_1, \sigma_2, \dots, \sigma_k\}$ έχουμε

$$\sigma = (x \ \sigma_x \ \sigma_x^2 \ \dots \ \sigma_x^{k-1}) .$$

Τέλος , ο αντίστροφος του κύκλου $\sigma = (\sigma_1 \sigma_2 \dots \sigma_k)$ είναι ο κύκλος $\sigma^{-1} = (\sigma_k \sigma_{k-1} \dots \sigma_1)$.

ΟΡΙΣΜΟΣ . Δύο μεταθέσεις $\sigma, \tau \in S_n$ θα λέγονται ξένες μεταξύ τους αν

α) Για κάθε $k \in \{1, \dots, n\}$ με $\sigma(k) \neq k$, συνεπάγεται $\tau(k) = k$.



Είναι εύκολα να δούμε ότι η συνθήκη (α) είναι ισοδύναμη με την
β) Για κάθε $k \in \{1, \dots, n\}$ με $\tau(k) \neq k$ συνεπάγεται $\sigma(k) = k$.

Από τον ορισμό είναι φανερό ότι, κάθε μη-ταυτοτική μετάθεση
είναι ξένη με την ταυτοτική μετάθεση. Έτσι, κάθε κύκλος μήκους 1
(δηλαδή η ταυτοτική μετάθεση) είναι ξένος με κάθε κύκλο μήκους
 $k \geq 2$ στην S_n , ενώ δύο κύκλοι

$$\sigma = (\sigma_1 \sigma_2 \dots \sigma_k) \quad \text{και} \quad \tau = (\tau_1 \tau_2 \dots \tau_v)$$

στην S_n με $k \geq 2$ και $v \geq 2$ είναι ξένοι μεταξύ τους, όταν

$$\{\sigma_1, \dots, \sigma_k\} \cap \{\tau_1, \dots, \tau_v\} = \emptyset,$$

δηλαδή όταν οι κύκλοι μεταθέτουν διαφορετικά στοιχεία από το σύνολο
 $\{1, 2, \dots, n\}$.

Για παράδειγμα, οι κύκλοι $(1 \ 2 \ 3)$ και $(4 \ 5 \ 6)$ στην S_6 εί-
ναι ξένοι μεταξύ τους.

Είναι φανερό τώρα ότι κύκλοι της S_n , $\sigma = (\sigma_1, \dots, \sigma_k)$ και
 $\tau = (\tau_1, \dots, \tau_v)$ ξένοι μεταξύ τους, αντιμετατίθενται, δηλαδή

$$(\tau_1, \dots, \tau_v) \cdot (\sigma_1, \dots, \sigma_k) = (\sigma_1, \dots, \sigma_k) (\tau_1, \dots, \tau_v).$$

Αυτό ισχύει γενικότερα για μεταθέσεις $\sigma, \tau \in S_n$ ξένες μεταξύ
τους, δηλαδή τότε έχουμε $\sigma \tau = \tau \sigma$. (Άσκηση).

ΘΕΩΡΗΜΑ 6.

Κάθε μη ταυτοτική μετάθεση της S_n αναλύεται κατά μοναδικό τρό-
πο σε γινόμενο κύκλων ξένων μεταξύ τους ανά δύο, μήκους ≥ 2 . (Η τά-
ξη των παραγόντων στην ανάλυση αυτή δεν λαμβάνεται υπόψη, αφού δύο
κύκλοι ξένοι μεταξύ τους αντιμετατίθενται).

Απόδειξη.

Έστω $\sigma \in S_n$, με $\sigma(1) \neq 1$ (αν $\sigma(1) = 1$, τότε παύνουμε τον



πρώτο ακέραιο i , για τον οποίο ισχύει $\sigma(i) \neq i$.

Εφαρμόζοντας διαδοχικά την σ στο 1 , παίρνουμε τα στοιχεία

$$1, \sigma(1), \sigma^2(1), \sigma^3(1), \dots$$

Τα στοιχεία αυτά δεν είναι όλα διακεκριμένα μεταξύ τους , αφού αυτά είναι στοιχεία του συνόλου $\{1, 2, \dots, n\}$.

Έστω k ο ελάχιστος θετικός ακέραιος τέτοιος ώστε τα στοιχεία $1, \sigma(1), \sigma^2(1), \dots, \sigma^{k-1}(1)$ να είναι διακεκριμένα , ενώ :

$$\sigma^k(1) = \sigma^j(1) , \text{ για κάποιο } j \text{ με } 0 \leq j < k .$$

Τότε

$$\sigma^{k-j}(1) = 1 , \quad 0 < k-j \leq k$$

που είναι αντίθετο με την εκλογή του k , εκτός αν $k-j = k$, δηλαδή $j = 0$. Έτσι $\sigma^k(1) = 1$.

Η σ περιέχει λοιπόν τον κύκλο

$$\sigma_1 = (1 \ \sigma(1) \ \sigma^2(1) \ \dots \ \sigma^{k-1}(1))$$

Αν ο αριθμός 2 δεν εμφανίζεται στον κύκλο σ_1 (αν εμφανίζεται χρησιμοποιούμε τον μικρότερο αριθμό από το σύνολο $\{1, 2, \dots, n\}$ που δεν ανήκει στον κύκλο σ_1) , τότε , με την ίδια διαδικασία , παίρνουμε ένα δεύτερο κύκλο

$$\sigma_2 = (2 \ \sigma(2) \ \sigma^2(2) \ \dots \ \sigma^{\lambda-1}(2))$$

όπου λ ο ελάχιστος θετικός ακέραιος τέτοιος ώστε $\sigma^\lambda(2) = 2$.

Η σ λοιπόν περιέχει και τον κύκλο σ_2 .

Οι κύκλοι σ_1 και σ_2 είναι ξένοι μεταξύ τους , δηλαδή

$$\{1, \sigma(1), \dots, \sigma^{k-1}(1)\} \cap \{2, \sigma(2), \dots, \sigma^{\lambda-1}(2)\} = \emptyset$$

Πραγματικά , ας υποθέσουμε ότι η τομή τους είναι $\neq \emptyset$, τότε θα υπάρχουν φυσικοί μ, ν τέτοιοι ώστε $\sigma^\mu(1) = \sigma^\nu(2)$.

Έτσι $\sigma^{\mu-\nu}(1) = 2$.

Από τον Αλγόριθμο διαίρεσης παίρνουμε



$$\mu - \nu = kq + r, \quad 0 \leq r < k,$$

οπότε

$$\sigma^{\mu-\nu}(1) = \sigma^{kq+r}(1) = \sigma^r(\sigma^{kq}(1)) = \sigma^r(1).$$

Επομένως

$$\sigma^r(1) = 2, \quad \text{με} \quad 0 \leq r < k,$$

δηλαδή το $2 \in \{1, \sigma(1), \dots, \sigma^{k-1}(1)\}$ άτοκο, όπως το επιθυμούσαμε.

Εξακολουθούμε την ίδια τακτική, μέχρι να εξαντλήσουμε τα στοιχεία του πεδίου ορισμού της σ και έστω σ_m ο τελευταίος κύκλος που περιέχει η σ . Οι κύκλοι $\sigma_1, \dots, \sigma_m$ με μήκη ≥ 2 είναι ξένοι μεταξύ τους ανά δύο και το γινόμενο $\sigma_1 \sigma_2 \dots \sigma_m$ ενεργεί επί των στοιχείων $1, 2, \dots, n$ όπως η σ , οπότε

$$\sigma = \sigma_1 \sigma_2 \dots \sigma_m \quad (**)$$

Αν κάποιο στοιχείο t από τα $1, 2, \dots, n$ μένει αμετάβλητο από την σ , δηλαδή $\sigma(t) = t$, τότε ο κύκλος που παράγει το t έχει μήκος 1, δηλαδή είναι η ταυτοτική μετάθεση και γι' αυτό την παραλείπουμε από την παραπάνω ανάλυση (**).

Φανερό δεν ισχύει $\sigma(t) = t$, $\forall t \in \{1, 2, \dots, n\}$, αφού η σ είναι μη-ταυτοτική μετάθεση.

Η μοναδικότητα της ανάλυσης (**) προκύπτει αυτόματα από την προηγούμενη κατασκευή. ■

Παράδειγμα 5.

$$\text{Για τη μετάθεση} \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 6 & 4 & 7 & 5 & 2 & 1 & 9 & 10 & 8 \end{pmatrix}$$

της S_{10} εργαζόμαστε ως εξής, για να πάρουμε την ανάλυσή της σε γινόμενο κύκλων, ξένων μεταξύ τους ανά δύο, μήκους ≥ 2 .

Αρχίζουμε από το φυσικό 1 και βρίσκουμε



$$\sigma(1) = 3, \quad \sigma(3) = 4, \quad \sigma(4) = 7, \quad \sigma(7) = 1.$$

Ένας κύκλος της ανάλυσης είναι ο $(1 \ 3 \ 4 \ 7)$.

Στη συνέχεια, παίρνουμε το μικρότερο φυσικό του συνόλου $\{1, 2, \dots, 10\} - \{1, 3, 4, 7\}$, δηλαδή τον 2, και βρίσκουμε

$$\sigma(2) = 6, \quad \sigma(6) = 2$$

ο κύκλος λοιπόν $(2 \ 6)$ περιέχεται στην ανάλυση. Όμοια, ο μικρότερος φυσικός του συνόλου

$$\{1, 2, \dots, 10\} - \{1, 3, 4, 7, 2, 6\}, \text{ δηλαδή ο } 5, \text{ μας δίνει}$$

$$\sigma(5) = 5,$$

οπότε ο κύκλος (5) , δηλαδή η ταυτοτική μετάθεση παραλείπεται από την ανάλυση.

Τέλος, ο μικρότερος φυσικός του συνόλου

$$\{1, 2, \dots, 10\} - \{1, 3, 4, 7, 2, 6, 5\}, \text{ δηλαδή ο } 8, \text{ μας δίνει}$$

$$\sigma(8) = 9, \quad \sigma(9) = 10, \quad \sigma(10) = 8$$

οπότε ο κύκλος $(8, 9, 10)$ περιέχεται στην ανάλυση. Έτσι,

$$\sigma = (1 \ 3 \ 4 \ 7)(2 \ 6)(8 \ 9 \ 10).$$

ΟΡΙΣΜΟΣ. Ονομάζουμε *μετάβαση* στην S_n , κάθε κύκλο $(i \ j)$ μήκους 2, δηλαδή κάθε μετάθεση που ανταλλάσσει δύο στοιχεία και αφήνει σταθερά τα υπόλοιπα:

$$(i \ j) = \begin{pmatrix} 1 & 2 \dots i \dots j \dots n \\ 1 & 2 \dots j \dots i \dots n \end{pmatrix}$$

Συχνά χρησιμοποιούμε τον συμβολισμό $\tau_{ij} = (i \ j)$.

Είναι φανερό ότι $\tau_{ij}^2 = \tau_{ij} \cdot \tau_{ij} = (1)$, που σημαίνει ότι, κάθε μετάβαση συμπίπτει με την αντίστροφή της, δηλαδή $\tau_{ij}^{-1} = \tau_{ij}$. Αν



τώρα $\alpha \in \mathbb{Z}$, έχουμε

$$\tau_{ij}^\alpha = \begin{cases} (1), & \text{αν } \alpha = 2k, \quad k \in \mathbb{Z} \\ \tau_{ij}, & \text{αν } \alpha = 2k+1, \quad k \in \mathbb{Z} \end{cases} \quad (\acute{\alpha}\sigma\kappa\eta\sigma\eta)$$

θα παρατηρήσουμε τώρα ότι το πλήθος των μεταβάσεων στην S_n είναι $\frac{n(n-1)}{2}$.

Πραγματικά, αφού $(ij) = (ji)$, για να πάρουμε όλες τις μεταβάσεις της S_n , μεταθέτουμε καθένα από τα στοιχεία $1, 2, \dots, n$ με τα επόμενά του. Συνεπώς, το πλήθος τους είναι

$$(n-1) + (n-2) + \dots + 2 + 1 = \frac{n(n-1)}{2}.$$

ΠΡΟΤΑΣΗ 14.

Κάθε μετάβαση είναι περιττή μετάθεση.

Απόδειξη.

Ας είναι τ_{ij} μια μετάβαση. Θα δείξουμε ότι, $\epsilon(\tau_{ij}) = -1$. Θεωρούμε την μετάβαση $\sigma = (12)$ και την μετάθεση

$$\rho = \begin{pmatrix} 1 & 2 \dots i \dots j \dots n \\ i & j \dots 1 \dots 2 \dots n \end{pmatrix},$$

τότε

$$\tau_{ij} = \rho^{-1} \sigma \rho.$$

Πραγματικά, για κάθε $k \in \{1, 2, \dots, n\}$, με $k \neq i, j$, έχουμε $\rho(k) \neq 1, 2$ και συνεπώς $\sigma(\rho(k)) = \rho(k)$, έτσι

$$(\rho^{-1} \sigma \rho)(k) = \rho^{-1}(\sigma(\rho(k))) = \rho^{-1}(\rho(k)) = k = \tau_{ij}(k).$$

Για $k = i, j$ παίρνουμε



$$(\rho^{-1} \sigma \rho)(i) = \rho^{-1}(\sigma(\rho(i))) = \rho^{-1}(\sigma(1)) = \rho^{-1}(2) = j = \tau_{ij}(i) ,$$

$$(\rho^{-1} \sigma \rho)(j) = \rho^{-1}(\sigma(\rho(j))) = \rho^{-1}(\sigma(2)) = \rho^{-1}(1) = i = \tau_{ij}(j) .$$

θα έχουμε λοιπόν ,

$$\varepsilon(\tau_{ij}) = \varepsilon(\rho^{-1} \sigma \rho) = \varepsilon(\rho^{-1}) \varepsilon(\sigma) \varepsilon(\rho) = \varepsilon(\sigma) = -1 ,$$

αφού η $\sigma = (12)$ είναι περιττή μετάθεση (βλέπε παράδειγμα 4) . ■

ΠΡΟΤΑΣΗ 15.

Κάθε μετάθεση στην S_n ($n \geq 2$) μπορεί να αναλυθεί σε γινόμενο μεταβάσεων (όχι αναγκαία ξένων μεταξύ τους ανά δύο) .

Απόδειξη.

Η ταυτοτική μετάθεση (1) γράφεται $(1) = (12)(12)$. Ας είναι τώρα σ μια μετάθεση στην S_n διαφορετική από την ταυτότητα . Σύμφωνα με το θεώρημα 6 , η σ αναλύεται σε γινόμενο κύκλων , ξένων μεταξύ τους ανά δύο , μήκους ≥ 2 . Αρκεί λοιπόν να δείξουμε ότι κάθε κύκλος μπορεί να γράφει σαν γινόμενο μεταβάσεων . Πράγματι , ένας κύκλος μήκους $k > 1$ γράφεται

$$(\sigma_1 \sigma_2 \dots \sigma_k) = (\sigma_1 \sigma_k)(\sigma_1 \sigma_{k-1}) \dots (\sigma_1 \sigma_3)(\sigma_1 \sigma_2) . \blacksquare$$

Για παράδειγμα , η μετάθεση $\sigma \in S_{10}$ του παραδείγματος 5 αναλύεται

$$\sigma = (1 \ 3 \ 4 \ 7)(2 \ 6)(8 \ 9 \ 10) = (17)(14)(13)(26)(810)(89) .$$

Η ανάλυση μιας μετάθεσης σε γινόμενο μεταβάσεων δεν είναι μοναδική , ούτε ως προς την μορφή των μεταβάσεων , ούτε ως προς το πλήθος τους π.χ.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1 \ 2 \ 3) = (13)(12) = (12)(23) =$$



$$= (1\ 3)(2\ 3)(1\ 2)(1\ 3) = (1\ 2)(2\ 3)(3\ 2)(2\ 3) .$$

Ισχύει όμως η επόμενη πρόταση .

ΠΡΟΤΑΣΗ 16 .

Αν μια μετάθεση σ της S_n γράφεται σαν γινόμενο άρτιου (αντ. περιττού) πλήθους μεταβάσεων , τότε , κάθε άλλη ανάλυσή της σε γινόμενο μεταβάσεων , περιέχει άρτιο (αντ. περιττό) πλήθος παραγόντων .

Απόδειξη.

Ας είναι

$$\sigma = \tau_1 \dots \tau_k , \quad \sigma = \pi_1 \dots \pi_\lambda$$

δύο αναλύσεις της σ σε γινόμενο μεταβάσεων , τότε

$$\varepsilon(\sigma) = \varepsilon(\tau_1 \dots \tau_k) = \varepsilon(\tau_1) \dots \varepsilon(\tau_k) = (-1) \dots (-1) = (-1)^k$$

και όμοια $\varepsilon(\sigma) = (-1)^\lambda$.

Για να συμβαίνει λοιπόν $(-1)^k = (-1)^\lambda$, πρέπει οι k και λ να είναι ταυτόχρονα άρτιοι ή περιττοί . ■

ΠΟΡΙΣΜΑ 1.

Μια μετάθεση $\sigma \in S_n$ είναι άρτια (αντ. περιττή) , εάν και μόνον εάν αναλύεται σε γινόμενο άρτιου (αντ. περιττού) πλήθους μεταβάσεων . ■

Για παράδειγμα , η μετάθεση $\sigma \in S_{10}$ (βλέπε παράδειγμα 5)

$$\sigma = (1\ 7)(1\ 4)(1\ 3)(2\ 6)(8\ 1\ 0)(8\ 9)$$

γράφεται σε γινόμενο έξι μεταβάσεων , είναι επομένως άρτια μετάθεση .

Ας δούμε όμως τι συμβαίνει με το πρόσημο των κύκλων . Αν $(\sigma_1\ \sigma_2 \dots \sigma_k)$ είναι ένας k -κύκλος ($k \geq 2$) , αυτός γράφεται σε γινόμενο $k-1$ σε πλήθος μεταβάσεων ως εξής :

$$(\sigma_1\ \sigma_2 \dots \sigma_k) = (\sigma_1\ \sigma_k)(\sigma_1\ \sigma_{k-1}) \dots (\sigma_1\ \sigma_2)$$



επομένως $\varepsilon((\sigma_1 \sigma_2 \dots \sigma_k)) = (-1)^{k-1}$.

Έτσι

ΠΡΟΤΑΣΗ 17 .

Ένας κύκλος μήκους k στην S_n είναι άρτιος (αντ. περιττός), εάν και μόνο εάν ο αριθμός $k-1$ είναι άρτιος (αντ. περιττός) . ■

Για παράδειγμα, κάθε κύκλος μήκους 3 είναι άρτια μετάθεση .

§6.4. Συστήματα μεταθέσεων που παράγουν την S_n .

Ας είναι M το σύνολο όλων των μεταβάσεων της S_n . Είναι φανερό ότι $\langle M \rangle \subseteq S_n$.

Από την άλλη μεριά, η πρόταση 15 μας δίνει $S_n \subseteq \langle M \rangle$, οπότε

$$\langle M \rangle = S_n$$

δηλαδή το σύστημα των $\frac{n(n-1)}{2}$ μεταβάσεων της S_n παράγει την S_n .

Το σύστημα όμως αυτό για $n > 2$ δεν είναι ανάγωγο αφού όπως θα δείξουμε παρακάτω υπάρχουν γνήσια υποσυστήματα του που παράγουν επίσης την S_n .

ΠΡΟΤΑΣΗ 18 .

Τα επόμενα συστήματα από $n-1$ μεταβάσεις της S_n

$$\alpha) (12), (13), (14), \dots, (1n)$$

$$\beta) (12), (23), (34), \dots, (n-1 n)$$

είναι ανάγωγα συστήματα που παράγουν την S_n .

Απόδειξη . Για το σύστημα (α) .

Αφού η S_n παράγεται από τις $\frac{n(n-1)}{2}$ μεταβάσεις, αρκεί να δείξουμε ότι κάθε μετάβαση (ij) στην S_n μπορεί να γραφεί σαν γινόμενο μεταβάσεων από το σύστημα (α) .



Πραγματικά $(ij) = (1i)(1j)(1i)$.

Το ότι το σύστημα (α) είναι ανάγωγο , προκύπτει από το εξής γεγονός : αν από το σύστημα (α) βγάλουμε π.χ. τη μετάβαση (12) , τότε οι υπόλοιπες θα παράγουν μια γνήσια υποομάδα H της S_n , αφού κάθε μετάθεση $\sigma \in H$ θα μεταθέτει μόνο τα $1, 3, \dots, n$ και όχι το 2 .

Για το σύστημα (β) .

Αφού το σύστημα (α) παράγει την S_n , αρκεί να δείξουμε ότι κάθε μετάβαση $(1j)$, από το σύστημα (α) , γράφεται σαν γινόμενο μεταβάσεων από το σύστημα (β) .

Παρατηρούμε ότι , για $j > 2$, έχουμε

$$\begin{aligned} (1j) &= (1j-1)(j-1j)(1j-1) = \\ &= (1j-2)(j-2j-1)(1j-2)(j-1j)(1j-2)(j-2j-1)(1j-2) = \\ &= (1j-2)(j-2j-1)(j-1j)(1j-2)^2(j-2j-1)(1j-2) = \\ &= (1j-2)(j-2j-1)(j-1j)(j-2j-1)(1j-2) = \\ &\dots\dots\dots \\ &= (12)(23)(34) \dots (j-2j-1)(j-1j)(j-2j-1) \dots (34)(23)(12) \end{aligned}$$

Το ότι το σύστημα (β) είναι ανάγωγο προκύπτει με το ίδιο τρόπο όπως και για το (α) .

ΠΟΡΙΣΜΑ 2 .

Οι μεταθέσεις της S_n ($n \geq 3$)

$$\sigma = (12) \quad \text{και} \quad \tau = (123 \dots n)$$

είναι ένα ανάγωγο σύστημα που παράγει την S_n .

Απόδειξη .

Είναι φανερό ότι $H = \langle \sigma, \tau \rangle \leq S_n$. Αρκεί να δείξουμε ότι $S_n \leq \langle \sigma, \tau \rangle$. Αλλά



$$S_n = \langle \{(1\ 2), (2\ 3), \dots, (n-1, n)\} \rangle ,$$

επομένως αρκεί να δείξουμε ότι οι μεταβάσεις

$$(2, 3), \dots, (n-1, n) \text{ ανήκουν στην } H$$

Πραγματικά ,

$$\tau \sigma \tau^{-1} = (2\ 3) \in H$$

$$\tau^2 \sigma \tau^{-2} = \tau(2\ 3) \tau^{-1} = (3\ 4) \in H$$

.....

$$\tau^{n-2} \sigma \tau^{-(n-2)} = (n-1, n) \in H .$$

Το ότι το σύστημα αυτών των δύο μεταθέσεων είναι ανάγωγο , είναι φανερό . ■

§6.5. Η εναλλάσσουσα ομάδα βαθμού n , A_n

Η ομάδα A_n περιέχει , όπως είδαμε , όλες τις άρτιες μεταθέσεις, ενώ κάθε στοιχείο της μπορεί να γραφεί σαν γινόμενο άρτιου πλήθους μεταβάσεων . Επίσης , για $n \geq 3$, η A_n περιέχει όλους τους κύκλους μήκους 3 .

Η ομάδα A_n ($n \geq 2$) περιέχει $\frac{n!}{2}$ στοιχεία δηλαδή

$$|A_n| = \frac{n!}{2} .$$

Πραγματικά , αν B_n είναι το σύνολο των περιττών μεταθέσεων , τότε

$$S_n = A_n \cup B_n \text{ και } A_n \cap B_n = \emptyset ,$$

οπότε

$$|S_n| = |A_n| + |B_n| .$$

θα δείξουμε ότι $|A_n| = |B_n|$.

Αν τ είναι τυχούσα μετάβαση της S_n , ορίζουμε την απεικόνιση



$$f_\tau : A_n \longrightarrow B_n, \quad f_\tau(\sigma) = \tau\sigma, \quad \forall \sigma \in A_n$$

$$(\varepsilon(\tau\sigma) = \varepsilon(\tau)\varepsilon(\sigma) = (-1)(1) = -1, \quad \text{δηλαδή } \tau\sigma \in B_n).$$

Η f_τ είναι αμφύεση (Άσκηση).

$$\text{Έτσι } n! = 2|A_n|, \text{ επομένως } |A_n| = \frac{n!}{2}.$$

ΠΡΟΤΑΣΗ 19.

α) Για $n \geq 3$, η ομάδα A_n παράγεται απ' όλους τους κύκλους μήκους 3.

β) Έστω r, s διακεκριμένα στοιχεία του συνόλου $\{1, 2, \dots, n\}$, $n \geq 3$.

Η A_n παράγεται από τους κύκλους

$$(r s i), \quad 1 \leq i \leq n, \quad i \neq r, s.$$

Απόδειξη.

α) Έστω H η υποομάδα της A_n , που παράγουν οι κύκλοι μήκους 3. Αρκεί να δείξουμε ότι $A_n \leq H$.

Αφού όμως κάθε στοιχείο της A_n μπορεί να γραφεί σαν γινόμενο άρτιου πλήθους μεταβάσεων, αρκεί να δείξουμε ότι το γινόμενο δύο μεταβάσεων είναι γινόμενο κύκλων μήκους 3.

Αν $(i j)$ και $(k l)$ είναι μεταβάσεις ξένες μεταξύ τους, τότε

$$(i j)(k l) = (i k j)(i k l),$$

ενώ, στην περίπτωση που οι $(i j)$, $(k l)$ έχουν κοινό στοιχείο έστω $i = k$, έχουμε

$$(i j)(i l) = (i l j).$$

β) Αν H είναι η υποομάδα της A_n που παράγουν οι 3-κύκλοι $(r s i)$, $1 \leq i \leq n$, $i \neq r, s$, για να έχουμε $H = A_n$, αρκεί να δείξουμε ότι $A_n \leq H$ και, αν λάβουμε υπόψη μας το (α), αρκεί να δείξουμε ότι κάθε 3-κύκλος $(i j k)$ γράφεται σαν γινόμενο κύκλων της



μορφής $(r \ s \ i) \quad 1 \leq i \leq n$. Παρατηρούμε ότι

$$(i \ j \ k) = (r \ s \ i)^2 (r \ s \ k) (r \ s \ j)^2 (r \ s \ i) \quad ,$$

πράγμα που επιθυμούσαμε . ■

Το (β) μας λέει ότι οι 3-κύκλοι δεν αποτελούν ανάγωγο γενετικό σύστημα της A_n .

Παράδειγμα 6 .

Τα στοιχεία της ομάδας S_3 (βλέπε παράδ.2) , γραμμένα με μορφή κύκλων , είναι τα

$$(1), (1 \ 2), (1 \ 3), (2 \ 3), (1 \ 2 \ 3), (1 \ 3 \ 2) \quad .$$

Εδώ η υποομάδα A_3 έχει τάξη $\frac{3!}{2}$ και είναι η

$$A_3 = \{(1), (1 \ 2 \ 3), (1 \ 3 \ 2)\} \quad .$$

Οι άλλες υποομάδες της S_3 είναι οι $H = \{(1), (1 \ 2)\}$, $H_1 = \{(1), (1 \ 3)\}$, $H_2 = \{(1), (2 \ 3)\}$ και η τετριμμένη $\{(1)\}$.

§7. Θεώρημα Lagrange.

Στην παράγραφο αυτή θα πάρουμε τα πρώτα σημαντικά αποτελέσματα που συσχετίζουν τη δομή μιας πεπερασμένης ομάδας G με αριθμοθεωρητικές ιδιότητες της τάξης της $|G|$. Πιο συγκεκριμένα , θα δείξουμε ότι κάθε υποομάδα H μιας ομάδας G μας επιφέρει δυο διαμελισμούς του συνόλου G , το διαμελισμό των δεξιών και αριστερών συμπλοκών της H στην G . Το θεώρημα του Lagrange (η τάξη μιας υποομάδας H μιας ομάδας G διαιρεί την τάξη της ομάδας) συνεπάγεται από το γεγονός ότι όλα τα σύμπλοκα της H στην G έχουν τον ίδιο πληθικό αριθμό .

Ας είναι G μια ομάδα και H μια υποομάδα της .

Στο σύνολο G ορίζουμε δύο σχέσεις ισοδυναμίας R_δ και R_α , ως εξής :



$$x \equiv y(R_\delta) \iff xy^{-1} \in H \quad \text{και} \quad x \equiv y(R_\alpha) \iff x^{-1}y \in H .$$

Η R_δ είναι σχέση ισοδυναμίας . Πραγματικά

i) Ανακλαστική : Για κάθε $x \in G$ έχουμε $xx^{-1} = 1 \in H$, δηλαδή $x \equiv x(R_\delta)$.

ii) Συμμετρική : Αν $x \equiv y(R_\delta)$, τότε $xy^{-1} \in H$ επομένως , αφού $H \leq G$,

$$(xy^{-1})^{-1} = yx^{-1} \in H , \quad \text{δηλαδή} \quad y \equiv x(R_\delta)$$

iii) Μεταβατική : Αν $x \equiv y(R_\delta)$ και $y \equiv z(R_\delta)$, δηλαδή , αν $xy^{-1} \in H$ και $yz^{-1} \in H$, τότε και

$$(xy^{-1})(yz^{-1}) = xz^{-1} \in H , \quad \text{δηλαδή} \quad x \equiv z(R_\delta) .$$

Με ίδιο τρόπο δείχνουμε ότι και η R_α είναι σχέση ισοδυναμίας .

Η R_δ (αντισ. R_α) καλείται δεξιά σχέση ισοδυναμίας της H στην G (αντισ. αριστερή σχέση ισοδυναμίας της H στην G)

Παρατήρηση:

Αν η G είναι αβελιανή ομάδα και H μια υποομάδα της , τότε $R_\delta = R_\alpha$ (Πραγματικά $x \equiv y(R_\delta) \iff xy^{-1} \in H \iff (xy^{-1})^{-1} = yx^{-1} \in H \iff x^{-1}y \in H \iff x \equiv y(R_\alpha)$) . Υπάρχουν όμως μη-αβελιανές ομάδες και υποομάδες τους , για τις οποίες $R_\delta \neq R_\alpha$, όπως θα δούμε στην επόμενη παράγραφο .

Η κλάση ισοδυναμίας $R_\delta(x)$ ενός στοιχείου $x \in G$ είναι το σύνολο

$$R_\delta(x) = Hx = \{hx / h \in H\}$$

Πραγματικά ,

$$R_\delta(x) = \{y / y \in G , y \equiv x(R_\delta)\} = \{y / y \in G , yx^{-1} \in H\} =$$



$$= \{y/y \in G, yx^{-1} = h \in H\} = \{y/y \in G, y = hx, h \in H\}$$

$$= \{hx / h \in H\} = Hx .$$

Το σύνολο Hx καλείται και δεξιό σύμπλοκο της H στην G .
Όμοια η κλάση $R_\alpha(x)$ του στοιχείου $x \in G$ είναι το σύνολο

$$R_\alpha(x) = xH = \{xh / h \in H\} .$$

Το σύνολο xH καλείται ένα αριστερό σύμπλοκο της H στην G .
Έτσι, αν $x, y \in G$, τότε :

- i) $Hx = Hy \iff R_\delta(x) = R_\delta(y) \iff x \equiv y(R_\delta) \iff xy^{-1} \in H$
- ii) $xH = yH \iff R_\alpha(x) = R_\alpha(y) \iff x \equiv y(R_\alpha) \iff x^{-1}y \in H$
- iii) $Hx = H \iff x \in H$.

ΠΡΟΤΑΣΗ 20 .

Ας είναι H μια υποομάδα της ομάδας G . Τότε

$$|Hx| = |H| = |xH| , \text{ για κάθε } x \in G .$$

Δηλαδή όλα τα δεξιά (αντιστ. αριστερά) σύμπλοκα της H στην G έχουν τον ίδιο πληθικό αριθμό .

Απόδειξη .

Η απεικόνιση $f: Hx \longrightarrow H$, $hx \longmapsto h$

είναι φανερά επί είναι και 1-1, γιατί $h = h' \implies hx = h'x$.

Είναι λοιπόν η f 1+1 και επί, επομένως $|Hx| = |H|$.

Όμοια η απεικόνιση $g: xH \longrightarrow H$, $xh \longmapsto h$ είναι 1-1 και επί, δηλαδή $|xH| = |H|$. ■

Παρατήρηση .

Αν η G είναι προσθετική ομάδα και H μια υποομάδα της, τότε



$$x \equiv y(R_\delta) \iff x-y \in H \quad \text{και} \quad x \equiv y(R_\alpha) \iff -x+y \in H.$$

Στην περίπτωση αυτή, αν $x \in G$, τότε :

$$R_\delta(x) = H+x = \{h+x / h \in H\}$$

και

$$R_\alpha(x) = x+H = \{x+h / h \in H\}.$$

Είναι φανερό τώρα ότι το σύνολο $\Delta = G/R_\delta$ όλων των διακεκριμένων δεξιών συμπλόκων της H στην G και όμοια το σύνολο $A = G/R_\alpha$ όλων των διακεκριμένων αριστερών συμπλόκων της H στη G , αποτελούν δύο διαφορετικούς διαμελισμούς του συνόλου G , επομένως

$$G = \bigcup_{Hx \in \Delta} Hx, \quad G = \bigcup_{xH \in A} xH.$$

Θα δείξουμε στη συνέχεια ότι τα σύνολα Δ και A είναι ισοδύναμα, δηλαδή $|\Delta| = |A|$. Μ'άλλα λόγια, ότι υπάρχουν τόσα δεξιά σύμπλοκα της H στην G όσα είναι και τα αριστερά σύμπλοκά της.

Ορίζουμε την απεικόνιση

$$f: \Delta \longrightarrow A, \quad Hx \longmapsto x^{-1}H$$

και παρατηρούμε ότι

$$Hx = Hy \iff xy^{-1} \in H \iff (x^{-1})^{-1}y^{-1} \in H \iff x^{-1}H = y^{-1}H.$$

Η f είναι λοιπόν καλά ορισμένη και ένεση. Είναι και έφεση, αφού για κάθε $yH \in A$ υπάρχει $Hy^{-1} \in \Delta$, ώστε $f(Hy^{-1}) = (y^{-1})^{-1}H = yH$. Η f είναι λοιπόν αμφίεση, οπότε $|\Delta| = |A|$.

ΟΡΙΣΜΟΣ. Έστω H μια υποομάδα μιας ομάδας G . Ο δείκτης της H στην G είναι ο κληθικός αριθμός του συνόλου όλων των διακεκριμένων δεξιών (αντ.αριστερών) συμπλοκών της H στην G και συμβολίζεται $[G:H]$, δηλαδή

$$[G:H] = |\Delta| = |A|.$$



Παράδειγμα 7 . Ας είναι G μια ομάδα και η υποομάδα της $H=\{1\}$. Τότε , για κάθε $x \in G$, το σύμπλοκο $x\{1\}=\{x\}$ και επομένως $[G:\{1\}]=|G|$.

Παράδειγμα 8 . Έστω $V=\{e,a,b,c\}$ η ομάδα του Klein και η υποομάδα της $\langle a \rangle = \{e,a\}$. Έχουμε $|\langle a \rangle| = 2$ και $|V| = 4$, επομένως $4 = [V:\langle a \rangle] \cdot 2 \implies [V:\langle a \rangle] = 2$.

Πραγματικά , τα διακεκριμένα σύμπλοκα της $\langle a \rangle$ είναι $\langle a \rangle e = \{e,a\}$ και $\langle a \rangle b = \{b,c\} = \langle a \rangle \cdot c$.

Παράδειγμα 9 . Έστω $(\mathbb{Z}, +)$ και η υποομάδα της $\langle m \rangle = m\mathbb{Z}$. Επειδή η $\mathbb{Z}$ είναι αβελτιανή , έχουμε $R_\delta = R_\delta = R_m$

$$a \equiv b(R_m) \iff a-b \in \langle m \rangle$$

Επομένως , τα διακεκριμένα σύμπλοκα είναι

$$\langle m \rangle + 0 = \langle m \rangle = \{km/k \in \mathbb{Z}\}$$

$$\langle m \rangle + 1 = \{(k(m+1))/k \in \mathbb{Z}\}$$

$$\vdots$$

$$\langle m \rangle + m-1 = \{km+(m-1)/k \in \mathbb{Z}\}$$

Έτσι , $[\mathbb{Z} : \langle m \rangle] = m$.

ΘΕΩΡΗΜΑ 7 . (LAGRANGE)

Αν H είναι μια υποομάδα της πεπερασμένης ομάδας G , τότε η τάξη της ομάδας H διαιρεί την τάξη της ομάδας G , και μάλιστα

$$|G| = [G:H] \cdot |H| \quad (*)$$

Απόδειξη.

Αφού η G είναι πεπερασμένη , και ο δείκτης της H στην G είναι πεπερασμένος , έστω $[G:H] = k$. Υπάρχουν λοιπόν k διακεκριμένα δεξιά σύμπλοκα και ας είναι αυτά τα $Hx_1, \dots, Hx_k$.



Έχουμε λοιπόν

$$G = Hx_1 \cup \dots \cup Hx_k$$

Επειδή όμως τα σύμπλοκα $Hx_1, \dots, Hx_k$ είναι ξένα μεταξύ τους ανά δύο και $|Hx_i| = |H|$, $i = 1, \dots, k$, παίρνουμε

$$|G| = \underbrace{|H| + \dots + |H|}_{k\text{-φορές}} = k|H| = [G:H] \cdot |H| \quad \blacksquare$$

Παρατήρηση .

Η σχέση (*) ισχύει γενικότερα και για τυχούσα ομάδα G . Πραγματικά, αν I είναι ένα σύνολο δεικτών με $|I| = [G:H]$, τότε

$$G = \bigcup_{i \in I} Hx_i, \quad x_i \in G$$

με τα σύμπλοκα Hx_i ξένα μεταξύ τους ανά δύο .

Η απεικόνιση $f: \bigcup_{i \in I} Hx_i \longrightarrow I \times H$, $hx_i \longmapsto (i, h)$ είναι καλά ορισμένη και μάλιστα 1-1 και επί . Έτσι

$$|G| = \left| \bigcup_{i \in I} Hx_i \right| = |I \times H| = |I| \cdot |H| = [G:H] \cdot |H|$$

Παράδειγμα 10 . Έστω $G = (\mathbb{Z}_{12}, +)$ και $H = \langle \bar{4} \rangle = \{\bar{0}, \bar{4}, \bar{8}\}$. Τα δεξιά σύμπλοκα της H είναι

$$H + \bar{0} = \{\bar{0}, \bar{4}, \bar{8}\} = H + \bar{4} = H + \bar{8}$$

$$H + \bar{1} = \{\bar{1}, \bar{5}, \bar{9}\} = H + \bar{5} = H + \bar{9}$$

$$H + \bar{2} = \{\bar{2}, \bar{6}, \bar{10}\} = H + \bar{6} = H + \bar{10}$$

$$H + \bar{3} = \{\bar{3}, \bar{7}, \bar{11}\} = H + \bar{7} = H + \bar{11}$$

οπότε

$$[\mathbb{Z}_{12} : \langle \bar{4} \rangle] = 4 \quad \text{και} \quad |\mathbb{Z}_{12}| = [\mathbb{Z}_{12} : \langle \bar{4} \rangle] \cdot |\langle \bar{4} \rangle|$$



Παράδειγμα 11 . Έστω η ομάδα S_n και η υποομάδα της A_n των άρτιων μεταθέσεων . Ένα από τα δεξιά σύμπλοκα της A_n στην S_n είναι η ίδια η A_n , ενώ τα υπόλοιπα θα είναι της μορφής $A_n \tau$, για κάθε $\tau \in B_n$, όπου B_n το σύνολο των περιττών μεταθέσεων . Αν τώρα $\tau, \tau_1 \in B_n$, επειδή $\tau \tau_1^{-1} \in A_n$, θα έχουμε $A\tau = A\tau_1$.

Έτσι τα διακεκριμένα σύμπλοκα είναι δύο , το A_n και το B_n , συνεπώς $[S_n : A_n] = 2$, που σημαίνει ότι $|A_n| = \frac{n!}{2}$ αποτέλεσμα που έχουμε ξαναδεί .

Παράδειγμα 12 . Ας πάρουμε τη συμμετρική ομάδα S_3

$$S_3 = \{(1), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$$

και την υποομάδα της $H = \{(1), (1\ 2)\}$.

Τα αριστερά σύμπλοκα της H στην S_3 είναι

$$(1)H = \{(1), (1\ 2)\} = H$$

$$(1\ 2)H = \{(1\ 2), (1)\} = H$$

$$(1\ 3)H = \{(1\ 3), (1\ 2\ 3)\}$$

$$(2\ 3)H = \{(2\ 3), (1\ 3\ 2)\}$$

$$(1\ 2\ 3)H = \{(1\ 2\ 3), (1\ 3)\}$$

$$(1\ 3\ 2)H = \{(1\ 3\ 2), (2\ 3)\}$$

Υπάρχουν επομένως τρία διακεκριμένα αριστερά σύμπλοκα της H στην S_3 , τα

$$H, \{(1\ 3), (1\ 2\ 3)\}, \{(2\ 3), (1\ 3\ 2)\}$$

Τα δεξιά σύμπλοκα της H στην S_3 είναι

$$H(1) = H$$

$$H(1\ 2) = H$$

$$H(1\ 3) = \{(1\ 3), (1\ 3\ 2)\}$$



$$H(2\ 3) = \{(2\ 3), (1\ 2\ 3)\}$$

$$H(1\ 2\ 3) = \{(1\ 2\ 3), (2\ 3)\}$$

$$H(1\ 3\ 2) = \{(1\ 3\ 2), (1\ 3)\}$$

Υπάρχουν λοιπόν τρία διακεκριμένα δεξιά σύμπλοκα της H στην S_3 ,
τα

$$H, \{(1\ 3), (1\ 3\ 2)\}, \{(2\ 3), (1\ 2\ 3)\}$$

Επομένως, τα δεξιά και αριστερά σύμπλοκα δεν είναι τα ίδια· μ' άλλα λόγια, ο διαμελισμός της S_3 από τα δεξιά σύμπλοκα είναι διαφορετικός εκείνου των αριστερών συμπλοκών.

Ο δείκτης της H στην G είναι 3, και ισχύει

$$|S_3| = [S_3 : H] \cdot |H|.$$

ΠΡΟΤΑΣΗ 21.

Αν G είναι μια πεπερασμένη ομάδα, τότε

- i) Η τάξη κάθε στοιχείου $x \in G$ διαιρεί την τάξη της ομάδας
- ii) Αν $|G| = m$, τότε $x^m = 1$, για κάθε $x \in G$.

Απόδειξη.

i) Η τάξη ενός στοιχείου $x \in G$ είναι η τάξη της υποομάδας $\langle x \rangle$, η οποία όμως διαιρεί την τάξη της ομάδας, σύμφωνα με το θεώρημα του Lagrange.

ii) Αν η τάξη του στοιχείου x είναι k , τότε $k|m$, δηλαδή $m = k \cdot \lambda$ επομένως $x^m = (x^k)^\lambda = 1^\lambda = 1$.

ΠΡΟΤΑΣΗ 22.

Κάθε πεπερασμένη ομάδα G , της οποίας η τάξη είναι πρώτος αριθμός, δηλαδή $|G| = p$, είναι κυκλική. Στην περίπτωση αυτή, κάθε στοιχείο της $\neq 1$ είναι γεννήτοράς της.



Απόδειξη .

Έστω $x \in G$ με $x \neq 1$ (αυτό είναι δυνατό , αφού ο p είναι πρώτος αριθμός) και ας πάρουμε την υποομάδα $\langle x \rangle$ της G .

Η τάξη της $\langle x \rangle$ θα διαιρεί την τάξη της ομάδας G επομένως , αφού $|\langle x \rangle| > 1$, θα έχουμε $|\langle x \rangle| = p = |G|$, δηλαδή $\langle x \rangle = G$.

Παράδειγμα 13. Κάνοντας χρήση των δύο παραπάνω προτάσεων θα δείξουμε ότι όλες οι ομάδες G τάξης ≤ 5 είναι αβελιανές . Πραγματικά, αν $|G| = 1, 2, 3$, ή 5 , τότε η G είναι κυκλική και επομένως αβελιανή. Αν $|G| = 4$, τότε κάθε στοιχείο $x \neq 1$ της G θα έχει τάξη 2 ή 4 . Αν υπάρχει στοιχείο x με τάξη 4 , τότε $G = \langle x \rangle = \{1, x, x^2, x^3\}$ είναι κυκλική . Σε κάθε άλλη περίπτωση $x^2 = 1$, για κάθε $x \in G$. Για κάθε $a, b \in G$ έχουμε $(ab)^2 = 1 \implies abab = 1$, οπότε $a^2b ab^2 = ab$, που σημαίνει $ab = ba$. Η G είναι λοιπόν αβελιανή .

Παρατήρηση .

Το αντίστροφο του θεωρήματος του **Lagrange** δεν αληθεύει γενικά. Πραγματικά , όπως θα δούμε στα επόμενα , η μη-αβελιανή ομάδα A_4 τάξης 12 δεν έχει υποομάδα τάξης 6 .

Αληθεύει όμως αυτό για κυκλικές ομάδες (θεωρ. 4) και γενικότερα για αβελιανές ομάδες .

Σημειώνουμε εδώ , χωρίς απόδειξη , ότι , εκείνο που γενικά ισχύει είναι το εξής : (Θεώρημα Sylow) .

Αν η ομάδα G έχει τάξη $|G| = p^n \cdot m$, $n \geq 1$, ο p πρώτος και $(p, m) = 1$, τότε η G περιέχει μια υποομάδα τάξης p^i , για κάθε $1 \leq i \leq n$.

58. Κανονικές Υποομάδες .

Ας είναι H μια υποομάδα μιας ομάδας G .

Είδαμε γενικά ότι τα αριστερά σύμπλοκα της H στην G είναι διαφορετικά από τα δεξιά σύμπλοκα (Παραδ. 12, Κεφ. II.7) .



Είναι φυσικό λοιπόν το ερώτημα , πότε τα αριστερά και δεξιά σύμπλοκα της H στην G είναι ίδια ; Αυτό είναι ισοδύναμο , όπως θα δούμε , με το ερώτημα , πότε η δεξιά σχέση ισοδυναμίας R_δ (όμοια η R_α) συμβιβάζεται με τον πολ/σμό της G ;

Το επόμενο θεώρημα θα μας δώσει την απάντηση , και θα μας οδηγήσει με φυσικό τρόπο στον ορισμό των κανονικών υποομάδων .

ΘΕΩΡΗΜΑ 8 .

Αν H είναι μια υποομάδα της ομάδας G , τότε τα παρακάτω είναι ισοδύναμα .

i) Η αριστερή R_α και δεξιά R_δ σχέση ισοδυναμίας της H στην G ταυτίζονται (δηλαδή ορίζουν την ίδια σχέση ισοδυναμίας στο G) .

ii) Κάθε αριστερό σύμπλοκο της H στην G είναι ένα δεξιό σύμπλοκο της H στην G .

iii) Για κάθε $x \in G$ είναι $xH = Hx$

iv) Για κάθε $x \in G$ είναι $xHx^{-1} = H$ όπου

$$xHx^{-1} = \{xhx^{-1} / h \in H\}$$

v) Για κάθε $x \in G$ είναι $xHx^{-1} \subseteq H$

vi) Η R_δ (όμοια η R_α) συμβιβάζεται με τον πολ/σμό της ομάδας G .

Απόδειξη .

(i) $\iff$ (iii) Δύο σχέσεις ισοδυναμίας R και S πάνω σ'ένα σύνολο G ταυτίζονται εαν και μόνο εαν $R(x) = S(x)$, $\forall x \in G$. Στην περίπτωση μας αυτό σημαίνει $xH = Hx$ $\forall x \in G$.

(ii) $\implies$ (iii) Αν xH είναι ένα αριστερό σύμπλοκο τότε $xH = Hy$ για κάποιο $y \in G$. Επειδή $x \in xH$, έχουμε $x \in Hy$ δηλαδή $x = hy$ για κάποιο $h \in H$, οπότε $xy^{-1} = h \in H$ που σημαίνει ότι $xH = Hy$. Τελικά $xH = Hx$ $\forall x \in G$.

(iii) $\implies$ (ii) . Είναι φανερό



(iii) $\iff$ (iv) . Αν $xH = Hx \iff xHx^{-1} = Hx x^{-1} = H$.

(iv) $\implies$ (v) . Είναι τετριμμένο .

(v) $\implies$ (iv) . Για κάθε $x \in G$ έχουμε $xHx^{-1} \subseteq H$. Για το $x^{-1} \in G$ θα είναι $x^{-1}Hx \subseteq H$. Την πολ/ζουμε από αριστερά με x και από δεξιά με x^{-1} και παίρνουμε

$$x(x^{-1}Hx)x^{-1} \subseteq xHx^{-1} \implies H \subseteq xHx^{-1} .$$

Έτσι $xHx^{-1} = H$, $\forall x \in G$.

(v) $\implies$ (vi) . Πρέπει να δείξουμε ότι αν $x \equiv y(R_\delta)$ και $x_1 \equiv y_1(R_\delta)$ τότε $xx_1 \equiv yy_1(R_\delta)$ δηλαδή αν $xy^{-1} \in H$ και $x_1y_1^{-1} \in H$ τότε $xx_1y_1^{-1}y_1^{-1} \in H$. Πραγματικά

$$x_1y_1^{-1} \in H \implies x(x_1y_1^{-1})x^{-1} \in H \text{ και αφού η } H \text{ είναι υποομάδα}$$

$$(xx_1y_1^{-1}x^{-1})(xy^{-1}) \in H \text{ δηλαδή } xx_1y_1^{-1}y^{-1} \in H .$$

(Όμοια εργαζόμαστε για την R_α) .

(vi) $\implies$ (v) . Για κάθε $h \in H$ και για κάθε $x \in G$ έχουμε $h \equiv 1(R_\delta)$ και $x \equiv x(R_\delta)$ οπότε $xh \equiv x(R_\delta)$.

Έτσι

$$xh \equiv x(R_\delta) \text{ και } x^{-1} \equiv x^{-1}(R_\delta) \implies xhx^{-1} \equiv xx^{-1}(R_\delta)$$

δηλαδή $xhx^{-1} \equiv 1(R_\delta)$ που σημαίνει ότι $xhx^{-1} \in H$.

Επομένως $xHx^{-1} \subseteq H$.

(Όμοια εργαζόμαστε για την R_α) . ■

ΟΡΙΣΜΟΣ . Μια υποομάδα H μιας ομάδας G που ικανοποιεί μια από τις ισοδύναμες συνθήκες του θεωρήματος 8 καλείται κανονική (normal) υποομάδα της G . Θα γράφουμε $H \trianglelefteq G$ (αντ. $H \ntrianglelefteq G$) για να δηλώσουμε ότι η H είναι (αντιστ. δεν είναι) κανονική υποομάδα της G .



Σημειώνουμε εδώ ότι από τις 6 ισοδύναμες συνθήκες του θεωρήματος 8 οι (v), (iv) και η (iii) είναι οι πιο εύχρηστες στην πράξη .

Παρατηρήσεις.

1) Οι υποομάδες $\{1\}$ και G μιας ομάδας G είναι κανονικές δηλαδή $\{1\} \triangleleft G$ και $G \triangleleft G$.

2) Αν $K \triangleleft G$ και $K \leq H \leq G$ τότε $K \triangleleft H$, αλλά γενικά $H \not\triangleleft G$. Για παράδειγμα , αν $G = S_3$, $K = \{(1)\}$ και $H = \{(1), (1\ 2)\}$ τότε $\{(1)\} \triangleleft S_3$, $\{(1)\} \leq H \leq S_3$ αλλά $H \not\triangleleft S_3$ (Παράδ.12, Κεφ. II.7.) .

3) Η σχέση " $\triangleleft$ " δεν είναι μεταβατική . Είναι δυνατόν δηλαδή να έχουμε $H \triangleleft K$ και $K \triangleleft G$ αλλά $H \not\triangleleft G$.

4) Κάθε κανονική υποομάδα H μιας ομάδας G παραμένει αναλλοίωτη σε κάθε εσωτερικό αυτομορφισμό της G δηλαδή για κάθε $\tau_g \in \text{Inn}(G)$ είναι $\tau_g(H) \subseteq H$.

Πραγματικά , για κάθε $h \in H$, $\tau_g(h) = ghg^{-1} \in H$.

Παράδειγμα 1 .

$$SL_n(\mathbb{R}) \triangleleft GL_n(\mathbb{R}) .$$

Είναι $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$ (παράδ.5, Κεφ. II.2.1), ενώ για κάθε $B \in SL_n(\mathbb{R})$ και $A \in GL_n(\mathbb{R})$ έχουμε $ABA^{-1} \in SL_n(\mathbb{R})$ αφού

$$\det(ABA^{-1}) = \det A \cdot \det B \cdot \det A^{-1} = \det A \cdot 1 \cdot \det A^{-1} = 1 .$$

Παράδειγμα 2 .

$$A_n \triangleleft S_n .$$

Είναι $A_n \leq S_n$ (βλέπε Κεφ. II, 6.2.) , ενώ για κάθε $\tau \in A_n$ και $\sigma \in S_n$ έχουμε $\sigma\tau\sigma^{-1} \in A_n$ αφού ,

$$\begin{aligned} \varepsilon(\sigma\tau\sigma^{-1}) &= \varepsilon(\sigma) \cdot \varepsilon(\tau) \cdot \varepsilon(\sigma^{-1}) = \varepsilon(\sigma) \cdot 1 \cdot \varepsilon(\sigma^{-1}) = \\ &= \varepsilon(\sigma\sigma^{-1}) = \varepsilon((1)) = 1 . \end{aligned}$$



Έτσι στην μη-αβελιανή ομάδα S_3 έχουμε ,

$$A_3 = \{(1), (1\ 2\ 3), (1\ 3\ 2)\} \trianglelefteq S_3 \text{ και } H = \{(1), (1\ 2)\} \not\trianglelefteq S_3 .$$

Παράδειγμα 3 .

Έστω G μια ομάδα . Αν $H \trianglelefteq G$ και $K \trianglelefteq G$ τότε $H \cap K \trianglelefteq G$. Πραγματικά , $H \cap K \leq G$ ενώ για κάθε $x \in G$ και $h \in H \cap K$ έχουμε , $xhx^{-1} \in H \cap K$ αφού , $xhx^{-1} \in H$ και $xhx^{-1} \in K$. Έτσι $x(H \cap K)x^{-1} \subseteq H \cap K$.

Η παρακάτω πρόταση μας δίνει πολλά παραδείγματα κανονικών υποομάδων , και μας λέει να στρέψουμε το ενδιαφέρον μας σε μη-αβελιανές ομάδες .

ΠΡΟΤΑΣΗ 23 .

Αν G είναι μια αβελιανή ομάδα , τότε κάθε υποομάδα της είναι κανονική .

Απόδειξη .

Έστω $H \leq G$. Για κάθε $x \in G$ έχουμε ,

$$xHx^{-1} = \{xhx^{-1} / h \in H\} = \{xx^{-1}h / h \in H\} = \{h / h \in H\} = H$$

Έτσι $H \trianglelefteq G$. ■

Το αντίστροφο της παραπάνω πρότασης δεν ισχύει . Για παράδειγμα, στη μη-αβελιανή ομάδα Q_8 των κουατερνίων όλες οι υποομάδες είναι κανονικές , όπως θα δούμε στο παράδειγμα 4 παρακάτω .

ΠΡΟΤΑΣΗ 24 .

Έστω H μια υποομάδα της ομάδας G τέτοια ώστε $[G:H] = 2$. Τότε η H είναι κανονική υποομάδα της G .



Απόδειξη .

Επειδή υπάρχουν δύο δεξιά σύμπλοκα της H στην G αυτά θα είναι τα H και $G \cdot H$. Όμοια , τα δύο αριστερά σύμπλοκα της θα είναι τα H και $G \cdot H$. Έτσι τα δεξιά σύμπλοκα είναι τα ίδια με τα αριστερά επομένως $H \trianglelefteq G$. ■

Έτσι , για την $A_n \trianglelefteq S_n$ έχουμε $[S_n : A_n] = 2$, οπότε $A_n \trianglelefteq S_n$, αποτέλεσμα που έχουμε ξαναδεί .

Ένα κριτήριο για κανονικές υποομάδες θα προκύψει σαν πόρισμα από την επόμενη πρόταση .

ΠΡΟΤΑΣΗ 25 .

Ας είναι H μια υποομάδα της ομάδας G και $x \in G$. Τότε το σύνολο

$$xHx^{-1} = \{xhx^{-1} / h \in H\}$$

είναι μια υποομάδα της G και μάλιστα

$$|xHx^{-1}| = |H| \quad .$$

Απόδειξη .

Το σύνολο xHx^{-1} είναι φανερά $\neq \emptyset$. Αν τώρα , xh_1x^{-1} και xh_2x^{-1} είναι τυχόντα στοιχεία του συνόλου xHx^{-1} , τότε ,

$$(xh_1x^{-1}) \cdot (xh_2x^{-1})^{-1} = xh_1x^{-1}xh_2^{-1}x^{-1} = xh_1h_2^{-1}x^{-1} \in xHx^{-1}$$

αφού $h_1h_2^{-1} \in H$. Τέλος , η απεικόνιση

$$f : H \longrightarrow xHx^{-1} \quad , \quad h \longmapsto xhx^{-1}$$

είναι φανερά 1-1 και επί . Επομένως $|H| = |xHx^{-1}|$. ■



ΠΟΡΙΣΜΑ 1 .

Αν H είναι μια πεπερασμένη υποομάδα τάξης m της ομάδας G και είναι η μοναδική υποομάδα της G με τάξη m τότε $H \trianglelefteq G$.

Απόδειξη .

Για κάθε $x \in G$ η υποομάδα xHx^{-1} της G έχει τάξη $|xHx^{-1}| = |H| = m$. Από την μοναδικότητα της H έχουμε $xHx^{-1} = H$ για κάθε $x \in G$ δηλαδή $H \trianglelefteq G$. ■

Παράδειγμα 4 .

Για την ομάδα Q_8 των κουατερνίων (Παράδ.13,Κεφ.ΙΙ,2.2) γνωρίζουμε ,

$$\text{Στοιχεία} : I_2, j, j^2, j^3, k, jk, k^3, kj$$

$$\text{Αντίστροφα} : I_2, j^3, j^2, j, k^3, kj, k, jk$$

$$\text{Τάξη} : 1, 4, 2, 4, 4, 4, 4, 4$$

Αφού $|Q_8| = 8$, σύμφωνα με το θεώρημα του Langrange , αν $H \leq Q_8$ τότε $|H| = 1$ ή 2 ή 4 ή 8 .

Ομάδα τάξης 1 είναι η $\{I_2\}$ ενώ τάξης 8 η ίδια η Q_8 που είναι φανερά κανονικές . Ομάδα τάξης 2 είναι μόνο η $\{I_2, j^2\}$ αφού , μόνο το j^2 έχει τάξη 2 . Συμφωνά με το πόρισμα 1 $\{I_2, j^2\} \trianglelefteq Q_8$.

Οι υπόλοιπες υποομάδες της θα έχουν τάξη 4 και θα είναι κυκλικές αφού μόνο ένα στοιχείο τάξης 2 υπάρχει . Αυτές είναι οι επόμενες

$$H_1 = \{I_2, j, j^2, j^3\} = \langle j \rangle = \langle j^3 \rangle$$

$$H_2 = \{I_2, k, j^2, k^3\} = \langle k \rangle = \langle k^3 \rangle$$

$$H_3 = \{I_2, kj, j^2, jk\} = \langle kj \rangle = \langle jk \rangle$$

Οι H_1, H_2, H_3 έχουν δείκτη 2 στην Q_8 και επομένως σύμφωνα με την πρόταση 24 είναι κανονικές υποομάδες της Q_8 .



Έχουμε δει ότι το κέντρο $Z(G)$ μιας ομάδας G είναι υποομάδα της G . Θα δείξουμε ότι $Z(G) \trianglelefteq G$. Πραγματικά,

ΠΡΟΤΑΣΗ 26 .

Κάθε υποομάδα H μιας ομάδας G που περιέχεται στο κέντρο της δηλαδή $H \leq Z(G)$ είναι κανονική υποομάδα της G .

Ιδιαίτερα $Z(G) \trianglelefteq G$.

Απόδειξη .

Θα δείξουμε ότι για κάθε $x \in G$ και για κάθε $h \in H$ έχουμε $xhx^{-1} \in H$. Αλλά $h \in Z(G)$ επομένως

$$xhx^{-1} = hxx^{-1} = h \in H \quad . \blacksquare$$

Σαν πόρισμα αυτής της πρότασης παίρνουμε την πρόταση

ΠΡΟΤΑΣΗ 27 .

Αν G είναι μια ομάδα και H μια υποομάδα της που περιέχει τον μεταθέτη $[G, G]$ δηλαδή $[G, G] \leq H$, τότε $H \trianglelefteq G$. Ιδιαίτερα, $[G, G] \trianglelefteq G$.

Απόδειξη .

Για κάθε $h \in H$, $x \in G$ έχουμε

$$xhx^{-1} = (xhx^{-1}h^{-1})h = [x, h] \cdot h \in H \quad .$$

Επομένως, $xhx^{-1} \in H$ που σημαίνει ότι $H \trianglelefteq G$. ■

ΠΡΟΤΑΣΗ 28 .

Αν $f: G \longrightarrow G'$ είναι ομομορφισμός ομάδων, τότε ο πυρήνας $\text{Ker}(f)$ είναι κανονική υποομάδα της G .



Απόδειξη .

Είναι γνωστό ότι , $\text{Ker}(f) = \{x/x \in G, \varphi(x) = 1_G\} \leq G$. Μένει να δείξουμε ότι , $\text{Ker}(f) \trianglelefteq G$. Για κάθε $x \in \text{Ker}(f)$ και για κάθε $g \in G$ έχουμε

$$f(gxg^{-1}) = f(g)f(x)f(g^{-1}) = f(g) \cdot 1 \cdot f(g^{-1}) = f(g)[f(g)]^{-1} = 1_G.$$

επομένως $gxg^{-1} \in \text{Ker}(f)$ δηλαδή $\text{Ker}(f) \trianglelefteq G$. ■

Για παράδειγμα ο πυρήνας του ομομορφισμού

$$\det : \text{GL}_n(\mathbb{R}) \longrightarrow \mathbb{R}^*, A \longmapsto \det A$$

είναι $\text{Ker}(\det) = \text{SL}_n(\mathbb{R})$, οπότε $\text{SL}_n(\mathbb{R}) \trianglelefteq \text{GL}_n(\mathbb{R})$ αποτέλεσμα που έχουμε ξαναδεί .

Όμοια , $A_n \trianglelefteq S_n$ αφού , ο πυρήνας του ομομορφισμού

$$\varepsilon : S_n \longrightarrow \{1, -1\}, \sigma \longmapsto \varepsilon(\sigma)$$

είναι

$$\text{Ker}(\varepsilon) = A_n .$$

ΠΡΟΤΑΣΗ 29 .

Έστω $f : G \longrightarrow G'$ ένας ομομορφισμός ομάδων . Ισχύουν τα επόμενα

1) Αν $K \trianglelefteq G'$ τότε και $f^{-1}(K) \trianglelefteq G$.

2) Αν ο f είναι επιμορφισμός δηλαδή $f(G) = G'$ και $H \trianglelefteq G$ τότε και $f(H) \trianglelefteq G'$.

Απόδειξη .

1) Είναι $f^{-1}(K) \leq G$ (βλέπε Κεφ. II, Πρωτ. 7) . Για κάθε $g \in G$ και για κάθε $x \in f^{-1}(K)$ έχουμε



$$f(gxg^{-1}) = f(g)f(x)[f(g)]^{-1} \in K \quad \text{αφού} \quad K \trianglelefteq G'$$

και $f(x) \in K$. Έτσι $f^{-1}(K) \trianglelefteq G$.

2) Όμοια $f(H) \trianglelefteq G'$. Για κάθε $g' \in G'$, $h' \in f(H)$, υπάρχουν στοι-
χεία $g \in G$, $h \in H$ τέτοια ώστε $f(g) = g'$ και $f(h) = h'$. Έχουμε

$$g'h'(g')^{-1} = f(g)f(h)[f(g)]^{-1} = f(ghg^{-1}).$$

Αλλά $ghg^{-1} \in H$ αφού, $H \trianglelefteq G$. Επομένως

$$g'h'(g')^{-1} \in f(H) \quad \text{δηλαδή} \quad f(H) \trianglelefteq G' \quad . \blacksquare$$

ΠΡΟΤΑΣΗ 30

Αν H είναι μια κανονική υποομάδα της A_n ($n \geq 3$) και η H περιέχει ένα κύκλο 3 τότε, $H = A_n$.

Απόδειξη.

Έστω $(rsk) \in H$. Είδαμε ότι, (Πρόταση 19, Κεφ. II)

$$A_n = \langle \{(rsi) / 1 \leq i \leq n, i \neq r, s \} \rangle$$

Για να δείξουμε λοιπόν ότι, $A_n = H$ αρκεί να δείξουμε ότι, οι κύκλοι (rsi) , $1 \leq i \leq n$, $i \neq r, s$ ανήκουν στην H .

Πραγματικά, για κάθε $i \neq r, s, k$ έχουμε

$$\begin{aligned} (rsi) &= (rs)(ki)(rsk)^2(ki)(rs) = \\ &= [(rs)(ki)](rsk)^2[(rs)(ki)]^{-1} \in H \end{aligned}$$

αφού $(rs)(ki) \in A_n$ και $H \trianglelefteq A_n$. ■

ΠΟΡΙΣΜΑ 2.

Η A_4 δεν έχει υποομάδα τάξης 6.

Απόδειξη.



θα υποθέσουμε ότι η A_4 έχει μια υποομάδα H τάξης 6 και θα καταλήξουμε σε άτοπο .

Έχουμε τότε , $[A_4:H] = \frac{|A_4|}{|H|} = 2$ επομένως , $H \trianglelefteq A_4$ σύμφωνα με την πρόταση 24 . Επειδή όμως 8 από τα 12 στοιχεία της A_4 είναι 3-κύκλοι, η H θα περιέχει ένα τουλάχιστο 3-κύκλο οπότε , $H = A_4$ σύμφωνα με την παραπάνω πρόταση . Έτσι $|H|=12$ άτοπο . ■

ΠΡΟΤΑΣΗ 31 .

Έστω K και H δύο υποομάδες μιας ομάδας G με την H κανονική στην G . Τότε

- α) Η τομή $H \cap K$ είναι κανονική υποομάδα της K .
- β) Η H είναι κανονική υποομάδα της $H \vee K$.
- γ) Οι H και K αντιμετατίθεται δηλαδή $HK = KH$ και μάλιστα $HK = H \vee K = KH$

δ) Αν και η K είναι κανονική υποομάδα της G με $H \cap K = \{1\}$ τότε $hk = kh$ για κάθε $h \in H$ και $k \in K$.

Απόδειξη.

α) Αρκεί να δείξουμε ότι για κάθε $x \in H \cap K$ και $k \in K$ έχουμε $kxk^{-1} \in H \cap K$. Πραγματικά , το $x \in H$ και $x \in K$, επομένως , $kxk^{-1} \in H$ αφού $H \trianglelefteq G$ και $kxk^{-1} \in K$ επειδή $k \in K$.

Έτσι $kxk^{-1} \in H \cap K$ όπως επιθυμούσαμε .

β) $H \trianglelefteq G$ και $H \leq H \vee K \leq G$ επομένως $H \trianglelefteq H \vee K$.

γ) θα δείξουμε αρχικά ότι , $\{hk/h \in H, k \in K\} = \{kh/k \in K, h \in H\}$.

Αφού $H \trianglelefteq G$ για κάθε $h \in H$ και $k \in K$ έχουμε

i) $khk^{-1} = h' \in H$ δηλαδή $kh = h'k$ επομένως $KH \subseteq HK$

ii) $k^{-1}hk = h'' \in H$ δηλαδή $hk = kh''$ επομένως $HK \subseteq KH$

Τελικά $HK = KH$. Στην μελέτη του supremum δύο υποομάδων είδαμε ότι αν $HK = KH$ τότε



$$HVK = \{hk/k \in H, k \in K\} = HK = KH.$$

δ) Για κάθε $h \in H$ και $k \in K$ έχουμε

$$hkh^{-1} \in K \text{ αφού } K \trianglelefteq G \text{ και } kh^{-1}k^{-1} \in H \text{ αφού } H \trianglelefteq G$$

επομένως αφού οι H και K είναι υποομάδες της G

$$(hkh^{-1})k^{-1} \in K \text{ και } h(kh^{-1}k^{-1}) \in H.$$

Αλλά ,

$$(hkh^{-1})k^{-1} = h(kh^{-1}k^{-1}) \in H \cap K = \{1\}$$

έτσι $hkh^{-1}k^{-1} = 1$ επομένως $hk = kh$. ■

§ 9. Ομάδα πηλίκο.

Ας είναι G μια ομάδα και R μια σχέση ισοδυναμίας στο σύνολο G συμβιβαστή με τον πολ/σμό της

$$G : x \equiv y(R) \text{ και } x' \equiv y'(R) \implies xx' \equiv yy'(R).$$

Αφού μια ομάδα είναι πολύ περισσότερο ένα μονοειδές , το σύνολο πηλίκο G/R με πολ/σμό

$$R(x) \cdot R(y) = R(xy) \text{ για κάθε } R(x), R(y) \in G/R$$

δομείται σε μονοειδές (βλέπε Κεφ.Ι.2.) με ουδέτερο στοιχείο την κλάση $R(1)$.

Το μονοειδές G/R είναι ομάδα . Πραγματικά , κάθε στοιχείο $R(x)$ έχει αντίστροφο το $R(x^{-1})$ αφού ,

$$R(x) \cdot R(x^{-1}) = R(xx^{-1}) = R(1) = R(x^{-1}x) = R(x^{-1})R(x).$$

Η ομάδα G/R καλείται **ομάδα πηλίκο** της G με την (συμβιβαστή) σχέση ισοδυναμίας R .

Στη συνέχεια , θα δείξουμε ότι υπάρχουν τόσες σχέσεις ισοδυναμίας στην G που συμβιβάζονται με τον πολ/σμό της όσες είναι και οι



κανονικές υποομάδες της G . Έτσι, οι κανονικές υποομάδες της G "ταυτίζονται" με τις ισοδυναμίες τις συμβιβαστές με τον πολ/σμό της G , πράγμα που μας επιτρέπει να μιλάμε για την ομάδα πηλίκο της G με μια κανονική υποομάδα της.

ΘΕΩΡΗΜΑ 9 .

Έστω G μια ομάδα. Το σύνολο $\mathcal{A}$ όλων των σχέσεων ισοδυναμίας στο σύνολο G που συμβιβάζονται με τον πολ/σμό της είναι ισοδύναμο με το σύνολο $\mathcal{B}$ όλων των κανονικών υποομάδων της G δηλαδή

$$|\mathcal{A}| = |\mathcal{B}|$$

Απόδειξη .

Κάθε κανονική υποομάδα H της G ορίζει στο σύνολο G μια σχέση ισοδυναμίας $R_H : x \equiv y(R_H) \iff xy^{-1} \in H$ που είναι συμβιβαστή με τον πολ/σμό της G . Πραγματικά $R_H = R_\delta = R_\alpha$ (θεώρημα 8, Κεφ. II).

Ορίζεται λοιπόν μια απεικόνιση

$$\Phi : \mathcal{B} \longrightarrow \mathcal{A}, \quad H \longmapsto R_H.$$

Από την άλλη μεριά, αν $R \in \mathcal{A}$ θα δείξουμε ότι η κλάση ισοδυναμίας $R(1)$ του μοναδιαίου στοιχείου της G :

$$(1) = \{x/x \in G, \quad x \equiv 1(R)\}$$

είναι κανονική υποομάδα της G .

α) $R(1) \leq G$.

Πραγματικά για κάθε $x, y \in R(1)$ δηλαδή $x \equiv 1(R)$ και $y \equiv 1(R)$ έχουμε $xy \equiv 1(R)$ αφού η R είναι συμβιβαστή με τον πολ/σμό της G .

Επίσης για κάθε $x \in R(1)$ έχουμε $x^{-1} \in R(1)$ αφού

$$\left. \begin{array}{l} x \equiv 1(R) \\ x^{-1} \equiv x^{-1}(R) \end{array} \right\} \implies xx^{-1} \equiv 1 \cdot x^{-1}(R) \text{ δηλαδή } x^{-1} \equiv 1(R).$$

β) $R(1) \trianglelefteq G$



Αρκεί να δείξουμε ότι για κάθε $g \in G$ είναι $gR(1)g^{-1} \subseteq R(1)$.
Πραγματικά, για κάθε $x \in R(1)$ και $g \in G$ έχουμε,

$$x \equiv 1(R) \text{ και } g \equiv g(R) \implies gx \equiv g(R)$$

Έτσι,

$$\left. \begin{array}{l} gx \equiv g(R) \\ g^{-1} \equiv g^{-1}(R) \end{array} \right\} \implies gxg^{-1} \equiv gg^{-1}(R) \text{ δηλαδή } gxg^{-1} \equiv 1(R)$$

που σημαίνει ότι $gxg^{-1} \in R(1)$.

Ορίζεται έτσι μια απεικόνιση

$$\Psi: \mathcal{A} \longrightarrow \mathcal{B}, \quad R \longmapsto R(1).$$

Θα δείξουμε ότι

$$\Phi \circ \Psi = I \quad \text{και} \quad \Psi \circ \Phi = I_B.$$

Αν $H \trianglelefteq G$ τότε $(\Psi \circ \Phi)(H) = \Psi(R_H) = R_H(1)$ αλλά

$$R_H(1) = \{x/x \in G, x \equiv 1(R_H)\} = \{x/x \in G, x1^{-1} \in H\} = \{x/x \in H\} = H$$

Έτσι, $\Psi \circ \Phi = I_B$.

Αν $R \in \mathcal{B}$ τότε $(\Phi \circ \Psi)(R) = \Phi(R(1)) = R_{R(1)}$.

Αλλά $x \equiv y(R_{R(1)}) \iff xy^{-1} \in R(1) \iff xy^{-1} \equiv 1(R) \iff x \equiv y(R)$ αφού η

R είναι συμβιβαστή.

Έτσι, $R_{R(1)} = R$, που σημαίνει ότι $\Phi \circ \Psi = I_{\mathcal{A}}$.

Απο τα παραπάνω έχουμε $|\mathcal{A}| = |\mathcal{B}|$. ■

Έστω $H \trianglelefteq G$ και R_H η σχέση ισοδυναμίας που ορίζει η H ,
όπου

$$x \equiv y(R_H) \iff xy^{-1} \in H.$$



Την ομάδα πηλίκο G/R_H θα την συμβολίζουμε στο εξής G/H και θα την καλούμε ομάδα πηλίκο της G με την H .

Τα στοιχεία της ομάδας G/H είναι όλα τα διακεκριμένα δεξιά σύμπλοκα της H στην G αφού, για κάθε $x \in G$ έχουμε

$$R_H(x) = Hx$$

(Υπενθυμίζουμε ότι $Hx = xH$ για κάθε $x \in G$ αφού $H \trianglelefteq G$).

Ο πολ/σμός στην G/H γράφεται,

$$Hx \cdot Hy = Hxy$$

το μονοδιαίο στοιχείο της είναι το $H1 = H$, ενώ το αντίστροφο του στοιχείου Hx είναι το Hx^{-1} .

Τέλος η ομάδα G/H έχει τάξη

$$|G/H| = [G : H] .$$

Πραγματικά, από τον ορισμό του δείκτη υποομάδας έχουμε

$$|G/R_H| = |G/R_\alpha| = [G : H] .$$

Ανακεφαλαιώνοντας, βλέπουμε ότι, αν $H \trianglelefteq G$ το σύνολο των δεξιών συμπλοκών της H στην G αποτελεί ομάδα ως προς τον πολ/σμό υποσυνόλων της G εάν και μόνο εάν $H \trianglelefteq G$.

Παρατήρηση .

Αν η ομάδα G είναι προσθετική, η ισοδυναμία R_H παίρνει τη μορφή $x \equiv y (R_H) \iff x - y \in H$.

Τα στοιχεία της ομάδας πηλίκο G/H είναι όλα τα διακεκριμένα δεξιά σύμπλοκα της H στην G αφού,

$$R_H(x) = H + x .$$

Η πρόσθεση στην G/H γράφεται,

$$(H+x) + (H+y) = H + (x+y) ,$$



το μηδενικό στοιχείο της G/H είναι το $H+0=H$ και το αντίθετο του $H+x$ είναι το $H+(-x)$.

Για να κάνουμε τα πράγματα πιο φανερά θα δώσουμε ορισμένα παραδείγματα ομάδας πηλίκου.

Παράδειγμα 1. Έστω G μια ομάδα. Είναι $\{1\} \trianglelefteq G$ και

$$x \equiv y(R_{\{1\}}) \iff xy^{-1} \in \{1\} \iff x = y$$

έτσι, $G/\{1\} = \{\{x\}/x \in G\}$.

Όμοια, $G \trianglelefteq G$ και $x \equiv y(R_G) \iff xy^{-1} \in G$

έτσι, η ομάδα πηλίκου περιέχει μόνο ένα στοιχείο την κλάση G δηλαδή $G/G = \{G\}$.

Παράδειγμα 2. Κάθε υποομάδα H της $(\mathbb{Z}, +)$ είναι της μορφής

$$H = \langle m \rangle = \{km/k \in \mathbb{Z}\} \quad (m \in \mathbb{Z}^+)$$

και μάλιστα κανονική αφού η $\mathbb{Z}$ είναι αβελιανή.

Η σχέση ισοδυναμίας $R_{\langle m \rangle}$ που αντιστοιχεί στην υποομάδα $\langle m \rangle$ ορίζεται από

$$x \equiv y(R_m) \iff x-y \in \langle m \rangle \iff m \mid x-y$$

δηλαδή η $R_{\langle m \rangle}$ δεν είναι παρά η αριθμητική ισοδυναμία R_m . Έτσι, σαν σύνολα $\mathbb{Z}_m = \mathbb{Z}/\langle m \rangle$. Επειδή όμως οι πράξεις πρόσθεσης στις ομάδες $(\mathbb{Z}_m, +)$ και $(\mathbb{Z}/\langle m \rangle, +)$ ταυτίζονται, η ομάδα $\mathbb{Z}/\langle m \rangle$ μπορεί να περιγραφεί ακριβώς σαν η ομάδα $\mathbb{Z}_m$.

Παράδειγμα 3. Στην πολ/κή ομάδα $\mathbb{C}^* = \mathbb{C} - \{0\}$, ο μοναδιαίος κύκλος του μιγαδικού επιπέδου

$$U = \{z/z \in \mathbb{C}, \text{ και } |z| = 1\},$$

είναι μια υποομάδα της και μάλιστα κανονική αφού η $\mathbb{C}^*$ είναι αβελιανή.



Η σχέση ισοδυναμίας R_U που αντιστοιχεί στην U ορίζεται από $z_1 \equiv z_2 (R_U) \iff z_1 z_2^{-1} \in U$.

Η κλάση ισοδυναμίας του $z_0 \in \mathbb{C}^*$ είναι

$$\begin{aligned} Uz_0 &= \{z/z \in \mathbb{C}^* \text{ και } zz_0^{-1} \in U\} = \{z/z \in \mathbb{C}^* \text{ και } |zz_0^{-1}| = 1\} = \\ &= \{z/z \in \mathbb{C}^* \text{ και } |z| = |z_0|\} . \end{aligned}$$

δηλαδή το Uz_0 είναι η περιφέρεια με κέντρο την αρχή των συνταταγμένων 0 και ακτίνα ίση με $|z_0|$.

Η ομάδα πηλίκου $\mathbb{C}^*/U$ περιέχει σαν στοιχεία όλες τις ομόκεντρες περιφέρειες που γράφονται με κέντρο το 0 και θετική ακτίνα.

Παράδειγμα 4. Στην ομάδα $(\mathbb{Q}, -)$ η υποομάδα της $\mathbb{Z}$ είναι κανονική, αφού η $\mathbb{Q}$ είναι αβελιανή.

Η σχέση ισοδυναμίας $R_{\mathbb{Z}}$ που αντιστοιχεί στην $\mathbb{Z}$ ορίζεται από

$$r_1 \equiv r_2 (R_{\mathbb{Z}}) \iff r_1 - r_2 \in \mathbb{Z} .$$

Δηλαδή, δύο ρητοί είναι ισοδύναμοι εάν-ν έχουν τον ίδιο κλασματικό μέρος.

Η κλάση ισοδυναμίας του $r \in \mathbb{Q}$ είναι το σύμπλοκο

$$\mathbb{Z} + r = \{n + r / n \in \mathbb{Z}\} .$$

ενώ τα διακεκριμένα σύμπλοκα της $\mathbb{Z}$ στην $\mathbb{Q}$ είναι τα $\mathbb{Z} + r$, $r \in \mathbb{Q}$, $0 \leq r < 1$ δηλαδή

$$\mathbb{Q}/\mathbb{Z} = \{\mathbb{Z} + r / r \in \mathbb{Q}, 0 \leq r < 1\} .$$

Για να δούμε αυτό παρατηρούμε : 1ον) Αν $r_1, r_2 \in \mathbb{Q}$, $0 \leq r_1 < 1$, $0 \leq r_2 < 1$ και $r_1 \neq r_2$ τότε $\mathbb{Z} + r_1 \neq \mathbb{Z} + r_2$. Πραγματικά, αν $\mathbb{Z} + r_1 = \mathbb{Z} + r_2$ δηλαδή $r_1 - r_2 = \alpha \in \mathbb{Z}$ τότε $|r_1 - r_2| = |\alpha| \geq 1$, πράγμα άτοπο αφού $0 \leq r_1, r_2 < 1$.

2ον) Κάθε σύμπλοκο $\mathbb{Z} + r \in \mathbb{G}/\mathbb{Z}$ περιέχει ένα ρητό r_1 με $0 \leq r_1 < 1$



δηλαδή $\mathbb{Z}+r=\mathbb{Z}+r_1$.

Πραγματικά , αν $r \in \mathbb{Q}$ τότε $r = \frac{p}{q}$ ($p, q \in \mathbb{Z}$, $q > 0$) . Διαιρώντας τον p με τον q παίρνουμε ,

$$p = aq + b \quad , \quad 0 \leq b < q$$

οπότε ,

$$\frac{p}{q} = a + \frac{b}{q} \quad \text{και συνεπώς} \quad \frac{p}{q} - \frac{b}{q} = a \in \mathbb{Z} \quad .$$

Έτσι , $\mathbb{Z}+r = \mathbb{Z} + \frac{b}{q}$ με $\frac{b}{q} \in \mathbb{Q}$ και $0 \leq \frac{b}{q} < 1$.

Από τα παραπάνω βλέπουμε ότι κάθε σύμπλοκο $\mathbb{Z}+r \in \mathbb{Q}/\mathbb{Z}$ περιέχει ένα και μόνο ένα ρητό r_1 με $0 \leq r_1 < 1$.

Έτσι το σύνολο $\mathbb{Q}/\mathbb{Z}$ είναι ισουδύναμο με το σύνολο των ρητών του μοναδιαίου διαστήματος $[0,1)$, μ'άλλα λόγια η ομάδα $\mathbb{Q}/\mathbb{Z}$ είναι άπειρης τάξης .

Η $\mathbb{Q}/\mathbb{Z}$ καλείται προσθετική ομάδα των ρητών modulo 1 .

Θα σημειώσουμε εδώ ότι , αν $\mathbb{Z} + \frac{p}{q} \in \mathbb{Q}/\mathbb{Z}$ τότε

$$q(\mathbb{Z} + \frac{p}{q}) = \mathbb{Z} + q \frac{p}{q} = \mathbb{Z}$$

που σημαίνει ότι όλα τα στοιχεία της έχουν πεπερασμένη τάξη δηλαδή η $\mathbb{Q}/\mathbb{Z}$ είναι περιοδική ομάδα .

§10. Θεωρήματα ισομορφισμών.

Στην παράγραφο αυτή θα δώσουμε τρία σπουδαία θεωρήματα γνωστά σαν θεωρήματα ισομορφισμών που μας δείχνουν την συγγένεια που υπάρχει μεταξύ των κανονικών υποομάδων , ομάδων πηλίκου και ομομορφισμών .

Έχουμε δει ότι ο πυρήνας κάθε ομομορφισμού ομάδων είναι κανονική υποομάδα (Προτ.28,Κεφ.II) , αλλά και αντίστροφα , όπως θα δούμε πιά κάτω , κάθε κανονική υποομάδα H μιας ομάδας G είναι ο πυρήνας ενός ομομορφισμού από την G σε μια κατάλληλη ομάδα .



Ας είναι H μια κανονική υποομάδα της G . Η απεικόνιση

$$p: G \longrightarrow G/H, \quad p(x) = Hx, \quad \forall x \in G$$

είναι ένας επιμορφισμός ομάδων με $\text{Ker } p = H$.

Πραγματικά, η p είναι φανερά επί και

$$p(xy) = Hxy = (Hx)(Hy) = p(x) \cdot p(y), \quad \forall x, y \in G.$$

Επιπλέον,

$$\text{Ker } p = \{x \in G / p(x) = H\} = \{x \in G / Hx = H\} = \{x \in G / x \in H\} = H.$$

Η απεικόνιση p καλείται κανονική προβολή της G στην G/H .

Το επόμενο λήμμα είναι βασικό.

ΛΗΜΜΑ 1.

Ας είναι $f: G \longrightarrow G'$ ένας ομομορφισμός ομάδων και H μια κανονική υποομάδα της G που περιέχεται στον πυρήνα της f δηλαδή $H \subseteq \text{Ker } f$. Τότε, υπάρχει μοναδικός ομομορφισμός

$$\bar{f}: G/H \longrightarrow G'$$

που κάνει το επόμενο διάγραμμα αντιμεταθετικό

$$\begin{array}{ccc} G & \xrightarrow{p} & G/H \\ & \searrow f & \downarrow \bar{f} \\ & & G' \end{array} \quad (I)$$

δηλαδή $f = \bar{f} \circ p$.

Απόδειξη.

Ορίζουμε την απεικόνιση $\bar{f}: G/H \longrightarrow G'$ ως εξής:

$$\bar{f}(Hx) = f(x), \quad \forall x \in G.$$

Η $\bar{f}$ είναι καλά ορισμένη. Θα δείξουμε ότι, αν $Hx = Hy$ τότε

$$\bar{f}(Hx) = \bar{f}(Hy) \quad \text{ή ισοδύναμα} \quad f(x) = f(y).$$



Πραγματικά, αν $Hx = Hy$ τότε $xy^{-1} \in H \subseteq \text{Ker } f$. Έτσι, $f(xy^{-1}) = 1$ ή $f(x)[f(y)]^{-1} = 1$ ή $f(x) = f(y)$.

Η $\bar{f}$ κάνει το διάγραμμα (I) αντιμεταθετικό αφού,

$$(\bar{f} \circ p)(x) = \bar{f}(p(x)) = \bar{f}(Hx) = f(x) \quad \forall x \in G$$

και είναι ομομορφισμός: για κάθε $Hx, Hy \in G/H$

$$\bar{f}[(Hx)(Hy)] = \bar{f}(Hxy) = f(xy) \stackrel{f \text{ ομομ.}}{=} f(x)f(y) = \bar{f}(Hx) \cdot \bar{f}(Hy).$$

Μένει να δείξουμε ότι ο $\bar{f}$ είναι ο μοναδικός ομομορφισμός τέτοιος ώστε $f = \bar{f} \circ p$. Ας είναι $h: G/H \rightarrow G'$ ένας άλλος ομομορφισμός με

$$f = h \circ p. \quad (1)$$

Τότε για κάθε $Hx \in G/H$ έχουμε

$$\bar{f}(Hx) = f(x) \stackrel{(1)}{=} (h \circ p)(x) = h(p(x)) = h(Hx)$$

δηλαδή $\bar{f} = h$ πράγμα που επιθυμούσαμε. ■

Παράδειγμα 1. Κάθε ομομορφισμός $f: G \rightarrow A$ από μια ομάδα G σε μια αβελιανή ομάδα A ορίζει έναν ομομορφισμό

$$\bar{f}: G/[G, G] \rightarrow A, \quad \bar{f}([G, G]x) = f(x) \quad \forall x \in G,$$

όπου $[G, G]$ είναι η ομάδα μεταθέτης της G .

Αρκεί να δείξουμε ότι $[G, G] \subseteq \text{Ker}(f)$.

Αρχικά παρατηρούμε ότι, για κάθε μεταθέτη $[x, y] = xyx^{-1}y^{-1}$ έχουμε

$$\begin{aligned} f([x, y]) &= f(xyx^{-1}y^{-1}) = f(x)f(y)[f(x)]^{-1}[f(y)]^{-1} = \\ &= f(x)[f(x)]^{-1}f(y)[f(y)]^{-1} \quad (\text{η } A \text{ αβελιανή}) \\ &= 1 \cdot 1 = 1. \end{aligned}$$

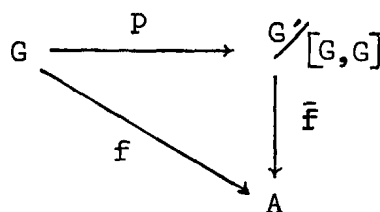
Αν τώρα $[x_1, y_1] \dots [x_k, y_k]$ είναι ένα τυχόν στοιχείο της ομάδας $[G, G]$ τότε,



$$f([x_1, y_1] \dots [x_k, y_k]) = f([x_1, y_1]) \dots f([x_k, y_k]) = 1 \dots 1 = 1 ,$$

πράγμα που επιθυμούσαμε .

Το προηγούμενο λήμμα τώρα μας βεβαιώνει ότι υπάρχει ο ζητούμενος ομομορφισμός $\bar{f}$, που κάνει δηλαδή το επόμενο διάγραμμα αντιμεταθετικό



ΘΕΩΡΗΜΑ 10 (Θεμελιώδες θεώρημα ομομορφισμών)

Κάθε ομομορφισμός ομάδων $f: G \longrightarrow G'$ ορίζει ένα μοναδικό μονομορφισμό

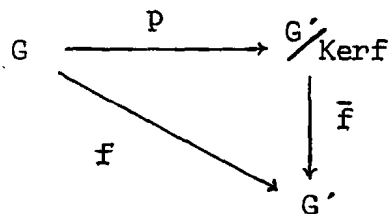
$$\bar{f}: G/\text{Ker}f \longrightarrow G' , \quad \bar{f}[(\text{Ker}f)x] = f(x) , \quad \forall x \in G .$$

ιδιαίτερα,

$$G/\text{Ker}f \cong \text{Im}(f) .$$

Απόδειξη.

Σύμφωνα με το λήμμα 1 υπάρχει μοναδικός ομομορφισμός $\bar{f}: G/\text{Ker}f \longrightarrow G'$ που κάνει το παρακάτω διάγραμμα αντιμεταθετικό



δηλαδή $f = \bar{f} \circ p$. Έτσι $\bar{f}[(\text{Ker}f)x] = f(x) , \quad \forall x \in G$.

Θα δείξουμε ότι ο $\bar{f}$ είναι μονομορφισμός . Αρκεί να δείξουμε ότι



$$\text{Ker } \bar{f} = \{\text{ker } f\} \quad ,$$

αφού $\text{Ker } f$ είναι το μοναδιαίο στοιχείο της ομάδας $G/\text{Ker } f$.

Ας είναι $(\text{Ker } f)x$ ένα στοιχείο του $\text{Ker } \bar{f}$, τότε

$$\bar{f}[(\text{Ker } f)x] = 1_{G'} \Rightarrow f(x) = 1_G \Rightarrow x \in \text{Ker } f$$

οπότε $(\text{Ker } f)x = \text{Ker } f$, όπως το επιθυμούσαμε .

Αφού ο $\bar{f}$ είναι μονομορφισμός έχουμε $G/\text{Ker } f \cong \text{Im}(\bar{f})$.

Αλλά $\text{Im}(\bar{f}) = \text{Im } f$ οπότε

$$G/\text{Ker } f \cong \text{Im}(f) \quad . \blacksquare$$

ΠΡΟΤΙΜΑ 1 .

Αν $f: G \longrightarrow G'$ είναι ένας επιμορφισμός τότε

$$G/\text{Ker } f \cong G' \quad . \blacksquare$$

Παράδειγμα 2.

Ας είναι $U = \{z/z \in \mathbb{C} \text{ , και } |z| = 1\}$ ο μοναδιαίος κύκλος του μιγαδικού επιπέδου . θεωρούμε την απεικόνιση

$$f: \mathbb{R} \longrightarrow U \quad , \quad f(x) = \cos 2\pi x + i \sin 2\pi x \quad , \quad \forall x \in \mathbb{R} \quad .$$

Η f είναι ένας επιμορφισμός της ομάδας $(\mathbb{R}, +)$ στην $(U, \cdot)$. Πραγματικά , για κάθε $x, y \in \mathbb{R}$ έχουμε

$$\begin{aligned} f(x+y) &= \cos(2\pi x + 2\pi y) + i \sin(2\pi x + 2\pi y) = \\ &= (\cos 2\pi x \cos 2\pi y - \sin 2\pi x \sin 2\pi y) - \\ &\quad - i(\sin 2\pi x \cos 2\pi y + \cos 2\pi x \sin 2\pi y) = \\ &= (\cos 2\pi x + i \sin 2\pi x)(\cos 2\pi y + i \sin 2\pi y) = \\ &= f(x) \cdot f(y) \quad , \end{aligned}$$

ενώ είναι φανερά "επύ" . Επιπλέον ,



$$\text{Ker}(f) = \{x \in \mathbb{R} / \sin 2\pi x = 1 \text{ και } \eta \mu 2\pi x = 0\} = \mathbb{Z}$$

Έτσι

$$(\mathbb{R}, +) / \mathbb{Z} \simeq \mathbb{U}.$$

Παράδειγμα 3 .

Έχουμε δεί ότι η απεικόνιση $\det : GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^*$ είναι ένας επιμορφισμός δηλαδή $\text{Im}(\det) = \mathbb{R}^*$ και $\text{Ker}(\det) = SL_n(\mathbb{R})$, Έτσι

$$GL_n(\mathbb{R}) / SL_n(\mathbb{R}) \simeq \mathbb{R}^*.$$

Παράδειγμα 4 .

Για τον ομομορφισμό $\epsilon : S_n \longrightarrow \{-1, +1\}$ γνωρίζουμε ότι $\text{Ker}(\epsilon) = A_n$ και $\text{Im}(\epsilon) = \{-1, +1\}$. Επομένως

$$S_n / A_n \simeq \{-1, +1\}.$$

Έτσι $|S_n / A_n| = 2$ οπότε $|A_n| = \frac{n!}{2}$, αποτέλεσμα που έχουμε ξαναδεί .

Παράδειγμα 5 .

Για κάθε ομάδα G ορίζουμε μια απεικόνιση

$$\tau : G \longrightarrow \text{Aut}(G) , \quad \tau(g) = \tau_g , \quad \forall g \in G$$

όπου τ_g είναι ο εσωτερικός αυτομορφισμός της G με $\tau_g(x) = gxg^{-1}$, $\forall x \in G$. (Βλέπε Παράδ.3, Κεφ. II.4). Η τ είναι ένας ομομορφισμός . Πραγματικά , για κάθε $g_1, g_2 \in G$ έχουμε $\tau(g_1 g_2) = \tau_{g_1 g_2} = \tau_{g_1} \circ \tau_{g_2}$.

Θα βρούμε τον πυρήνα του τ .

$$g \in \text{Ker}(\tau) \iff \tau_g = I_G \iff \tau_g(x) = I_G(x) , \quad \forall x \in G \iff$$

$$\iff gxg^{-1} = x , \quad \forall x \in G \iff gx = xg , \quad \forall x \in G$$



$$\iff g \in Z(G) \quad ,$$

όπου $Z(G)$ το κέντρο της ομάδας G (Βλέπε Παράδ.10, Κεφ. II 2.1.) .

Επομένως $\text{Ker}(\tau) = Z(G)$.

Επιπλέον $\text{Im}(\tau) = \text{Inn}(G)$, όπου $\text{Inn}(G)$ η ομάδα των εσωτερικών αυτομορφισμών της G . Οπότε

$$G/Z(G) \cong \text{Inn}(G) \quad .$$

Παράδειγμα 6.

Ας είναι G μια πολ/κή ομάδα και $a \in G$. Η απεικόνιση

$$f: \mathbb{Z} \longrightarrow G \quad , \quad f(n) = a^n \quad , \quad \forall n \in \mathbb{Z} \quad ,$$

είναι ένας ομομορφισμός από την $(\mathbb{Z}, +)$ στην G με

$$\text{Ker}(f) = \{n \in \mathbb{Z} / a^n = 1\} \quad \text{και} \quad \text{Im}(f) = \langle a \rangle \quad .$$

Συνεπώς

$$\mathbb{Z} / \text{Ker}(f) \cong \langle a \rangle$$

Έτσι

1) Αν $\text{Ker}(f) = \{0\}$ δηλαδή το στοιχείο a έχει άπειρη τάξη τότε

$$\mathbb{Z} / \text{Ker}(f) = \mathbb{Z} \quad .$$

2) Αν $\text{Ker}(f) \neq \{0\}$, τότε $\text{Ker}(f) = \langle n \rangle$ δηλαδή το στοιχείο a έχει τάξη n , οπότε $\mathbb{Z} / \langle n \rangle \cong \mathbb{Z}_n$.

Ανακεφαλαιώνοντας , αν το a είναι απείρου τάξης τότε $\langle a \rangle \cong \mathbb{Z}$ ενώ αν έχει πεπερασμένη τάξη n τότε $\langle a \rangle \cong \mathbb{Z}_n$, αποτελέσματα που έχουμε ξαναδεί .

Παράδειγμα 7 .

Θεωρούμε τον επιμορφισμό $p: (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}_n, +) \quad p(k) = \bar{k} \quad ,$
 $\forall k \in \mathbb{Z}$. Έχουμε



$$\begin{aligned} \text{Ker}(p) &= \{x/x \in \mathbb{Z}, h(x) = \bar{0}\} = \{x/x \in \mathbb{Z}, \bar{x} = \bar{0}\} = \\ &= \{x/x \in \mathbb{Z}, x = \lambda n, \lambda \in \mathbb{Z}\} = \{n\lambda/\lambda \in \mathbb{Z}\} = \langle n \rangle. \end{aligned}$$

Έτσι ,

$$\mathbb{Z} / \langle n \rangle \cong \mathbb{Z}_n.$$

Το θεμελιακό θεώρημα των ομομορφισμών συχνά αναφέρεται και σαν πρώτο θεώρημα ισομορφισμών .

Στην συνέχεια , θα δώσουμε το δεύτερο και τρίτο θεώρημα ισομορφισμών .

ΘΕΩΡΗΜΑ 11 (Δεύτερο θεώρημα ισομορφισμών)

Αν K και H είναι δύο υποομάδες μιας ομάδας G με την $H \trianglelefteq G$ τότε

$$K / H \cap K \cong HK / H$$

Απόδειξη .

Αρχικά παρατηρούμε ότι οι ομάδες πηλίκου $K / H \cap K$ και HK / H ορίζονται αφού ,

$$H \cap K \trianglelefteq K \quad \text{και} \quad H \trianglelefteq HK = H \vee K \quad (\text{βλέπε Πρότ. 31, Κεφ. II}) .$$

Θεωρούμε τώρα την απεικόνιση $f = p \circ i$

$$K \xrightarrow{i} HK \xrightarrow{p} HK / H$$

όπου $i(k) = k$, $\forall k \in K$ αφού $K < HK$, και p η κανονική προβολή .
Έτσι $f(k) = Hk$, $\forall k \in K$. Η f είναι προφανώς ένας ομομορφισμός με

$$\begin{aligned} \text{Ker} f &= \{k/k \in K \text{ και } f(k) = H\} = \{k/k \in K \text{ και } Hk = H\} = \\ &= \{k/k \in K \text{ και } k \in H\} = H \cap K . \end{aligned}$$



Από το θεμελιακό θεώρημα των ομομορφισμών έχουμε

$$K/H \cap K \simeq \text{Im}(f) .$$

Θα δείξουμε ότι ο f είναι επιμορφισμός δηλαδή ότι $\text{Im}(f) = HK/H$.

Πραγματικά, κάθε στοιχείο της ομάδας HK/H είναι της μορφής $H(hk)$ για κάποια $h \in H$, $k \in K$ και επί πλέον

$$H(hk) = (Hh) \cdot (Hk) = H \cdot Hk = Hk ,$$

οπότε ,

$$f(k) = H \cdot (hk) .$$

Τελικά

$$K/H \cap K \simeq HK/H . \blacksquare$$

Παρατήρηση .

Στην περίπτωση που η ομάδα G είναι προσθετική από το δεύτερο θεώρημα των ομομορφισμών έχουμε

$$K/H \cap K \simeq H+K/H .$$

Παράδειγμα 8 .

Θεωρούμε τις κυκλικές υποομάδες $\langle 3 \rangle = 3\mathbb{Z}$, $\langle 4 \rangle = 4\mathbb{Z}$ της ομάδας $(\mathbb{Z}, +)$. Οι $\langle 3 \rangle$, $\langle 4 \rangle$ είναι κανονικές υποομάδες της αφού η $(\mathbb{Z}, +)$ είναι αβελιανή .

Το παραπάνω θεώρημα μας λέει ότι

$$\langle 3 \rangle / \langle 3 \rangle \cap \langle 4 \rangle \simeq \langle 3 \rangle + \langle 4 \rangle / \langle 4 \rangle$$

δηλαδή ότι

$$\langle 3 \rangle / \langle 12 \rangle \simeq \mathbb{Z} / \langle 4 \rangle$$

αφού

$$\langle 3 \rangle \cap \langle 4 \rangle = \langle 12 \rangle \text{ και } \langle 3 \rangle + \langle 4 \rangle = \langle 1 \rangle = \mathbb{Z} \text{ (Άσκηση) .}$$



Βασική Παρατήρηση .

Από το παραπάνω θεώρημα μπορούμε να βρούμε την τάξη της υποομάδας HK όταν η ομάδα G είναι πεπερασμένης τάξης .

Έτσι έχουμε,

$$|K / H \cap K| = |HK / H|$$

και από το θεώρημα του Langrange $\frac{|K|}{|H \cap K|} = \frac{|HK|}{|H|}$

οπότε ,

$$\boxed{|HK| = \frac{|H||K|}{|H \cap K|}} \quad (*)$$

Η $(*)$ ισχύει στην περίπτωση που $H \trianglelefteq G$, (ή όταν $K \trianglelefteq G$) . Μπορούμε όμως να δείξουμε ότι η $(*)$ ισχύει και στην περίπτωση όπου οι H, K είναι απλά υποομάδες της G . (Σημειώνουμε ότι σ'αυτή την περίπτωση το σύνολο HK δεν είναι απαραίτητα υποομάδα της G) . (Άσκηση)

ΘΕΩΡΗΜΑ 12 . (Τρίτο θεώρημα ισομορφισμών) .

Αν H και K είναι κανονικές υποομάδες μιας ομάδας G έτσι ώστε $K \leq H$ τότε $H/K \trianglelefteq G/K$ και

$$G/K / H/K \cong G/H .$$

Απόδειξη .

Ορίζουμε την απεικόνιση $f : G/K \longrightarrow G/H$ ως εξής

$$f(Kx) = Hx \quad \forall x \in G .$$

Η f είναι καλά ορισμένη . Θα δείξουμε ότι αν $Kx = Ky$ τότε

$$f(Kx) = f(Ky) \quad \text{δηλαδή} \quad Hx = Hy .$$

Πραγματικά , $Kx = Ky \iff xy^{-1} \in K \leq H$ επομένως $Hx = Hy$. Η f είναι ένας επιμορφισμός . Πραγματικά ,



$$f(Kx)(ky)) = f(kxy) = Hxy = (Hx) \cdot (Hy) = f(kx) \cdot (f(ky))$$

για κάθε $kx, ky \in G/K$, ενώ είναι φανερό επί .

Στη συνέχεια θα βρούμε τον $\text{Ker} f$. Είναι

$$Kx \in \text{Ker} f \iff f(Kx) = H \iff Hx = H \iff x \in H$$

έτσι

$$\text{Ker} f = \{Kx / x \in H\} = H/K$$

συνεπώς

$$H/K \trianglelefteq G/K .$$

Σύμφωνα τώρα με το θεμελιώδες θεώρημα ομομορφισμού

$$G/K / H/K \cong \text{Im}(f) = G/H . \blacksquare$$

Παράδειγμα 9 .

Στην ομάδα Q_8 των κουατερνίων όλες οι υποομάδες της είναι κανονικές . (Βλέπε παραδ. 4, Κεφ. II, 8.) .

Θεωρούμε τις υποομάδες $H = \langle J \rangle = \{I_2, J, J^2, J^3\}$ και $K = \{I_2, J^2\}$. Είναι $K \leq H$, οπότε σύμφωνα με το παραπάνω θεώρημα $\langle J \rangle / K \trianglelefteq Q_8 / K$ και

$$Q_8 / K / \langle J \rangle / K \cong Q_8 / \langle J \rangle .$$

Αλλά και από τις τάξεις των ομάδων πηλίκων μπορεί κανείς να διαπιστώσει ότι οι ομάδες πηλίκων

$$Q_8 / K / \langle J \rangle / K \text{ και } Q_8 / \langle J \rangle \text{ είναι ισομορφες .}$$

Λήμμα 2 .

Αν $f: G \longrightarrow G'$ είναι ένας ομομορφισμός ομάδων και H μια υποομάδα της G που περιέχει τον πυρήνα της f δηλαδή $\text{Ker} f \subseteq H$ τότε

$$f^{-1}(f(H)) = H .$$



Απόδειξη .

Από τον ορισμό της αντίστροφης εικόνας υποσυνόλου έχουμε

$$H \subseteq f^{-1}(f(H)) .$$

Απ' την άλλη μεριά αν $x \in f^{-1}(f(H))$ τότε $f(x) \in f(H)$ δηλαδή $f(x) = f(h)$ για κάποιο $h \in H$. Έτσι

$$f(x)[f(h)]^{-1} = f(xh^{-1}) = 1$$

δηλαδή $xh^{-1} \in \text{Ker} f \subseteq H$ οπότε $(xh^{-1})h \in H$ δηλαδή $x \in H$.

Επομένως $f^{-1}(f(H)) \subseteq H$, πράγμα που επιθυμούσαμε . ■

ΘΕΩΡΗΜΑ 13 .

Έστω $f: G \longrightarrow G'$ ένας επιμορφισμός ομάδων . Αν $\mathcal{L}_f(G)$ είναι το σύνολο όλων των υποομάδων H της G με $\text{Ker} f \subseteq H$ και $\mathcal{L}(G')$ το σύνολο όλων των υποομάδων της G' τότε η απεικόνιση

$$\Psi: \mathcal{L}_f(G) \longrightarrow \mathcal{L}(G') , \quad H \longmapsto f(H)$$

είναι 1-1 και επί .

Επιπλέον αν $H \in \mathcal{L}_f(G)$ τότε

$$f(H) \trianglelefteq G' \text{ εάν-ν } H \trianglelefteq G$$

και έτσι

$$G/H \cong G'/f(H) .$$

Απόδειξη .

Η Ψ είναι καλά ορισμένη αφού η εικόνα $f(H) \trianglelefteq G'$. (Προτ.7, Κεφ. II) .

Η Ψ είναι ένεση . Πραγματικά , αν $f(H) = f(H_1)$ τότε

$f^{-1}[f(H)] = f^{-1}[f(H_1)]$ δηλαδή $H = H_1$ σύμφωνα με το παραπάνω λήμμα .

Η Ψ είναι επί . Αν $K \in \mathcal{L}(G')$ τότε $f^{-1}(K) \trianglelefteq G$ και μάλιστα

$\text{Ker} f \subseteq f^{-1}(K)$. Επειδή η f είναι επί έχουμε

$$f(f^{-1}(K)) = K$$



πράγμα που επιθυμούσαμε .

$H \cong \Psi$ είναι λοιπόν 1-1 και επί . (Η αντίστροφη της είναι η $\Psi^{-1}: \mathcal{L}(G') \longrightarrow \mathcal{L}_f(G)$, $K \longmapsto f^{-1}(K)$.)

Έστω $H \in \mathcal{L}_f(G)$.

Αν $H \trianglelefteq G$ τότε $f(H) \trianglelefteq G'$ αφού ο f είναι επιμορφισμός (Βλέπε Προτ. 29, Κεφ. II) .

Απ' την άλλη μεριά αν $f(H) \trianglelefteq G'$ τότε $f^{-1}(f(H)) = H$ σύμφωνα με το παραπάνω λήμμα , επομένως $H \trianglelefteq G$ (Βλέπε Προτ. 29 , II.)

Μένει να δείξουμε ότι αν $H \in \mathcal{L}_f(G)$ και $H \trianglelefteq G$ τότε

$$G/H \cong G'/f(H)$$

θεωρούμε την απεικόνιση $p \circ f$

$$G \xrightarrow{f} G' \xrightarrow{p} G'/f(H)$$

Η $p \circ f$ είναι φανερά ένας επιμορφισμός με

$$\begin{aligned} \text{Ker}(p \circ f) &= \{x/x \in G \text{ , } (p \circ f)(x) = f(H)\} = \\ &= \{x/x \in G \text{ , } p(f(x)) = f(H)\} = \\ &= \{x/x \in G \text{ , } [f(H)]f(x) = f(H)\} = \{x/x \in G \text{ , } f(x) \in f(H)\} = \\ &= \{x/x \in G \text{ , } x \in H\} = H \text{ .} \end{aligned}$$

Σύμφωνα λοιπόν με το θεμελιακό θεώρημα

$$G/H \cong \text{Im}(p \circ f) \cong G'/f(H) \text{ .} \blacksquare$$

Η μορφή των υποομάδων μιας ομάδας ηλίκου δίνεται από το επόμενο πρόγραμμα .

ΠΟΡΙΣΜΑ 2 .

Αν H είναι μια κανονική υποομάδα μιας ομάδας G , τότε κάθε υποομάδα της ομάδας ηλίκου G/H είναι της μορφής K/H όπου $K \leq G$ τέτοια ώστε $H \subseteq K$. Επιπλέον η $K/H \trianglelefteq G/H$ εάν και μόνο εάν $K \trianglelefteq G$.



Απόδειξη .

Θεωρούμε την κανονική προβολή $p: G \longrightarrow G/H$. Η p είναι ένας επιμορφισμός με $\text{Ker } p = H$. Σύμφωνα με το προηγούμενο θεώρημα αν $J \leq G/H$ θα υπάρξει υποομάδα $K \leq G$ με $H \subseteq K$ έτσι ώστε $p(K) = J$ δηλαδή

$$p(K) = \{Hx / x \in K\} = K/H = J \quad ,$$

ενώ $K/H \trianglelefteq G/H \iff K \trianglelefteq G$. ■

Παράδειγμα 10 .

Οι υποομάδες της $S_3 = \{(1), (1\ 2\ 3), (1\ 3\ 2), (1\ 2), (1\ 3), (2\ 3)\}$ είναι οι $A_3 = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$, $H_1 = \{(1), (1\ 3)\}$, $H_2 = \{(1), (2\ 3)\}$, $\{(1)\}$ και η S_3 . Είναι $A_3 \trianglelefteq S_3$. Θεωρούμε την κανονική προβολή $p: S_3 \longrightarrow S_3/A_3$ με $\text{Ker } p = A_3$. Οι υποομάδες της S_3 που περιέχουν τον πυρήνα A_3 είναι η A_3 και η S_3 , ενώ , επειδή $|S_3/A_3| = 2$ οι υποομάδες της είναι οι $\{A_3\}$ και η S_3/A_3 , οπότε η αντιστοιχία αυτή είναι η εξής :

$$A_3 \longmapsto A_3/A_3 = \{A_3\}$$

$$S_3 \longmapsto S_3/A_3 \quad .$$



ΚΕΦΑΛΑΙΟ III

ΔΑΚΤΥΛΙΟΙ - ΣΗΜΑΤΑ

§1.1. Δακτύλιοι

Ορισμός . Ένας δακτύλιος είναι ένα σύνολο R μαζί με δύο πράξεις, μια "πρόσθεση" $(x,y) \longmapsto x+y$ και ένα "πολ/σμός" $(x,y) \longmapsto xy$ έτσι ώστε :

(i) Το ζεύγος $(R,+)$ να είναι αβελιανή ομάδα .

(ii) Ο πολ/σμός είναι προσεταιριστικός :

$$x(yz) = (xy)z \quad \text{για κάθε } x,y,z \in R$$

(iii) Ο πολ/σμός είναι επιμεριστικός ως προς την πρόσθεση :

$$x(y+z) = xy+xz$$

$$\text{για κάθε } x,y,z \in R .$$

$$(x+y)z = xz+yz$$

Θα καλούμε ένα δακτύλιο R .

Αντιμεταθετικό , αν $xy = yx$ για κάθε $x,y \in R$

Δακτύλιο με μονάδα , αν υπάρχει στοιχείο $1_R \in R$ τέτοιο ώστε :

$$x1_R = x = 1_R x \quad \text{για κάθε } x \in R ,$$

μ'άλλα λόγια αν το σύνολο R μαζί με τον πολ/σμό είναι ένα μονοειδές.



Πεπερασμένο , αν το σύνολο R είναι πεπερασμένο .

Παρατήρηση.

Το ουδέτερο στοιχείο της ομάδας $(R,+)$ καλείται μηδενικό στοιχείο του δακτύλιου R και θα το συμβολίζουμε 0_R ή 0 .

Παράδειγμα 1.

Τα σύνολα $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ των ακεραίων , ρητών , πραγματικών και μιγαδικών αριθμών αντίστοιχα , εφοδιασμένα με την συνηθισμένη πρόσθεση και πολ/σμό είναι δακτύλιοι και μάλιστα αντιμεταθετικού με μονάδα .

Παράδειγμα 2.

Το σύνολο $M_{n \times n}$ όλων των $n \times n$ πινάκων με στοιχεία από το $\mathbb{Q}$ ή $\mathbb{R}$ ή $\mathbb{C}$, εφοδιασμένο με τις γνωστές από την Γραμμική Άλγεβρα πράξεις , πρόσθεσης και πολ/σμού πινάκων , γίνεται δακτύλιος με μονάδα μη- αντιμεταθετικός.

Παράδειγμα 3.

Το σύνολο $R = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} / a, b \in \mathbb{Z} \right\}$ εφοδιασμένο με τις γνωστές πράξεις πρόσθεσης και πολ/σμού 2×2 πινάκων με στοιχεία ακεραίους , δομείται σε δακτύλιο χωρίς μονάδα . Ο R δεν είναι αντιμεταθετικός .

Υπάρχουν βέβαια και πεπερασμένοι δακτύλιοι.

Παράδειγμα 4.

Για κάθε θετικό αλλά σταθερό ακέραιο m , το σύνολο

$$\mathbb{Z}_m = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-1}\}$$

όλων των modulo m κλάσεων ισοδυναμίας , εφοδιασμένο με τις παρακάτω πράξεις (βλέπε Κεφ.0) .



$$\bar{a} + \bar{b} = \overline{a+b}$$

$$\bar{a} - \bar{b} = \overline{a-b}$$

για κάθε $\bar{a}, \bar{b} \in \mathbb{Z}_m$

γίνεται ένας αντιμεταθετικός δακτύλιος με μονάδα .

Ένα σύνολο μπορεί να γίνει δακτύλιος με πολλούς τρόπους .
Πραγματικά .

Παράδειγμα 5 .

Στο σύνολο $\mathbb{Z}$ ορίζουμε δύο πράξεις πρόσθεσης και πολ/σμού ως
εξής : για κάθε $x, y \in \mathbb{Z}$

$$x \oplus y = x+y-1 \quad \text{και} \quad x \odot y = x+y-xy \quad .$$

Το σύνολο $\mathbb{Z}$ των ακεραίων με τις παραπάνω πράξεις γίνεται δακτύλιος
με μηδενικό στοιχείο το 1 και μονάδα το 0 ! ! .

Παράδειγμα 6 . (Δακτύλιος των πολωνύμων $R[X]$)

Ας είναι R ένας δακτύλιος και έστω $R[X]$ το σύνολο των πολυ-
νύμων μιας απροσδιόριστης μεταβλητής X με συντελεστές από τον δακτύ-
λιο R .

Δύο πολυώνυμα του $R[X]$.

$$P(X) = a_0 + a_1 X + \dots + a_n X^n \quad \text{και} \quad Q(X) = b_0 + b_1 X + \dots + b_m X^m$$

είναι ίσα εάν και μόνο εάν $m=n$ και $a_0 = b_0, \dots, a_n = b_n$.

Το σύνολο $R[X]$ εφοδιασμένο με τις γνωστές μας πράξεις πρόσθεσης
και πολ/σμού πολωνύμων δομείται σε δακτύλιο , που τον καλούμε δακτύ-
λιο των πολωνύμων μιας απροσδιόριστης με συντελεστές από το δακτύλιο R .

Θα παρατηρήσουμε εδώ ότι αν ο R έχει μονάδα 1_R , τότε και ο
δακτύλιος $R[X]$ έχει μονάδα το σταθερό πολυώνυμο 1_R ενώ , αν ο R
είναι αντιμεταθετικός τότε , και ο $R[X]$ είναι αντιμεταθετικός .



Παράδειγμα 7 . (Δακτύλιος του Gauss) .

θεωρούμε το σύνολο

$$\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\} \quad (i^2 = -1) .$$

Παρατηρούμε ότι για κάθε $a+bi, c+di \in \mathbb{Z}[i]$ έχουμε ,

$$(a+bi) + (c+di) = (a+c) + (b+d)i \in \mathbb{Z}[i]$$

$$(a+bi) \cdot (c+di) = (ac-bd) + (ad+bc)i \in \mathbb{Z}[i] ,$$

μ'άλλα λόγια , το σύνολο $\mathbb{Z}[i]$ είναι κλειστό ως προς τις πράξεις πρόσθεσης και πολ/σμού μεγάλων αριθμών .

Εφοδιασμένο μ'αυτές το $\mathbb{Z}[i]$ δομείται σε αντιμεταθετικό δακτύλιο με μονάδα . Τα στοιχεία του $\mathbb{Z}[i]$ καλούνται **ακέραιοι του Gauss** και ο δακτύλιος $\mathbb{Z}[i]$ **δακτύλιος του Gauss** .

Παράδειγμα 8 .

Αν X είναι ένα μη-κενό σύνολο και R ένας δακτύλιος τότε , το σύνολο $\text{Hom}(X, R)$ όλων των απεικονίσεων του X στο R δομείται σε δακτύλιο με τον ακόλουθο τρόπο :

Για κάθε $f, g \in \text{Hom}(X, R)$

το άθροισμα $f+g: X \longrightarrow R$ ορίζεται ως εξής :

$$(f+g)(x) = f(x) + g(x) \quad \text{για κάθε } x \in X$$

το γινόμενο $fg: X \longrightarrow R$ ορίζεται ως εξής :

$$(fg)(x) = f(x)g(x) \quad \text{για κάθε } x \in X .$$

Το μηδενικό στοιχείο του δακτύλιου $\text{Hom}(X, R)$ είναι η απεικόνιση $0: X \longrightarrow R$, $0(x) = 0_R$, για κάθε $x \in X$, ενώ το αντίθετο του στοιχείου $f: X \longrightarrow R$ είναι η απεικόνιση

$$-f: X \longrightarrow R , \quad (-f)(x) = -f(x) \quad \text{για κάθε } x \in X .$$

θα παρατηρήσουμε εδώ ότι οι αλγεβρικές ιδιότητες του δακτυλίου



$\text{Hom}(X, R)$ ορίζονται από τις ιδιότητες του R .

Για παράδειγμα, αν ο R έχει μονάδα 1_R τότε και ο δακτύλιος $\text{Hom}(X, R)$ έχει μονάδα την απεικόνιση

$$I : X \longrightarrow R, \quad I(x) = 1_R \quad \text{για κάθε } x \in X,$$

ενώ, αν ο R είναι αντιμεταθετικός όμοια είναι και ο $\text{Hom}(X, R)$.

Παράδειγμα 9. (Ευθύ άθροισμα δακτυλίων)

Έστω $R_1, \dots, R_n$ ένας πεπερασμένος αριθμός δακτυλίων (όχι αναγκαία διακεκριμένων). Το σύνολο,

$$R_1 \times \dots \times R_n = \prod_{i=1}^n R_i = \{(r_1, \dots, r_n) / r_i \in R_i, \quad i=1, \dots, n\}$$

εφοδιασμένο με τις πράξεις "πρόσθεση και πολ/σμός συνιστώσα με συνιστώσα"

$$(r_1, \dots, r_n) + (r'_1, \dots, r'_n) = (r_1 + r'_1, \dots, r_n + r'_n)$$

$$(r_1, \dots, r_n) \cdot (r'_1, \dots, r'_n) = (r_1 r'_1, \dots, r_n r'_n)$$

δομείται σε δακτύλιο που καλείται ευθύ άθροισμα των $R_1, \dots, R_n$ και συμβολίζεται $R_1 \oplus \dots \oplus R_n$.

Είναι φανερό ότι, το ευθύ άθροισμα $R_1 \oplus \dots \oplus R_n$ είναι αντιμεταθετικός δακτύλιος εάν και μόνο εάν κάθε παράγοντας R_i είναι αντιμεταθετικός δακτύλιος. Όμοια αυτό έχει μονάδα εάν και μόνο εάν κάθε δακτύλιος R_i έχει μονάδα.

§1.2. Στοιχειώδεις ιδιότητες δακτυλίων.

Πρόταση 1.

Αν R είναι ένας δακτύλιος, τότε και για κάθε $x, y, z \in R$ έχουμε

$$i) \quad 0_R x = 0_R = x 0_R$$



$$\text{ii)} (-x)y = x(-y) = -(xy)$$

$$\text{iii)} (-x)(-y) = xy$$

Απόδειξη .

$$\text{i)} 0_R x = (0_R + 0_R)x = 0_R x + 0_R x \quad \text{οπότε} \quad 0_R x = 0_R$$

$$\text{Όμοια} \quad x 0_R = 0_R$$

$$\text{ii)} xy + x(-y) = x(y + (-y)) = x 0_R = 0_R \quad \text{επομένως και} \quad x(-y) + xy = 0_R$$

Από την μοναδικότητα του αντιθέτου στοιχείου του xy παίρνουμε

$$-(xy) = x(-y)$$

$$\text{Όμοια} \quad \text{δείχνουμε ότι} \quad -(xy) = (-x)y$$

$$\text{iii)} (-x)(-y) \stackrel{(\text{ii})}{=} -(-x)y \stackrel{(\text{ii})}{=} -(-(xy)) = xy \quad \blacksquare$$

Ας είναι τώρα R ένας δακτύλιος , και $x_1, \dots, x_v$, $y_1, \dots, y_k$ τυχόντα στοιχεία του . Εργαζόμενοι επαγωγικά παίρνουμε ότι :

$$(x_1 + \dots + x_v)(y_1 + \dots + y_k) = \left(\sum_{i=1}^v x_i \right) \left(\sum_{j=1}^k y_j \right) = \sum_{i=1}^v \sum_{j=1}^k x_i y_j$$

Τον δακτύλιο $R = \{0\}$ που αποτελείται από ένα μόνο στοιχείο τον καλούμε τετριμμένο δακτύλιο .

Αν λοιπόν R είναι ένας δακτύλιος με μονάδα 1_R και είναι διαφορετικός από τον τετριμμένο δακτύλιο , τότε $1_R \neq 0_R$.

Πραγματικά , αν $1_R = 0_R$ τότε για κάθε $x \in R$ θα είχαμε $x = 1_R x = 0_R x = 0_R$ δηλαδή $R = \{0\}$, άτοπο .

Σ' ένα δακτύλιο R , μπορούμε να ορίσουμε τα ανέρρια πολ/σια ενός οποιουδήποτε στοιχείου του x , όπως ακριβώς και στις προσθετικές ομάδες , δηλαδή

$$0x = 0_R \quad , \quad 1x = x \quad , \dots \quad , \quad nx = \underbrace{x + \dots + x}_{n\text{-φορές}}$$



και

$$(-n)x = n(-x) = -(nx) \quad \text{για κάθε } n \in \mathbb{Z}^+$$

Είναι εύκολο να διαπιστώσουμε ότι για κάθε $x, y \in R$ και $m, n \in \mathbb{Z}$ έχουμε

$$(1) \quad n(x+y) = nx+ny$$

$$(2) \quad (n+m)x = nx+mx$$

$$(3) \quad (nx)y = n(xy) = x(ny) \quad (\text{'Άσκηση})$$

$$(4) \quad (nm)x = n(mx)$$

$$(5) \quad (nx)(my) = (nm)(xy)$$

Παρατήρηση .

Το nx δεν είναι γενικά το γινόμενο δυο στοιχείων του δακτυλίου R . Στην περίπτωση όμως που ο R έχει μονάδα 1_R , το nx παριστά το γινόμενο δύο στοιχείων του R αφού

$$nx = (n 1_R) x \quad .$$

Σ'ένα δακτύλιο R αφού ο πολ/σμός είναι προσεταιριστικός μπορούμε να ορίσουμε τις φυσικές δυνάμεις ενός οποιουδήποτε στοιχείου του x ως εξής :

$$x^1 = x \quad , \quad x^2 = xx \quad , \dots , \quad x^n = \underbrace{xx \dots x}_{n\text{-φορές}}$$

Έχουμε τους επόμενους κανόνες :

$$(6) \quad x^n \cdot x^m = x^{n+m}$$

$$(7) \quad (x^n)^m = x^{nm} \quad .$$

Η παρακάτω πρόταση είναι πολύ χρήσιμη στους υπολογισμούς μας . Υπενθυμίζουμε ότι για ακραίους n, k με $0 \leq k \leq n$, έχουμε



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

(όπου $0! = 1$, $1! = 1$ και $n! = 1 \cdot 2 \cdot \dots \cdot (n-1)n$ για $n > 1$) ενώ , ο

$\binom{n}{k}$ είναι πάντα ένας ακέραιος .

Πρόταση 2 . (Τύπος του διωνύμου)

Ας είναι R ένας δακτύλιος και x, y δύο στοιχεία του που αντιμετατίθενται δηλαδή $xy = yx$. Τότε για κάθε θετικό ακέραιο n έχουμε ,

$$(x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \dots + \binom{n}{k}x^{n-k}y^k + \dots + \binom{n}{n}y^n .$$

Απόδειξη .

Η πρόταση ισχύει για $n=1$. Πραγματικά , $(x+y)^1 = x+y = \binom{1}{0}x + \binom{1}{1}y$. Υποθέτουμε ότι ισχύει για τον φυσικό αριθμό n . Θα έχουμε ,

$$\begin{aligned} (x+y)^{n+1} &= (x+y)^n(x+y) = \left\{ \binom{n}{0}x^n + \dots + \binom{n}{k}x^{n-k}y^k + \dots + \binom{n}{n}y^n \right\} (x+y) = \\ &= \binom{n}{0}x^{n+1} + \left\{ \binom{n}{0} + \binom{n}{1} \right\} x^n y + \dots + \left\{ \binom{n}{k-1} + \binom{n}{k} \right\} x^{(n+1)-k} y^k + \\ &+ \dots + \binom{n}{n} y^{n+1} . \end{aligned}$$

$$\text{Αλλά } \binom{n}{0} = 1 = \binom{n+1}{0} , \quad \binom{n}{n} = 1 = \binom{n+1}{n+1} \quad \text{και} \quad \binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1} .$$

Επομένως

$$(x+y)^{n+1} = \binom{n+1}{0}x^{n+1} + \dots + \binom{n+1}{k}x^{(n+1)-k}y^k + \dots + \binom{n+1}{n+1}y^{n+1} .$$

Η πρόταση λοιπόν ισχύει και για τον φυσικό $n+1$, ισχύει επομένως για κάθε φυσικό αριθμό n . ■



Παρατήρηση .

Είναι φανερό ότι ο τύπος του διωνύμου ισχύει για κάθε $x, y \in R$ όταν ο R είναι αντιμεταθετικός δακτύλιος .

Είναι γνωστό ότι στους αριθμητικούς δακτύλιους $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ το γινόμενο δύο μη-μηδενικών στοιχείων τους είναι $\neq 0$ δηλαδή

$$xy = 0 \quad \text{συνεπάγεται} \quad x = 0 \quad \text{ή} \quad y = 0 \quad .$$

Αυτό όμως δεν ισχύει γενικά σε οποιοδήποτε δακτύλιο . Υπάρχουν δηλαδή δακτύλιοι που το γινόμενο δύο μη-μηδενικών στοιχείων τους είναι ίσο με μηδέν !! .

Για παράδειγμα , στον δακτύλιο $\mathbb{Z}_8$ έχουμε $\bar{2} \cdot \bar{4} = \bar{8} = \bar{0}$ και όμως $\bar{2} \neq \bar{0}$ και $\bar{4} \neq \bar{0}$.

Αυτό μας οδηγεί στον παρακάτω ορισμό .

ΟΡΙΣΜΟΣ . Ένα μη-μηδενικό στοιχείο a ενός δακτυλίου R θα λέμε ότι είναι **δεξιός** (αντιστ. **αριστερός**) **διαιρέτης του μηδενός** , αν υπάρχει ένα μη-μηδενικό στοιχείο $b \in R$ τέτοιο ώστε

$$ba = 0_R \quad (\text{αντιστ. } ab = 0_R) \quad .$$

Ένας διαιρέτης του μηδενός στον δακτύλιο R , είναι ένα στοιχείο του που είναι ταυτόχρονα ένας δεξιός και αριστερός διαιρέτης του μηδενός .

Παράδειγμα 10 .

Αν m είναι ένας σύνθετος θετικός ακέραιος , τότε ο δακτύλιος $\mathbb{Z}_m$ είναι δακτύλιος με διαιρέτες του μηδενός .

Πραγματικά , αν $m = m_1 m_2$ με $1 < m_1, m_2 < m$, τότε για τις κλάσεις $\bar{m}_1, \bar{m}_2 \in \mathbb{Z}_m$ έχουμε

$$\bar{m}_1 \bar{m}_2 = \overline{m_1 m_2} = \bar{m} = \bar{0} \quad \text{και} \quad \text{όμοια} \quad \bar{m}_2 \bar{m}_1 = \bar{0}$$



ενώ, $\bar{m}_1 \neq \bar{0}$ και $\bar{m}_2 \neq \bar{0}$.

Παράδειγμα 11.

Ο δακτύλιος $M_{2 \times 2}(\mathbb{C})$ είναι δακτύλιος με διαιρέτες του μηδενός.

Πραγματικά, για τον πίνακα $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ έχουμε

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{και} \quad \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Θα τονίσουμε ιδιαίτερα ότι σε δακτύλιους R χωρίς διαιρέτες του μηδενός, αν $x, y \in R$ τότε

$$xy = 0_R \implies x = 0_R \quad \text{ή} \quad y = 0_R$$

ή διαφορετικά, το γινόμενο δύο μη-μηδενικών στοιχείων του είναι $\neq 0_R$.

Πρόταση 3.

Ένας δακτύλιος R δεν έχει διαιρέτες του μηδενός εάν και μόνο εάν ισχύουν οι νόμοι της απλοποίησης στον R δηλαδή για κάθε $a, b, x \in R$ με $x \neq 0_R$ έχουμε

$$i) \quad xa = xb \implies a = b$$

$$ii) \quad ax = bx \implies a = b.$$

Απόδειξη.

Ας υποθέσουμε ότι ο R δεν έχει διαιρέτες του μηδενός.

Αν $x \neq 0_R$ και $xa = xb$ τότε $xa - xb = x(a - b) = 0_R$ συνεπώς $a - b = 0_R$ οπότε $a = b$.

Όμοια δείχνουμε και το ii).

Απ' την άλλη μεριά, ας υποθέσουμε ότι ισχύουν οι νόμοι της απλοποίησης. Αρκεί να δείξουμε ότι αν $x, y \in R$ και $xy = 0_R$ τότε $x = 0_R$ ή $y = 0_R$.



Πραγματικά αν $x \neq 0_R$ τότε $xy = 0_R = x0_R$ και από την i) έχουμε $y = 0_R$. Αν $y \neq 0_R$ τότε $xy = 0_R = 0_R y$ οπότε από την ii) έχουμε $x = 0_R$. ■

ΟΡΙΣΜΟΣ. Ένας αντιμεταθετικός δακτύλιος με μονάδα $1_R \neq 0_R$ χωρίς διαιρέτες του μηδενός καλείται πεδίο ακεραιότητας ή ακεραία περιοχή.

Σ' ένα πεδίο ακεραιότητας λοιπόν ισχύουν οι νόμοι της απλοποίησης, ενώ το γινόμενο δύο μη-μηδενικών στοιχείων του είναι πάντα $\neq 0_R$.

Ο δακτύλιος $M_{2 \times 2}(\mathbb{C})$ δεν είναι αντιμεταθετικός, συνεπώς δεν είναι πεδίο ακεραιότητας.

Ο δακτύλιος $\mathbb{Z}_m$ (m σύνθετος) ενώ είναι αντιμεταθετικός έχει διαιρέτες του μηδενός, δεν είναι επομένως πεδίο ακεραιότητας.

Μπορούμε όμως να δείξουμε ότι ο δακτύλιος $\mathbb{Z}_m$ είναι πεδίο ακεραιότητας εάν και μόνο εάν ο m είναι πρώτος αριθμός. (Άσκηση)

Παράδειγμα 12.

Οι γνωστοί μας δακτύλιοι $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ είναι πεδία ακεραιότητας.

Παράδειγμα 13.

Αν R είναι ένα πεδίο ακεραιότητας, τότε και ο δακτύλιος των πολωνύμων $R[X]$ είναι πεδίο ακεραιότητας.

Πραγματικά, αφού ο R είναι αντιμεταθετικός δακτύλιος όμοια αντιμεταθετικός είναι και ο δακτύλιος $R[X]$. (Βλέπε Κεφ. III, §1.1, παραδ.6). Επί πλέον αν $P(X) = a_0x + \dots + a_m x^m$, $a_m \neq 0_R$ και

$$Q(X) = b_0 + b_1 X + \dots + b_n X^n, \quad b_n \neq 0_R$$

είναι δύο μη-μηδενικά στοιχεία του $R[X]$, τότε στο γινόμενό τους

$$P(X) \cdot Q(X) = a_0 b_0 + (a_0 b_1 + a_1 b_0)X + \dots + a_n b_m X^{n+m}$$



παρατηρούμε ότι $a_n b_m \neq 0_R$ αφού ο R είναι πεδίο ακεραιότητας δηλαδή

$$P(X) \cdot Q(X) \neq 0$$

που σημαίνει ότι ο $R[X]$ δεν έχει διαιρέτες του μηδενός πράγμα που επιθυμούσαμε .

Παράδειγμα 14 .

Ο δακτύλιος $\mathbb{Z}[i]$ των ακεραίων του Gauss είναι πεδίο ακεραιότητας .

Ο $\mathbb{Z}[i]$ είναι φανερά αντιμεταθετικός δακτύλιος . Επιπλέον αν $a+bi$, $c+di \in \mathbb{Z}[i]$ με $a+bi \neq 0$, τότε εύκολα διαπιστώνουμε ότι η σχέση

$$(a+bi)(c+di) = 0$$

συνεπάγεται $c+di = 0$.

§2. Σώματα .

Ας είναι R ένας δακτύλιος με μονάδα $1_R \neq 0_R$. Ένα στοιχείο $x \in R$ λέγεται αντιστρέψιμο αν υπάρχει στοιχείο $y \in R$ τέτοιο ώστε

$$xy = 1_R = yx .$$

Είναι φανερό ότι το αντίστροφο ενός στοιχείου $x \in R$ (όταν υπάρχει) είναι μοναδικό * θα το συμβολίζουμε x^{-1} .

Στην συνέχεια θα δείξουμε ότι το σύνολο $U(R)$ όλων των αντιστρέψιμων στοιχείων ενός δακτυλίου με μονάδα $1_R \neq 0_R$ αποτελεί ομάδα με πράξη τον πολ/σμό , που είναι γνωστή σαν ομάδα των αντιστρέψιμων στοιχείων του R .

Το σύνολο $U(R) \neq \emptyset$ γιατί $1_R, -1_R \in U(R)$ και είναι κλειστό ως προς τον πολ/σμό, αφού αν $x, y \in U(R)$ τότε $x^{-1}, y^{-1} \in R$ και



$(xy)^{-1} = y^{-1}x^{-1} \in R$ οπότε $xy \in U(R)$.

Ο προσεταιριστικός νόμος πληρούται για τα στοιχεία του $U(R)$ και τέλος, αν $x \in U(R)$ τότε $x^{-1} \in U(R)$ αφού $(x^{-1})^{-1} = x \in R$.

Σ'ένα δακτύλιο με μονάδα $1_R \neq 0_R$ ένα στοιχείο $x \in R$ δεν μπορεί να είναι ταυτόχρονα αντιστρέψιμο και διαιρέτης του μηδενός.

Πραγματικά.

Πρόταση 4.

Σ'ένα δακτύλιο R με μονάδα $1_R \neq 0_R$ κάθε αντιστρέψιμο στοιχείο του δεν είναι διαιρέτης του μηδενός.

Απόδειξη.

Έστω $x \in U(R)$, αρκεί να δείξουμε ότι αν $b \in R$ τέτοιο ώστε

$$bx = 0_R \text{ ή } xb = 0_R \text{ τότε } b = 0_R.$$

Πραγματικά, αν $bx = 0_R$ τότε $(bx)x^{-1} = 0_R x^{-1} = 0_R$ δηλαδή $b = 0_R$.

Όμοια εργαζόμαστε όταν $xb = 0_R$. ■

Παράδειγμα 1.

Στο δακτύλιο Z των ακεραίων, τα μόνα αντιστρέψιμα στοιχεία του είναι το 1 και το -1 έτσι

$$U(Z) = \{1, -1\}.$$

Παράδειγμα 2.

Στον δακτύλιο $M_{n \times n}(C)$. Τα αντιστρέψιμα στοιχεία του είναι όλοι οι $n \times n$ πίνακες A με $\det A \neq 0$ δηλαδή

$$U(M_{n \times n}(C)) = GL_n(C).$$



Παράδειγμα 3 .

Στον δακτύλιο $\mathbb{Z}[i]$ των ακεραίων του Gauss τα μόνα αντιστρέψιμα στοιχεία είναι τα $1, -1, i, -i$ δηλαδή

$$U(\mathbb{Z}[i]) = \{1, -1, i, -i\}$$

Είναι φανερό ότι τα στοιχεία $1, -1, i, -i$ είναι αντιστρέψιμα στοιχεία στον δακτύλιο $\mathbb{Z}[i]$. Θα δείξουμε ότι αυτά είναι όλα τα αντιστρέψιμα στοιχεία του .

Ας υποθέσουμε ότι το στοιχείο $a+bi \in \mathbb{Z}[i]$ είναι αντιστρέψιμο . Θα υπάρξει λοιπόν στοιχείο $c+di \in \mathbb{Z}[i]$ τέτοιο ώστε

$$(a+bi)(c+di) = 1$$

Επομένως και

$$(a-bi)(c-di) = 1$$

οπότε

$$1 = (a+bi)(c+di)(a-bi)(c-di) = (a^2+b^2)(c^2+d^2) \quad (1)$$

Από τη σχέση (1) παίρνουμε

$$a^2+b^2 = 1 \quad (2)$$

αφού $a, b, c, d \in \mathbb{Z}$.

Οι μόνες λύσεις της (2) είναι οι :

$$a = \pm 1, \quad b = 0 \quad \text{ή} \quad a = 0, \quad b = \pm 1 .$$

Τα αντιστρέψιμα στοιχεία είναι τα $\pm 1, \pm i$ δηλαδή

$$U(\mathbb{Z}[i]) = \{1, -1, i, -i\} .$$

Παράδειγμα 4 .

Αν R είναι ένα πεδίο ακεραιότητας , τότε τα αντιστρέψιμα στοιχεία του πεδίου ακεραιότητας $R[X]$ των πολυωνύμων είναι ακριβώς τα αντιστρέψιμα στοιχεία του R , δηλαδή



$$U(R[X]) = U(R) .$$

Είναι φανερό ότι αν το $a \in R$ είναι αντιστρέψιμο στο R τότε αυτό είναι αντιστρέψιμο και στο $R[X]$.

Απ' την άλλη μεριά , αν $P(X)$ είναι ένα αντιστρέψιμο στοιχείο του $R[X]$ τότε υπάρχει $Q(X) \in R[X]$ τέτοιο ώστε

$$P(X) \cdot Q(X) = 1_R \quad (3)$$

Τότε όμως $\deg(P(X)Q(X)) = \deg P(X) + \deg Q(X) = 0$ επομένως $\deg P(X) = 0$ και $\deg Q(X) = 0$, που σημαίνει ότι αυτά είναι σταθερά πολυώνυμα δηλαδή

$$P(X) = a \in R \quad \text{και} \quad Q(X) = b \in R .$$

Από την (3) παίρνουμε ότι $ab = 1_R = ba$ δηλαδή το $a \in R$ είναι αντιστρέψιμο .

Εφαρμόζοντας το παραπάνω έχουμε

$$U(Q[X]) = Q - \{0\} , \quad U(R[X]) = R - \{0\} , \quad U(Z[X]) = \{1, -1\} .$$

Πρόταση 5 .

Ένα μη-μηδενικό στοιχείο $\bar{a} \in \mathbb{Z}_m$ είναι αντιστρέψιμο στον δακτύλιο $\mathbb{Z}_m$ εάν και μόνο εάν $(a, m) = 1$.

Απόδειξη .

Αν $(a, m) = 1$, τότε υπάρχουν ακέραιοι x, y τέτοιοι ώστε $ax + my = 1$. Αυτό δίνει

$$\bar{1} = \overline{ax + my} = \overline{ax} + \overline{my} = \overline{ax} + \bar{0} = \bar{a} \cdot \bar{x}$$

οπότε η κλάση $\bar{x}$ είναι αντίστροφη της $\bar{a}$.

Αντίστροφα , αν $\bar{b}$ είναι η αντίστροφη της κλάσης $\bar{a}$ τότε

$$\bar{a} \bar{b} = \bar{1} = \bar{b} \bar{a} .$$

Έτσι $\bar{a} \bar{b} = \bar{1} \iff ab \equiv 1 \pmod{m}$ δηλαδή $ab - 1 = km$ για κάποιο ακέραιο



k , επομένως $ab+m(-k)=1$ που σημαίνει ότι $(a,m)=1$. ■

Για παράδειγμα $U(\mathbb{Z}_{10}) = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$.

ΟΡΙΣΜΟΣ .

Ένας αντιμεταθετικός δακτύλιος με μονάδα $1_R \neq 0_R$ καλείται σώμα , αν κάθε μη-μηδενικό στοιχείο του είναι αντιστρέψιμο .

Σ' ένα σώμα F λοιπόν το σύνολο των μη-μηδενικών του στοιχείων $F - \{0_F\}$ αποτελεί με πράξη τον πολ/σμό αντιμεταθετική ομάδα .

Οι γνωστού μας δακτύλιοι $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ είναι σώματα ενώ ο δακτύλιος $\mathbb{Z}$ δεν είναι σώμα .

Δεν είναι όμως όλα τα σώματα άπειρα . Πραγματικά ,

Πρόταση 6 .

Ο δακτύλιος $\mathbb{Z}_p$ των ακεραίων $(\text{mod } p)$ είναι σώμα εάν και μόνο εάν ο p είναι πρώτος αριθμός .

Απόδειξη .

Αν ο p είναι πρώτος αριθμός , τότε για κάθε $\bar{a} \in \mathbb{Z}_p - \{\bar{0}\}$ θα είναι $(a,p)=1$, που σημαίνει ότι η κλάση $\bar{a}$ είναι αντιστρέψιμη σύμφωνα με την πρόταση 5 δηλαδή το $\mathbb{Z}_p$ είναι σώμα . Αντίστροφα αν το $\mathbb{Z}_p$ είναι σώμα , τότε κάθε κλάση $\bar{a} \in \mathbb{Z}_p - \{\bar{0}\}$ είναι αντιστρέψιμη , οπότε $(a,p)=1$ σύμφωνα με την πρόταση 5 . Δηλαδή για κάθε $1 \leq a \leq p-1$ είναι $(a,p)=1$ που σημαίνει ότι ο p είναι πρώτος αριθμός . ■

Θα παρατηρήσουμε εδώ ότι :

Κάθε σώμα F (πεπερασμένο ή άπειρο) είναι ένα πεδίο ακεραιότητας .



Πραγματικά το F είναι ένας αντιμεταθετικός δακτύλιος με μονάδα $1_R \neq 0_R$ και τα αντιστρέψιμα στοιχεία του δηλαδή τα στοιχεία του $F - \{0\}$ δεν είναι διαιρέτες του μηδενός σύμφωνα με την πρόταση 4 .

Υπάρχουν όμως πεδία ακεραιότητας που δεν είναι σώματα .

Για παράδειγμα , τα πεδία ακεραιότητας $\mathbb{Z}$ των ακεραίων , και $\mathbb{Z}[i]$ των ακεραίων του Gauss δεν είναι σώματα . Όμοια

Παράδειγμα 5.

Αν F είναι ένα σώμα , τότε το πεδίο ακεραιότητας $F[X]$ των πολυωνύμων με συντελεστές από το σώμα F , δεν είναι σώμα .

Πραγματικά , το F είναι πολύ περισσότερο ένα πεδίο ακεραιότητας επομένως τα μόνα αντιστρέψιμα στοιχεία του πεδίου ακεραιότητας $F[X]$ είναι τα σταθερά μη-μηδενικά πολυώνυμα , δηλαδή

$$U(F[X]) = F - \{0\}$$

Έτσι τα πολυώνυμα $P(X) \in F[X]$ με $\deg P(X) > 1$ δεν είναι αντιστρέψιμα στο $F[X]$. Το $F[X]$ δεν είναι λοιπόν σώμα .

Πεπερασμένα όμως πεδία ακεραιότητας είναι σώματα . Πραγματικά ,

Πρόταση 7 .

Κάθε πεπερασμένο πεδίο ακεραιότητας είναι σώμα .

Απόδειξη .

Ας είναι R ένα πεπερασμένο πεδίο ακεραιότητας και ας είναι $x_1, x_2, \dots, x_n$ όλα τα στοιχεία του . Θα δείξουμε ότι κάθε μη-μηδενικό στοιχείο $x \in R$ είναι αντιστρέψιμο .

Θεωρούμε τα n σε πλήθος στοιχεία του R

$$xx_1, \dots, xx_n$$



Αυτά είναι όλα διακεκριμένα γιατί αν $xx_i = xx_j$ $i \neq j$, τότε ο νόμος απλοποίησης δίνει $x_i = x_j$ άτοπο.

Κάθε στοιχείο λοιπόν του R είναι της μορφής xx_i για κάποιο i . Ιδιαίτερα για το $1_R \in R$ θα έχουμε

$$xx_i = 1_R$$

και από το αντιμεταθετικό νόμο $x_i x = 1_R$ πράγμα που επιθυμούσαμε. ■

Από τα παραπάνω συμπεραίνουμε ότι οι έννοιες "πεδίο ακεραιότητας" και "αύμα" ταυτίζονται για πεπερασμένους δακτύλιους.

Ορισμός.

Ένας δακτύλιος R με μονάδα $1_R \neq 0_R$ στον οποίο κάθε μη-μηδενικό στοιχείο είναι αντιστρέψιμο καλείται δακτύλιος με διαίρεση ή σκεβρόσυμα.

Σ' ένα δακτύλιο με διαίρεση R το σύνολο $R - \{0_R\}$ αποτελεί ομάδα με πράξη τον πολ/σμό (όχι απαραίτητα αντιμεταθετική).

Κάθε αύμα (πεπερασμένο ή άπειρο) είναι φανερά ένας δακτύλιος με διαίρεση.

Υπάρχουν όμως δακτύλιοι με διαίρεση που δεν είναι αύματα.

Παράδειγμα 6.

Στον δακτύλιο $M_{2 \times 2}(\mathbb{C})$ θεωρούμε τους πίνακες

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad J = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad K = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{και} \quad L = JK = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Για τους πίνακες αυτούς ισχύει :



$$\left. \begin{aligned} J^2 = K^2 = L^2 = -I & , & JK = -KJ = L \\ KL = -LK = J & , & LJ = -JL = K \end{aligned} \right\} \quad (4)$$

Έστω $Q(\mathbb{R})$ το ακόλουθο υποσύνολο του $M_{2 \times 2}(\mathbb{C})$:

$$\begin{aligned} Q(\mathbb{R}) &= \{ \alpha I + bJ + cK + dL \mid \alpha, b, c, d \in \mathbb{R} \} = \\ &= \left\{ \begin{pmatrix} \alpha + bi & c + di \\ -c + di & \alpha - bi \end{pmatrix} \mid \alpha, b, c, d \in \mathbb{R} \right\} . \end{aligned}$$

Το σύνολο $Q(\mathbb{R})$ είναι κλειστό ως προς τις πράξεις πρόσθεσης και πολ/σμού 2×2 πινάκων και μάλιστα εφοδιασμένο μ'αυτές γίνεται δακτύλιος (μη-αντιμεταθετικός) .

Το μηδενικό στοιχείο και η μονάδα του $Q(\mathbb{R})$ είναι αντίστοιχα οι πίνακες

$$0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} , \quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\text{Αν} \quad x = \begin{pmatrix} \alpha + bi & c + di \\ -c + di & \alpha - bi \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

δηλαδή αν ένα τουλάχιστον από τα α, b, c, d είναι $\neq 0$ τότε

$$\begin{vmatrix} \alpha + bi & c + di \\ -c + di & \alpha - bi \end{vmatrix} = \alpha^2 + b^2 + c^2 + d^2 \neq 0$$

επομένως ο πίνακας

$$x^{-1} = \frac{1}{\alpha^2 + b^2 + c^2 + d^2} \begin{pmatrix} \alpha - bi & -c - di \\ c - di & \alpha + bi \end{pmatrix} \in Q(\mathbb{R})$$

είναι ο αντίστροφος του x .

Ο $Q(\mathbb{R})$ λοιπόν είναι ένας δακτύλιος με διαίρεση αλλά δεν είναι σώμα αφού ο πολ/σμός δεν είναι αντιμεταθετικός . Ο $Q(\mathbb{R})$ ονομάζεται δακτύλιος των πραγματικών κουατερνίων .



Ας δούμε όμως τι συμβαίνει με τους πεπερασμένους δακτυλίους με διαίρεση . Το 1905 ο J.H.M. Wedderburn απόδειξε το επόμενο βασικό θεώρημα

ΘΕΩΡΗΜΑ 1.

Κάθε πεπερασμένος δακτύλιος με διαίρεση είναι σώμα .

Δεν θα δώσουμε εδώ την απόδειξη του γιατί κάτι τέτοιο θα μας οδηγούσε πολύ μακριά .

Έτσι οι έννοιες "δακτύλιος με διαίρεση" και "σώμα" ταυτίζονται για πεπερασμένους δακτυλίους .

§3. Χαρακτηριστική δακτυλίου

Ορισμός .

Ας είναι R ένας δακτύλιος . Αν υπάρχει ελάχιστος θετικός ακέραιος n τέτοιος ώστε

$$nx = 0_R \quad \text{για κάθε } x \in R$$

τότε θα λέμε ότι ο R έχει χαρακτηριστική n και θα το σημειώνουμε $\text{char } R = n$.

Αν τέτοιος θετικός ακέραιος δεν υπάρχει (δηλαδή ο $n=0$ είναι ο μόνος ακέραιος για τον οποίο $nx = 0_R$ για κάθε $x \in R$) τότε θα λέμε ότι ο R είναι χαρακτηριστικής μηδέν. ($\text{char } R = 0$) .

Είναι φανερό τώρα ότι $\text{char } R = 1 \iff R = \{0\}$.

Θα δείξουμε στη συνέχεια ότι σε δακτυλίους R με μονάδα 1_R , η χαρακτηριστική τους είναι πλήρως ορισμένη από τη μονάδα τους . Πραγματικά ,



Πρόταση 8 .

Αν R είναι ένας δακτύλιος με μονάδα 1_R τότε , $\text{char } R = n > 0$ εάν και μόνο εάν ο n είναι ο ελάχιστος θετικός ακέραιος τέτοιος ώστε $n \cdot 1_R = 0_R$.

Απόδειξη .

Αν $\text{char } R = n > 0$, τότε $nx = 0_R$ για κάθε $x \in R$, επομένως $n1_R = 0_R$. Έστω m είναι ακέραιος τέτοιος ώστε $0 < m < n$ και $m1_R = 0_R$.

Τότε για κάθε $x \in R$ έχουμε

$$mx = m(1_R x) = (m1_R)x = 0_R x = 0_R ,$$

άτοπο , αφού ο n είναι ο ελάχιστος θετικός ακέραιος με $nx = 0_R$ για κάθε $x \in R$.

Απ' την άλλη μεριά , αν n είναι ο ελάχιστος θετικός ακέραιος τέτοιος ώστε $n1_R = 0_R$, τότε για κάθε $x \in R$ έχουμε

$$nx = n(1_R x) = (n1_R)x = 0_R x = 0_R ,$$

συνεπώς $\text{char } R = k$ με $0 < k \leq n$.

Τότε όμως $k1_R = 0_R$, και από την υπόθεση μας έχουμε $n \leq k$.

Τελικά $n = k$ πράγμα που επιθυμούσαμε . ■

Παραδείγματα

α) Οι γνωστοί μας δακτύλιοι $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ είναι δακτύλιοι χαρακτηριστικής μηδέν .

β) Ο δακτύλιος $\mathbb{Z}_m$ των modulo m κλάσεων ισοτιμίας είναι χαρακτηριστική m δηλαδή

$$\text{char } \mathbb{Z}_m = m$$

αφού ο m είναι ο ελάχιστος θετικός ακέραιος για τον οποίο ισχύει

$$m\bar{1} = \underbrace{\bar{1} + \dots + \bar{1}}_{m\text{-φορές}} = \overline{1 + \dots + 1} = \bar{m} = \bar{0} .$$



γ) Αν F είναι ένα σώμα τότε για τον δακτύλιο των πολυωνύμων $F[X]$ έχουμε $\text{char } F[X] = \text{char } F$.

Πρόταση 9 .

Αν R είναι ένας δακτύλιος με μονάδα $1_R \neq 0_R$ χωρίς διαιρέτες του μηδενός (ιδιαίτερα όταν ο R είναι πεδίο ακεραιότητας) τότε

$$\text{char } R = 0 \quad \text{ή} \quad \text{char } R = p, \quad p \text{ πρώτος αριθμός.}$$

Απόδειξη .

Έστω $\text{char } R = p \neq 0$. Υποθέτουμε ότι ο p είναι σύνθετος και έστω $p = mn$ με $1 < m, n < p$. Τότε

$$0_R = p1_R = (mn)1_R = (mn)1_R 1_R = (m1_R)(n1_R)$$

Ο R όμως δεν έχει διαιρέτες του μηδενός, επομένως $m1_R = 0_R$ ή $n1_R = 0_R$, άτοπο αφού $m, n < p$ και ο p είναι ο ελάχιστος θετικός ακέραιος με $p1_R = 0_R$. Ο p λοιπόν είναι πρώτος αριθμός. ■

Πόρισμα 1.

Η χαρακτηριστική δακτυλίου με διαίρεση (ιδιαίτερα σώματος) είναι μηδέν ή πρώτος αριθμός. ■

Πρόταση 10 .

Ας είναι R ένα πεδίο ακεραιότητας. Έχουμε

i) Αν $\text{char } R = 0$ τότε όλα τα μη-μηδενικά στοιχεία της προσθετικής ομάδας $(R, +)$ έχουν άπειρη τάξη.

ii) Αν $\text{char } R = p \neq 0$, τότε όλα τα μη-μηδενικά στοιχεία της ομάδας $(R, +)$ έχουν τάξη p .

Απόδειξη .

i) Έστω $\text{char } R = 0$ και $x \in R$, $x \neq 0_R$.



Υποθέτουμε ότι η τάξη του x είναι m τότε

$$0_R = mx = (m1_R)x$$

οπότε $m1_R = 0_R$, επομένως $m = 0$ αφού $\text{char } R = 0$. Το x έχει λοιπόν άπειρη τάξη.

ii) Έστω $\text{char } R = p > 0$ και $x \in R$, $x \neq 0_R$.

Από τον ορισμό της χαρακτηριστικής προκύπτει ότι κάθε στοιχείο $x \in R$, $x \neq 0_R$ θα έχει τάξη m με

$$m \leq p \quad (5)$$

Η σχέση όμως $0_R = mx = (m1_R)x$ μας δίνει $m1_R = 0_R$ αφού ο R δεν έχει διαιρέτες του μηδενός.

Επομένως

$$p \leq m \quad (6)$$

αφού $\text{char } R = p$. Από τις (5) και (6) παίρνουμε $m = p$ πράγμα που επιθυμούσαμε. ■

Πόρισμα 2.

Αν R είναι ένα πεπερασμένο πεδίο ακεραιότητας (επομένως ένα πεπερασμένο σώμα) τότε η χαρακτηριστική του είναι πρώτος αριθμός. ■

Πρόταση 11.

Αν R είναι ένα πεδίο ακεραιότητας (ιδιαίτερα σώμα) με $\text{char } R = p \neq 0$ (ο p πρώτος αριθμός) τότε για κάθε $a, b \in R$ έχουμε

$$(a \pm b)^p = a^p \pm b^p$$

Απόδειξη.

Από τον τύπο του διωνύμου έχουμε

$$(a+b)^p = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k + b^p.$$



Για κάθε k όμως με $1 \leq k \leq p-1$ έχουμε $p \mid \binom{p}{k}$. Πραγματικά,

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} \quad \text{οπότε} \quad p! = \binom{p}{k} k! (p-k)!$$

Ο p όμως διαιρεί τον $p! = 1 \cdot 2 \cdot \dots \cdot p$ συνεπώς $p \mid \binom{p}{k} k! (p-k)!$.

Αλλά $p \nmid k!$ και $p \nmid (p-k)!$ οπότε $p \mid \binom{p}{k}$. Έτσι $\binom{p}{k} a^{p-k} b^k = 0_R$

για κάθε $k=1, \dots, p-1$ αφού $\text{char } R = p$. Τελικά

$$(a+b)^p = a^p + b^p.$$

Θα παρατηρήσουμε τώρα ότι αν $p=2$ τότε $2b=0_R$ δηλαδή $b=-b$ και ότι αν $p>2$ τότε ο p είναι περιττός πρώτος. Έτσι για p πρώτο έχουμε

$$(a-b)^p = (a+(-b))^p = a^p + (-b)^p = a^p - b^p. \quad \blacksquare$$

§4. Υποδακτύλιοι.

Ορισμός.

Έστω R ένας δακτύλιος. Ένα μη-κενό υποσύνολο S του R καλείται υποδακτύλιος του R αν

i) Για κάθε $x, y \in S \implies x-y \in S$

ii) Για κάθε $x, y \in S \implies xy \in S$.

Η σχέση (i) μας βεβαιώνει ότι το $(S, +)$ είναι μια υποομάδα της $(R, +)$, δηλαδή ότι το $(S, +)$ είναι μια ομάδα και μάλιστα αβελιανή και η (ii) ότι το S είναι κλειστό ως προς τον πολ/σμό.

Αφού $S \subseteq R$ η επιμεριστικότητα του πολ/σμού ως προς την προσ-
θεση και ο προσεταιριστικός νόμος του πολ/σμού ισχύουν και για τα
στοιχεία του S .

Από τα παραπάνω συμπεραίνουμε ότι :

Ένα υποσύνολο $S \neq \emptyset$ του R είναι υποδακτύλιος του R εάν



και μόνο εάν το S είναι ένας δακτύλιος με πράξεις τους περιορισμούς της πρόσθεσης και του πολ/σμού του R στο S .

Κάθε δακτύλιος έχει δύο υποδακτύλιους, τον εαυτό του και τον τετριμμένο υποδακτύλιο $\{0_R\}$.

Κάθε υποδακτύλιο S του R τέτοιο ώστε

$$S \neq \{0_R\} \quad \text{και} \quad S \neq R$$

θα τον καλούμε γνήσιο υποδακτύλιο.

Παράδειγμα 1.

Ο δακτύλιος $\mathbb{Z}$ των ακεραίων είναι υποδακτύλιος του δακτυλίου $\mathbb{Q}$ των ρητών· ο $\mathbb{Q}$ είναι υποδακτύλιος του δακτυλίου $\mathbb{R}$ των πραγματικών αριθμών και αυτός με την σειρά του υποδακτύλιος του δακτυλίου $\mathbb{C}$ των μιγαδικών αριθμών.

Παράδειγμα 2. Κάθε δακτύλιος R είναι υποδακτύλιος του δακτυλίου $R[X]$ των πολυωνύμων με συντελεστές από το R .

Παράδειγμα 3. Ο δακτύλιος $\mathbb{Z}$ των ακεραίων είναι υποδακτύλιος του δακτυλίου $\mathbb{Z}[i]$ των ακεραίων του Gauss και αυτός με την σειρά του είναι υποδακτύλιος του δακτυλίου $\mathbb{C}$ των μιγαδικών αριθμών.

Παράδειγμα 4. (Κέντρο δακτυλίου)

Το κέντρο $Z(R)$ ενός δακτυλίου R είναι το σύνολο όλων εκείνων των στοιχείων του R που αντιμετατίθενται με όλα τα στοιχεία του δηλαδή

$$Z(R) = \{z/z \in R \quad \text{και} \quad zx = xz, \quad \forall x \in R\}$$

Είναι εύκολο να διαπιστώσουμε ότι :

Ένας δακτύλιος R είναι αντιμεταθετικός εάν-ν $Z(R) = R$.

Το κέντρο $Z(R)$ είναι υποδακτύλιος του R .



Πραγματικά, $0 \in Z(R)$, οπότε $Z(R) \neq \emptyset$.

Αν $z_1, z_2 \in Z(R)$, τότε για κάθε $x \in R$

$$z_1 x = x z_1 \quad \text{και} \quad z_2 x = x z_2 \quad (7)$$

Συνεπώς

$$(z_1 - z_2)x = z_1 x - z_2 x \stackrel{(7)}{=} x z_1 - x z_2 = x(z_1 - z_2)$$

δηλαδή $z_1 - z_2 \in Z(R)$.

Επίσης

$$\begin{aligned} (z_1 z_2)x &= z_1(z_2 x) \stackrel{(7)}{=} z_1(x z_2) = (z_1 x)z_2 \stackrel{(*)}{=} (x z_1)z_2 = \\ &= x(z_1 z_2) \end{aligned}$$

δηλαδή $z_1 z_2 \in Z(R)$.

Παράδειγμα 5.

Το σύνολο $2\mathbb{Z} = \{2k / k \in \mathbb{Z}\}$ είναι ένας υποδακτύλιος $\mathbb{Z}$ των ακέραιων. Πραγματικά, αν $2m, 2n \in 2\mathbb{Z}$ τότε $(2n) + (2m) = 2(n+m) \in 2\mathbb{Z}$ και $(2n) \cdot (2m) = 2(2nm) \in 2\mathbb{Z}$.

Στο παραπάνω παράδειγμα βλέπουμε ότι $1 \notin 2\mathbb{Z}$. Έτσι :

A) Αν S είναι ένας υποδακτύλιος ενός δακτύλιου R με μονάδα 1_R , είναι δυνατόν $1_R \notin S$.

Συνεχίζοντας παρατηρούμε :

B) Μερικοί υποδακτύλιοι έχουν μονάδα αλλά ο αρχικός δακτύλιος δεν έχει.

Για παράδειγμα, ο δακτύλιος $R = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} / a, b \in \mathbb{Z} \right\}$ (βλέπε Κεφ. III, §1.1, παραδ.3) δεν έχει μονάδα ενώ ο υποδακτύλιος του $S = \left\{ \begin{pmatrix} d & 0 \\ 0 & 0 \end{pmatrix} / d \in \mathbb{Z} \right\}$ έχει μονάδα τον πίνακα $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.

Γ) Ένας δακτύλιος R με μονάδα 1_R μπορεί να έχει ένα υποδακτύλιο S με μονάδα 1_S και $1_S \neq 1_R$.



Για παράδειγμα το ευθύ άθροισμα $R = \mathbb{Z} \oplus \mathbb{Z}$ έχει μονάδα το ζεύγος $(1,1)$. Ένας υποδακτύλιος του είναι ο $\mathbb{Z} \times \{0\} = \{(m,0) / m \in \mathbb{Z}\}$ με μονάδα το ζεύγος $(1,0)$.

Παρατηρούμε ότι $(1,1) \neq (1,0)$. ■

Ας είναι S, T δύο υποδακτύλιοι ενός δακτυλίου R . Ο τετριμμένος υποδακτύλιος $\{0_R\}$ περιέχεται και στους δύο. Θα δείξουμε ότι η τομή τους $S \cap T$ είναι ο μεγαλύτερος υποδακτύλιος του R που περιέχεται και στους δύο. Πραγματικά.

Πρόταση 12.

Αν S, T είναι δύο υποδακτύλιοι ενός δακτυλίου R , τότε και η τομή τους $S \cap T$ είναι υποδακτύλιος του R .

Απόδειξη.

$S \cap T \neq \emptyset$ αφού $0_R \in S \cap T$.

Για κάθε $x, y \in S \cap T$ έχουμε $x, y \in S$ και $x, y \in T$ επομένως

$$x-y \in S, \quad x-y \in T, \quad xy \in S, \quad xy \in T$$

αφού οι S, T είναι υποδακτύλιοι του R . Έτσι

$$x-y \in S \cap T \quad \text{και} \quad xy \in S \cap T$$

πράγμα που επιθυμούσαμε. ■

Είναι φανερό τώρα ότι η $S \cap T$ είναι ο μεγαλύτερος υποδακτύλιος που περιέχεται και στον S και στον T .

Γενικότερα.

Αν $(S_i)_{i \in I}$ είναι μια μη-κενή οικογένεια υποδακτύλιων ενός δακτυλίου R τότε και η τομή τους $\bigcap_{i \in I} S_i$ είναι υποδακτύλιος του R .



Όπως και στις ομάδες έτσι και εδώ ορίζεται ο υποδακτύλιος που παράγεται από ένα υποσύνολο X ενός δακτυλίου R .

Ορισμός. Αν X είναι ένα υποσύνολο ενός δακτυλίου R , η τομή όλων των υποδακτυλίων του R που περιέχουν το X , καλείται υποδακτύλιος παραγόμενος από το X και συμβολίζεται (X) .

Ο (X) είναι ο μικρότερος υποδακτύλιος του R που περιέχει το X με την εξής έννοια :

Αν S είναι ένας υποδακτύλιος του R που περιέχει το X τότε $(X) \subseteq S$.

Σημειώνουμε εδώ ότι τα στοιχεία του υποδακτυλίου (X) είναι της μορφής

$$\sum \pm x_1 x_2 \dots x_r$$

δηλαδή αθροίσματα από πεπερασμένα γινόμενα στοιχείων x_i του X και αντίθετα τέτοιων γινομένων.

Παράδειγμα 6.

Ο υποδακτύλιος που παράγεται από ένα στοιχείο a ενός δακτυλίου R , αποτελείται από όλα τα στοιχεία του R της μορφής

$$n_1 a + n_2 a^2 + \dots + n_k a^k, \quad n_i \in \mathbb{Z} \text{ και } k \in \mathbb{Z}^+.$$

Και στους δακτυλίους ισχύει κάτι ανάλογο με τις ομάδες.

Αν S, T είναι δύο υποδακτύλιοι ενός δακτυλίου R , η ένωση τους $S \cup T$ δεν είναι γενικά υποδακτύλιος του R .

Για παράδειγμα, η ένωση των υποδακτυλίων

$$\mathbb{Z} \times \{0\} \text{ και } \{0\} \times \mathbb{Z}$$

του ευθέως αθροίσματος $\mathbb{Z} \oplus \mathbb{Z}$ δεν είναι υποδακτύλιος του, αφού

$$(1,0) + (0,1) = (1,1) \notin (\mathbb{Z} \times \{0\}) \cup (\{0\} \times \mathbb{Z}).$$



Έτσι η ένωση $S \cup T$ δεν μπορεί γενικά να παύσει τον ρόλο του μικρότερου υποδακτύλιου του R που περιέχει τους S και T .

Ορισμός. Ονομάζουμε **supremum** δύο υποδακτύλων S, T ενός δακτύλιου R (συμβολισμός SVT) τον υποδακτύλιο του R που παράγεται από την ένωση $S \cup T$ δηλαδή

$$SVT = (S \cup T) = \bigcap \{W/W \text{ υποδακτ. του } R \text{ με } S \cup T \subseteq W\}$$

Το **supremum** SVT είναι φανερά ο μικρότερος υποδακτύλιος του R που περιέχει και τον S και τον T .

Θα παρατηρήσουμε εδώ ότι τα στοιχεία του SVT είναι αθροίσματα από πεπερασμένα γινόμενα στοιχείων από τους S και T .

§5. Υποσώματα

Ας είναι F ένα σώμα και S ένας υποδακτύλιος του. Αφού το F είναι ένα πεδίο ακεραιότητας, αν $1_F \in S$ τότε και το S είναι ένα πεδίο ακεραιότητας.

Για παράδειγμα, ο δακτύλιος $\mathbb{Z}[i]$ των ακεραίων του Gauss είναι υποδακτύλιος του σώματος $\mathbb{C}$ των μιγαδικών αριθμών και $1 \in \mathbb{Z}[i]$, είναι λοιπόν το $\mathbb{Z}[i]$ ένα πεδίο ακεραιότητας, αποτέλεσμα που έχουμε ξαναδεί.

Το $\mathbb{Z}[i]$ δεν είναι σώμα.

Πραγματικά, έχουμε δείξει (βλέπε Κεφ. III, §2, Παραδ. 3) ότι τα μόνα αντιστρέψιμα στοιχεία του $\mathbb{Z}[i]$ είναι τα $1, -1, i, -i$. Αν λοιπόν $a+bi \in \mathbb{Z}[i]$ με $a, b \neq 0$ τότε $(a+bi)^{-1} = \frac{1}{a+bi} \in \mathbb{C}$ αλλά

$$(a+bi)^{-1} \notin \mathbb{Z}[i].$$

Υπάρχουν όμως υποδακτύλιοι σωμάτων που είναι σώματα.

Ορισμός. Έστω F ένα σώμα και F' ένα μη-κενό υποσύνολο του F που περιέχει ένα τουλάχιστο μη-μηδενικό στοιχείο του F . Το F'



είναι ένα υπόσωμα του F εάν

$$i) \text{ Για κάθε } a, b \in F' \implies a-b \in F'$$

$$ii) \text{ Για κάθε } a, b \in F' \text{ με } b \neq 0_F \implies ab^{-1} \in F' .$$

Είναι φανερό ότι ένα υπόσωμα του σώματος F είναι ένας υποδακτύλιος F' του F τέτοιος ώστε :

$$iii) \text{ Για κάθε } b \in F', b \neq 0_F \text{ να είναι } b^{-1} \in F' .$$

Θα παρατηρήσουμε εδώ ότι τα στοιχεία $0_F, 1_F$ ενός σώματος F ανήκουν σε κάθε υπόσωμά του .

Όπως και στους υποδακτύλιους έτσι και εδώ :

Η τομή δύο υποσωμάτων K, L ενός σώματος F είναι ένα υπόσωμα του F .

Πραγματικά , η τομή τους $K \cap L$ είναι ένας υποδακτύλιος του F , εκείνο που μένει να δείξουμε είναι ότι αν $x \in K \cap L$ τότε και $x^{-1} \in K \cap L$ που είναι φανερό .

Παράδειγμα 1 .

Το σώμα $\mathbb{Q}$ των ρητών είναι υπόσωμα του σώματος $\mathbb{R}$ των πραγματικών αριθμών και αυτό με την σειρά του υπόσωμα του σώματος $\mathbb{C}$ των μιγαδικών αριθμών .

Παράδειγμα 2 .

Το σύνολο

$$\mathbb{Q}[\sqrt{5}] = \{a+b\sqrt{5} / a, b \in \mathbb{Q}\}$$

είναι ένα υπόσωμα του σώματος $\mathbb{R}$ των πραγματικών αριθμών .

Εύκολα βλέπουμε ότι η διαφορά και το γινόμενο δύο στοιχείων του $\mathbb{Q}[\sqrt{5}]$ ανήκουν στο $\mathbb{Q}[\sqrt{5}]$.



Αν τώρα, $0 \neq a+b\sqrt{5} \in \mathbb{Q}[\sqrt{5}]$, τότε

$$(a+b\sqrt{5})^{-1} = \frac{1}{a+b\sqrt{5}} = \left(\frac{a}{a^2-5b^2} \right) - \left(\frac{b}{a^2-5b^2} \right) \sqrt{5}$$

ανήκει στο $\mathbb{Q}[\sqrt{5}]$ αφού έχει τη μορφή

$$a' + b'\sqrt{5} \text{ με } a' = \frac{a}{a^2-5b^2} \in \mathbb{Q}, \quad b' = \frac{b}{a^2-5b^2} \in \mathbb{Q}$$

$$(a^2 - 5b^2 \neq 0) \quad .$$

§6.1. Ομομορφισμοί δακτυλίων .

Ορισμός . Ας είναι R και R' δύο δακτύλιοι . Μια απεικόνιση $f: R \longrightarrow R'$ θα λέγεται **ομομορφισμός** από τον δακτύλιο R στον R' αν για κάθε $x, y \in R$ είναι

$$i) f(x+y) = f(x) + f(y)$$

$$ii) f(xy) = f(x)f(y) \quad .$$

Ένας ομομορφισμός $f: R \longrightarrow R'$ δακτυλίων καλείται

1) **Επιμορφισμός**, αν η απεικόνιση f είναι επί .

2) **Μονομορφισμός**, αν η απεικόνιση f είναι 1-1 .

3) **Ισομορφισμός**, αν η απεικόνιση f είναι 1-1 και επί .

περίπτωση αυτή λέμε ότι οι δακτύλιοι είναι **ισόμορφοι** και το συμβολίζουμε $R \cong R'$.

Παραδείγματα .

1) Για τυχόντες δακτύλιους R και R' υπάρχει πάντα ένας ομομορφισμός ο **τετριμμένος**, που ορίζεται ως εξής :

$$f: R \longrightarrow R', \quad f(x) = 0_{R'}, \quad \text{για κάθε } x \in R \quad .$$

2) Για κάθε δακτύλιο R η ταυτοτική απεικόνιση $I_R: R \longrightarrow R$ είναι ένας ισομορφισμός του R .



3) Η κανονική προβολή

$$p: \mathbb{Z} \longrightarrow \mathbb{Z}_m, \quad p(n) = \bar{n}, \quad \text{για κάθε } n \in \mathbb{Z}$$

είναι ένας ομομορφισμός από τον δακτύλιο $\mathbb{Z}$ των ακεραίων στον δακτύλιο των $\text{mod } m$ κλάσεων ισοτιμίας, αφού για κάθε $n, k \in \mathbb{Z}$ έχουμε

$$p(n+k) = \overline{n+k} = \bar{n} + \bar{k} = p(n) + p(k)$$

$$p(nk) = \overline{nk} = \bar{n} \cdot \bar{k} = p(n) \cdot p(k).$$

Ο p είναι φανερά ένας ομομορφισμός ενώ δεν είναι μονομορφισμός

4) Έστω K ένα σώμα, $\xi \in K$ και $K[X]$ ο δακτύλιος των πολυωνύμων με συντελεστές από το K . Η απεικόνιση $\phi_\xi: K[X] \longrightarrow K$,

$$p(x) = \alpha_0 + \alpha_1 x + \dots + \alpha_n x^n \longmapsto p(\xi) = \alpha_0 + \alpha_1 \xi + \dots + \alpha_n \xi^n$$

είναι ένας ομομορφισμός δακτυλίων. Πραγματικά, θεωρούμε δύο πολυώνυμα του $K[X]$

$$P = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \dots$$

$$Q = b_0 + b_1 x + b_2 x^2 + \dots$$

το άθροισμά τους

$$P+Q = (\alpha_0 + b_0) + (\alpha_1 + b_1)x + (\alpha_2 + b_2)x^2 + \dots$$

και το γινόμενό τους

$$PQ = (\alpha_0 b_0) + (\alpha_0 b_1 + \alpha_1 b_0)x + (\alpha_0 b_2 + \alpha_1 b_1 + \alpha_2 b_0)x^2 + \dots$$

Τότε

$$\begin{aligned} (P+Q)(\xi) &= (\alpha_0 + b_0) + (\alpha_1 + b_1)\xi + (\alpha_2 + b_2)\xi^2 + \dots = \\ &= P(\xi) + Q(\xi) \end{aligned} \tag{8}$$

και

$$\begin{aligned} (PQ)(\xi) &= (\alpha_0 b_0) + (\alpha_0 b_1 + \alpha_1 b_0)\xi + (\alpha_0 b_2 + \alpha_1 b_1 + \alpha_2 b_0)\xi^2 + \dots = \\ &= P(\xi)Q(\xi) \end{aligned} \tag{9}$$

Οι (8) και (9) εκφράζουν το γεγονός ότι η ϕ_ξ είναι ομομορφισμός.



5) Η απεικόνιση

$$f: \mathbb{R} \longrightarrow \mathbb{R} \oplus \mathbb{R}, \quad f(x) = (x, 0) \quad \text{για κάθε } x \in \mathbb{R}$$

είναι ένας ομομορφισμός δακτυλίων. Πραγματικά, για κάθε $x, y \in \mathbb{R}$ έχουμε

$$f(x+y) = (x+y, 0) = (x, 0) + (y, 0) = f(x) + f(y)$$

$$f(xy) = (xy, 0) = (x, 0)(y, 0) = f(x)f(y)$$

Ο f είναι φανερά ένας μονομορφισμός ενώ δεν είναι επιμορφισμός.

Δεν είναι βέβαια όλες οι απεικονίσεις από ένα δακτύλιο σ' ένα άλλο ομομορφισμοί. Για παράδειγμα, η απεικόνιση

$$f: \mathbb{Z} \longrightarrow 2\mathbb{Z}, \quad f(n) = 2n \quad \text{για κάθε } n \in \mathbb{Z}$$

δεν είναι ομομορφισμός δακτυλίων (ο $2\mathbb{Z}$ δακτύλιος με τις συνηθισμένες πράξεις), αφού

$$f(nm) = 2nm \neq (2n)(2m) = f(n)f(m).$$

Ένας ομομορφισμός δακτυλίων $f: R \longrightarrow R'$ είναι ιδιαιτέρως ένας ομομορφισμός ομάδων $f: (R, +) \longrightarrow (R', +)$ και σαν τέτοιος έχει πολλές από τις γνωστές ιδιότητες, Έτσι

$$\alpha) f(0_R) = 0_{R'}.$$

$$\beta) f(nx) = nf(x) \quad \text{για κάθε } x \in R \text{ και } n \in \mathbb{Z}.$$

$$\gamma) f(x^n) = [f(x)]^n \quad \text{για κάθε } x \in R \text{ και } n \in \mathbb{Z}^+,$$

αφού ο f διατηρεί τα γινόμενα.

Θα παρατηρήσουμε εδώ ότι αν οι δακτύλιοι R και R' έχουν μονάδες 1_R και $1_{R'}$, αντίστοιχα είναι δυνατόν για ένα ομομορφισμό $f: R \longrightarrow R'$ να έχουμε

$$f(1_R) \neq 1_{R'}.$$



και επομένως είναι δυνατόν για ένα αντιστρέψιμο στοιχείο $x \in R$ η εικόνα του $f(x)$ να μην είναι αντιστρέψιμο στοιχείο στον R' .

Έτσι για τον ομομορφισμό (βλέπε Κεφ. III, §1.1, Παραδ. 9)

$$f: R \longrightarrow R \oplus R, \quad f(x) = (x, 0) \quad \text{για κάθε } x \in R,$$

έχουμε $f(1) = (1, 0)$ που δεν είναι η μονάδα $(1, 1)$ του $R \oplus R$, ενώ η f απεικονίζει κάθε αντιστρέψιμο $x \in R$ $x \neq 0$ σε μη-αντιστρέψιμο στοιχείο $(x, 0)$ στον $R \oplus R$.

Είναι χρήσιμο λοιπόν να γνωρίζουμε πότε για ένα ομομορφισμό $f: R \longrightarrow R'$ έχουμε

$$f(1_R) = 1_{R'}.$$

Πρόταση 13.

Ας είναι R και R' δακτύλιοι με μονάδες 1_R και $1_{R'}$ αντίστοιχα και $f: R \longrightarrow R'$ ένας ομομορφισμός. Ισχύουν:

i) Αν ο f είναι επιμορφισμός τότε $f(1_R) = 1_{R'}$.

ii) Αν ο f δεν είναι τετριμμένος ομομορφισμός και ο R' είναι δακτύλιος με διαίρεση (ιδιαίτερα σώμα) ή πεδίο ακεραιότητας τότε

$$f(1_R) = 1_{R'}.$$

Απόδειξη.

i) Αφού ο f είναι επιμορφισμός, θα υπάρχει στοιχείο $x \in R$ τέτοιο ώστε $f(x) = 1_{R'}$, οπότε

$$f(1_R) = f(x)f(1_R) = f(x1_R) = f(x) = 1_{R'}.$$

ii) Αφού ο f δεν είναι ο τετριμμένος ομομορφισμός θα υπάρχει $x \in R$ με $f(x) \neq 0_{R'}$, οπότε

$$f(x)(f(1_R) - 1_{R'}) = f(x)f(1_R) - f(x)1_{R'} = f(x) - f(x) = 0_{R'}.$$



δηλαδή

$$f(x)(f(1_R) - 1_{R'}) = 0_{R'} \quad (10)$$

Αν ο R' είναι δακτύλιος με διαίρεση ή σώμα αφού $f(x) \neq 0_{R'}$ πολ/ζοντας και τα δύο μέλη της (10) με $f(x)^{-1}$ από αριστερά παίρνουμε

$$f(1_R) = 1_{R'}.$$

Αν ο R' είναι πεδίο ακεραιότητας, τότε από τους νόμους απλοποίησης παίρνουμε

$$f(x)(f(1_R) - 1_{R'}) = f(x)0_{R'} \implies f(1_R) - 1_{R'} = 0_{R'}.$$

δηλαδή $f(1_R) = 1_{R'}$. ■

Θα παρατηρήσουμε εδώ ότι, αν R, R' είναι δύο δακτύλιοι με μονάδες και $f: R \longrightarrow R'$ ένας ομομορφισμός τέτοιος ώστε $f(1_R) = 1_{R'}$, τότε για κάθε αντιστρέψιμο στοιχείο $x \in R$ έχουμε

$$f(x^{-1}) = [f(x)]^{-1}.$$

Πραγματικά,

$$f(x)f(x^{-1}) = f(xx^{-1}) = f(1_R) = 1_{R'}, \quad \text{και όμοια}$$

$$f(x^{-1})f(x) = 1_{R'}.$$

Για τη σύνθεση ομομορφισμών δακτυλίων και για ισομορφισμούς ισχύουν ανάλογα αποτελέσματα όπως και στις ομάδες. Έτσι

$$1) \text{ Αν } f: R \longrightarrow S \text{ και } g: S \longrightarrow T$$

είναι ομομορφισμοί δακτυλίων, τότε και η σύνθεση τους

$$g \circ f: R \longrightarrow T$$

είναι ομομορφισμός. (Άσκηση)

$$2) \text{ Αν } f: R \longrightarrow R' \text{ είναι ένας ισομορφισμός δακτυλίων τότε και}$$



η αντίστροφη απεικόνιση $f^{-1}: R' \longrightarrow R$ είναι ισομορφισμός. (Άσκηση)
Απ' τα παραπάνω εύκολα συμπεραίνουμε ότι :

3) Αν $f: R \longrightarrow R'$ είναι ένας ομομορφισμός δακτυλίων, ο f είναι ισομορφισμός δακτυλίων εάν και μόνο εάν υπάρχει ομομορφισμός $g: R' \longrightarrow R$ έτσι ώστε

$$g \circ f = I_R \quad \text{και} \quad f \circ g = I_{R'}$$

Ένας ομομορφισμός $f: R \longrightarrow R$ από τον δακτύλιο R στον εαυτό του καλείται ενδομορφισμός του R .

Είναι φανερό τώρα ότι το σύνολο $\text{End}(R)$ όλων των ενδομορφισμών ενός δακτυλίου R με πράξη τη σύνθεση απεικονίσεων αποτελεί μονοειδές.

Πρόταση 14 .

Οι μόνοι ενδομορφισμοί του δακτυλίου $\mathbb{Z}$ των ακεραίων είναι ο τετριμμένος ομομορφισμός και ο ταυτοτικός .

Απόδειξη .

Αν ο $f: \mathbb{Z} \longrightarrow \mathbb{Z}$ δεν είναι ο τετριμμένος ομομορφισμός τότε $f(1) = 1$ (βλέπε πρόταση 13) .

Για κάθε $n \in \mathbb{Z}^+$ έχουμε λοιπόν

$$f(n) = f(1 + \dots + 1) = \underbrace{f(1) + \dots + f(1)}_{n\text{-φορές}} = \underbrace{1 + \dots + 1}_{n\text{-φορές}} = n$$

και

$$f(-n) = -f(n) = -n, \quad \text{ενώ} \quad f(0) = 0 .$$

Έτσι $f(n) = n$ για κάθε $n \in \mathbb{Z}$ δηλαδή $f = I_{\mathbb{Z}}$. ■

Πόρισμα 1 .

Υπάρχει το πολύ ένας ισομορφισμός από ένα τυχόντα δακτύλιο R στον δακτύλιο $\mathbb{Z}$ των ακεραίων .



Απόδειξη .

Αν υποθέσουμε ότι υπάρχουν δύο ισομορφισμοί $f, g: R \longrightarrow Z$ τότε η σύνθεση $f \circ g^{-1}$ είναι ένας ενδομορφισμός του Z , επομένως $f \circ g^{-1} = I_Z$ δηλαδή $f = g$. ■

Ένας ισομορφισμός $f: R \longrightarrow R$ από τον δακτύλιο R στον εαυτό του καλείται αυτομορφισμός του R .

Είναι εύκολο να δούμε ότι το σύνολο όλων των αυτομορφισμών ενός δακτυλίου R με πράξη τη σύνθεση απεικονίσεων αποτελεί ομάδα που θα την παριστάνουμε $\text{Aut}(R)$.

Παράδειγμα 1 .

Στο δακτύλιο $\mathbb{Q}[\sqrt{5}]$ (βλέπε παραδ. 2, §5) η απεικόνιση $f: \mathbb{Q}[\sqrt{5}] \longrightarrow \mathbb{Q}[\sqrt{5}]$, $f(a+b\sqrt{5}) = a-b\sqrt{5}$ για κάθε $a+b\sqrt{5} \in \mathbb{Q}[\sqrt{5}]$ είναι ένας αυτομορφισμός. (Άσκηση).

ΟΡΙΣΜΟΣ . Ας είναι $f: R \longrightarrow R'$ ένας ομομορφισμός δακτυλίων. Ονομάζουμε πυρήνα του f , και τον συμβολίζουμε $\text{Ker}(f)$, το ακόλουθο υποσύνολο του R

$$\text{Ker}(f) = \{x/x \in R, f(x) = 0_{R'}\}.$$

Ο πυρήνας του f είναι ακριβώς ο πυρήνας του ομομορφισμού ομάδων $f: (R, +) \longrightarrow (R', +)$.

Είναι λοιπόν υποομάδα της $(R, +)$ · επιπλέον αν $x, y \in \text{Ker}(f)$ τότε $xy \in \text{Ker}(f)$ αφού

$$f(xy) = f(x)f(y) = 0_{R'} \cdot 0_{R'} = 0_{R'}.$$

Δείξαμε λοιπόν :



Πρόταση 15 .

Ο πυρήνας $\text{Ker}(f)$ ενός ομομορφισμού δακτυλίων $f: R \longrightarrow R'$ είναι υποδακτύλιος του R . ■

Έχουμε το επόμενο κριτήριο για μονομορφισμούς .

Αν $f: R \longrightarrow R'$ είναι ένας ομομορφισμός δακτυλίων , τότε :
 $0 \neq f$ είναι μονομορφισμός $\iff \text{Ker}(f) = \{0_R\}$.

Η απόδειξη του προκύπτει αμέσως από το αντίστοιχο κριτήριο για ομομορφισμούς ομάδων αφού ο πυρήνας ομομορφισμού δακτυλίων δεν είναι παρά ο πυρήνας του ομομορφισμού ομάδων $f(R,+) \longrightarrow (R',+)$.

Πρόταση 16 .

Ας είναι $f: R \longrightarrow R'$ ένας ομομορφισμός δακτυλίων . Ισχύουν τα επόμενα :

i) Αν S είναι ένας υποδακτύλιος του R , τότε και η εικόνα του $f(S)$ είναι υποδακτύλιος του R' .

ii) Αν T είναι ένας υποδακτύλιος του R' τότε και η αντίστροφη εικόνα του $f^{-1}(T)$ είναι υποδακτύλιος του R .

Απόδειξη .

i) Είναι $f(S) = \{f(x)/x \in S\}$. Αν $f(x), f(y) \in f(S)$ τότε ,
 $x-y \in S$ και $xy \in S$ αφού ο S είναι υποδακτύλιος του R οπότε ,

$$f(x)-f(y) = f(x-y) \in f(S)$$

$$f(x)f(y) = f(xy) \in f(S)$$

Το $f(S)$ είναι λοιπόν υποδακτύλιος του R' .

ii) Αν $x, y \in f^{-1}(T)$ τότε $f(x), f(y) \in T$ επομένως

$$f(x)-f(y) \in T \quad \text{και} \quad f(x)f(y) \in T$$

αφού ο T είναι υποδακτύλιος του R' . Έτσι



$$f(x-y) = f(x) - f(y) \in T \quad \text{και} \quad f(xy) = f(x)f(y) \in T$$

δηλαδή $x-y$, $xy \in f^{-1}(T)$.

Είναι λοιπόν το $f^{-1}(T)$ υποδακτύλιος του R . ■

Ας είναι τώρα $f: R \longrightarrow R'$ ένας ομομορφισμός δακτυλίων .

Η εικόνα $\text{Im}(f) = f(R)$ του ομομορφισμού f είναι σύμφωνα με την προηγούμενη πρόταση , υποδακτύλιος του R' . Έτσι ο f είναι επιμορφισμός εάν και μόνο εάν $\text{Im}(f) = R'$, ενώ ο f είναι ισομορφισμός εάν και μόνο εάν $\text{Ker}(f) = \{0_R\}$ και $\text{Im}(f) = R'$.

Είναι φανερό τώρα ότι ο ομομορφισμός $f: R \longrightarrow R'$ είναι ένας επιμορφισμός του δακτυλίου R στον δακτύλιο $\text{Im}(f)$, ενώ ο μονομορφισμός $f: R \longrightarrow R'$ είναι ένας ισομορφισμός του δακτυλίου R στον δακτύλιο $\text{Im}(f)$.

ΟΡΙΣΜΟΣ . Θα λέμε ότι ο δακτύλιος R εμφυτεύεται στον δακτύλιο R' αν υπάρχει μονομορφισμός

$$f: R \longrightarrow R' .$$

Στην περίπτωση αυτή $R \simeq \text{Im}(f)$, δηλαδή ο R είναι ισομορφος προς ένα υποδακτύλιο του R' .

Παράδειγμα 2 .

Έστω $\mathbb{C}$ το σώμα των μιγαδικών αριθμών και $Q(R)$ ο δακτύλιος των πραγματικών κουατερνίων (βλέπε Κεφ. III, §2, Παραδ. 6) .

Η απεικόνιση $f: \mathbb{C} \longrightarrow Q(R)$ που ορίζεται ως εξής : Για κάθε $a+bi \in \mathbb{C}$

$$f(a+bi) = aI + bJ = \begin{pmatrix} a+bi & 0 \\ 0 & a-bi \end{pmatrix}$$

είναι ένας μονομορφισμός . Πραγματικά για κάθε $a+bi$, $c+di \in \mathbb{C}$ έχουμε



$$\begin{aligned} f((a+bi)+(c+di)) &= (a+b)I + (b+d)J = \\ &= (aI+bJ) + (cI+dJ) = \\ &= f(a+bi) + f(c+di) \end{aligned}$$

$$\begin{aligned} f((a+bi)(c+di)) &= (ac-bd)I + (ad+bc)J = \\ &= (aI+bJ)(cI+dJ) = \\ &= f(a+bi)f(c+di) \end{aligned}$$

δηλαδή ο f είναι ομομορφισμός. Ο f είναι φανερά ένας μονομορφισμός, έτσι

$$C \cong \text{Im}(f) .$$

Αυτό σημαίνει ότι τα πραγματικά κουατέρνια μπορούν να θεωρηθούν σαν μια κατάλληλη γενύκευση των μιγαδικών αριθμών.

Πρόταση 17 .

Κάθε δακτύλιος R μπορεί να εμφυτευθεί σ'ένα δακτύλιο με μονάδα .

Απόδειξη .

Παίρνουμε το καρτεσιανό γινόμενο ,

$$S = R \times \mathbb{Z} = \{(r, n) / r \in R, n \in \mathbb{Z}\}$$

και ορίζουμε σ'αυτό την πρόσθεση και τον πολ/σμό ως εξής :

$$(r, n) + (s, m) = (r+s, m+n)$$

$$(r, n) \cdot (s, m) = (rs + ns + mr, nm)$$

Εύκολα αποδεικνύεται ότι το σύνολο S εφοδιασμένο με τις παραπάνω πράξεις γίνεται ένας δακτύλιος, με μηδενικό στοιχείο το ζεύγος $(0_R, 0)$ και μονάδα το ζεύγος $(0_R, 1)$.



Η απεικόνιση

$$f: R \longrightarrow S, \quad f(r) = (r, 0) \quad \text{για κάθε} \quad r \in R$$

είναι φανερά 1-1, και ομομορφισμός αφού για κάθε $r, r_1 \in R$ έχουμε

$$f(r+r_1) = (r+r_1, 0) = (r, 0) + (r_1, 0) = f(r) + f(r_1)$$

$$f(rr_1) = (rr_1, 0) = (r, 0) \cdot (r_1, 0) = f(r)f(r_1)$$

Ο f είναι λοιπόν ένα μονομορφισμός, μ'άλλα λόγια ο R εμφυτεύεται στον S . Επιπλέον

$$\text{Im}(f) = \{(r, 0) / r \in R\} = R \times \{0\}$$

και έτσι ο δακτύλιος R είναι ισόμορφος με τον υποδακτύλιο $R \times \{0\}$ του S .

Παρατηρήσεις.

1) Αν ο R έχει μονάδα 1_R , τότε ο υποδακτύλιος $R \times \{0\}$ έχει μονάδα $(1_R, 0)$ που είναι διαφορετική από την μονάδα $(0_R, 1)$ του S .

2) Αν ο R δεν έχει διαλυτές του μηδενός, δεν έπεται ότι και ο $R \times \mathbb{Z}$ δεν έχει διαλυτές του μηδενός π.χ. αν $R = \mathbb{Z}$ τότε

$$(-2, 2)(2n, 0) = (0 + 4n - 4n, 0) = (0, 0).$$

6.2. Ομομορφισμοί σωμάτων.

ΟΡΙΣΜΟΣ. Έστω F και E δύο σώματα. Μια απεικόνιση $f: F \longrightarrow E$ θα λέγεται ομομορφισμός από το σώμα F στο E , αν για κάθε $x, y \in F$ έχουμε

$$i) f(x+y) = f(x) + f(y)$$

$$ii) f(xy) = f(x)f(y).$$

Μ'άλλα λόγια ο f δεν είναι παρά ένας ομομορφισμός από τον δακτύλιο F στον E . Έτσι



$$\alpha) f(0_F) = 0_E$$

$$\beta) f(-x) = -f(x) \quad \text{για κάθε } x \in F.$$

ενώ αν ο f δεν είναι ο τετριμμένος ομομορφισμός τότε σύμφωνα με την πρόταση 13, έχουμε

$$\gamma) f(1_F) = 1_E$$

$$\delta) f(x^{-1}) = [f(x)]^{-1} \quad \text{για κάθε } x \in F - \{0\}.$$

Παράδειγμα 1.

Αν F είναι ένα σώμα $\text{char } F = p \neq 0$ τότε η απεικόνιση

$$f: F \longrightarrow F, \quad f(x) = x^p \quad \text{για κάθε } x \in F$$

είναι ομομορφισμός. Πραγματικά για κάθε $x, y \in F$ έχουμε

$$\begin{aligned} f(x+y) &= (x+y)^p = x^p + y^p && (\text{Πρόταση 11}) \\ &= f(x) + f(y) \end{aligned}$$

και $f(xy) = (xy)^p = x^p y^p$ αφού σε σώμα ο πολ/σμός είναι αντιμεταθετικός.

ΠΡΟΤΑΣΗ 18.

Αν $f: F \longrightarrow E$ είναι ένας ομομορφισμός σωμάτων διάφορος από τον τετριμμένο ομομορφισμό τότε ο f είναι μονομορφισμός.

Απόδειξη.

Αρκεί να δείξουμε ότι αν $f(x) = f(y)$ τότε $x = y$. Αν $f(x) = f(y)$ τότε $f(x-y) = 0_E$. Υποθέτουμε ότι $x-y \neq 0_F$, τότε υπάρχει $(x-y)^{-1} \in F$ οπότε $f((x-y)^{-1}) = [f(x-y)]^{-1}$. Πολλώνοντας και τα δύο μέλη της σχέσης $f(x-y) = 0_E$ με $[f(x-y)]^{-1}$ παίρνουμε.



$$[f(x-y)]^{-1}f(x-y) = [f(x-y)]^{-1}0_E \quad \text{δηλαδή} \quad 1_E = 0_E$$

άρα αφού το E είναι σώμα, συνεπώς $x-y=0_F$ οπότε $x=y$. ■

Αν λοιπόν $f: E \longrightarrow E$ είναι ένας επιμορφισμός σωμάτων (επομένως μη-τετριμμένος) ο f θα είναι ένας ισομορφισμός, σύμφωνα με την παραπάνω πρόταση.

Όπως και στους δακτύλιους έτσι και εδώ το σύνολο $\text{Aut}(F)$ όλων των αυτομορφισμών ενός σώματος F , αποτελεί ομάδα με πράξη τη σύνθεση απεικονίσεων.

§7. Το σώμα κλασμάτων πεδίου ακεραιότητας.

Αν D είναι ένα σώμα τότε, η εξίσωση $ax=b$, $a \neq 0$ έχει μοναδική λύση στο D την $x=a^{-1}b$.

Στην περίπτωση που το D είναι πεδίο ακεραιότητας η παραπάνω εξίσωση δεν έχει πάντα λύση στο D .

Το ερώτημά μας λοιπόν είναι αν μπορούμε να εμφυτεύσουμε το πεδίο ακεραιότητας D μέσα σ'ένα σώμα F , έτσι ώστε η εξίσωση $ax=b$, $a \neq 0$, $a, b \in D$ να έχει πάντα λύση στο F .

Στην πεπερασμένη περίπτωση βέβαια δεν υπάρχει δυσκολία αφού κάθε πεπερασμένο πεδίο ακεραιότητας είναι σώμα.

Το ερώτημα λοιπόν παρουσιάζει ενδιαφέρον μόνο στην περίπτωση που το πεδίο ακεραιότητας D είναι άπειρο και δεν είναι σώμα.

Η απάντηση στο ερώτημα είναι καταφατική όπως θα δούμε στη συνέχεια.

Έστω D ένα πεδίο ακεραιότητας.

Θεωρούμε το σύνολο $E = D \times D^*$ όπου $D^* = D - \{0\}$ δηλαδή



$$E = \{(a,b)/a,b \in D, \quad b \neq 0\}$$

Στο σύνολο E ορίζουμε μια σχέση R με τον ακόλουθο τρόπο

$$(a,b) = (c,d)(R) \quad \text{εάν-ν} \quad ad = cb \quad .$$

Δεν είναι δύσκολο να δείξουμε ότι η σχέση R είναι μια σχέση ισοδυναμίας στο E . Η μεταβατική ιδιότητα είναι ύψως η λιγότερο προφανής. Για να την αποδείξουμε υποθέτουμε ότι

$$(a,b) \equiv (c,d)(R) \quad \text{και} \quad (c,d) \equiv (r,s)(R)$$

οπότε

$$ad = bc \quad \text{και} \quad cs = rd \quad .$$

Πολ/ζουμε την πρώτη ισότητα με s και την δεύτερη με b και παίρνουμε

$$ads = cbs \quad \text{και} \quad csd = rdb \quad \text{οπότε} \quad ads = rdb \quad .$$

Αφού ο d δεν είναι διαιρέτης του μηδενός ο νόμος απλοποίησης μας δίνει $as = rb$, δηλαδή $(a,b) \equiv (r,s)(R)$

Το σύνολο E λοιπόν διαμελίζεται σε κλάσεις ισοδυναμίας. Την κλάση ισοδυναμίας του στοιχείου (a,b) την συμβολίζουμε $\frac{a}{b}$ δηλαδή

$$\frac{a}{b} = \{(c,d) \in E / (c,d) \equiv (a,b)(R)\} = \{(c,d) \in E / ad = cb\}$$

και την καλούμε κλάσμα με αριθμητή a και παρονομαστή b .

Έτσι

$$\frac{a}{b} = \frac{c}{d} \iff ad = cb \quad (11)$$

Συμβολίζουμε με F το σύνολο όλων των κλασμάτων δηλαδή $F = E/R$.

Στο σύνολο F ορίζουμε δύο πράξεις, πρόσθεση και πολ/σμό ως εξής

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd} \quad (12)$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \quad (13)$$



Παρατηρούμε ότι , αφού το σύνολο D^* είναι κλειστό ως προς τον πολ/σμό οι δεξιού όροι αυτών των ισοτήτων έχουν έννοια .

Οφείλουμε όμως να ελέγξουμε ότι οι παραπάνω πράξεις (12) και (13) είναι καλά ωρισμένες δηλαδή ανεξάρτητες από τους εκλεγόμενους αντιπροσώπους των κλάσεων .

Πρέπει να δείξουμε ότι αν

$$\frac{a}{b} = \frac{a'}{b'} \quad \text{και} \quad \frac{c}{d} = \frac{c'}{d'} \quad (14)$$

τότε

$$\frac{ad+cb}{bd} = \frac{a'd'+c'b'}{b'd'} \quad (15)$$

και

$$\frac{ac}{bd} = \frac{a'c'}{d'd'} \quad (16)$$

θα δείξουμε την (15) .

Σύμφωνα με την (11) οι σχέσεις (14) ισοδυναμούν με τις

$$ab' = a'b \quad \text{και} \quad cd' = c'd \quad (17)$$

Πολ/ζουμε την πρώτη των (17) με dd' , την δεύτερη με bb' και προσθέτουμε κατά μέλη τις προκύπτουσες ισότητες . θα έχουμε

$$ab'dd' + cd'bb' = a'bdd' + c'dbb'$$

ή

$$(ad+cb)b'd' = (a'd' + c'b')bd$$

σχέση που σύμφωνα με την (11) συνεπάγεται την (15) .

Η απόδειξη της (16) γίνεται με όμοιο τρόπο .

ΛΗΜΜΑ.

Το σύνολο F όλων των κλασμάτων με πρόσθεση και πολ/σμό που δύνονται από τις σχέσεις (12) και (13) αποτελεί σώμα .

Απόδειξη .

Υπολογιστικά βλέπουμε , ότι η πρόσθεση και ο πολ/σμός είναι



πράξεις προσεταιριστικές και αντιμεταθετικές και ότι πληρούνται οι επιμεριστικούς νόμους. Επιπλέον

α) Το μηδενικό στοιχείο είναι το κλάσμα $\frac{0}{1}$.

Πραγματικά για κάθε $\frac{a}{b} \in F$ έχουμε

$$\frac{a}{b} + \frac{0}{1} = \frac{a1+0b}{b1} = \frac{a}{b}.$$

Σημειώνουμε ότι $\frac{0}{1} = \frac{0}{x}$ για κάθε $x \neq 0$.

β) Το αντίθετο του κλάσματος $\frac{a}{b}$ είναι το κλάσμα $\frac{-a}{b}$ γιατί

$$\frac{a}{b} + \frac{-a}{b} = \frac{ab+(-a)b}{b^2} = \frac{0}{b^2} = \frac{0}{1} \quad \text{δηλαδή} \quad -\frac{a}{b} = \frac{-a}{b}.$$

γ) Το μοναδιαίο στοιχείο είναι το κλάσμα $\frac{1}{1}$.

Πραγματικά για κάθε $\frac{a}{b} \in F$ έχουμε

$$\frac{a}{b} \cdot \frac{1}{1} = \frac{a1}{b1} = \frac{a}{b}.$$

Σημειώνουμε ότι το κλάσμα $\frac{1}{1} = \frac{x}{x}$ για κάθε $x \neq 0$.

δ) Αν $\frac{a}{b} \in F - \{\frac{0}{1}\}$, που σημαίνει $a \neq 0$, τότε το κλάσμα $\frac{b}{a}$ είναι το σντίστροφός του.

$$\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ab} = \frac{1}{1}.$$

Είναι λοιπόν το F με τις πράξεις (12) και (13) σώμα. ■

Το σώμα F καλεῖται σώμα κλασμάτων ή σώμα πηλίκων, του πεδίου ακεραιότητας D .

ΘΕΩΡΗΜΑ 2.

Κάθε πεδίο ακεραιότητας D μπορεί να εμφυτευθεῖ σ'ένα σώμα.



Απόδειξη .

Αν F είναι το σώμα κλασμάτων της D τότε η απεικόνιση
 $i : D \longrightarrow F$, $i(a) = \frac{a}{1}$ για κάθε $a \in D$ είναι ένας ομομορφισμός.
 Πραγματικά ,

$$i(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = i(a) + i(b)$$

$$i(ab) = \frac{ab}{1} = \frac{a}{1} \cdot \frac{b}{1} = i(a)i(b) .$$

Η i είναι φανερά 1-1 , επομένως η i είναι ένας μονομορφισμός ,
 που καλείται κανονική ένεση του D στο F . ■

Συνεχίζοντας παρατηρούμε ότι η εικόνα

$$\text{Im}(i) = \{a/1 / a \in D\}$$

του μονομορφισμού i είναι ένας υποδακτύλιος του F και μάλιστα

$$D \cong \{a/1 / a \in D\}$$

Μ'αυτό τον τρόπο το πεδίο ακεραιότητας D (κατά προσέγγιση ισομορφισμού) μπορεί να επεκταθεί σ'ένα σώμα F .

Μπορούμε λοιπόν να ταυτίσουμε το D με την εικόνα του $\{a/1 / a \in D\}$ και να θεωρούμε ότι το D πραγματικά ανήκει στο σώμα κλασμάτων F .

Στο εξής :

δεν θα γράφουμε $\frac{a}{1}$ αλλά a .

Κάθε στοιχείο $a \in D$, $a \neq 0$ έχει στο σώμα F αντίστροφο το στοιχείο $\frac{1}{a}$ που θα το συμβολίζουμε a^{-1} . Έτσι κάθε $\frac{a}{b} \in F$ μπορεί να γραφεί

$$\frac{a}{b} = \frac{a}{1} \cdot \frac{1}{b} = ab^{-1}$$

μ'άλλα λόγια το σώμα F μπορεί να θεωρηθεί ότι αποτελεί από όλα τα κηλύκα

$$ab^{-1} , a, b \in D , b \neq 0 .$$



Πρόταση 19 .

Αν D είναι ένα πεδίο ακεραιότητας , τότε το σώμα κλασμάτων F του D είναι το μικρότερο σώμα που περιέχει το D .

Απόδειξη .

Έστω F' ένα άλλο σώμα που περιέχει το D .

Για κάθε $a, b \in D$ ($b \neq 0$) , το $ab^{-1} \in F'$ αφού το F' είναι σώμα και $D \subseteq F'$.

Αλλά ταυτίσαμε το στοιχείο $\frac{a}{b}$ με το ab^{-1} έτσι το τυχόν στοιχείο $ab^{-1} \in F$ ανήκει στο F' δηλαδή $F \subseteq F'$. ■

Πρόταση 20 .

Αν D και D_1 είναι δύο ισομορφα πεδία ακεραιότητας τότε και τα σώματα κλασμάτων F και F_1 των D και D_1 αντίστοιχα είναι ισομορφα .

Απόδειξη .

Αν $\varphi: D \longrightarrow D_1$ είναι ένας ισομορφισμός τότε η απεικόνιση

$$\bar{\varphi}: F \longrightarrow F_1, \quad \bar{\varphi}\left(\frac{a}{b}\right) = \frac{\varphi(a)}{\varphi(b)}, \quad \text{για κάθε } \frac{a}{b} \in F$$

είναι εύκολο να δείξουμε ότι είναι ένας ισομορφισμός . ■

Παράδειγμα 1 .

Έστω Z το πεδίο ακεραιότητας των ακεραίων . Το σώμα κλασμάτων του Z είναι φανερά από την κατασκευή το σώμα Q των ρητών .

Παράδειγμα 2 .

Αν F είναι ένα σώμα , το σύνολο $F[X]$ όλων των πολυωνύμων μιας απροσδιορίστης μεταβλητής είναι ένα πεδίο ακεραιότητας .



Το σώμα κλασμάτων του πεδίου ακεραιότητας $F[X]$ συμβολίζεται $F(X)$.

Αυτό αποτελείται από όλα τα κλάσματα

$$\frac{P(X)}{Q(X)} \text{ με } P(X), Q(X) \in F[X], \quad Q(X) \neq 0 .$$

Θα καλούμε το $F(X)$ σώμα των ρητών συναρτήσεων πάνω στο F .

Θα σημειώσουμε όμως ότι η ονομασία αυτή δεν είναι κατάλληλη όταν το σώμα F είναι πεπερασμένο γιατί στην περίπτωση αυτή τα πολυώνυμα διαφέρουν από τις πολυωνυμικές συναρτήσεις του F .

§8.1. Ιδεώδη .

Όπως ακριβώς οι κανονικές υποομάδες παίζουν σπουδαίο ρόλο στην θεωρία ομάδων , έτσι και τα ιδεώδη παίζουν ανάλογο ρόλο στη θεωρία δακτυλίων .

Ορισμός . Ας είναι J ένα μη-κενό υποσύνολο ενός δακτυλίου R . Το J καλείται **αμφοίπλευρο ιδεώδες** του R ή απλά **ιδεώδες** , αν

i) Για κάθε $x, y \in J \implies x - y \in J$

ii) Για κάθε $x \in J$ και $r \in R \implies xr \in J$ και $rx \in J$.

Αν στην συνθήκη ii) απαιτήσουμε μόνο το γινόμενο xr (αντίστ. το rx) να ανήκει στο J τότε το ιδεώδες καλείται **δεξιό ιδεώδες** (αντιστ. **αριστερό ιδεώδες**) του R .

Βέβαια σ'ένα αντιμεταθετικό δακτύλιο δεν υπάρχει διαφορά μεταξύ δεξιού , αριστερού και αμφοίπλευρου ιδεώδους .

Είναι φανερό από τον ορισμό ότι ένα ιδεώδες J του δακτυλίου R δεν είναι παρά ένας υποδακτύλιος του R που πληροί τη συνθήκη (ii) . (Το ίδιο ισχύει και για δεξιό ή αριστερό ιδεώδες) .



Παρατήρηση .

Η συνθήκη (i) μας λέει ότι το ζεύγος $(J, +)$ είναι μια υποομάδα της ομάδας $(R, +)$ και μάλιστα κανονική αφού η $(R, +)$ είναι αβελιανή .

$$A \in \begin{pmatrix} R & R \\ R & R \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Κάθε δακτύλιος R έχει προφανώς δύο ιδεώδη το $\{0\}$ και τον εαυτό του .

Κάθε άλλο ιδεώδες του $J \neq \{0\}$, R καλείται γνήσιο ιδεώδες του R .

Σημειώνουμε ιδιαίτερα :

Ένα σώμα F έχει δύο μόνο ιδεώδη , τα $\{0\}$, F .

Πραγματικά , αν $J \neq \{0\}$ είναι ένα ιδεώδες του F , τότε για κάθε $x \in J$, $x \neq 0$ και $x^{-1} \in F$ έχουμε $xx^{-1} = 1 \in J$. Έτσι για κάθε $y \in F$ έχουμε

$$1 \in J \text{ και } y \in F \implies 1 \cdot y = y \in J$$

δηλαδή $F \subseteq J$, και αφού πάντα $J \subseteq F$ παίρνουμε $J = F$.

Αν R είναι ένας δακτύλιος με μονάδα , τότε κάθε ιδεώδες του J που περιέχει τη μονάδα συμπίπτει με το R .

Έτσι , κάθε γνήσιο ιδεώδες του J δεν περιέχει αντιστρέφσιμα στοιχεία , δηλαδή $J \cap U(R) = \emptyset$. (Άσκηση)

Παράδειγμα 1 .

Για κάθε φυσικό αριθμό n το σύνολο

$$(n) = \{nk / k \in \mathbb{Z}\}$$

είναι ένα ιδεώδες του δακτυλίου $\mathbb{Z}$ των ακεραίων . $(n) = (n)(1)$

Παράδειγμα 2 .

Το υποσύνολο $A = \left\{ \begin{pmatrix} 0 & x \\ 0 & y \end{pmatrix} / x, y \in R \right\}$ του δακτυλίου $M_{2 \times 2}(R)$ είναι ένα αριστερό ιδεώδες του , αφού



i) Για κάθε $\begin{pmatrix} 0 & x_1 \\ 0 & y_1 \end{pmatrix}, \begin{pmatrix} 0 & x_2 \\ 0 & y_2 \end{pmatrix} \in A$ έχουμε

$$\begin{pmatrix} 0 & x_1 \\ 0 & y_1 \end{pmatrix} - \begin{pmatrix} 0 & x_2 \\ 0 & y_2 \end{pmatrix} = \begin{pmatrix} 0 & x_1 - x_2 \\ 0 & y_1 - y_2 \end{pmatrix} \in A$$

ii) Για κάθε $\begin{pmatrix} 0 & x \\ 0 & y \end{pmatrix} \in A$ και $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2 \times 2}(\mathbb{R})$ έχουμε

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & x \\ 0 & y \end{pmatrix} = \begin{pmatrix} 0 & ax+by \\ 0 & cx+dy \end{pmatrix} \in A.$$

Επίσης το σύνολο $B = \left\{ \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} / x, y \in \mathbb{R} \right\}$ είναι ένα δεξιό ιδεώδες του $M_{2 \times 2}(\mathbb{R})$.

Γενικότερα, αν F είναι ένα σώμα, στον δακτύλιο $M_{n \times n}(F)$ για κάθε $k, 1 \leq k \leq n$, τα υποσύνολα του

$$A_k = \{ (a_{ij}) / (a_{ij}) \in M_{n \times n}(F), a_{ij} = 0 \quad j \neq k \}$$

$$B_k = \{ (b_{ij}) / (b_{ij}) \in M_{n \times n}(F), b_{ij} = 0 \quad i \neq k \}$$

είναι αντίστοιχα αριστερά και δεξιά ιδεώδη του.

Παράδειγμα 3.

Ας είναι R ένας δακτύλιος και $\emptyset \neq X \subseteq R$.

Θεωρούμε τον δακτύλιο $\text{Hom}(X, R)$ και το σύνολο

$$J_\alpha = \{ f \in \text{Hom}(X, R) / f(\alpha) = 0 \}, \quad \alpha \in X.$$

Το J_α είναι ένα ιδεώδες του $\text{Hom}(X, R)$. Πραγματικά για κάθε $f, h \in J_\alpha$ έχουμε

$$(f-h)(\alpha) = h(\alpha) - f(\alpha) = 0 \quad \text{οπότε} \quad f-h \in J_\alpha.$$

Επιπλέον, για κάθε $f \in J_\alpha$ και $g \in \text{Hom}(X, R)$ είναι

$$(fg)(\alpha) = f(\alpha)g(\alpha) = 0g(\alpha) = 0 \quad \text{δηλαδή} \quad fg \in J_\alpha.$$



και

$$(gf)(\alpha) = g(\alpha)f(\alpha) = g(\alpha) = 0 \quad \text{δηλαδή} \quad gf \in J_{\alpha}.$$

Παράδειγμα 4 .

Θεωρούμε τον δακτύλιο $\mathbb{Z} \times \mathbb{Z}$. Οι υποδακτύλιοι $\mathbb{Z} \times \{0\}$ και $\{0\} \times \mathbb{Z}$ είναι ιδεώδη του .

Πραγματικά , για κάθε $(x,0) \in \mathbb{Z} \times \{0\}$ και $(m,n) \in \mathbb{Z} \times \mathbb{Z}$ έχουμε

$$(x,0)(m,n) = (xm,0) = (m,n)(x,0) = (mx,0) \in \mathbb{Z} \times \{0\}$$

Όμοια εργαζόμαστε και για το $\{0\} \times \mathbb{Z}$.

Παράδειγμα 5 .

Θεωρούμε τον δακτύλιο $M_{n \times n}(\mathbb{R})$ και συμβολίζουμε με E_{ij} τον $n \times n$ πίνακα που έχει τη μονάδα στη ij -θέση και παντού αλλού μηδέν .

Αν $J \neq \{0\}$ είναι κάποιο ιδεώδες του $M_{n \times n}(\mathbb{R})$ τότε το J περιέχει κάποιο μη-μηδενικό πίνακα (a_{ij}) . Υποθέτουμε $a_{rs} \neq 0$ και θεωρούμε τον πίνακα (b_{ij}) που έχει το στοιχείο a_{rs}^{-1} στην κύρια διαγώνιο και παντού αλλού μηδέν .

Αφού το J είναι ιδεώδες του $M_{n \times n}(\mathbb{R})$ έχουμε

$$E_{rr}(b_{ij})(a_{ij})E_{ss} = E_{rs} \in J.$$

Υπενθυμίζουμε ότι

$$E_{pq}E_{rs} = \begin{cases} 0 & \text{αν } q \neq r \\ E_{ps} & \text{αν } q = r \end{cases}$$

οπότε για τους n^2 σε πλήθος πίνακες ισχύει

$$E_{ij} = E_{ir}E_{rs}E_{sj} \in J \quad (i,j=1,\dots,n)$$

Τώρα ,

$$I_n = E_{11} + E_{22} + \dots + E_{nn} \in J$$



δηλαδή η μονάδα του $M_{n \times n}(R)$ ανήκει στο J και έτσι

$$J = M_{n \times n}(R).$$

Με άλλα λόγια, ο δακτύλιος $M_{n \times n}(R)$ δεν έχει γνήσια ιδεώδη.

ΟΡΙΣΜΟΣ. Ένας δακτύλιος $R \neq \{0\}$ που δεν έχει άλλα ιδεώδη εκτός των $\{0\}$ και R καλείται απλός.

Ο δακτύλιος λοιπόν $M_{n \times n}(R)$ είναι απλός.

(Ο $M_{n \times n}(R)$ έχει όμως δεξιά και αριστερά ιδεώδη, βλέπε παράδειγμα 2).

Πρόταση 21.

Ο πυρήνας $\text{Ker}(f)$ ενός ομομορφισμού $f: R \longrightarrow R'$ δακτυλίων, είναι ιδεώδες του R .

Απόδειξη.

Ο $\text{Ker}(f) = \{x / x \in R, f(x) = 0_{R'}\}$, είναι ένας υποδακτύλιος του R (βλέπε πρόταση 15).

Μένει να δείξουμε ότι για κάθε $x \in \text{Ker}(f)$ και $r \in R$ τα rx , $rx \in \text{Ker}(f)$. Πραγματικά,

$$f(rx) = f(x) = 0_{R'} \quad \text{και} \quad f(r) = 0_{R'}$$

$$f(rx) = f(r)f(x) = f(r) \cdot 0_{R'} = 0_{R'}. \quad \blacksquare$$

Πρόταση 22.

Ας είναι $f: R \longrightarrow R'$ ένας ομομορφισμός δακτυλίων. Ισχύουν τα επόμενα

i) Αν J' είναι ένα ιδεώδες του R' τότε $f^{-1}(J')$ είναι ένα ιδεώδες του R .



ii) Αν ο f είναι επιμορφισμός και J ιδεώδες του R τότε και $f(J)$ είναι ιδεώδες του R' .

Απόδειξη .

i) Το $f^{-1}(J')$ είναι υποδακτύλιος του R (βλέπε πρόταση 16) . Μένει να δείξουμε ότι για κάθε $x \in f^{-1}(J')$ και $r \in R$ έχουμε $xr, rx \in f^{-1}(J')$. Πραγματικά , είναι $f(x) \in J'$, $f(r) \in R'$ και το J' ιδεώδες του R' οπότε

$$f(xr) = f(x)f(r) \in J' \quad \text{δηλαδή} \quad xr \in f^{-1}(J')$$

$$f(rx) = f(r)f(x) \in J' \quad \text{δηλαδή} \quad rx \in f^{-1}(J') .$$

ii) Το $f(J)$ είναι υποδακτύλιος του R' (βλέπε πρόταση 16) . Μένει να δείξουμε ότι για κάθε $f(x) \in f(J)$ και $r' \in R'$ έχουμε $f(x)r', r'f(x) \in f(J)$.

Πραγματικά , αφού $f(R) = R'$, υπάρχει $r \in R$ τέτοιο ώστε $f(r) = r'$, οπότε

$$f(x)r' = f(x)f(r) = f(xr) \in f(J)$$

$$r'f(x) = f(r)f(x) = f(rx) \in f(J)$$

επειδή το J είναι ιδεώδες του R και $xr, rx \in J$. ■

Πρόταση 23 .

Αν $\{J_i\}_{i \in I}$ είναι μια οικογένεια αμφίπλευρων (αντιστ. δεξιών, αριστερών) ιδεωδών ενός δακτυλίου R , τότε η $\bigcap_{i \in I} J_i$ είναι ένα αμφίπλευρο (αντιστ. δεξιό, αριστερό) ιδεώδες του R .

Απόδειξη .

Θα δώσουμε την απόδειξη για την περίπτωση των αμφίπλευρων ιδεωδών .

Το σύνολο $\bigcap_{i \in I} J_i \neq \emptyset$ είναι ένας υποδακτύλιος του R . Μένει να



δείξουμε ότι , για κάθε $x \in \bigcap_{i \in I} J_i$ και $r \in R$ έχουμε xr και $rx \in \bigcap_{i \in I} J_i$. Πραγματικά $x \in J_i$ για κάθε $i \in I$ επομένως $xr, rx \in J_i$ για κάθε $i \in I$ αφού το J_i ιδεώδες . Έτσι , $xr, rx \in \bigcap_{i \in I} J_i$. ■

Θα παρατηρήσουμε εδώ ότι , αν J_1 και J_2 είναι ιδεώδη ενός δακτυλίου R τότε η τομή τους $J_1 \cap J_2$ είναι το μεγαλύτερο ιδεώδες του R που περιέχεται και στο J_1 και στο J_2 .

§8.2. Παραγόμενα ιδεώδη .

Ας είναι X ένα υποσύνολο ενός δακτυλίου R .

Η τομή όλων των αμφίπλευρων ιδεωδών του R που περιέχουν το X , καλείται ιδεώδες παραγόμενο από το X και συμβολίζεται (X) . Είναι δηλαδή

$$(X) = \bigcap \{J / J \text{ ιδεώδες του } R, X \subseteq J\}$$

Αυτό είναι το "μικρότερο ιδεώδες" του R που περιέχει το X .

Αν το $X = \{x_1, \dots, x_n\}$ τότε το ιδεώδες (X) συμβολίζεται $(x_1, \dots, x_n)$ και λέμε ότι είναι πεπερασμένα παραγόμενο .

Ιδιαίτερα , το ιδεώδες (x) που παράγεται από το μονοσύνολο $\{x\}$ ονομάζεται κύριο ιδεώδες του R .

Παρατήρηση .

Με τον ίδιο τρόπο ορίζουμε το δεξιό (αντιστ. αριστερό) ιδεώδες που παράγεται από το X , συμβολισμός $(X)_\delta$ (αντιστ. $(X)_\alpha$) , σαν την τομή όλων των δεξιών (αντιστ. αριστερών) ιδεωδών του R που περιέχουν το X .

Η επόμενη πρόταση μας περιγράφει το κύριο ιδεώδες (x) σ'ένα αντιμεταθετικό δακτύλιο R με μονάδα .



Πρόταση 24 .

Αν ο δακτύλιος R είναι αντιμεταθετικός με μονάδα 1_R , τότε το κύριο ιδεώδες που παράγεται από το x είναι της μορφής

$$(x) = \{rx / r \in R\} .$$

Απόδειξη .

Το σύνολο $J = \{rx / r \in R\}$ είναι ένα ιδεώδες του R .

Πραγματικά, $J \neq \emptyset$ αφού $x = 1_R \cdot x \in J$. Επιπλέον

α) Για κάθε $r_1x, r_2x \in J$ έχουμε

$$r_1x - r_2x = (r_1 - r_2)x \in J$$

β) Για κάθε $r_1x \in J$ και $r \in R$ έχουμε

$$r_1xr = r_1rx \in J \quad \text{και} \quad rr_1x \in J .$$

Το J είναι το μικρότερο ιδεώδες του R που περιέχει το x , αφού αν $\mathcal{I}$ είναι ένα ιδεώδες του R που περιέχει το x τότε για κάθε $r \in R$ έχουμε $rx \in \mathcal{I}$ δηλαδή

$$J \subseteq \mathcal{I} .$$

Έτσι $J = (x)$. ■

Γενικότερα :

Αν R είναι ένας αντιμεταθετικός δακτύλιος με μονάδα και $X \subseteq R$, τότε το

$$(X) = \{ \sum r_i x_i / r_i \in R, x_i \in X \text{ και } \sum \text{ πεπερ. άθροισμα} \}$$

(Άσκηση)

Παρατήρηση .

Αν R είναι τυχόν δακτύλιος και $x \in R$ τότε :

1) Το αριστερό ιδεώδες που παράγεται από το x είναι της μορφής



$$(x)_\alpha = \{rx + nx / r \in R, n \in \mathbb{Z}\}.$$

2) Το δεξιό ιδεώδες που παράγεται από το x είναι της μορφής

$$(x)_\delta = \{xr + nx / r \in R, n \in \mathbb{Z}\}$$

3) Το αμφίπλευρο ιδεώδες που παράγεται από το x είναι της μορφής

$$(x) = \{nx + rx + xr' + \sum r_i xr'_i / r, r', r_i, r'_i \in R, n \in \mathbb{Z}, \sum \text{ πεπερ. άθροισμα} \}$$

Τέλος, αν ο R έχει μονάδα και δεν είναι αντιμεταθετικός έχουμε

$$4) (x)_\alpha = \{rx / r \in R\}$$

$$5) (x)_\delta = \{xr / r \in R\}$$

$$6) (x) = \left\{ \sum_{i=1}^n r_i xr'_i / r_i, r'_i \in R, n \in \mathbb{Z}^+ \right\} \quad (\text{Άσκηση}).$$

Πρόταση 25.

Κάθε πεδίο ακεραιότητας R με πεπερασμένο αριθμό ιδεωδών είναι σώμα.

Απόδειξη.

Αρκεί να δείξουμε ότι κάθε $x \in R, x \neq 0_R$ είναι αντιστρέψιμο. Θεωρούμε το σύνολο των κύριων ιδεωδών (x^n) όπου $n \in \mathbb{Z}^+$. Σύμφωνα με την πρόταση 24, έχουμε

$$(x^n) = \{rx^n / r \in R\}.$$

Αφού το R έχει πεπερασμένο αριθμό ιδεωδών θα έχουμε

$$(x^n) = (x^m)$$

για κάποιους θετικούς ακεραίους n, m .

Υποθέτουμε ότι $m < n$.



Αφού ο R έχει μονάδα $x^m \in (x^m)$ επομένως

$$x^m \in (x^n) \quad \text{δηλαδή} \quad x^m = r_1 x^n \quad \text{για κάποιο} \quad r_1 \in R.$$

Έτσι, $x^m = r_1 \cdot x^{n-m} \cdot x^m$ και από τους νόμους απλοποίησης

$$1_R = r_1 x^{n-m}$$

ή

$$(r_1 x^{n-m-1})x = 1_R = x(r_1 x^{n-m-1})$$

δηλαδή

$$x^{-1} = r_1 x^{n-m-1}, \quad \text{πράγμα που επιθυμούσαμε.} \blacksquare$$

Σαν πόρισμα της παραπάνω πρότασης μπορούμε να πάρουμε το γνωστό αποτέλεσμα, ότι κάθε πεπερασμένο πεδίο ακεραιότητας είναι σώμα (πρότ.7).

Πρόταση 26 .

Ας είναι R ένας αντιμεταθετικός δακτύλιος με μονάδα. Ο R είναι σώμα εάν και μόνο εάν δεν έχει μη-τετριμμένα ιδεώδη.

Απόδειξη .

Αν ο R είναι σώμα τότε τα μόνα ιδεώδη του είναι τα $\{0\}$ και R .

Αντίστροφα, αρκεί να δείξουμε ότι κάθε $x \in R$, $x \neq 0$ είναι αντιστρέψιμο. Θεωρούμε το κύριο ιδεώδες (x) που παράγεται από το x , είναι $(x) = \{rx / r \in R\}$.

Το $(x) \neq \{0\}$ αφού $x = 1x \in (x)$, οπότε σύμφωνα με την υπόθεση $(x) = R$. Έτσι $1 \in (x)$ δηλαδή $1 = rx$ με $r \in R$. Ο R όμως είναι αντιμεταθετικός οπότε έχουμε

$$rx = 1 = xr$$

δηλαδή $x^{-1} = r$, πράγμα που επιθυμούσαμε. $\blacksquare$

Σαν πόρισμα παίρνουμε την γνωστή πρόταση :



Ένας ομομορφισμός σωμάτων $f: F \longrightarrow F'$ είναι είτε ο τετριμμένος ομομορφισμός είτε ένας μονομορφισμός .

Πραγματικά , ο $\text{Ker}(f)$ σαν ιδεώδες του F θα είναι είτε $\{0\}$ είτε το F . Στην πρώτη περίπτωση ο f είναι μονομορφισμός ενώ στην δεύτερη ο τετριμμένος ομομορφισμός .

Όμοια παύρνουμε , ότι κάθε επιμορφισμός $f: F \longrightarrow F'$ σωμάτων είναι ένας ισομορφισμός .

§8.3. Supremum ιδεωδών .

Ας είναι R ένας δακτύλιος και J_1, J_2 δύο ιδεώδη του . Ο R είναι το μεγαλύτερο ιδεώδες που περιέχει τα J_1, J_2 . Γεννάται τώρα το ερώτημα . Ποιό είναι το μικρότερο ιδεώδες του R που περιέχει το J_1 και το J_2 ;

Η απάντηση στο ερώτημα αυτό θα ήταν απλή , αν το σύνολο $J_1 \cup J_2$ ήταν ιδεώδες του R . Αυτό όμως δεν συμβαίνει γενικά . Για παράδειγμα, η ένωση των ιδεωδών $\mathbb{Z} \times \{0\}$ και $\{0\} \times \mathbb{Z}$ του δακτυλίου $\mathbb{Z} \times \mathbb{Z}$ δεν είναι ιδεώδες του , αφού

$$(x, 0) - (0, y) = (x, -y) \notin (\mathbb{Z} \times \{0\}) \cup (\{0\} \times \mathbb{Z}) .$$

Ορισμός . Ονομάζουμε **Supremum** δύο ιδεωδών J_1 και J_2 ενός δακτυλίου R , και το συμβολίζουμε $J_1 \vee J_2$, το ιδεώδες που παράγεται από την ένωση $J_1 \cup J_2$ δηλαδή

$$J_1 \vee J_2 = (J_1 \cup J_2) .$$

Έτσι , $J_1 \vee J_2 = \bigcap \{ \mathfrak{I} / \mathfrak{I} \text{ ιδεώδες του } R \text{ με } J_1 \cup J_2 \subseteq \mathfrak{I} \}$.

Επομένως , το supremum $J_1 \vee J_2$ είναι το μικρότερο ιδεώδες του R που περιέχει και το J_1 και το J_2 .

Η επόμενη πρόταση μας περιγράφει το $J_1 \vee J_2$.



είναι σώμα . (βλέπε παραδ.13, §1.2) .

Έστω J ένα ιδεώδες του $F[x]$. Αν $J = \{0\}$ τότε $J = (0)$.

Υποθέτουμε ότι $J \neq \{0\}$, το J θα περιέχει επομένως και μη-μηδενικά πολυώνυμα . Αν M είναι το σύνολο των βαθμών των πολυωνύμων του J τότε $M \subseteq \mathbb{N}$, άρα το M έχει ελάχιστο στοιχείο m .

Υπάρχει λοιπόν $0 \neq P(x) \in J$ με $\deg P(x) = m$. Αν $D(x)$ είναι ένα τυχόν πολυώνυμο του J , τότε από την Ευκλείδεια διαίρεση υπάρχουν μοναδικά πολυώνυμα $q(x)$ και $r(x) \in F[x]$ έτσι ώστε

$$D(x) = P(x)q(x) + r(x) \quad \text{και} \quad r(x) = 0 \quad \text{ή} \quad \deg r(x) < m$$

Παρατηρούμε ότι

$$r(x) = D(x) - P(x)q(x) \in J$$

αφού το J είναι ιδεώδες .

Αν $r(x) \neq 0$, τότε θα υπάρχει πολυώνυμο του J με $\deg r(x) < m$ άτοπο από την υπόθεση μας , συνεπώς $r(x) = 0$ οπότε $D(x) = P(x)q(x)$. Επομένως $J \subseteq (P(x))$ αφού

$$(P(x)) = \{P(x)w(x) / w(x) \in F[x]\} .$$

Απ' την άλλη μεριά , για κάθε $w(x) \in F[x]$ έχουμε $P(x)w(x) \in J$ αφού το J είναι ιδεώδες , επομένως $(P(x)) \subseteq J$. Έτσι $J = (P(x))$.

Πρόταση 30 .

Ο δακτύλιος $\mathbb{Z}[i] = \{a+bi / a, b \in \mathbb{Z}\}$ των ακεραίων του Gauss είναι πεδίο κυρίων ιδεωδών .

Απόδειξη .

Ο δακτύλιος $\mathbb{Z}[i]$ είναι ένα πεδίο ακεραιότητας (βλέπε παραδ. 14, §1.2) .

Έστω J ένα ιδεώδες του $\mathbb{Z}[i]$. Αν $J = \{0\}$, τότε $J = (0)$. Υποθέτουμε ότι $J \neq \{0\}$ και εκλέγουμε ένα μη-μηδενικό στοιχείο $\alpha \in J$ με ελάχιστη απόλυτη τιμή (μέτρο) . Θα δείξουμε ότι $J = (\alpha)$.



Έστω $\beta \in J$, είναι φανερό τώρα ότι

$$\frac{\beta}{\alpha} \in Q[i] = \{r+si / r,s \in Q\}$$

Έστω

$$\frac{\beta}{\alpha} = r+si \quad \text{για κάποια } r,s \in Q.$$

Εκλέγουμε ακέραιους p και q τέτοιους ώστε

$$0 \leq |r-p| \leq \frac{1}{2}, \quad 0 \leq |s-q| \leq \frac{1}{2}$$

Έστω $\gamma = p+qi \in Z[i]$ οπότε

$$\left| \frac{\beta}{\alpha} - \gamma \right| = \sqrt{(r-p)^2 + (s-q)^2} \leq \sqrt{\frac{1}{4} + \frac{1}{4}} = \frac{1}{\sqrt{2}} < 1 \quad (18)$$

Ας είναι τώρα $\delta = \beta - \alpha\gamma$. Επειδή $\alpha \in J$, $\beta \in J$ το $\gamma \in Z[i]$ και το J ιδεώδες έχουμε $\delta \in J$. Επιπλέον

$$|\delta| = |\beta - \alpha\gamma| = \left| \alpha \left(\frac{\beta}{\alpha} - \gamma \right) \right| = |\alpha| \left| \frac{\beta}{\alpha} - \gamma \right| < |\alpha| \quad (\text{λόγω της (18)})$$

Αν $\delta \neq 0$, τότε θα υπάρξει $\delta \in J$ με $|\delta| < |\alpha|$ άτοπο από την υπόθεσή μας. Έτσι $\delta = 0$ και επομένως $\beta = \alpha\gamma$, οπότε $J \subseteq (\alpha)$.

Απ' την άλλη μεριά,

$$(\alpha) = \{\alpha\gamma / \gamma \in Z[i]\}$$

και αφού το $\alpha \in J$ και το J ιδεώδες θα έχουμε $\alpha\gamma \in J$ για κάθε $\gamma \in Z[i]$ δηλαδή

$$(\alpha) \subseteq J.$$

Έτσι $J = (\alpha)$ πράγμα που επιθυμούσαμε. ■

Δεν είναι όμως όλοι οι δοκτύλιοι δοκτύλιοι κύριων ιδεωδών, όπως φαίνεται από το παρακάτω παράδειγμα.

Παράδειγμα 6.

Το πεδίο ακεραιότητας $Z[x]$ των πολυωνύμων με ακέραιους συντε-



λεστές δεν είναι περιοχή κυρίων ιδεωδών .

Για το ιδεώδες $(2, x)$ του $\mathbb{Z}[x]$ που παράγεται από τα στοιχεία 2 και x του $\mathbb{Z}[x]$ έχουμε

$$(2, x) = \{2h(x) + xk(x) / h(x), k(x) \in \mathbb{Z}[x]\} \quad (\text{Άσκηση}) .$$

Το $(2, x)$ λοιπόν περιέχει όλα τα πολυώνυμα του $\mathbb{Z}[x]$ που έχουν σταθερό όρο άρτιο αριθμό .

Θα δείξουμε ότι το ιδεώδες $(2, x)$ δεν είναι κύριο ιδεώδες .

Πραγματικά αν ήταν κύριο ιδεώδες θα υπήρχε πολυώνυμο $f(x) \in \mathbb{Z}[x]$ τέτοιο ώστε

$$(2, x) = (f(x)) .$$

Αλλά $2 \in (2, x)$ και $x \in (2, x)$, οπότε

$$2 = f(x)h(x) \quad h(x) \in \mathbb{Z}[x]$$

$$x = f(x)h'(x) \quad h'(x) \in \mathbb{Z}[x]$$

πράγμα άτοπο , αν λάβουμε υπ' όψη μας ότι

$$\deg(\varphi(x)g(x)) = \deg\varphi(x) + \deg g(x)$$

για κάθε $\varphi(x), g(x) \in \mathbb{Z}[x]$. ■

§8.5. Πρόξεις επί των ιδεωδών .

A. Άθροισμα ιδεωδών .

Έστω J_1, J_2 δύο ιδεώδη ενός δακτυλίου R .

Ορίζουμε το άθροισμά τους ως εξής :

$$J_1 + J_2 = \{x+y / x \in J_1, y \in J_2\}$$

Το σύνολο $J_1 + J_2$ είναι ένα ιδεώδες του R .

Πραγματικά , είδαμε ότι το supremum $J_1 \vee J_2 = J_1 + J_2$. Έτσι το άθροισμα $J_1 + J_2$ είναι το ιδεώδες που παράγεται από την ένωση $J_1 \cup J_2$, με άλλα λόγια είναι το $J_1 + J_2$ το μικρότερο ιδεώδες του R που περιέ-



χει το J_1 και το J_2 .

Παράδειγμα 7 .

Στο δακτύλιο $\mathbb{Z}$ των ακεραίων θεωρούμε τα ιδεώδη (κύρια)
 $J_1 = (m)$ και $J_2 = (n)$. Το άθροισμά τους

$$(m) + (n) = (d)$$

όπου $d = (m, n)$ είναι ο Μ.Κ.Δ. των m, n .

Πραγματικά, $(m) + (n) = \{km + \lambda n / k, \lambda \in \mathbb{Z}\}$, και επειδή κάθε ιδεώδες του $\mathbb{Z}$ είναι κύριο, θα υπάρχει ακέραιος d τέτοιος ώστε

$$\{km + \lambda n / k, \lambda \in \mathbb{Z}\} = (d)$$

Έτσι $m \in (d)$ και $n \in (d)$ οπότε $d|m$ και $d|n$, δηλαδή ο d είναι ένας κοινός διαιρέτης των m και n . Απ' την άλλη μεριά, υπάρχουν ακέραιοι k, λ με

$$km + \lambda n = d \quad . \quad (19)$$

Έτσι αν δ είναι ένας άλλος κοινός διαιρέτης των m και n θα είναι $m = \delta m'$ και $n = \delta n'$ οπότε από την (19) έχουμε $\delta | d$, επομένως $d = (m, n)$.

Όμοια το άθροισμα πεπερασμένου πλήθους ιδεωδών $J_1, J_2, \dots, J_n$ ενός δακτύλιου R ορίζεται ως εξής

$$J_1 + J_2 + \dots + J_n = \{x_1 + x_2 + \dots + x_n / x_i \in J_i\}$$

Το $J_1 + J_2 + \dots + J_n$ είναι ένα ιδεωδές του R και μάλιστα είναι το ιδεωδες που παράγεται από την ένωση $J_1 \cup J_2 \cup \dots \cup J_n$. Με άλλα λόγια το $J_1 + J_2 + \dots + J_n$ είναι το μικρότερο ιδεώδες που περιέχει τα J_i .

Β.Γινόμενο ιδεωδών .

Έστω J_1, J_2 δύο ιδεώδη ενός δακτυλίου R . Ορίζουμε το γινόμενο τους ως εξής :



Γενικότερα, αν $J_1, \dots, J_n$ είναι ιδεώδη ενός δακτυλίου R το γινόμενο τους $J_1 J_2 \dots J_n$ είναι το ιδεώδες του R που ορίζεται ως εξής :

$$J_1 J_2 \dots J_n = \{ \sum x_1 \dots x_n / x_i \in J_i, \sum \text{ πεπερ. άθροισμα} \}$$

Στην ειδική περίπτωση όπου $J_1 = J_2 = \dots = J_n = J$ θα δηλώνουμε το γινόμενο $J_1 J_2 \dots J_n = J J \dots J$ με J^n . Έτσι

$$J^n = \{ \sum x_{i_1} \dots x_{i_k} / x_{i_k} \in J, \sum \text{ πεπερ. άθροισμα} \}.$$

Θα παρατηρήσουμε εδώ ότι τα ιδεώδη

$$J \supseteq J^2 \supseteq \dots \supseteq J^n \supseteq \dots$$

σχηματίζουν μια φθίνουσα αλυσή ιδεωδών.

Αν $J, J_1, \dots, J_n, W, \mathfrak{f}$ είναι ιδεώδη ενός δακτυλίου R τότε:

$$(1) J+W = W+J$$

$$(2) J+(W+\mathfrak{f}) = (J+W)+\mathfrak{f}$$

$$(3) J(W \mathfrak{f}) = (JW)\mathfrak{f}$$

$$(4) W(J_1 + \dots + J_n) = WJ_1 + \dots + WJ_n \quad \text{και}$$

$$(J_1 + \dots + J_n)\mathfrak{f} = J_1\mathfrak{f} + \dots + J_n\mathfrak{f}.$$

(5) Αν ο R είναι αντιμεταθετικός δακτύλιος

$$JW = WJ \quad . \quad (\text{Άσκηση})$$

8.6. Δακτύλιος πηλίκο .

Υπενθυμίζουμε εδώ και πάλι ότι τα ιδεώδη στην θεωρία δακτυλίων παίζουν τον ίδιο ρόλο που παίζουν και οι κανονικές υποομάδες στην θεωρία ομάδων .



Έστω R ένας δακτύλιος και J ένα ιδεώδες του .

Επειδή η προσθετική ομάδα $(R,+)$ είναι αβελιανή η υποομάδα της $(J,+)$ είναι κανονική . Ορίζεται επομένως η προσθετική ομάδα πηλίκου R/J με πρόσθεση ορισμένη από :

$$(J+x)+(J+y) = J+x+y \quad (20)$$

Η ομάδα R/J δομείται σε δακτύλιο .

Πρόταση 31 .

Έστω R ένα δακτύλιος και J ένα ιδεώδες του . Η προσθετική ομάδα R/J είναι ένας δακτύλιος με πολ/σμό που ορίζεται από τη σχέση

$$(J+x)(J+y) = J+xy \quad (21)$$

Αν ο R είναι αντιμεταθετικός ή έχει μονάδα τότε το ίδιο ισχύει και για τον δακτύλιο R/J .

Απόδειξη .

Πρώτα θα δείξουμε ότι ο πολ/σμός είναι καλά ορισμένος , δηλαδή αν

$$J+x = J+x_1 \text{ και } J+y = J+y_1 \text{ τότε } J+xy = J+x_1y_1$$

$$\text{ή } xy - x_1y_1 \in J .$$

Πραγματικά από την υπόθεση $x-x_1 \in J$ και $y-y_1 \in J$ οπότε

$$xy - x_1y_1 = x(y-y_1) + (x-x_1)y_1 \in J$$

πράγμα που επιθυμούσαμε .

Είναι εύκολο τώρα να διαπιστώσουμε ότι ο πολ/σμός είναι προσεταιριστικός και ότι ισχύουν οι επιμεριστικοί νόμοι .

Το σύνολο πηλίκου R/J εφοδιασμένο με τις πράξεις (20) και (21) γίνεται λοιπόν ένας δακτύλιος .

Αν ο R είναι αντιμεταθετικός τότε και ο δακτύλιος R/J είναι αντιμεταθετικός αφού



$$(J+x)(J+y) = J+xy = J+yx = (J+y)(J+x) .$$

Τέλος , αν ο R έχει μονάδα 1_R , τότε το στοιχείο $J+1_R$ είναι μονάδα στον δακτύλιο R/J αφού

$$(J+x)(J+1_R) = J+x = (J+1_R)(J+x) .$$

Ο δακτύλιος R/J καλείται **δακτύλιος πηλίκου** . ■

Υπενθυμίζουμε ότι το μηδενικό στοιχείο του είναι το συμπλοκο J ενώ

$$\alpha) J+x = J \text{ εάν και μόνο εάν } x \in J$$

$$\beta) J+x = J+y \text{ εάν και μόνο εάν } x-y \in J .$$

Για να ξεκαθαρίσουμε περισσότερο τον ρόλο που παίζουν τα ιδεώδη στον σχηματισμό του δακτυλίου πηλίκου δίνουμε το επόμενο θεώρημα .

Θεώρημα 3 .

Έστω R ένας δακτύλιος . Το σύνολο $\mathcal{A}$ όλων των σχέσεων ισοδυναμίας στο R που συμβιβάζονται με τις πράξεις του δακτυλίου είναι ισοδύναμο με το σύνολο $\mathcal{B}$ όλων των ιδεωδών του R δηλαδή

$$|\mathcal{A}| = |\mathcal{B}|$$

Με άλλα λόγια υπάρχουν τόσες σχέσεις ισοδυναμίας στο R που συμβιβάζονται με τις πράξεις του R όσα είναι και τα ιδεώδη του R .

Απόδειξη .

α) Κάθε ιδεώδες J του δακτυλίου R ορίζει στο σύνολο R μια σχέση ισοδυναμίας S_J συμβιβαστή με την πρόσθεση και τον πολ/σμό του R :

$$x \equiv y(S_J) \iff x-y \in J .$$

Το ότι η S_J είναι μια σχέση ισοδυναμίας συμβιβαστή με την πρόσθεση του R προκύπτει από το αντίστοιχο αποτέλεσμα της θεωρία ομάδων



(βλέπε Θεωρ. 9, Κεφ. II) παρατηρώντας ότι το $(J, +)$ είναι κανονική υποομάδα της $(R, +)$.

Μένει να δείξουμε ότι είναι συμβιβαστή και με τον πολ/σμό δηλαδή ότι

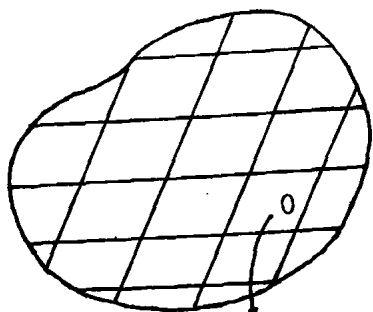
$$\left. \begin{array}{l} x \equiv y (S_J) \\ x' \equiv y' (S_J) \end{array} \right\} \implies xx' \equiv yy' (S_J)$$

Αλλά οι $x \equiv y (S_J)$ και $x' \equiv y' (S_J)$ σημαίνουν $x - y \in J$ και $x' - y' \in J$ οπότε αφού το J είναι ιδεώδες

$$x(x' - y') + (x - y)y' \in J \quad \text{δηλαδή} \quad xx' - yy' \in J$$

που ισοδυναμεί με $xx' \equiv yy' (S_J)$.

β) Αντίστροφα, αν S είναι μια σχέση ισοδυναμίας στο R συμβιβαστή και με την πρόσθεση και τον πολ/σμό του R , τότε η κλάση ισοδυναμίας του μηδενικού στοιχείου του



$$S(0) = \{x/x \in R, x \equiv 0(S)\}$$

είναι ένα ιδεώδες του R .

Πραγματικά,

$$x, y \in S(0) \iff \begin{cases} x \equiv 0(S) \\ y \equiv 0(S) \end{cases}$$

και επειδή η S είναι συμβιβαστή με την πρόσθεση του R θα έχουμε $x - y \equiv 0(S)$ δηλαδή $x - y \in S$. Επίσης για κάθε $x \in S(0)$ και $r \in R$ έχουμε

$$\left. \begin{array}{l} x \equiv 0(S) \\ r \equiv r(S) \end{array} \right\} \implies xr \equiv 0(S) \quad \text{και} \quad rx \equiv 0(S)$$

δηλαδή $xr \in S$ και $rx \in S$.



γ) Ορίζουμε τις απεικονίσεις :

$$\psi : A \longrightarrow B, \quad s \longmapsto s(0)$$

και

$$\phi : B \longrightarrow A, \quad j \longmapsto s_j$$

Είναι εύκολο να δείξουμε ότι :

$$\phi \circ \psi = I_A \quad \text{και} \quad \psi \circ \phi = I_B \quad . \quad \blacksquare$$

Παράδειγμα 9 .

Έστω (n) ένα κύριο ιδεώδες του δακτυλίου Z . Το σύνολο πηλίκου $Z/(n)$ έχει στοιχεία σύμπλοκα

$$(n)+x = \{kn+x / k \in Z\}, \quad x \in Z$$

που είναι ακριβώς η κλάση ισοδυναμίας $\bar{x} \in Z_n$. Τα διακεκριμένα λοιπόν στοιχεία του είναι τα σύμπλοκα

$$(n), (n)+1, \dots, (n)+n-1 .$$

Οι πράξεις στο $Z/(n)$ ορίζονται από τις σχέσεις

$$((n)+x) + ((n)+y) = (n)+x+y$$

$$((n)+x) \cdot ((n)+y) = (n)+xy .$$

Ο δακτύλιος πηλίκου $Z/(n)$ μπορεί να περιγραφεί ακριβώς σαν ο δακτύλιος Z_n .

Παράδειγμα 10 .

Στο δακτύλιο των πολυωνύμων $\mathbb{R}[X]$ με συντελεστές από το σώμα $\mathbb{R}$ των πραγματικών αριθμών , θεωρούμε το ιδεώδες

$$(x^2+1) = \{P(x)(x^2+1) / P(x) \in \mathbb{R}[X]\}$$

Τα στοιχεία του δακτυλίου πηλίκου $\mathbb{R}[X]/(x^2+1)$ είναι σύμπλοκα

$$(x^2+1)+P(x), \quad P(x) \in \mathbb{R}[X]$$



ενώ η πρόσθεση και ο πολ/σμός ορίζονται από τις σχέσεις

$$\begin{aligned}(x^2+1)+P(x) + (x^2+1)+W(x) &= (x^2+1)+P(x)+W(x) \\ (x^2+1)+P(x) \cdot (x^2+1)+W(x) &= (x^2+1)+P(x)W(x) \quad .\end{aligned}$$

8.7. Θεωρήματα ισομορφισμών .

Έχουμε δει ότι ο πυρήνας κάθε ομομορφισμού δακτυλίων είναι ένα ιδεώδες (βλέπε προτ.21) αλλά και αντίστροφα , όπως θα δούμε πιο κάτω, κάθε ιδεώδες J ενός δακτυλίου R είναι ο πυρήνας ενός ομομορφισμού από τον R στον R/J .

Ας είναι J ένα ιδεώδες του R . Η απεικόνιση

$$p: R \longrightarrow R/J, \quad p(x) = J+x, \quad \forall x \in R$$

είναι ένας ομομορφισμός δακτυλίων με $\text{Ker } p = J$.

Πραγματικά , η p είναι φανερά επί και

$$p(x+y) = J+x+y = (J+x)+(J+y) = p(x)+p(y)$$

$$p(xy) = J+xy = (J+x)(J+y) = p(x)p(y)$$

για κάθε $x, y \in R$ και επιπλέον

$$\text{Ker } p = \{x \in R / p(x) = J\} = \{x \in R / J+x = J\} = \{x \in R / x \in J\} = J$$

Η απεικόνιση p καλείται κανονική προβολή του R στο R/J .

Όπως θα δούμε παρακάτω τα θεωρήματα ισομορφισμών στις ομάδες μεταφέρονται και στους δακτύλιους αντικαθιστώντας τις έννοιες κανονική υποομάδα και ομάδα με τις έννοιες ιδεώδες και δακτύλιος αντίστοιχα .

Εκείνο όμως που θα τονίσουμε είναι ότι , στις ομάδες στα θεωρήματα ισομορφισμών χρησιμοποιήσαμε πολ/κες ομάδες ενώ , οι ομάδες που χρησιμοποιούμε εδώ είναι προσθετικές .



ΛΗΜΜΑ 1 .

Ας είναι $f: R \longrightarrow R'$ ένας ομομορφισμός δακτυλίων και J ένα ιδεώδες του R που περιέχεται στον πυρήνα της f δηλαδή $J \subseteq \text{Ker } f$. Τότε υπάρχει μοναδικός ομομορφισμός δακτυλίων

$$\bar{f}: R/J \longrightarrow R'$$

που κάνει το επόμενο διάγραμμα αντιμεταθετικό

$$\begin{array}{ccc} R & \xrightarrow{p} & R/J \\ & \searrow f & \downarrow \bar{f} \\ & & R' \end{array} \quad (I)$$

δηλαδή $f = \bar{f} \circ p$

Απόδειξη .

Αφού ο f είναι ομομορφισμός προσθετικών αβελιανών ομάδων $f: (R, +) \longrightarrow (R', +)$ και J μια κανονική υποομάδα της $(R, +)$ το ΛΗΜΜΑ 1 (Κεφ. II, §10) μας δίνει μοναδικό ομομορφισμό ομάδων

$\bar{f}: (R/J, +) \longrightarrow (R', +)$ ορισμένον από

$$\bar{f}(J+x) = f(x) \quad \text{για κάθε } x \in R$$

που κάνει το διάγραμμα (I) αντιμεταθετικό .

Μένει να δείξουμε ότι ο $\bar{f}$ είναι ομομορφισμός δακτυλίων . Πραγματικά , για κάθε $J+x, J+y \in R/J$.

$$\bar{f}((J+x)(J+y)) = \bar{f}(J+xy) = f(xy) = f(x)f(y) = \bar{f}(J+x)\bar{f}(J+y) \quad . \blacksquare$$

ΘΕΩΡΗΜΑ 4 . (Θεμελιώδες θεώρημα Ομομορφισμών) .

Κάθε ομομορφισμός δακτυλίων $f: R \longrightarrow R'$ ορίζει ένα μοναδικό μονομορφισμό

$$\bar{f}: R/\text{Ker } f \longrightarrow R' , \quad \bar{f}[\text{Ker } f + x] = f(x) , \quad \forall x \in R$$

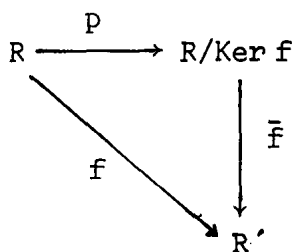


Ιδιαίτερα

$$R/\text{Ker } f \simeq \text{Im}(f) .$$

Απόδειξη .

Σύμφωνα με το λήμμα 1 υπάρχει μοναδικός ομομορφισμός $\bar{f} : R/\text{Ker } f \longrightarrow R'$ που κάνει το παρακάτω διάγραμμα αντιμεταθετικό



δηλαδή $f = \bar{f} \circ p$.

Έτσι $\bar{f}[\text{Ker } f + x] = f(x)$, $\forall x \in R$

Η απόδειξη ότι ο $\bar{f}$ είναι μονομορφισμός γίνεται με τον ίδιο τρόπο όπως και στο θεώρημα 10 (Κεφ. II, §10) .

Αφού ο $\bar{f}$ είναι μονομορφισμός έχουμε

$$R/\text{Ker } f \simeq \text{Im}(\bar{f})$$

Αλλά $\text{Im}(\bar{f}) = \text{Im}(f)$ οπότε $R/\text{Ker } f \simeq \text{Im}(f)$. ■

ΠΟΡΙΣΜΑ 1.

Αν $f : R \longrightarrow R'$ είναι ένας επιμορφισμός δακτυλίων τότε

$$R/\text{Ker } f \simeq R' . \quad \blacksquare$$

Παράδειγμα 11 .

Κάθε επιμορφισμός από ένα δακτύλιο R στο δακτύλιο $\mathbb{Z}$ των ακεραίων είναι μοναδικά ορισμένος από τον πυρήνα του .

Πραγματικά, υποθέτουμε ότι $f, h : R \longrightarrow \mathbb{Z}$ είναι δύο επιμορφισμοί έτσι ώστε $\text{Ker } f = \text{Ker } h$.



Από το προηγούμενο πόρισμα υπάρχουν δύο ισομορφισμούς

$$f' : R/\text{Ker } f \longrightarrow \mathbb{Z} \quad , \quad h' : R/\text{Ker } h \longrightarrow \mathbb{Z}$$

Αλλά $\text{Ker } f = \text{Ker } h$, οπότε έχουμε δύο ισομορφισμούς από τον δακτύλιο $R/\text{Ker } f$ στον $\mathbb{Z}$. Αλλά όπως γνωρίζουμε (βλέπε Κεφ. II, §6.1) υπάρχει το πολύ ένας ισομορφισμός από ένα τυχόντα δακτύλιο στο δακτύλιο $\mathbb{Z}$ των ακεραίων , άρα $f' = h'$. Τελικά , από τις σχέσεις $f = f' \circ p$, $h = h' \circ p'$ όπου p, p' οι κανονικές προβολές

$$p : R \longrightarrow R/\text{Ker } f \quad , \quad p' : R \longrightarrow R/\text{Ker } h$$

έχουμε $f = h$.

Παράδειγμα 12 .

Έστω $f : \mathbb{Z} \longrightarrow F$ ένας επιμορφισμός από τον δακτύλιο $\mathbb{Z}$ των ακεραίων σε ένα σώμα F .

Από το προηγούμενο πόρισμα έχουμε

$$\mathbb{Z} / \text{Ker } (f) \cong F$$

όπου $\text{Ker } f = (n)$ για κάποιο θετικό ακέραιο n αφού , ο δακτύλιος $\mathbb{Z}$ είναι δακτύλιος κυρίων ιδεωδών . Επίσης $(n) \neq \{0\}$ γιατί διαφορετικά $\mathbb{Z} \cong F$, άτοπο . Αλλά $\mathbb{Z}/(n) \cong \mathbb{Z}_n$ οπότε

$$\mathbb{Z}_n \cong F$$

και έτσι το σώμα F έχει n -στοιχεία όπου n πρώτος αριθμός αφού ο $\mathbb{Z}_n$ είναι σώμα εάν και μόνο εάν ο n είναι πρώτος αριθμός (βλέπε πρότ. 6) .

Παράδειγμα 13 .

Έστω R ένας δακτύλιος με μοναδα 1_R , τότε η απεικόνιση

$$\varphi : \mathbb{Z} \longrightarrow R \quad , \quad \varphi(n) = n1_R \quad , \quad \forall n \in \mathbb{Z}$$

είναι ένας ομομορφισμός δακτυλίων με $\text{Ker } \varphi = (p)$ όπου $p = \text{char } R$.



Επιπλέον

α) Αν $\text{char } R = p > 1$ τότε ο R περιέχει ένα υποδακτύλιο ισομόρφο με τον $\mathbb{Z}_p$.

β) Αν $\text{char } R = 0$ τότε περιέχει ο R ένα υποδακτύλιο ισομόρφο με τον $\mathbb{Z}$.

Πραγματικά, η φ είναι ομομορφισμός αφού για κάθε $m, n \in \mathbb{Z}$ έχουμε

$$\varphi(n+m) = (n+m)1_R = n1_R + m1_R = \varphi(n) + \varphi(m)$$

$$\varphi(nm) = (nm)1_R = n(m1_R) = (n1_R)(m1_R) = \varphi(n)\varphi(m)$$

Επιπλέον $\text{Ker } \varphi = \{n \in \mathbb{Z} / n1_R = 0\} = (p)$ $p \geq 0$. $0 \neq p = \text{char } R$, πραγματικά ισχύει $\varphi(p) = p1_R = 0$ αφού $p \in \text{Ker } \varphi$ και ο p είναι ο ελάχιστος θετικός ακέραιος με την ιδιότητα αυτή, αφού αν $\lambda \in \mathbb{Z}^+$ με $\lambda 1_R = 0$ τότε $\lambda \in \text{Ker } \varphi$ οπότε $\lambda = pk$, $k > 0$ άρα $\lambda \geq p$.

α) Αν $p > 1$ τότε

$$\mathbb{Z}/\text{Ker } \varphi = \mathbb{Z}/(p) \cong \varphi(\mathbb{Z})$$

ή $\mathbb{Z}_p \cong \varphi(\mathbb{Z})$ με $\varphi(\mathbb{Z})$ υποδακτύλιο του R .

β) Αν $\text{char } R = 0$ τότε $n1_R \neq 0$ για κάθε $n \neq 0$ και έτσι $\text{Ker } \varphi = (0)$ συνεπώς

$$\mathbb{Z}/\text{Ker } \varphi = \mathbb{Z}/(0) = \mathbb{Z} \cong \varphi(\mathbb{Z})$$

ΘΕΩΡΗΜΑ 5. (Δεύτερο θεώρημα ισομορφισμών)

Αν $\mathcal{I}$ και J είναι δύο ιδεώδη ενός δακτυλίου R , τότε

$$\mathcal{I}/\mathcal{I} \cap J \cong \mathcal{I} + J/J$$

Απόδειξη.

Αρχικά παρατηρούμε ότι οι δακτύλιοι πηλύκο $\mathcal{I}/\mathcal{I} \cap J$ και $\mathcal{I} + J/J$ ορίζονται αφού το $\mathcal{I} \cap J$ είναι ιδεώδες του $\mathcal{I}$ και το J είναι ιδεώδες του $\mathcal{I} + J$ ($J \subseteq \mathcal{I} + J$). Τώρα, αφού η $(J, +)$ είναι κανονική υποομά-



δα της $(R, +)$ το δεύτερο θεώρημα ισομορφισμών για ομάδες μας δίνει τον ισομορφισμό ομάδων

$$f: \mathfrak{I}/\mathfrak{I} \cap J \longrightarrow \mathfrak{I} + J/J$$

$$f((\mathfrak{I} \cap J) + x) = J + x \quad \text{για κάθε } (\mathfrak{I} \cap J) + x \in \mathfrak{I}/\mathfrak{I} \cap J$$

Αρκεί να δείξουμε ότι ο f είναι ομομορφισμός δακτυλίων .

Πραγματικά , ο f είναι ομομορφισμός ομάδων και επιπλέον για κάθε $(\mathfrak{I} \cap J) + x$, $(\mathfrak{I} \cap J) + y \in \mathfrak{I}/\mathfrak{I} \cap J$ έχουμε

$$\begin{aligned} f[(\mathfrak{I} \cap J) + x](\mathfrak{I} \cap J) + y] &= f((\mathfrak{I} \cap J) + xy) = J + xy \\ &= (J + x)(J + y) = f(\mathfrak{I} \cap J) + x)f(\mathfrak{I} \cap J) + y) . \end{aligned}$$

ΘΕΩΡΗΜΑ 6 . (Τρίτο Θεώρημα Ισομορφισμών)

Αν $\mathfrak{I}$ και J είναι ιδεώδη ενός δακτυλίου R έτσι ώστε το $J \subseteq \mathfrak{I}$, τότε το $\mathfrak{I}/J$ είναι ιδεώδες του δακτυλίου R/J και

$$R/J / \mathfrak{I}/J \cong R/\mathfrak{I}$$

Απόδειξη .

Εργαζόμαστε όπως στο αντίστοιχο θεώρημα για ομάδες . Δηλαδή ορίζουμε την απεικόνιση

$$f: R/J \longrightarrow R/\mathfrak{I} , \quad f(J+x) = \mathfrak{I} + x , \quad \forall x \in R$$

και αποδεικνύουμε ότι η f είναι καλά ορισμένη , και ότι είναι ένας επιμορφισμός δακτυλίων με $\text{Ker } f = \mathfrak{I}/J$, οπότε το $\mathfrak{I}/J$ είναι ιδεώδες του δακτυλίου R/J . Σύμφωνα τώρα με το θεώρημα 4

$$R/J / \mathfrak{I}/J \cong \text{Im}(f) = R/\mathfrak{I} .$$

ΛΗΜΜΑ 2 .

Αν $f: R \longrightarrow R'$ είναι ένας ομομορφισμός δακτυλίων και $\mathfrak{I}$ ένα ιδεώδες του R που περιέχει τον πυρήνα δηλαδή $\text{Ker } f \subseteq \mathfrak{I}$ τότε

$$f^{-1}(f(\mathfrak{I})) = \mathfrak{I} .$$



Απόδειξη .

Εργαζόμαστε όπως και στο Λήμμα 2 , (Κεφ. II, §10)

ΘΕΩΡΗΜΑ 7 .

Έστω $f: R \longrightarrow R'$ ένας επιμορφισμός δακτυλίων . Αν U είναι το σύνολο όλων των ιδεωδών $\mathfrak{f}$ του R με $\text{Ker } f \subseteq \mathfrak{f}$ και W το σύνολο όλων των ιδεωδών του R' τότε η απεικόνιση

$$\psi: U \longrightarrow W, \quad \mathfrak{f} \longmapsto f(\mathfrak{f})$$

είναι 1-1 και επί .

Απόδειξη .

Η απόδειξη αφήνεται στον αναγνώστη , (βλέπε Θεωρ. 13, Κεφ. II, §10) ■

Η μορφή των ιδεωδών ενός δακτυλίου πηλίκου δίνεται από το παρακάτω πόρισμα .

ΠΟΡΙΣΜΑ 2 .

Αν $\mathfrak{f}$ είναι ένα ιδεώδες ενός δακτυλίου R , τότε κάθε ιδεώδες του $R/\mathfrak{f}$ είναι της μορφής $J/\mathfrak{f}$ όπου J ιδεώδες του R τέτοιο ώστε $\mathfrak{f} \subseteq J$.

Απόδειξη .

Όπως και στο πόρισμα 2 (Κεφ. II, §10) .

Παράδειγμα 14 .

Ο δακτύλιος $\mathbb{Z}_m$ των ακεραίων mod m έχει ακριβώς ένα ιδεώδες για κάθε θετικό διαιρέτη n του m και όχι άλλα ιδεώδη .

Πραγματικά , αφού $\mathbb{Z}_m \cong \mathbb{Z}/(m)$ το προηγούμενο πόρισμα μας λέει ότι τα ιδεώδη του $\mathbb{Z}/(m)$ είναι της μορφής $(n)/(m)$ όπου (n)



ιδεώδες του $\mathbb{Z}$ τέτοιο ώστε $(m) \subseteq (n)$. Η τελευταία σχέση όμως ισχύει εάν και μόνο εάν $n \mid m$.

8.8. Πρωτοσώματα

Ένα υπόσωμα S ενός σώματος F καλείται γνήσιο αν $S \neq F$.

Ορισμός. Ονομάζουμε πρωτόσωμα κάθε σώμα που δεν έχει γνήσια υποσώματα.

Παράδειγμα 15.

Το σώμα $\mathbb{Z}_p$ των ακεραιών $\text{mod } p$, p πρώτος, είναι πρωτόσωμα.

Πραγματικά, αν S είναι ένα υπόσωμα του $\mathbb{Z}_p$, η ομάδα $(S, +)$, σύμφωνα με το θεώρημα του Lagrange, έχει τάξη 1 ή p αφού ο p πρώτος. Αλλά $|S| \neq 1$ αφού το S είναι σώμα, επομένως $|S| = p$ δηλαδή $S = \mathbb{Z}_p$.

Παράδειγμα 16.

Το σώμα $\mathbb{Q}$ των ρητών είναι πρωτόσωμα.

Πραγματικά, έστω F ένα υπόσωμα του $\mathbb{Q}$ και $a \in F$, $a \neq 0$. Το υπόσωμα F περιέχει τη μονάδα αφού $a \cdot a^{-1} = 1 \in F$ οπότε για κάθε $n \in \mathbb{Z}$ έχουμε

$$n = n \cdot 1 \in F$$

δηλαδή $\mathbb{Z} \subseteq F$. Έτσι για κάθε $\frac{m}{n} \in \mathbb{Q}$, $n \neq 0$ έχουμε

$$\frac{m}{n} = mn^{-1} \in F$$

οπότε $\mathbb{Q} \subseteq F$, καθώς όμως $F \subseteq \mathbb{Q}$ παίρνουμε $\mathbb{Q} = F$.

Παράδειγμα 17.

Έστω $\{F_i\}_{i \in I}$ η οικογένεια όλων των υποσωμάτων ενός σώματος



F . Το υπόσωμα $\bigcap_{i \in I} F_i$ είναι πρωτόσωμα .

Πραγματικά , αν S είναι ένα υπόσωμα του $\bigcap_{i \in I} F_i$, τότε το S θα είναι υπόσωμα του F συνεπώς $S \in \{F_i\}_{i \in I}$ άρα $\bigcap_{i \in I} F_i \subseteq S$.

Καθώς όμως $S \subseteq \bigcap_{i \in I} F_i$ συνεπάγεται

$$S = \bigcap_{i \in I} F_i$$

δηλαδή το σώμα $\bigcap_{i \in I} F_i$ δεν έχει γνήσια υποσώματα .

Πρόταση 32 .

Κάθε σώμα F περιέχει ένα μοναδικό πρωτοῦπόσωμα .

Απόδειξη .

Η τομή της οικογένειας $\{F_i\}_{i \in I}$ όλων των υποσωμάτων του F

είναι ένα πρωτοῦπόσωμα του F .

Μένει να δείξουμε την μοναδικότητα .

Ας είναι F_1, F_2 δύο πρωτοῦποσώματα του F . Η τομή τους $F_1 \cap F_2$ είναι ένα υπόσωμα του F τέτοιο ώστε

$$F_1 \cap F_2 \subseteq F_1 \quad \text{και} \quad F_1 \cap F_2 \subseteq F_2 .$$

Αλλά τα F_1, F_2 σαν πρωτοσώματα δεν έχουν γνήσια υποσώματα έτσι

$$F_1 \cap F_2 = F_1 = F_2 . \quad \blacksquare$$

Στη συνέχεια θα δείξουμε ότι κατά προσέγγιση ισομορφισμού τα μόνα πρωτοσώματα είναι το σώμα $\mathbb{Z}_p$ ή το σώμα $\mathbb{Q}$ των ρητών .

Πρόταση 33 .

Ας είναι F ένα πρωτόσωμα . Τότε



$$i) F \cong \mathbb{Z}_p \quad \text{αν} \quad \text{char } F = p \neq 0$$

$$ii) F \cong \mathbb{Q} \quad \text{αν} \quad \text{char } F = 0 .$$

Απόδειξη .

Θεωρούμε την απεικόνιση

$$f: \mathbb{Z} \longrightarrow F, \quad f(n) = n1_F, \quad \forall n \in \mathbb{Z} .$$

Η f είναι ένας ομομορφισμός δακτυλίων και μάλιστα $\text{Ker } f = (p)$ όπου $p = \text{char } F$ (Κεφ. III, §8.7, Παραδ. 12) .

Αν $\text{char } F = p \neq 0$, p πρώτος τότε

$$\mathbb{Z}_p \cong f(\mathbb{Z}) = \{n1_F / n = 0, 1, \dots, p-1\}$$

ενώ αν $\text{char } F = 0$, $\mathbb{Z} \cong f(\mathbb{Z})$ (Κεφ. III, §8.7, Παραδ. 13)

$$i) \text{ Υποθέτουμε πρώτα ότι } \mathbb{Z}_p \cong f(\mathbb{Z}) .$$

Αφού ο p είναι πρώτος έχουμε ότι το $\mathbb{Z}_p$ είναι σώμα άρα σώμα είναι και το $f(\mathbb{Z})$. Αλλά το F είναι πρωτόσωμα δεν περιέχει εκομέ-
ως γνήσια υποσώματα άρα $f(\mathbb{Z}) = F$ και έτσι $F \cong \mathbb{Z}_p$

$$ii) \text{ Έστω τώρα } \mathbb{Z} \cong f(\mathbb{Z}) .$$

Ο υποδακτύλιος λοιπόν $f(\mathbb{Z})$, είναι πεδίο ακεραιότητας και το σώμα κλασμάτων του (βλέπε Κεφ. III, §7, πρόταση 19)

$$F' = \{a, b^{-1} / a, b \in f(\mathbb{Z}), b \neq 0\} = \{(n1_F)(m1_F)^{-1} / n, m \in \mathbb{Z}, m \neq 0\}$$

περιέχεται στο σώμα F οπότε $F' = F$ αφού το F είναι πρωτόσωμα .

Από την υπόθεση όμως, τα πεδία ακεραιότητας $\mathbb{Z}$ και $f(\mathbb{Z})$ είναι ισομορφα, οπότε και τα σώματα κλασμάτων τους θα είναι ισομορφα (βλέ-
πε Κεφ. III, §7, Πρόταση 20), δηλαδή,

$$\mathbb{Q} \cong F ,$$

μέσω του ισομορφισμού

$$g: \mathbb{Q} \longrightarrow F, \quad g\left(\frac{n}{m}\right) = (n1_F)(m1_F)^{-1} . \blacksquare$$



Πόρισμα 1 .

Κάθε σώμα F περιέχει ένα υπόσωμα F' τέτοιο ώστε

i) $F' \cong \mathbb{Z}_p$ αν $\text{char } F = p \neq 0$, p πρώτος

ii) $F' \cong \mathbb{Q}$ αν $\text{char } F = 0$.

Με την βοήθεια της παραπάνω πρότασης αποδεικνύεται ότι τα πρωτοσώματα δεν έχουν αυτομορφισμούς εκτός της ταυτότητας . Πραγματικά .

Πόρισμα 2 .

Αν f είναι ένας αυτομορφισμός ενός πρωτοσώματος F τότε ο f είναι η ταυτότητα .

Απόδειξη .

Σύμφωνα με την προηγούμενη πρόταση το F θα είναι :

i) $F = \{(n1_F)(m1_F)^{-1} / n, m \in \mathbb{Z} , m \neq 0\}$ αν $\text{char } F = 0$

ή

ii) $F = \{n1_F / n = 0, 1, \dots, p-1\}$ αν $\text{char } F = p \neq 0$

Αφού όμως για κάθε αυτομορφισμό f σώματος F έχουμε $f(1_F) = 1_F$ εύκολα αποδεικνύεται ότι ο f είναι ο ταυτοτικός ομομορφισμός .
(Άσκηση) .

8.9. Maximal και πρώτα ιδεώδη .

ΟΡΙΣΜΟΣ . Ένα ιδεώδες $\mathfrak{m}$ του δακτυλίου R λέγεται maximal ιδεώδες όταν $\mathfrak{m} \neq R$ και για κάθε ιδεώδες J του R με $\mathfrak{m} \subset J \subset R$ ισχύει $J = R$.

Μ'άλλα λόγια , ένα ιδεώδες $\mathfrak{m}$ του R είναι maximal όταν $\mathfrak{m} \neq R$ και δεν υπάρχει ιδεώδες J του R τέτοιο ώστε $J \neq \mathfrak{m}$, $J \neq R$ και $\mathfrak{m} \subset J \subset R$. Έτσι , το μόνο ιδεώδες που περιέχει γνήσια ένα maximal ιδεώδες είναι ο ίδιος ο δακτύλιος R .



Μ' ανάλογο τρόπο ορίζεται το δεξιό (αντιστ. αριστερό) maximal ιδεώδες . Δίνουμε όμως τον ορισμό για αμφίπλευρα ιδεώδη , γιατί τα πιο σημαντικά αποτελέσματα που αφορούν maximal ιδεώδη εμφανίζονται σε αντιμεταθετικούς δακτύλιους .

Παρατήρηση .

Αν R είναι ένας δακτύλιος και συμβολίσουμε με S το σύνολο όλων των ιδεωδών του R τέτοιων ώστε $J \neq R$ δηλαδή

$$S = \{J / J \text{ ιδεώδες του } R, J \neq R\}$$

τότε , το S είναι ένα μερικά διατεταγμένο σύνολο από τη σχέση του περιέχεσθαι . Βλέπουμε λοιπόν ότι :

Το $\mathcal{M}$ είναι ένα maximal ιδεώδες του R εάν και μόνο εάν το $\mathcal{M}$ είναι ένα maximal στοιχείο στο μερικά διατεταγμένο σύνολο S .

Γενικώτερα , πολλές φορές μιλάμε για ένα ιδεώδες $\mathcal{I}$ που είναι maximal ως προς μια δοθείσα ιδιότητα , εννοώντας ότι υπεράνω της σχέσης του περιέχεσθαι το $\mathcal{I}$ είναι maximal στοιχείο στο σύνολο όλων των ιδεωδών του R που έχουν την δοθείσα ιδιότητα . Στην περίπτωση αυτή , το $\mathcal{I}$ δεν είναι απαραίτητα ένα maximal ιδεώδες του R με την έννοια του ορισμού .

Είναι δύσκολο στην πράξη να αποδείξουμε , ότι ένα ιδεώδες είναι maximal στηριζόμενοι μόνο στον ορισμό του maximal ιδεώδους . Για τον λόγο αυτό , θα δώσουμε στη συνέχεια ορισμένα αποτελέσματα που μας βοηθούν να ορίσουμε πότε ένα ιδεώδες είναι maximal ή όχι .

Πρόταση 34

Έστω J ένα ιδεώδες του δακτυλίου R . Το J είναι maximal ιδεώδες εάν και μόνο εάν $(J, \alpha) = R$, για κάθε στοιχείο $\alpha \notin J$, όπου (J, α) παριστάνει το ιδεώδες που παράγεται από το $J \cup \{\alpha\}$.



Απόδειξη .

Ας είναι J ένα maximal ιδεώδες του R . Το ιδεώδες (J, α) φανερά ικανοποιεί τη σχέση $J \subset (J, \alpha) \subseteq R$, οπότε $(J, \alpha) = R$. Αντίστροφα , ας είναι $\mathfrak{I}$ ένα ιδεώδες του R τέτοιο ώστε $J \subset \mathfrak{I} \subseteq R$.

Αν $\alpha \in \mathfrak{I}$ και $\alpha \notin J$ τότε $J \subset (J, \alpha) \subseteq \mathfrak{I}$. Αλλά από την υπόθεσή μας $(J, \alpha) = R$ οπότε $\mathfrak{I} = R$, που σημαίνει ότι το J είναι maximal ιδεώδες του R . ■

Παρατήρηση .

Αν R είναι ένας αντιμεταθετικός δακτύλιος με μονάδα , J ένα ιδεώδες του και $\alpha \notin J$, τότε ,

$$(J, \alpha) = \{x + r\alpha / x \in J, r \in R\} ,$$

όπου (J, α) είναι το ιδεώδες που παράγεται από το $J \cup \{\alpha\}$.
(Άσκηση) .

Παράδειγμα 18 .

Στο δακτύλιο $\mathbb{Z} \oplus \mathbb{Z}$ το ιδεώδες του $\mathfrak{M} = \{(x, 2y) / x, y \in \mathbb{Z}\}$ είναι maximal . Πραγματικά , αν J είναι ένα ιδεώδες του $\mathbb{Z} \oplus \mathbb{Z}$ τέτοιο ώστε

$$\mathfrak{M} \subset J \subseteq \mathbb{Z} \oplus \mathbb{Z}$$

τότε , υπάρχει $(\alpha, 2b+1) \in J$ για κάποια $\alpha, b \in \mathbb{Z}$. Επειδή $(\alpha, 2b) \in \mathfrak{M}$ θα έχουμε $(\alpha, 2b+1) - (\alpha, 2b) = (0, 1) \in J$. Αλλά $(1, 0) \in \mathfrak{M} \subset J$, επομένως

$$(0, 1) + (1, 0) = (1, 1) \in J$$

που σημαίνει ότι $J = \mathbb{Z} \oplus \mathbb{Z}$.

Παράδειγμα 19 .

Στον υποδακτύλιο $S = \left\{ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} / x, y, z \in \mathbb{R} \right\}$ του $M_{2 \times 2}(\mathbb{R})$ το σύνολο



$$\mathfrak{M} = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} / a, b \in \mathbb{R} \right\}$$

είναι φανερά ένα ιδεώδες του S . Το $\mathfrak{M}$ είναι maximal ιδεώδες του S . Πραγματικά, αν J είναι ένα άλλο ιδεώδες του S τέτοιο ώστε

$$\mathfrak{M} \subset J \subseteq S$$

τότε υπάρχει $\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \in J$ με $x, y, z \in \mathbb{R}$ και $z \neq 0$, επομένως

$$\begin{pmatrix} 0 & 0 \\ 1 & 1/z \end{pmatrix} \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in J.$$

Επειδή όμως $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in J$ θα έχουμε $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in J$ οπότε

$J = S$ όπως επιθυμούσαμε.

Παράδειγμα 20.

Στο δακτύλιο $\mathbb{Z}_A = 2\mathbb{Z}$ των άρτιων ακераίων, που είναι αντιμεταθετικός χωρίς μονάδα, το ιδεώδες (4) είναι maximal.

Πραγματικά, στο δακτύλιο αυτό έχουμε

$$(4) = \{(2m)4 + 4n / m, n \in \mathbb{Z}\}.$$

Είναι φανερό τώρα ότι $(4) = \{4k / k \in \mathbb{Z}\} = 4\mathbb{Z}$, ενώ για το δακτύλιο $\mathbb{Z}_A$ έχουμε $\mathbb{Z}_A = (2)$.

Για να είναι το ιδεώδες (4) στο δακτύλιο $\mathbb{Z}_A$ maximal αρκεί να δείξουμε ότι για κάθε $\alpha \in \mathbb{Z}_A$ με $\alpha \notin (4)$ το ιδεώδες

$$J = ((4), \alpha) = \mathbb{Z}_A$$

σύμφωνα με την πρόταση 34.

Πραγματικά, ο α είναι άρτιος ακέραιος που δεν διαιρείται από τον 4, επομένως

$$\alpha = 4q + 2 \quad \text{για κάποιο } q \in \mathbb{Z}$$

Έτσι,

$$2 = \alpha + 4(-q) \in J$$



αφού $a, 4(-q) \in J$ και το J είναι ιδεώδες . Άρα $Z_A = (2) \subseteq J$ και επειδή $J \subseteq Z_A$ θα έχουμε $J = Z_A$ πράγμα που επιθυμούσαμε .

Παράδειγμα 21 .

Στο δακτύλιο $Z[x]$ των πολωνύμων με ακέραιους συντελεστές , το ιδεώδες $(2, x)$ που παράγεται πό τα στοιχεία 2 και x είναι maximal .

Για το ιδεώδες $(2, x)$ έχουμε (βλέπε παραδ.6, Κεφ. III, §8.4)

$$(2, x) = \{2h(x) + xk(x) / h(x), k(x) \in Z[x]\} .$$

Μ' άλλα λόγια , το ιδεώδες $(2, x)$ είναι το σύνολο όλων των πολωνύμων του $Z[x]$ με σταθερό όρο πολ/σιο του 2 .

Για να δείξουμε ότι το ιδεώδες $(2, x)$ είναι maximal αρκεί να δείξουμε ότι για κάθε $f(x) \in Z[x]$ με $f(x) \notin (2, x)$ έχουμε

$$\mathfrak{M} = ((2, x), f(x)) = Z[x]$$

Πραγματικά , αν $f(x) \in Z[x]$ και $f(x) \notin (2, x)$ τότε ο σταθερός όρος του $f(x)$ είναι περιττός αριθμός και ας είναι αυτό το

$$f(x) = 2m-1 + xg(x) \quad , \quad m \in Z \quad , \quad g(x) \in Z[x]$$

Για το ιδεώδες $\mathfrak{M}$ έχουμε

$$\mathfrak{M} = \{2h(x) + xk(x) + f(x)p(x) / h(x), k(x), p(x) \in Z[x]\} .$$

Έτσι $2m \in \mathfrak{M}$, $xg(x) \in \mathfrak{M}$, και $f(x) \in \mathfrak{M}$ και αφού το $\mathfrak{M}$ είναι ιδεώδες θα έχουμε

$$1 = 2m + xg(x) - f(x) \in \mathfrak{M}$$

που σημαίνει ότι $\mathfrak{M} = Z[x]$.

Θα παρατηρήσουμε εδώ ότι στο δακτύλιο $Z[x]$ το ιδεώδες (x) δεν είναι maximal . Πραγματικά , έχουμε ότι

$$(x) \subset (2, x) \subset Z[x]$$

δηλαδή , υπάρχει γνήσιο ιδεώδες το $(2, x)$ που περιέχει γνήσια το ιδεώδες (x) πράγμα που επιθυμούσαμε .



Στην συνέχεια θα δώσουμε ένα γενικό συμπέρασμα που μας βεβαιώνει για την ύπαρξη maximal ιδεωδών . Το αποφασιστικό βήμα στην απόδειξη , εξαρτάται από το λήμμα του Zorn , όπως θα δούμε .

ΛΗΜΜΑ ΤΟΥ ZORN .

Αν $(\mathcal{U}, \leq)$ είναι ένα μερικά διατεταγμένο σύνολο με την ιδιότητα ότι , κάθε αλυσίδα στο $\mathcal{U}$ έχει ένα άνω φράγμα στο $\mathcal{U}$ τότε , το $\mathcal{U}$ έχει ένα τουλάχιστον maximal στοιχείο .

Υπενθυμίζουμε ότι αν $\mathcal{U}$ είναι μία μη-κενή οικογένεια κάποιου σταθερού μη-κενού συνόλου , τότε η $\mathcal{U}$ με την σχέση του περιέχεται γίνεται ένα μερικά διατεταγμένο σύνολο . Ένα άνω φράγμα για κάθε αλυσίδα $\mathcal{C}$ της $\mathcal{U}$ είναι το σύνολο $\bigcup \mathcal{C}$.

Μπορούμε να δώσουμε το λήμμα του Zorn ως εξής :

Έστω $\mathcal{U}$ μια μη-κενή οικογένεια υποσυνόλων κάποιου σταθερού μη-κενού συνόλου , με την ιδιότητα ότι για κάθε αλυσίδα $\mathcal{C}$ της $\mathcal{U}$, η ένωση $\bigcup \mathcal{C}$ ανήκει επίσης στην $\mathcal{U}$. Τότε , η $\mathcal{U}$ περιέχει ένα σύνολο που είναι maximal , με την έννοια ότι δεν περιέχεται σε κανένα μέλος της $\mathcal{U}$.

ΘΕΩΡΗΜΑ 7 . (Krull-Zorn) .

Έστω R ένας μη-μηδενικός δακτύλιος με μονάδα 1_R . Αν J είναι ένα ιδεώδες του R και $J \neq R$ τότε , υπάρχει ένα maximal ιδεώδες $\mathfrak{M}$ του R τέτοιο ώστε $J \subseteq \mathfrak{M}$.

Απόδειξη .

Η απόδειξη είναι μια εφαρμογή του λήμματος του Zorn . θεωρούμε το σύνολο

$$\mathcal{U} = \{ \mathfrak{I} / \mathfrak{I} \text{ ιδεώδες του } R , \text{ με } \mathfrak{I} \neq R \text{ και } J \subseteq \mathfrak{I} \} .$$



Το $\mathcal{U} \neq \emptyset$ αφού $J \in \mathcal{U}$, ενώ το $(\mathcal{U}, \subseteq)$ είναι ένα μερικά διατεταγμένο σύνολο. Για να εφαρμόσουμε το λήμμα του Zorn, οφείλουμε να δείξουμε ότι κάθε αλυσίδα

$$\mathcal{C} = \{C_i / i \in I\}$$

ιδεωδών από το $\mathcal{U}$, έχει ένα άνω φράγμα στο $\mathcal{U}$. Έστω

$$K = \bigcup_{i \in I} C_i$$

Θα δείξουμε ότι το $K \in \mathcal{U}$. Έστω $a, b \in K$ και $r \in R$, τότε για κάποια $i, j \in I$ θα έχουμε $a \in C_i$ και $b \in C_j$. Αλλά η $\mathcal{C}$ είναι μια αλυσίδα οπότε $C_i \subseteq C_j$ ή $C_j \subseteq C_i$. Υποθέτουμε ότι $C_i \subseteq C_j$, έτσι $a, b \in C_j$. Αλλά το C_j είναι ιδεώδες του R συνεπώς $a-b \in C_j \subseteq K$. Επίσης ar και $ra \in C_j \subseteq K$. Δείξαμε λοιπόν ότι το K είναι ένα ιδεώδες του R . Επιπλέον, επειδή $J \subseteq C_i$ για κάθε $i \in I$, έχουμε

$$J \subseteq \bigcup_{i \in I} C_i = K$$

Μένει να δείξουμε ότι το ιδεώδες $K \neq R$. Πραγματικά, επειδή κάθε $C_i \in \mathcal{U}$, $C_i \neq R$ για όλα τα $i \in I$. Έτσι $1_R \notin C_i$ (για διαφορετικά $C_i = R$) οπότε

$$1_R \notin \bigcup_{i \in I} C_i = K$$

που σημαίνει ότι το $K \neq R$.

Το K είναι φανερά ένα άνω φράγμα για την αλυσίδα $\mathcal{C}$. Το λήμμα του Zorn μας δίνει τώρα, ότι το σύνολο $\mathcal{U}$ έχει ένα maximal στοιχείο $\mathcal{M}$. Το $\mathcal{M}$ είναι ένα γνήσιο ιδεώδες του R με $J \subseteq \mathcal{M}$.

Θα δείξουμε ότι το $\mathcal{M}$ είναι ένα maximal ιδεώδες του δακτυλίου R . Υποθέτουμε ότι N είναι ένα άλλο ιδεώδες του R τέτοιο ώστε

$$\mathcal{M} \subset N \subset R.$$

Αφού το ιδεώδες $\mathcal{M}$ είναι ένα maximal στοιχείο του $\mathcal{U}$ το $N \notin \mathcal{U}$. Αλλά $J \subseteq N$, συνεπώς το N πρέπει να είναι μη-γνήσιο ιδεώδες του R δηλαδή $N = R$ πράγμα που επιθυμούσαμε. ■



Πόρισμα 1 .

Κάθε μη-μηδενικός δακτύλιος R με μονάδα 1_R έχει ένα τουλάχιστον maximal ιδεώδες .

Απόδειξη .

Το (0) ιδεώδες είναι $\neq R$ και επομένως υπάρχει πάντα ένα maximal ιδεώδες $\mathfrak{M}$ του R τέτοιο ώστε $(0) \subseteq \mathfrak{M}$.

Πόρισμα 2 .

Έστω R ένας αντιμεταθετικός δακτύλιος με μονάδα 1_R . Κάθε μη-αντιστρέψιμο στοιχείο του R περιέχεται σ'ένα maximal ιδεώδες .

Απόδειξη .

Ας είναι x ένα τυχόν μη-αντιστρέψιμο στοιχείο του R . Το ιδεώδες $(x) = \{rx / r \in R\}$ είναι $\neq R$ γιατί αν $(x) = R$ τότε το x θα ήταν αντιστρέψιμο .

Υπάρχει λοιπόν maximal ιδεώδες $\mathfrak{M}$ του R τέτοιο ώστε

$$(x) \subseteq \mathfrak{M}$$

επομένως $x \in \mathfrak{M}$ πράγμα που επιθυμούσαμε .

Στο δακτύλιο $\mathbb{Z}$ των ακεραίων τα maximal ιδεώδη "αντιστοιχούν" στους πρώτους αριθμούς . (Υπενθυμίζουμε ότι ο $\mathbb{Z}$ είναι δακτύλιος κυρίων ιδεωδών) . Πιο συγκεκριμένα :

Πρόταση 35 .

Στο δακτύλιο $\mathbb{Z}$ ένα ιδεώδες (p) , $p > 1$ είναι maximal εάν και μόνο εάν ο p είναι πρώτος αριθμός .

Απόδειξη .



Υποθέτουμε ότι το $\mathcal{L}$ δεώδες

$$(p) = \{pk / k \in \mathbb{Z}\} = p\mathbb{Z}$$

του $\mathbb{Z}$ είναι maximal . Αν ο p δεν είναι πρώτος τότε

$$p = n_1 n_2 \quad \text{με} \quad 1 < n_1, n_2 < p$$

Έτσι για τα $\mathcal{L}$ δεώδη (n_1) και (n_2) έχουμε

$$(p) \subset (n_1) \subset \mathbb{Z} \quad \text{και} \quad (p) \subset (n_2) \subset \mathbb{Z}$$

πράγμα άτοπο αφού το (p) είναι maximal . Ο p είναι λοιπόν πρώτος αριθμός .

Αντίστροφα , υποθέτουμε ότι ο p είναι πρώτος αριθμός και (m) ένα $\mathcal{L}$ δεώδες του $\mathbb{Z}$ τέτοιο ώστε

$$(p) \subset (m) \subset \mathbb{Z}$$

Αφού $(p) \subset (m)$ θα είναι $p = km$, $k \in \mathbb{Z}$ δηλαδή mp οπότε $m=1$ ή p αφού ο p είναι πρώτος αριθμός . Ο $m \neq p$ γιατί διαφορετικά $(m) = (p)$ συνεπώς $m=1$ δηλαδή $(m) = \mathbb{Z}$.

Το (p) είναι λοιπόν ένα maximal $\mathcal{L}$ δεώδες . ■

Έστω F είναι σώμα και $F[x]$ ο δακτύλιος των πολυωνύμων με συντελεστές από το F . Είναι γνωστό ότι ο $F[x]$ είναι περιοχή κυρίων $\mathcal{L}$ δεωδών .

ΟΡΙΣΜΟΣ . Ένα πολυώνυμο $p(x) \in F[x]$ λέγεται ανάγωγο (irreducible) στον $F[x]$ αν

$$a) \deg p(x) \geq 1$$

$$b) \text{ Αν } p(x) = p_1(x)p_2(x) \text{ με } p_1(x), p_2(x) \in F[x]$$

τότε

$$p_1(x) \in F \quad \text{ή} \quad p_2(x) \in F$$

θα δείξουμε ότι στο δακτύλιο $F[x]$ τα maximal $\mathcal{L}$ δεώδη "αντιστοιχούν" στα ανάγωγα πολυώνυμα του $F[x]$.



Πρόταση 36 .

Στο δακτύλιο $F[x]$ ένα ιδεώδες $(p(x))$ είναι maximal εάν και μόνο εάν το $p(x)$ είναι ανάγωγο στον $F[x]$.

Απόδειξη .

Έστω $(p(x))$ ένα maximal ιδεώδες του $F[x]$.

Ο $\deg p(x) \geq 1$ γιατί αν το $p(x)$ ήταν ένα σταθερό πολυώνυμο τότε το ιδεώδες $(p(x))$ θα ήταν ή (0) ή ολόκληρος ο δακτύλιος $F[x]$ που φανερά δεν είναι maximal ιδεώδη .

Αν το $p(x)$ δεν ήταν ανάγωγο , τότε ,

$$p(x) = p_1(x)p_2(x) \text{ με } 1 \leq \deg p_1(x) , \deg p_2(x) < \deg p(x) .$$

Για τα ιδεώδη $(p_1(x))$ και $(p_2(x))$ έχουμε

$$(p(x)) \subset (p_1(x)) \subset F[x] \text{ και } (p(x)) \subset (p_2(x)) \subset F[x]$$

πράγμα άτοπο που υποθέσαμε ότι το $(p(x))$ είναι maximal .

Αντίστροφα,ας υποθέσουμε ότι το $p(x)$ είναι ανάγωγο πολυώνυμο του $F[x]$ και έστω $(\varphi(x))$ ένα ιδεώδες του $F[x]$ τέτοιο ώστε

$$(p(x)) \subset (\varphi(x)) \subseteq F[x] .$$

θα δείξουμε ότι $(\varphi(x)) = F[x]$.

Αφού $(p(x)) \subset (\varphi(x))$ θα είναι

$$p(x) = \varphi(x)h(x) , \quad h(x) \in F[x] ,$$

επομένως

$$\varphi(x) \in F \quad \text{ή} \quad h(x) \in F$$

γιατί το $p(x)$ είναι ανάγωγο .

Το $h(x) \notin F$ γιατί τότε $(p(x)) = (\varphi(x))$, επομένως $\varphi(x) \in F$, δηλαδή $\varphi(x) = \alpha \in F$, $\alpha \neq 0$. Έτσι $\alpha^{-1} = 1 \in F$ που σημαίνει ότι $(\varphi(x)) = F[x]$.



Παράδειγμα 22 .

Στο δακτύλιο $\mathbb{R}[x]$ το ιδεώδες (βλέπε παρ. 10)

$$(x^2+1) = \{P(x)(x^2+1) / P(x) \in \mathbb{R}(x)\}$$

είναι maximal ιδεώδες, αφού το πολυώνυμο x^2+1 είναι ανάγωγο στον $\mathbb{R}[x]$.

Στη συνέχεια θα χαρακτηρίσουμε τα maximal ιδεώδη με τη βοήθεια των δακτυλίων πηλίκων που ορίζουν.

ΘΕΩΡΗΜΑ 8 .

Ας είναι R ένας αντιμεταθετικός δακτύλιος με μονάδα και J ένα γνήσιο ιδεώδες του ($J \neq R$). Τότε το J είναι maximal ιδεώδες εάν και μόνο εάν ο δακτύλιος πηλίκος R/J είναι σώμα.

Απόδειξη .

Ας είναι J ένα maximal ιδεώδες του R . Αφού ο R είναι αντιμεταθετικός δακτύλιος με μονάδα 1_R όμοια και ο δακτύλιος πηλίκος R/J είναι αντιμεταθετικός με μονάδα $J+1_R \neq J$. Μένει να δείξουμε ότι κάθε μη-μηδενικό στοιχείο του R/J είναι αντιστρέψιμο.

Έστω $J+\alpha \neq J$ ($\alpha \notin J$), τυχόν μη μηδενικό στοιχείο του R/J . Θεωρούμε το ιδεώδες (J, α) που παράγεται από το $J \cup \{\alpha\}$, έχουμε

$$J \subset (J, \alpha) \subseteq R$$

και αφού το J είναι maximal

$$R = (J, \alpha) = \{x+r\alpha / x \in J, r \in R\}.$$

Κάθε στοιχείο λοιπόν του R μπορεί να γραφεί $x+r\alpha$, $x \in J$, $r \in R$. Υπάρχουν επομένως στοιχεία $x_0 \in J$ και $r_0 \in R$ έτσι ώστε

$$1_R = x_0 + r_0 \alpha$$

οπότε $1_R - r_0 \alpha = x_0 \in J$. Έτσι

$$J+1_R = J+r_0 \alpha = (J+r_0)(J+\alpha) \quad \text{επομένως}$$



$$(J+\alpha)^{-1} = J+r_0 \quad \text{πράγμα που επιθυμούσαμε .}$$

Αντίστροφα , υποθέτουμε ότι ο R/J είναι σώμα , και ας είναι $\sqrt{}$ ένα ιδεώδες του R για το οποίο

$$J\sqrt{} \subseteq R .$$

θα δείξουμε ότι $\sqrt{} = R$, οπότε τα J θα είναι maximal ιδεώδες .
Αφού $J \neq R$ υπάρχει $x \in \sqrt{}$ και $x \notin J$, επομένως $J+x \neq J$ όπου J είναι το μηδενικό στοιχείο του σώματος R/J . Το $J+x$ είναι αντιστρέψιμο και ας είναι $J+y$ το αντίστροφό του .

θα έχουμε λοιπόν $(J+x)(J+y) = J+xy = J+1_R$ που σημαίνει ότι $1_R - xy \in J \subseteq \sqrt{}$. Αλλά το $xy \in \sqrt{}$ (αφού το $x \in \sqrt{}$) οπότε

$$1_R = (1-xy) + xy \in \sqrt{} .$$

Αφού $1_R \in \sqrt{}$ θα είναι $\sqrt{} = R$ όπως το ζητούσαμε . ■

Παρατήρηση .

Στο δακτύλιο $\mathbb{Z}_A$ που δεν έχει μονάδα το ιδεώδες (4) είναι maximal (βλέπε παράδειγμα 20, §8.9) . Στον δακτύλιο πηλίκου $\mathbb{Z}_A/(4)$ όμως ισχύει

$$((4)+2)((4)+2) = (4)+4 = (4)$$

δηλαδή , ο δακτύλιος $\mathbb{Z}_A/(4)$ έχει διαιρέτες του μηδενός , άρα δεν είναι σώμα .

Βλέπουμε λοιπόν ότι η ύπαρξη μοναδιαίου στοιχείου στον δακτύλιο R , είναι απαραίτητα στο παραπάνω θεώρημα .

Παράδειγμα 23 .

Στο δακτύλιο $\mathbb{R}[x]$ το ιδεώδες (x^2+1) είναι maximal (βλέπε Κεφ. III, §8.9, Παράδ. 22) . Ο δακτύλιος πηλίκου $\mathbb{R}[x]/(x^2+1)$ είναι λοιπόν σώμα σύμφωνα με το προηγούμενο θεώρημα , και μάλιστα



$$\mathbb{C} \simeq \mathbb{R}[x]/(x^2+1) \quad .$$

Αυτό μας δίνει μια κατασκευή του σώματος $\mathbb{C}$ των μιγαδικών αριθμών από τους πραγματικούς αριθμούς .

Παράδειγμα 24 .

Δείξαμε στα προηγούμενα με κλασσικό τρόπο ότι το ιδεώδες (x) στο δακτύλιο $\mathbb{Z}[x]$ δεν είναι maximal . Ένας άλλος τρόπος για να διαπιστώσουμε αυτό είναι ο εξής : θεωρούμε την απεικόνιση

$$h : \mathbb{Z}[x] \longrightarrow \mathbb{Z} \quad , \quad f(x) \longrightarrow f(0) \quad .$$

Είναι εύκολο να δείξουμε ότι αυτή είναι ένας επιμορφισμός με $\text{Ker}(h) = (x)$ οπότε

$$\mathbb{Z}[x]/(x) \simeq \mathbb{Z} \quad .$$

Το $\mathbb{Z}$ όμως δεν είναι σώμα , συνεπώς το ιδεώδες (x) δεν είναι maximal .

Πόρισμα 3 .

Έστω F ένας αντιμεταθετικός δακτύλιος με μονάδα . Το ιδεώδες (0) είναι maximal εάν και μόνο εάν ο F είναι σώμα .

Απόδειξη .

Παρατηρούμε ότι $F \simeq F/(0)$.

Πραγματικά η απεικόνιση $f : F \longrightarrow F/(0)$, $x \longmapsto (0)+x$ είναι ένας ισομορφισμός . Σύμφωνα λοιπόν με το θεώρημα ο $F \simeq F/(0)$ είναι σώμα ένα και μόνο εάν το (0) είναι maximal .

Ορισμός . Ένα ιδεώδες P ενός δακτυλίου R θα λέγεται πρώ-
το ιδεώδες αν $P \neq R$ και για κάθε ζεύγος ιδεωδών A, B του R
ισχύει :



$$AB \subseteq P \implies A \subseteq P \quad \text{ή} \quad B \subseteq P .$$

Για ιστορικούς και τεχνικούς λόγους εξαιρούμε από τα πρώτα ιδεώδη τον δακτύλιο $\mathbb{R}$.

Παράδειγμα 25 .

Στον μη-αντιμεταθετικό δακτύλιο $M_{n \times n}(\mathbb{R})$ το ιδεώδες (0) είναι πρώτο .

Υπενθυμίζουμε ότι ο $M_{n \times n}(\mathbb{R})$ είναι απλός δακτύλιος δηλαδή τα μόνα ιδεώδη του είναι τα (0) και $M_{n \times n}(\mathbb{R})$ (βλέπε παράδειγμα 5, Κεφ III, §8.1) .

Είναι φανερό τώρα ότι , αν για ιδεώδη A, B του $M_{n \times n}(\mathbb{R})$ ισχύει $AB \subseteq (0)$ τότε $A \subseteq (0)$ ή $B \subseteq (0)$.

Θεώρημα 9 .

Ας είναι R ένας αντιμεταθετικός δακτύλιος και P ένα ιδεώδη του με $P \neq R$. Το P είναι πρώτο ιδεώδες εάν και μόνο εάν για κάθε $a, b \in R$ ισχύει

$$ab \in P \implies a \in P \quad \text{ή} \quad b \in P .$$

Απόδειξη .

Έστω P ένα πρώτο ιδεώδες του R . Αν $ab \in P$ θα δείξουμε ότι $a \in P$ ή $b \in P$. Γνωρίζουμε ότι

$$(a) = \{ra + na \mid r \in R, n \in \mathbb{Z}\}$$

$$(b) = \{sb + mb \mid s \in R, m \in \mathbb{Z}\}$$

και ότι τα στοιχεία του γινομένου $(a)(b)$ θα είναι πεπερασμένα αθροίσματα από γινόμενα στοιχείων της μορφής

$$ra + na \quad \text{και} \quad sb + mb, \quad r, s \in R \quad \text{και} \quad n, m \in \mathbb{Z} .$$



Αλλά

$$(ra + na)(sb + mb) = rsab + mraab + nsab + nmaab,$$

και αφού $ab \in P$ και το P ιδεώδες παίρνουμε ότι το γινόμενο $(ra + na)(sb + mb)$ και πεπερασμένα αθροίσματα από όμοια γινόμενα ανήκουν στο P , που σημαίνει ότι

$$(a)(b) \subseteq P.$$

Επειδή το P είναι το πρώτο ιδεώδες, έχουμε $(a) \subseteq P$ ή $(b) \subseteq P$ που συνεπάγεται ότι $a \in P$ ή $b \in P$.

Αντίστροφα. Έστω A, B ιδεώδη του R τέτοια ώστε $AB \subseteq P$. Υποθέτουμε ότι $A \not\subseteq P$, υπάρχει τότε στοιχείο $a \in A - P$. Για κάθε $b \in B$ είναι $ab \in AB \subseteq P$ οπότε $a \in P$ ή $b \in P$. Αλλά $a \notin P$ επομένως $b \in P$ για κάθε $b \in B$ δηλαδή $B \subseteq P$, που σημαίνει ότι το P είναι πρώτο ιδεώδες του R .

Παράδειγμα 26.

Το ιδεώδες $P = \{(x, 0) / x \in \mathbb{Z}\}$ του δακτυλίου $\mathbb{Z} \oplus \mathbb{Z}$ είναι πρώτο. Πραγματικά αν $(x, y)(z, w) \in P$ δηλαδή $(xz, yw) \in P$ θα είναι $yw = 0$ οπότε $y = 0$ ή $w = 0$. Άρα $(x, y) \in P$ ή $(z, w) \in P$ πράγμα που επιθυμούσαμε.

Η παραπάνω πρόταση χαρακτηρίζει τον δακτύλιο πηλίκο με την βοήθεια των πρώτων ιδεωδών.

Πρόταση 37.

Σ' ένα αντιμεταθετικό δακτύλιο R με μονάδα $1_R \neq 0$ ένα ιδεώδες P είναι πρώτο εάν και μόνο εάν ο δακτύλιος πηλίκο R/P είναι πεδίο ακεραιότητας.

Απόδειξη.

Αρχικά παρατηρούμε ότι ο δακτύλιος R/P είναι αντιμεταθετικός



δακτύλιος με μονάδα το στοιχείο $P+1_R$ και μηδενικό στοιχείο το P .

Έστω τώρα ότι το ιδεώδες P είναι πρώτο. Αφού $P \neq R$ θα είναι $P+1_R \neq P$. Θα δείξουμε ότι ο δακτύλιος R/P δεν έχει διαιρέτες του μηδενός οπότε είναι ένα πεδίο ακεραιότητας.

Πραγματικά,

$$(P+x)(P+y) = P \implies P+xy = P \implies xy \in P \xrightarrow{P \text{ πρώτο}}$$

$$x \in P \quad \text{ή} \quad y \in P \implies P+x = P \quad \text{ή} \quad P+y = P.$$

Αντίστροφα, υποθέτουμε ότι R/P είναι πεδίο ακεραιότητας τότε

$$P+1_R \neq P, \text{ επομένως } 1_R \notin P, \text{ δηλαδή } P \neq R.$$

Επειδή ο R/P δεν έχει διαιρέτες του μηδενός

$$xy \in P \implies P+xy = P \implies (P+x)(P+y) = P \implies$$

$$P+x = P \quad \text{ή} \quad P+y = P \implies x \in P \quad \text{ή} \quad y \in P$$

οπότε το P είναι ένα πρώτο ιδεώδες.

Παράδειγμα 27.

Ένας αντιμεταθετικός δακτύλιος R με μονάδα $1_R \neq 0$ είναι πεδίο ακεραιότητας εάν και μόνο εάν το μηδενικό ιδεώδες (0) είναι πρώτο ιδεώδες του R .

Παρατηρούμε ότι $R/(0) \cong R$. Πραγματικά η απεικόνιση

$$h: R/(0) \longrightarrow R, \quad (0)+x \longmapsto x$$

είναι ένας ισομορφισμός. Σύμφωνα λοιπόν με την πρόταση 37 ο

$R/(0) \cong R$ είναι πεδίο ακεραιότητας εάν-ν το (0) είναι πρώτο ιδεώδες.

Παράδειγμα 28.

Στο δακτύλιο $\mathbb{Z}$ των ακεραίων ένα ιδεώδες $(p) \neq (0)$ είναι πρώτο εάν-ν ο p είναι πρώτος αριθμός.

Πραγματικά $\mathbb{Z}/(p) \cong \mathbb{Z}_p$.



Αν λοιπόν ο p είναι πρώτος, το $\mathbb{Z}_p$ είναι σώμα που σημαίνει ότι το $\mathbb{Z}/(p)$ είναι πεδίο ακεραιότητας, οπότε το (p) είναι πρώτο ιδεώδες. Αντίστροφα αν (p) είναι πρώτο ιδεώδες, το $\mathbb{Z}_p$ είναι πεδίο ακεραιότητας (πεπερασμένο) συνεπώς σώμα (βλέπε Πρόταση 7, §1.2, Κεφ. III) οπότε ο p πρώτος αριθμός.

Πόρισμα 4 .

Κάθε maximal ιδεώδες ενός αντιμεταθετικού δακτύλιου με μονάδα είναι ένα πρώτο ιδεώδες.

Απόδειξη .

Αν $\mathfrak{M}$ είναι ένα maximal ιδεώδες του R , τότε, ο $R/\mathfrak{M}$ είναι σώμα (βλέπε Θεώρημα 8) άρα και πεδίο ακεραιότητας οπότε το $\mathfrak{M}$ είναι πρώτο ιδεώδες. ■

Παρατήρηση .

Το πόρισμα 4 δεν ισχύει για δακτύλιους χωρίς μονάδα. Πραγματικά, στο δακτύλιο $\mathbb{Z}_A = 2\mathbb{Z}$ των άρτιων ακεραίων το ιδεώδες (4) είναι maximal (βλέπε παράδ. 20, Κεφ. III, §8.9) αλλά δεν είναι πρώτο αφού

$$6 \cdot 2 \in (4) \text{ και } 6 \notin (4), 2 \notin (4).$$

Το αντίστροφο του πορίσματος 4 δεν ισχύει γενικά, υπάρχουν δηλαδή πρώτα ιδεώδη που δεν είναι maximal.

Για παράδειγμα στο δακτύλιο $\mathbb{Z}$ των ακεραίων το ιδεώδες (0) είναι πρώτο όχι όμως maximal.

Επίσης στο δακτύλιο $\mathbb{Z} \oplus \mathbb{Z}$ το πρώτο ιδεώδες $\mathbb{Z} \times \{0\}$ (βλέπε παρ. 26, Κεφ. III, §8.9) δεν είναι maximal αφού υπάρχει ιδεώδες $\mathbb{Z} \times 2\mathbb{Z}$ έτσι ώστε

$$\mathbb{Z} \times \{0\} \subset \mathbb{Z} \times 2\mathbb{Z} \subset \mathbb{Z} \oplus \mathbb{Z}.$$



Παράδειγμα 29 .

Στο δακτύλιο $Z[x]$ το ιδεώδες (x) είναι πρώτο όχι όμως maximal .

Πραγματικά, $Z[x]/(x) \cong Z$ (βλέπε Παραδ.24, Κεφ. III, §8.9) και επειδή το Z είναι πεδίο ακεραιότητας το ιδεώδες (x) είναι πρώτο . Δεν είναι maximal όμως όπως δείξαμε στο παράδειγμα 24 .

Θα δούμε στη συνέχεια ορισμένες κατηγορίες δακτυλίων στους οποίους ισχύει το αντίστροφο του παρίσματος 4 .

Πρόταση 38 .

Σ' ένα πεπερασμένο αντιμεταθετικό δακτύλιο R με μονάδα κάθε πρώτο ιδεώδες είναι και maximal .

Απόδειξη .

Έστω P ένα πρώτο ιδεώδες του R και J ένα ιδεώδες του R τέτοιο ώστε

$$P \subset J \subseteq R$$

θα υπάρχει τότε $x \in J - P$.

Για κάθε φυσικό k ισχύει $x^k \in J$ και $x^k \notin P$ αφού το P είναι πρώτο ιδεώδες . Τα στοιχεία

$$x, x^2, x^3, \dots$$

δεν μπορεί να είναι όλα διακεκριμένα μεταξύ τους (αφού το J είναι πεπερασμένο ιδεώδες), συνεπώς υπάρχουν φυσικοί αριθμοί r, s με $r > s$ έτσι ώστε

$$x^r = x^s$$

Επομένως $x^r - x^s = 0$ ή $x^s(x^{r-s} - 1) = 0$ άρα

$$x^s(x^{r-s} - 1) \in P$$

και επειδή $x^s \notin P$ και το P πρώτο θα είναι



$$x^{r-s}-1 \in P \subset J \quad .$$

Αλλά $x^{r-s} \in J$, επομένως $1 \in J$ που σημαίνει ότι $J=R$ πράγμα που επιθυμούσαμε .

Παράδειγμα 30 .

Θα βρούμε όλα τα πρώτα και maximal ιδεώδη του $\mathbb{Z}_m$. Αφού ο $\mathbb{Z}_m$ είναι ένας πεπερασμένος δακτύλιος με μονάδα , ένα ιδεώδες του είναι πρώτο εάν-ν είναι maximal (βλέπε παραδ.4 και πρότ.38) . Αρκεί λοιπόν να βρούμε όλα τα πρώτα του ιδεώδη . Υπενθυμίζουμε ότι ο δακτύλιος $\mathbb{Z}_m$ έχει ακριβώς ένα ιδεώδες για κάθε φυσικό διαιρέτη d του m και όχι άλλα ιδεώδη (βλέπε παραδ.14,Κεφ.III,§8.7) . Έτσι αν $d_1, d_2, \dots, d_{\tau(m)}$ είναι όλοι οι φυσικοί διαιρέτες του m όλα τα ιδεώδη του $\mathbb{Z}_m$, είναι τα

$$(\bar{d}_1), (\bar{d}_2), \dots, (\bar{d}_{\tau(m)}) \quad .$$

Θα δείξουμε στην συνέχεια ότι ένα ιδεώδες $(\bar{d})$ του $\mathbb{Z}_m$ είναι πρώτο εάν-ν ο d είναι πρώτος αριθμός . Αν $(\bar{d})$ είναι ένα πρώτο ιδεώδες του $\mathbb{Z}_m$ και ο d σύνθετος τότε $d = \alpha\beta$ όπου $1 < \alpha < d$ και $1 < \beta < d$. Θα έχουμε

$$\bar{\alpha}\bar{\beta} \in (\bar{d}) \xrightarrow{(d)\text{πρώτο}} \bar{\alpha} \in (\bar{d}) \quad \text{ή} \quad \bar{\beta} \in (\bar{d}) \implies$$

$d|\alpha$ ή $d|\beta$ πράγμα άτοπο . Ο d είναι λοιπόν πρώτος αριθμός .

Αντίστροφα , αν d είναι πρώτος αριθμός (με $d|m$) θα δείξουμε ότι το ιδεώδες $(\bar{d})$ είναι πρώτο στον $\mathbb{Z}_m$. Θα δείξουμε δηλαδή ότι αν $\bar{\alpha}\bar{\beta} \in (\bar{d})$ και $\bar{\alpha} \notin (\bar{d})$ τότε $\bar{\beta} \in (\bar{d})$.

Πραγματικά , θα έχουμε $d|\alpha\beta$ και $d \nmid \alpha$ οπότε $d|\beta$ αφού ο d πρώτος αριθμός που σημαίνει ότι $\bar{\beta} \in (\bar{d})$.

Αν λοιπόν $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ είναι η πρωτογενής ανάλυση



του m τα πρώτα (και επομένως maximal) ιδεώδη του δακτυλίου Z_m είναι τα

$$(\bar{p}_1), (\bar{p}_2), \dots, (\bar{p}_k) .$$

Για παράδειγμα στο δακτύλιο Z_{30} τα πρώτα του ιδεώδη είναι τα εξής :

$$(2) = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \dots, \bar{28}\}$$

$$(3) = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}, \dots, \bar{27}\}$$

$$(5) = \{\bar{0}, \bar{5}, \bar{10}, \bar{15}, \bar{20}, \bar{25}\}$$

αφού

$$30 = 2 \cdot 3 \cdot 5$$

Πρόταση 39 .

Έστω R ένα πεδίο κυρίων ιδεωδών . Ένα μη-τετριμμένο ιδεώδες (x) του R είναι πρώτο εάν και μόνο εάν είναι maximal .

Απόδειξη .

Αρκεί να δείξουμε ότι κάθε πρώτο ιδεώδες είναι maximal . Έστω (x) ένα πρώτο ιδεώδες του R και (b) ένα ιδεώδες του τέτοιου ώστε

$$(x) \subset (b) \subseteq R$$

Το $x \in (x) \subset (b)$ άρα $x = yb$ για κάποιο $y \in R$. Το $yb \in (x)$ οπότε $y \in (x)$ ή $b \in (x)$ αφού το (x) είναι πρώτο ιδεώδες . Αλλά $b \notin (x)$ γιατί αν $b \in (x)$ τότε $(b) \subset (x)$ πράγμα άτοπο . Αναγκαστικά λοιπόν $y \in (x)$ δηλαδή $y = zx$ για κάποιο $z \in R$.

Από τα παραπάνω παίρνουμε ότι

$$x = yb = zxb .$$



Αφού το $x \neq 0$ και ο R είναι πεδίο ακεραιότητας θα είναι $1 = zb$ δηλαδή $1 \in (b)$ οπότε $(b) = R$ πράγμα που επιθυμούσαμε .

Πόρισμα 5 .

Στο πεδίο ακεραιότητας $\mathbb{Z}$ των ακεραίων ένα μη-τετριμμένο ιδεώδες είναι πρώτο εάν-ν είναι maximal .

Πόρισμα 6 .

Στο πεδίο ακεραιότητας $F[x]$ των πολυωνύμων με συντελεστές από ένα σώμα F ένα μη-τετριμμένο ιδεώδες είναι πρώτο εάν-ν είναι maximal .

Πόρισμα 7 .

Στο δακτύλιο $\mathbb{Z}[i]$ των ακεραίων του Gauss ένα μη-τετριμμένο ιδεώδες είναι πρώτο εάν-ν είναι maximal .

Ορισμός . Ένας αντιμεταθετικός δακτύλιος R με μονάδα ονομάζεται δακτύλιος του Boole αν κάθε στοιχείο του πληρού τη σχέση $x^2 = x$.

Πρόταση 40 .

Έστω R ένας δακτύλιος του Boole . Ένα μη-τετριμμένο ιδεώδες P του R είναι πρώτο εάν-ν είναι maximal .

Απόδειξη .

Αρκεί να δείξουμε ότι κάθε πρώτο ιδεώδες P του R είναι maximal . Θα δείξουμε ότι αν $\mathfrak{F}$ είναι ένα ιδεώδες του R τέτοιου ώστε $P \subset \mathfrak{F} \subseteq R$ τότε $\mathfrak{F} = R$.

Πραγματικά , υπάρχει $x \in \mathfrak{F} - P$, επομένως



$$x^2 = x \quad \text{ή} \quad x(1-x) = 0 \in P$$

Αλλά το P είναι πρώτο ιδεώδες και αφού $x \notin P$ θα είναι $1-x \in P \subset \mathfrak{f}$.

Έτσι $x+(1-x) = 1 \in \mathfrak{f}$ που σημαίνει ότι $\mathfrak{f} = R$.



ΠΙΝΑΚΑΣ ΣΥΜΒΟΛΩΝ

ΣΥΜΒΟΛΟ	ΕΡΜΗΝΕΙΑ	ΣΕΛΙΔΑ
$\mathbb{N} = \{0, 1, 2, \dots\}$	σύνολο φυσικών αριθμών.....	27
$\mathbb{Z}$	δακτύλιος των ακεραίων αριθμών.....	171
$\mathbb{Q}, \mathbb{R}, \mathbb{C}$	σώμα των ρητών, πραγματικών, μιγαδικών αριθμών αντίστοιχα.....	185
$\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$	μη-μηδενικού ρητού, πραγματικού, μιγαδικού αριθμού, αντίστοιχα.....	67
$\implies$	συνεπάγεται.....	6
$\iff$ ή αν-ν	εάν και μόνο εάν.....	6
$\emptyset$	κενό σύνολο.....	79
$\subseteq$	υποσύνολο.....	5
$\subset$	γνήσιο υποσύνολο.....	5
$e, \notin$	ανήκει, δεν ανήκει.....	5
$\forall$	για κάθε.....	5
$\cup$	ένωση.....	5
$\cap$	τομή.....	5
$(A_i)_{i \in I}$	οικογένεια με σύνολο δεικτών I	18
$\bigcup_{i \in I} A_i$	ένωση της οικογένειας συνόλων A_i	18
$\bigcap_{i \in I} A_i$	τομή της οικογένειας συνόλων A_i	20
$\mathcal{P}(A)$	δυναμοσύνολο του A	11
$A-B$	διαφορά συνόλων.....	5
C_X^A	συμπληρωματικό του συνόλου A	40
$f: A \longrightarrow B$	f είναι απεικόνιση από το A στο B	9
$1-1$ ή ένεση	ένα προς ένα.....	13
$\alpha \longmapsto f(\alpha)$	η απεικόνιση f απεικονίζει το α στο $f(\alpha)$	9
$I_A: A \longrightarrow A$	η ταυτοτική απεικόνιση.....	13



ΣΥΜΒΟΛΟ	ΕΡΜΗΝΕΙΑ	ΣΕΛΙΔΑ
$g \circ f$	σύνθεση απεικονίσεων	10
$f(A)$	η εικόνα του συνόλου A μέσω της f	11
$f^{-1}(B)$	η αντίστροφη εικόνα του συνόλου B μέσω της f	12
$A \times B$	καρτεσιανό γινόμενο των συνόλων A και B	8
$A_1 \times \dots \times A_n$	καρτεσιανό γινόμενο των συνόλων $A_1, \dots, A_n$	8
R	σχέση ισοδυναμίας	17
$a \equiv b(R)$ ή $(a, b) \in R$	το a ισοδύναμο με το b κατά μέτρο της R	17
$[x]$ ή $\bar{x}$	η κλάση ισοδυναμίας του στοιχείου x	17
R_f	πυρηνική ισοδυναμία της f	22
$\bar{R}$	η παραγομένη ισοδυναμία από τη σχέση R	24
$a \mid b$	ο a διαιρεί τον b	102
$[a, b]$	ελάχιστο κοινό πολ/σιο των ακεραίων a και b	27
$d = (a, b)$	ο μ.κ.δ. των ακεραίων a και b	107
$a \equiv b \pmod{m}$	ο a ισότιμος με τον b κατά μέτρο m	20
$\mathbb{Z}_m$	το σύνολο των modulo m κλάσεων ισοδυναμίας	22
$\mathcal{A}$	αυτόματο	58
$ \mathcal{A} $	συμπεριφορά αυτομάτου	61
X^*	ελεύθερο μονοειδές που παράγεται από το σύνολο X	46
R_L	συντακτική ισοδυναμία	57
X^*/R_L	συντακτικό μονοειδές της γλώσσας L	57
$M_{m \times n}(K)$	το σύνολο των $m \times n$ πινάκων με στοιχεία από το σώμα K	171
$GL_n(R)$	γενική γραμμική ομάδα βαθμού n	68
$\prod_{i=1}^n G_i$	ευθύ γινόμενο ομάδων	69
$\mathcal{L}(G)$	το σύνολο όλων των υποομάδων μιας ομάδας G	73



ΣΥΜΒΟΛΟ	ΕΡΜΗΝΕΙΑ	ΣΕΛΙΔΑ
$O_n(R)$	υποομάδα των ορθογωνίων πινάκων βαθμού n	75
$SL_n(R)$	ειδική γραμμική ομάδα βαθμού n	76
$Z(G)$	κέντρο ομάδας	77
$SO_n(R)$	ειδική ορθογώνια ομάδα βαθμού n	78
$ G $	τάξη της ομάδας G	67
$\langle X \rangle$	(υπό)ομάδα παραγόμενη από το σύνολο X	79
$\langle \alpha \rangle$	κυκλική υποομάδα που παράγεται από το στοιχείο α	95
$H \leq G$, $(H < G)$	H είναι μία υποομάδα (γνήσια) της G	72
$[x, y]$	μεταθέτης των στοιχείων x και y	82
$[G, G]$	ομάδα μεταθέτης της G	82
$H \vee K$	supremum δύο υποομάδων	83
$HK = \{xy/x \in H, y \in K\}$	γινόμενο υποομάδων	85
$\text{End}(G)$	μονοειδές ενδομορφισμών ομάδας G	90
$\text{Aut}(G)$	ομάδα αυτομορφισμών της G	90
$\text{Ker}(f)$	πυρήνας του ομομορφισμού f	90
$\text{Inn}(G)$	ομάδα των εσωτερικών αυτομορφισμών της G	94
G_n	η ομάδα των n -στων ριζών της μονάδας	96
$\text{Im}(f)$	εικόνα του ομομορφισμού f	91
S_n	η συμμετρική ομάδα n -βαθμού	111
$\varepsilon(\sigma)$	πρόσημο μετάθεσης	114
A_n	η εναλλάσσουσα ομάδα n -βαθμού	129
$xH = \{xh/h \in H\}$	δεξιό σύμπλοκο της H	133
$Hx = \{hx/h \in H\}$	αριστερό σύμπλοκο της H	133
$C_G(x)$	η κεντροποιούσα του στοιχείου x στην G	78
$R \sim R'$	ισόμορφοι δακτύλιοι	200
$[G:H]$	δείκτης της H στην G	134



ΣΥΜΒΟΛΟ	ΕΡΜΗΝΕΙΑ	ΣΕΛΙΔΑ
$H \trianglelefteq G$	H κανονική υποομάδα της G	141
$H \not\trianglelefteq G$	η H δεν είναι κανονική υποομάδα της G	141
Q_8	η ομάδα των κουατερνίων	80
G/H	ομάδα πηλίκου της G με την H	150
$R[x]$	δακτύλιος των πολυωνύμων	172
$Z[i]$	δακτύλιος του Gauss	173
$R_1 + \dots + R_n$	ευθύ άθροισμα δακτυλίων	174
$U(R)$	ομάδα των αντιστρέψιμων στοιχείων του δακτυλίου R	181
char R	χαρακτηριστική δακτυλίου	189
$Z(R)$	κέντρο δακτυλίου R	194
$\text{Aut}(R)$	ομάδα αυτομορφισμών δακτυλίου R	206
$F(X)$	σώμα κλασμάτων του πεδίου ακεραιότητας $F[X]$	218
(X)	Ιδεώδες παραγόμενο από το X	224
$J_1 \vee J_2$	supremum δύο ιδεωδών	228
$J_1 + J_2$	άθροισμα ιδεωδών	233
$J_1 J_2$	γινόμενο ιδεωδών	234
R/J	δακτύλιος πηλίκου	236
(J, α)	ιδεώδες που παράγεται από το $J \cup \{\alpha\}$	252



ΒΙΒΛΙΟΓΡΑΦΙΑ

- [1] D.AMES : An Introduction to Abstract Algebra , International Textbook company , 1969 .
- [2] Σ.ΑΝΔΡΕΑΔΑΚΗ : Εισαγωγή στην Άλγεβρα , Αθήνα, 1986 .
- [3] M.BURTON : A First Course in Rings and ideals , Addison-Wesley , 1970 .
- [4] B.FRALEIGH : A First Course in Abstract Algebra , Addison-Wesley , 1976
- [5] G.GRATZER : Universal Algebra , 2nd edition , Springer-Verlag , New York , 1979 .
- [6] N.HERSTEIN : Topics in algebra , Blaisdell , 1964 .
- [7] J.HOPCROFT and J.ULLMAN : Introduction to Automata Theory Languages and Computation , Addison-Wesley , 1979 .
- [8] T.HUNGERFORD : Algebra , Holt , Rinehart and Winston , Inc. 1974 .
- [9] Κ.ΛΑΚΗ : Άλγεβρα , Θεσσαλονίκη , 1983 .
- [10] S.LANG : Algebra , Addison-Wesley , 1975 .
- [11] S.MACLANE and G.BIRKHOFF : Algebra , The Macmillan Company , 1967 .
- [12] M.MARCUS : Introduction to modern Algebra , Marcel Dekker , Inc 1978 .
- [13] Σ.ΜΠΟΖΑΠΑΛΙΔΗ : Εισαγωγή στην θεωρητική Πληροφορική , Θεσσαλονίκη , 1987 .
- [14] Σ.ΜΠΟΖΑΠΑΛΙΔΗ : Γραμμική Άλγεβρα , Μέρος Α και Β , Θεσσαλονίκη , 1984 .
- [15] J.ROTMAN : The Theory of Groups , Allyn and Bacon Inc. , 1973 .
- [16] D.SARACINO : Abstract Algebra , Addison-Wesley , 1980 .
- [17] L.SHAPIRO : Introduction to Abstract Algebra , McGraw-Hill Book Company , 1975 .
- [18] Α.ΦΥΡΑΡΙΔΗΣ : Θεωρία Αριθμών , Ιωάννινα 1986 .





ΕΥΡΕΤΗΡΙΟ ΟΡΩΝ

- | | | | |
|-------------------------------------|-----|-------------------------------|---------|
| άθροισμα ιδεωδών | 233 | δακτύλιος | |
| ακεραία περιολή | 180 | —— πηλίκιο | 238 |
| ακέραιτοι Gauss | 173 | —— του Boole | 271 |
| αλφάβητο εισόδου | 58 | —— του Gauss | 173 |
| αντιπρόσωπος κλάσης | 17 | —— $\mathbb{Z}_m$ | 171 |
| αντιστρέψιμο στοιχείο | 181 | δείκτης υποομάδας | 134 |
| αντίστροφη εικόνα υποσύνολου | 12 | διάγραμμα αντιμεταθετικό | 10 |
| απεικόνιση | 9 | —— δικτύου | 86 |
| —— αντιστρέψιμη | 13 | —— καταστάσεων | 59 |
| —— επί | 13 | | |
| —— 1-1 | 13 | ενδομορφισμός | 59 |
| —— μετάβασης | 59 | —— δακτυλίου | 205 |
| —— ταυτοτική | 13 | —— ομάδος | 90 |
| αυτόματο | 58 | —— σώματος | 212 |
| αυτομορφισμός | | ενελικτικό γινόμενο | 35 |
| —— δακτυλίου | 206 | ένωση γλωσσών | 55 |
| —— ομάδος | 90 | επιμορφισμός δακτυλίων | 200 |
| —— σώματος | 212 | —— μονοειδών | 40 |
| | | —— ομάδων | 88 |
| γενικευμένος προσεταιριστικός νόμος | 28 | —— σωματών | 212 |
| γινόμενο γλωσσών | 55 | εσωτερικές καταστάσεις | 58 |
| —— υποομάδων | 85 | ευθύ άθροισμα δακτυλίων | 174 |
| —— ιδεωδών | 234 | —— γινόμενο ομάδων | 69 |
| γλώσσα | 54 | | |
| —— αναγνωρίσιμη | 61 | θεώρημα Gayley | 44, 109 |
| δακτύλιος | 170 | —— Lagrange | 131 |
| —— αντιμεταθετικός | 170 | —— ομομορφισμού μονοειδών | 44 |
| —— απλός | 222 | θεωρήματα ισομορφισμών ομάδων | 156 |
| —— κυρίων ιδεωδών | 229 | —— δακτυλίων | 241 |
| —— με διαίρεση | 187 | θήκη γλώσσας | 55 |
| —— με μονάδα | 170 | | |



ιδεώδες αμφίπλευρο 218

— αριστερό 218

— δεξιό 218

— κύριο 224

— παραγόμενο 224

ισοδυναμία 17

— αριθμητική 20

— λεπτότερη 22

— παραγόμενο 24

— πυρηνική 22

— συμβιβαστή με πράξη 32

— συντακτική 57

ισομορφισμός δακτυλίων 200

— μονοειδών 40

— ομάδων 88

— σωμάτων 212

κανονική προβολή 41

κενή λέξη 46

κέντρο δακτυλίου 194

— ομάδας 77

κλάση ισοδυναμίας 17

μετάθεση 109

— κύκλος 118

— μετάβαση 123

μήκος κύκλου 118

— λέξης 46

μονοειδές 34

— αντιμεταθετικό 34

— ελεύθερο 46

— πηλύκο 39

μονοειδές

— συντακτικό 57

μονομορφισμός δακτυλίων 200

— μονοειδών 40

— ομάδων 88

— σωμάτων 211

ομάδα 66

— αβελιανή 66

— A_n 129

— $\text{Aut}(G)$ 90

— αντιστρέφειμων

στοιχείων δακτυλίου 181

— ελεύθερης στρέψης 101

— G_n 96

— $\text{GL}_n(R)$ 68

— $\text{Inn}(G)$ 94

— Klein 96

— κυκλική 95

ομάδα :

— μεταθέτης 82

— μικτή 101

— $\text{On}(R)$ 75

— περιοδική 101

— S_n 111

— $\text{SL}_n(R)$ 76

— $\mathbb{Q}/\mathbb{Z}$ 156

παράδοξο Russel 6

πεδίο ακεραιότητας 180

— των πολωνύμων $R[x]$ 180



Τυπώθηκε στο Πανεπιστημιακό Τυπογραφείο με δαπάνη
του Πανεπιστημίου Ιωαννίνων

Κ.Α. Πανεπιστημιακού Τυπογραφείου.

Ο.Τ.

Copyright : Πανεπιστήμιο Ιωαννίνων

Απαγορεύεται η μερική ή ολική ανατύπωση, καθώς και η
λήψη φωτοαντιγράφων από το βιβλίο χωρίς τη γραπτή
άδεια του Τμήματος Δημοσιευμάτων του Πανεπιστημίου
Ιωαννίνων και του συγγραφέα.

Διατίθεται και στο Βιβλιοπωλείο του Πανεπιστημίου
Ιωαννίνων, Δομπόλη, 451 10 Ιωάννινα τηλ. 21801.

ΔΙΑΝΕΜΕΤΑΙ ΔΩΡΕΑΝ στους φοιτητές.



