Ευάγγελος Ψωμόπουλος

Αλγεβρικές Δομές

I

ΕΚΔΟΣΕΙΣ ΖΗΤΗ

Πρόλογος

Η σύγχρονη Άλγεβρα είναι ένα σημαντικό και ουσιαστικό κομμάτι της μαθηματικής εκπαίδευσης σε όλα τα πανεπιστήμια του κόσμου. Αυτό δεν οφείλεται μόνο στο γεγονός ότι πολλοί άλλοι κλάδοι των μαθηματικών, και όχι μόνον, χρειάζονται τα αποτελέσματα της Άλγεβρας, αλλά και διότι η Άλγεβρα προσφέρει κομψές και αποτελεσματικές τεχνικές στην επίλυση προβλημάτων. Αυτό επιτυγχάνεται μέσα από την αφηρημένη προσέγγιση, και την αξιωματική μεθοδολογία. Θα πρέπει, όμως, να έχουμε πάντοτε υπόψη ότι η αξιωματική μεθοδολογία έχει να κάνει περισσότερο με την οργάνωση, και όχι με την ουσία της Άλγεβρας.

Δεν υπάρχει αμφιβολία, ότι πολλοί φοιτητές συναντούν δυσκολίες από την πρώτη τους επαφή με την Άλγεβρα. Οι δυσκολίες αυτές έχουν πολλές αιτίες, αλλά οι κυριότερες είναι δύο. Πρώτη είναι η αλλαγή της έμφασης από την αλγοριθμική προσέγγιση της μέσης εκπαίδευσης, σε μια περισσότερο αυστηρή και αφηρημένη προσέγγιση. Η αφηρημένη προσέγγιση δεν γίνεται μόνο για λόγους γενικότητας, αλλά κυρίως διότι διαπιστώθηκε ότι αυτού του είδους η προσέγγιση προσφέρει τις κομψές και αποτελεσματικές τεχνικές επίλυσης προβλημάτων, που προαναφέρθηκαν. Μια δεύτερη αιτία είναι ο αυξημένος ρυθμός της παρουσίασης του αντικειμένου, που συναντά κανείς σε κάθε πανεπιστήμιο, σε σχέση με τον ρυθμό παρουσίασης στη μέση εκπαίδευση. Οποιαδήποτε και αν είναι η αιτία, οι δυσκολίες αυτές αποθαρρύνουν αρκετούς φοιτητές από την περαιτέρω ενασχόληση με την Άλγεβρα, με αποτέλεσμα, και αυτό είναι λυπηρό, να χάνουν μια από τις ομορφότερες περιοχές των μαθηματικών.

Ακριβώς για το λόγο αυτό, ίσως συγχωρεθούν κάποιες συμβουλές, όσον αφορά τη μελέτη της Άλγεβρας. Καταρχήν σηκωθείτε από την πολυθρόνα, πάρτε μολύβι και χαρτί, και καθίστε στο γραφείο σας. Τα μαθηματικά, και πολύ περισσότερο η Άλγεβρα, δεν διαβάζονται σαν μυθιστόρημα, απαιτούν τη συμμετοχή μας. Αν συναντήσετε μια δυσκολία, και σας φαίνεται ανυπέρβλητη, μη διστάσετε να προχωρήσετε παρα-

κάτω. Μερικές φορές συνεχίζοντας τη μελέτη, τα πράγματα γίνονται περισσότερο ξεκάθαρα, και η κατανόηση είναι ευκολότερη. Αν όμως συναντήσετε περισσότερες δυσκολίες, τότε είναι βέβαιο ότι πρέπει να γυρίσετε πίσω, και να ξαναδιαβάσετε από την αρχή τα σημεία που σας προβληματίζουν. Αν σκέφτεστε ότι κάτι τέτοιο είναι κουραστικό, θυμηθείτε ότι η γνώση είναι μια προσωπική περιουσία, την οποία εσείς οι ίδιοι πρέπει να αποκτήσετε, και κανείς στον κόσμο δεν μπορεί να σας την αφαιρέσει.

Το βιβλίο «Αλγεβρικές Δομές Ι» αποτελεί μια εισαγωγή στη Θεωρία Ομάδων, και απευθύνεται σε προπτυχιακούς φοιτητές του Μαθηματικού Τμήματος, και σε κάθε άλλο που θα ήθελε να εξοικειωθεί με τις αλγεβρικές έννοιες. Γράφτηκε για να καλύψει κυρίως τη διδακτέα ύλη του αντίστοιχου υποχρεωτικού εξαμηνιαίου μαθήματος, το οποίο διδάσκεται στο Τμήμα Μαθηματικών του Πανεπιστημίου Θεσσαλονίκης.

Το βιβλίο αυτό αποτελείται από τέσσερα κεφάλαια. Στο πρώτο αναφέρονται βασικές εισαγωγικές έννοιες της ομάδας, η οποία είναι και η βασική αλγεβρική δομή. Το δεύτερο αφορά κυρίως την ομάδα πηλίκο, και φυσικά τους ισομορφισμούς ομάδων. Στο τρίτο κεφάλαιο γίνεται η ταξινόμηση των κυκλικών ομάδων, και αναφέρονται αποτελέσματα από το γινόμενο ομάδων. Στο τελευταίο κεφάλαιο αναπτύσσεται η ομάδα μεταθέσεων, και αναφέρονται κάποιες εφαρμογές που αφορούν τις μεταθέσεις. Ιδιαίτερη προσπάθεια έγινε ώστε η παρουσίαση των θεμάτων να είναι κατά το δυνατόν απλούστερη, έτσι ώστε το περιεχόμενο του βιβλίου να είναι κατανοητό από το φοιτητή.

Σχεδόν κάθε παράγραφος συνοδεύεται από ασκήσεις, οι οποίες δίνουν την ευκαιρία στον φοιτητή να ελέγξει αφενός τις γνώσεις που αποκτά σταδιακά, αφετέρου την ικανότητά του να συνδυάζει θεωρήματα που μαθαίνει, με στόχο να πετύχει νέα αποτελέσματα. Στο τέλος του βιβλίου υπάρχει μια συλλογή ασκήσεων, η οποία καλύπτει όλα τα θέματα που αναπτύσσονται στο βιβλίο αυτό. Σε κάθε μια από αυτές, δίνεται αναλυτική υπόδειξη.

Θεσσαλονίκη – Σεπτέμβριος 2009 Ευάγγελος Ψωμόπουλος

Περιεχόμενα

Εισαγωγή

Η μορφή και το περιεχόμενο της Άλγεβρας έχουν αλλάξει σημαντικά από την εποχή που πρωτοεμφανίστηκε μέχρι σήμερα. Στη συνέχεια θα δούμε τη σταδιακή αυτή αλλαγή του περιεχομένου της Άλγεβρας, κάνοντας μια σύντομη ιστορική αναδρομή στην εξέλιξή της.

Αρχικά το αντικείμενο της Άλγεβρας ήταν η επίλυση πολυωνυμικών εξισώσεων. Το πρόβλημα της εύρεσης των ριζών μιας πολυωνυμικής εξίσωσης είναι χωρίς αμφιβολία ένα από τα πιο σημαντικά στην ιστορία της Άλγεβρας. Υπάρχουν ενδείξεις ότι οι Κινέζοι γνώριζαν τη λύση εξισώσεων δευτέρου βαθμού κατά τον πρώτο π.Χ. αιώνα. Οι αρχαίοι Έλληνες χρησιμοποιούσαν γεωμετρικές κατασκευές για να βρουν τις ρίζες εξισώσεων δευτέρου και τρίτου βαθμού. Τέλος, οι Βαβυλώνιοι γνώριζαν την επίλυση ορισμένων μορφών της εξίσωσης δευτέρου βαθμού. Όμως, οι πρώτες αλγεβρικές μέθοδοι επίλυσης εξισώσεων δευτέρου βαθμού άρχισαν να εμφανίζονται γύρω στα 100 μ.Χ.

Η θεωρία εξισώσεων, για πολλά χρόνια, ήταν ένα σύνολο μεμονωμένων περιπτώσεων και ειδικών μεθόδων. Δηλαδή κάθε εξίσωση ήταν ένα διαφορετικό πρόβλημα, και αναπτυσσόταν μέθοδος για την επίλυσή του. Η πρώτη προσπάθεια συστηματοποίησης και ομαδοποίησης ορισμένων μεθόδων έγινε από τον M. M. Al-Khwarizmi το 825 μ.Χ. περίπου. Ο M. M. Al-Khwarizmi έδωσε κανόνες για την επίλυση εξισώσεων δευτέρου βαθμού, και ήταν ο πρώτος που χρησιμοποίησε την ονομασία Άλγεβρα. Η λέξη Άλγεβρα προέρχεται από μια αραβική λέξη που σημαίνει αναγωγή ή αποκατάσταση. Η μέθοδος που ανέπτυξε ο Al-Khwarizmi ήταν η εφαρμογή συγκεκριμένων βημάτων, και μετασχηματισμών με στόχο η προς επίλυση εξίσωση να μετασχηματιστεί σε κάποια μορφή, της οποίας η λύση ήταν γνωστή. Ακριβώς για αυτό το λόγο, το όνομά του έδωσε τη λέξη «αλγόριθμος», που περιγράφει τη διαδικασία εφαρμογής συγκεκριμένων βημάτων, με στόχο την επίλυση κάποιου προβλήματος. Χωρίς

αμφιβολία, η συνεισφορά του Al-Khwarizmi ήταν σημαντική.

Το επόμενο σημαντικό βήμα έγινε στα 1545, όταν ο H. Cardano εξέδωσε το βιβλίο του γνωστό με τον τίτλο «Ars Magna». Στο βιβλίο αυτό περιγράφονται λύσεις των εξισώσεων τρίτου και τετάρτου βαθμού. Δεν είναι απόλυτα εξακριβωμένο αν οι λύσεις αυτές οφείλονται αποκλειστικά στον H. Cardano. Στην πραγματικότητα υπήρξε κάποια διαμάχη ως προς αυτό το θέμα. Η λύση της εξίσωσης τρίτου βαθμού βασίστηκε σε προηγούμενη εργασία του S. Del Ferro, ενώ ο N. Fontana ισχυρίστηκε ότι αυτός έδωσε στον H. Cardano τη λύση της εξίσωσης τρίτου βαθμού. Η λύση της εξίσωσης τετάρτου βαθμού οφείλεται στον L. Ferrari, ο οποίος ήταν μαθητής του Cardano. Ανεξάρτητα, όμως, από τις όποιες διαμάχες, που είναι αντικείμενο της ιστορίας, το βιβλίο «Ars Magna» ήταν ο δεύτερος σημαντικός σταθμός στην εξέλιξη της Άλγεβρας.

Με τις λύσεις των εξισώσεων δευτέρου, τρίτου και τετάρτου βαθμού να είναι ένα γεγονός, ήταν φυσικό, οι μαθηματικοί της εποχής να ασχοληθούν με το επόμενο βήμα, που ήταν η επίλυση της εξίσωσης πέμπτου βαθμού. Μάλιστα υπήρχε αρκετή αισιοδοξία για το εγχείρημα, λόγω των προηγούμενων επιτυχιών. Προσπάθειες, όμως, προς την κατεύθυνση αυτή παρέμεναν άκαρπες για πολλά χρόνια, και αυτό γιατί πολύ απλά η εξίσωση πέμπτου βαθμού γενικά δεν επιλύεται. Αυτό, όμως, ήταν άγνωστο την εποχή εκείνη, και έτσι οι επιστήμονες συνέχισαν τις προσπάθειες για την επίλυση της εξίσωσης πέμπτου βαθμού. Βέβαια η απάντηση στο πρόβλημα δεν ερχόταν, γεγονός που ανάγκασε πολλούς μαθηματικούς να ασχοληθούν με άλλες πλευρές του ίδιου προβλήματος. Αποτέλεσμα αυτής της προσπάθειας ήταν να αποδειχθούν θεωρήματα που αφορούσαν την κατανομή των ριζών των πολυωνυμικών εξισώσεων, και να βρεθούν μέθοδοι με τις οποίες μπορούσαν να προσεγγίσουν τις ρίζες.

Το 1746 ο D' Alembert διατύπωσε και απέδειξε το θεμελιώδες θεώρημα της Άλγεβρας: «κάθε αλγεβρική εξίσωση n βαθμού έχει n ρίζες». Αν και η απόδειξη του D' Alembert ήταν λανθασμένη, το γεγονός αυτό δεν αναγνωρίστηκε πριν περάσουν αρκετά χρόνια. Την πρώτη σωστή απόδειξη του θεμελιώδους θεωρήματος της Άλγεβρας έδωσε ο Gauss το 1799. Όπως ήταν επόμενο, η παρουσία του θεωρήματος αυτού άλλαξε τον τρόπο με τον οποίο έβλεπαν οι μαθηματικοί το πρόβλημα της επίλυσης εξισώσεων. Δεν είχε πλέον νόημα να αποδείξουν ότι μια εξίσωση έχει ρίζες γιατί αυτό ήταν γνωστό. Το πρόβλημα ήταν αν οι ρίζες αυτές μπορούσαν να εκφραστούν σαν συναρτήσεις των συντελεστών της εξίσωσης, χρησιμοποιώντας μόνον, και πεπερασμένου πλήθους φορές, την πρόσθεση, την αφαίρεση, τον πολλαπλασιασμό,

την διαίρεση και την εξαγωγή ρίζας. Δηλαδή, να υπάρχει μια ή περισσότερες παραστάσεις, από τον υπολογισμό των οποίων να προκύπτουν οι ρίζες της εξίσωσης. Ένα γνωστό παράδειγμα είναι η παράσταση που δίνει τις ρίζες μιας εξίσωσης δευτέρου βαθμού. Όταν οι ρίζες μιας εξίσωσης μπορούν να εκφραστούν με αυτόν τον τρόπο, λέμε ότι η εξίσωση είναι επιλύσιμη με ριζικά.

Τα πρώτα βήματα προς την κατεύθυνση αυτή έκανε ο Lagrange γύρω στα 1770-1771. Οι μέθοδοι που εισήγαγε χρησιμοποιούσαν στην πραγματικότητα θεωρία ομάδων, χωρίς όμως να εισάγει την έννοια αυτή. Ο Lagrange, μελετώντας τις γνωστές εξισώσεις δευτέρου, τρίτου και τετάρτου βαθμού, διαπίστωσε ότι κάποιες παραστάσεις των ριζών τους, για παράδειγμα $\rho_1\rho_2 + \rho_2\rho_3 + \rho_3\rho_1$, δεν αλλάζουν τιμή, αν οι ρίζες μετατεθούν με οποιοδήποτε τρόπο. Κατέληξε, έτσι, στο συμπέρασμα ότι το πρόβλημα ήταν να βρεθούν κάποιες συναρτήσεις των ριζών της εξίσωσης, οι οποίες να παραμένουν αναλλοίωτες κάτω από ορισμένες μεταθέσεις. Εισήγαγε με τον τρόπο αυτό την έννοια της μετάθεσης, η οποία είναι ο πρόγονος της ομάδας. Ο Lagrange, όμως, δεν πρόλαβε να απαντήσει στο ερώτημα αν η εξίσωση πέμπτου βαθμού είναι επιλύσιμη με ριζικά ή όχι. Μόλις στα 1813 αποδείχθηκε, από τον P. Ruffini, ότι η γενική εξίσωση πέμπτου βαθμού δεν είναι επιλύσιμη με ριζικά. Η απόδειξή του, όμως, αν και ήταν σωστή είχε αρκετές ελλείψεις. Πλήρη και σωστή απόδειξη έδωσε ο N. H. Abel το 1826. Η εξαιρετική αυτή εργασία του Abel απάντησε σε ένα ερώτημα που βασάνισε τους μαθηματικούς για τρεις περίπου αιώνες, ενώ ταυτόχρονα έθετε ένα άλλο γενικότερο ερώτημα. Ποιες εξισώσεις, τελικά, είναι επιλύσιμες με ριζικά και ποιες δεν είναι.

Απάντηση στο ερώτημα αυτό έδωσε το 1832 ένας μεγαλοφυής μαθηματικός, ο Evariste Galois. Ο Galois αντιστοίχισε σε κάθε αλγεβρική εξίσωση ένα σύστημα μεταθέσεων των ριζών της, το οποίο ονόμασε ομάδα. Στη συνέχεια, απέδειξε ότι η εξίσωση αυτή είναι επιλύσιμη με ριζικά όταν η αντίστοιχη ομάδα έχει κάποια συγκεκριμένη ιδιότητα, και αντίστροφα. Έτσι, το πρόβλημα της επίλυσης αλγεβρικών εξισώσεων έγινε πλέον πρόβλημα της θεωρίας ομάδων. Δυστυχώς, ο Galois πέθανε πριν να γίνει απόλυτα κατανοητή η θεωρία του. Το γεγονός αυτό είχε σαν αποτέλεσμα να μείνει αναξιοποίητη η σημαντική αυτή εργασία για αρκετά χρόνια. Όταν αργότερα άρχισαν να ασχολούνται με το θέμα αυτό, διαπίστωσαν ότι έπρεπε να διευκρινίσουν προηγουμένως ορισμένα αποτελέσματα που αφορούσαν τη θεωρία ομάδων. Θα μπορούσαμε, λοιπόν, να πούμε ότι η ανάπτυξη της θεωρίας ομάδων οφείλεται κατά ένα μέρος στην προσπάθεια να γίνει περισσότερο κατανοητή η θεωρία που άφησε ο

Galois. Έτσι, από την κλασσική Άλγεβρα, της οποίας το αντικείμενο ήταν η επίλυση εξισώσεων, φθάσαμε στη σύγχρονη (abstract) Άλγεβρα, η οποία ελάχιστα ασχολείται με εξισώσεις.

Τα τελευταία χρόνια, έννοιες και αποτελέσματα από την Άλγεβρα χρησιμοποιούνται όχι μόνο σε άλλους κλάδους των μαθηματικών, αλλά και σε άλλες επιστήμες, όπως στη Φυσική, στη Χημεία, στους Ηλεκτρονικούς Υπολογιστές κ.α. Το γεγονός αυτό είχε σαν αποτέλεσμα την αύξηση του ενδιαφέροντος για την ίδια την Άλγεβρα, η οποία πολλές φορές είχε να απαντήσει σε ερωτήματα που τέθηκαν από άλλες επιστήμες. Επιπλέον, η χρησιμότητά της αυτή έκανε την Άλγεβρα να γίνει μέρος της βασικής εκπαίδευσης των μαθηματικών σχεδόν σε όλα τα πανεπιστήμια. Δυστυχώς, όμως, για να μπορέσει κανείς να δει εφαρμογές της Άλγεβρας σε άλλες επιστήμες, π.χ. στη Χημεία, δεν αρκεί να γνωρίζει μόνο Χημεία, αλλά πολλές φορές είναι απαραίτητο να προχωρήσει στην Άλγεβρα περισσότερο από ό,τι συνήθως δίνεται στο αντίστοιχο μάθημα των προπτυχιακών σπουδών.

Κεφάλαιο 1
Εισαγωγή στη Θεωρία Ομάδων

Αλγεβρική δομή είναι ένα μη κενό σύνολο εφοδιασμένο με μία τουλάχιστον πράξη. Συνήθως, για τις πράξεις αυτές, χρησιμοποιούμε τα σύμβολα της πρόσθεσης και του πολλαπλασιασμού, χωρίς αυτό να σημαίνει ότι πρόκειται για τις γνωστές πράξεις αριθμών. Στο κεφάλαιο αυτό θα θεωρήσουμε αλγεβρικές δομές με μια μόνο πράξη, και θα χρησιμοποιήσουμε το σύμβολο του πολλαπλασιασμού, εκτός αν με σαφήνεια αναφέρεται κάτι διαφορετικό. Φυσικά, με την πράξη του πολλαπλασιασμού θα χρησιμοποιήσουμε και την αντίστοιχη ορολογία. Μια από τις πιο θεμελιώδεις αλγεβρικές δομές με μια πράξη, με την οποία τελικά θα ασχοληθούμε, είναι η ομάδα.

1.1 Οι πρώτοι ορισμοί και βασικά αποτελέσματα

Στην παράγραφο αυτή θα αναφέρουμε τον ορισμό της ομάδας, της υποομάδας, και του ομομορφισμού ομάδων. Θα δούμε επίσης ορισμένα παραδείγματα.

Ορισμός 1.1.1 **Κάθε μη κενό σύνολο S εφοδιασμένο με μια προσεταιριστική πράξη λέγεται *ημιομάδα* . Μια ημιομάδα M με μοναδιαίο στοιχείο λέγεται *μονοειδές* . Τέλος, ένα μονοειδές G λέγεται *ομάδα* , όταν η G περιέχει τα αντίστροφα όλων των στοιχείων της.**

Επομένως, ομάδα είναι ένα σύνολο G εφοδιασμένο με μια πράξη, ως προς την οποία ισχύουν τα παρακάτω αξιώματα:

O1: $a(bc) = (ab)c$, για κάθε $a, b, c \in G$,
O2: υπάρχει στοιχείο $e \in G$ τέτοιο, ώστε $ae = a = ea$, για κάθε $a \in G$,
O3: για κάθε $a \in G$ υπάρχει $a^{-1} \in G$ τέτοιο, ώστε $aa^{-1} = e = a^{-1}a$.

Προφανώς, μια ομάδα είναι πάντα μη κενό σύνολο γιατί, σύμφωνα με τον ορισμό, περιέχει οπωσδήποτε το μοναδιαίο στοιχείο. Το μοναδιαίο στοιχείο μιας ομάδας καθώς και το αντίστροφο ενός στοιχείου είναι μοναδικά. Μια ομάδα G θα λέγεται ***αντιμεταθετική*** ή ***αβελιανή*** όταν ισχύει

$$ab = ba, \text{ για κάθε } a \in G \text{ και } b \in G.$$

Τα περισσότερα από τα επόμενα παραδείγματα είναι είτε απλά, είτε προφανή. Ορισμένα πρέπει να είναι γνωστά.

Παράδειγμα 1.1.2 (i). Το σύνολο $\mathbb{Z}$ των ακεραίων, $\mathbb{Q}$ των ρητών, και $\mathbb{R}$ των πραγματικών αριθμών είναι αντιμεταθετικές ομάδες με πράξη τη συνήθη πρόσθεση. Αν στα προηγούμενα σύνολα θεωρήσουμε σαν πράξη το συνήθη πολλαπλασιασμό, τότε κανένα απ' αυτά δεν είναι ομάδα, εφόσον το 0 δεν έχει αντίστροφο, είναι όμως οπωσδήποτε μονοειδή. Τα σύνολα $\mathbb{Q}^* = \mathbb{Q} - \{0\}$, και $\mathbb{R}^* = \mathbb{R} - \{0\}$ με πράξη το συνήθη πολλαπλασιασμό είναι ομάδες και μάλιστα αντιμεταθετικές.

(ii). Το σύνολο $\{0\}$ με πράξη τη συνήθη πρόσθεση αποτελεί μια αντιμεταθετική ομάδα με ένα στοιχείο. Η ομάδα αυτή λέγεται ***τετριμμένη ομάδα*** .

(iii). Όταν έχουμε ένα πεπερασμένο σύνολο A εφοδιασμένο με μια πράξη $*$, μπορούμε σχετικά εύκολα να ορίσουμε το αποτέλεσμα της πράξης για κάθε ένα ζεύγος στοιχείων του συνόλου αυτού. Για το σκοπό αυτό σχηματίζουμε ένα πίνακα, στην πρώτη γραμμή και πρώτη στήλη του οποίου αναγράφουμε όλα τα στοιχεία του συνόλου A με την ίδια σειρά. Στη διασταύρωση της γραμμής, που ορίζεται από ένα στοιχείο a, και της στήλης, που ορίζεται από ένα στοιχείο b, τοποθετούμε το αποτέλεσμα $a * b$.

Στον παρακάτω πίνακα

$\circ$	$\cdots$	x	$\cdots$	y	$\cdots$
$\vdots$		$\vdots$		$\vdots$	
x	$\cdots$	$\cdots$	$\cdots$	w	$\cdots$
$\vdots$		$\vdots$		$\vdots$	
y	$\cdots$	z	$\cdots$	$\cdots$	$\cdots$
$\vdots$		$\vdots$		$\vdots$	

βλέπουμε τον πίνακα της πράξης $\circ$ πάνω σε κάποιο σύνολο, το οποίο περιέχει, μεταξύ άλλων, και τα στοιχεία x και y. Από τον πίνακα αυτό προκύπτει ότι ισχύει $x \circ y = w$

και $y \circ x = z$. Με τον τρόπο αυτό μπορούμε να ορίσουμε οποιαδήποτε πράξη σε ένα πεπερασμένο σύνολο. Το μόνο που χρειάζεται να κάνουμε είναι να συμπληρώσουμε όλες τις θέσεις του πίνακα με στοιχεία του συνόλου αυτού. Ας δούμε ένα συγκεκριμένο παράδειγμα.

Το σύνολο $\{-1, 1\}$ με πράξη το συνήθη πολλαπλασιασμό είναι μια αντιμεταθετική ομάδα με δύο στοιχεία. Εύκολα διαπιστώνεται ότι ο πίνακας της ομάδας αυτής είναι:

$\cdot$	1	-1
1	1	-1
-1	-1	1

Ο έλεγχος της προσεταιριστικής ιδιότητας στην περίπτωση αυτή είναι απλός.▲

Το επόμενο παράδειγμα αφορά τους ακεραίους $\bmod m$, και είναι ιδιαίτερα χρήσιμο στις εφαρμογές.

Παράδειγμα 1.1.3 Έστω $m > 1$ ένας θετικός ακέραιος. Είναι γνωστό ότι η σχέση

$$x \sim y \Longleftrightarrow y - x = km, \text{ για κάποιο } k \in \mathbb{Z},$$

όπου x, y είναι τυχόντες ακέραιοι αριθμοί, είναι μια σχέση ισοδυναμίας στο σύνολο $\mathbb{Z}$ των ακεραίων.

Αν x είναι τυχαίος ακέραιος, τότε, από την ευκλείδεια διαίρεση, προκύπτει ότι θα ισχύει $x = m\pi + \upsilon$, όπου $0 \leq \upsilon < m$. Επομένως, θα έχουμε $x - \upsilon = m\pi$, δηλαδή οι ακέραιοι x και υ είναι ισοδύναμοι, οπότε θα ανήκουν στην ίδια κλάση ισοδυναμίας.

Επειδή κάθε ακέραιος είναι ισοδύναμος με το υπόλοιπο της διαίρεσής του με τον m, συμπεραίνουμε ότι θα έχουμε τόσες διαφορετικές κλάσεις ισοδυναμίας, όσα είναι τα δυνατά υπόλοιπα της διαίρεσης με τον m. Αυτά είναι τα $0, 1, 2, \ldots, m-1$, όπως προκύπτει από τη σχέση $0 \leq \upsilon < m$. Συμφωνούμε να χρησιμοποιούμε σαν αντιπρόσωπο της κάθε κλάσης το μικρότερο μη αρνητικό ακέραιο που περιέχεται στην κλάση αυτή. Έτσι, το σύνολο των κλάσεων ισοδυναμίας των ακεραίων $\bmod m$ θα είναι

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\},$$

όπου

$$\begin{aligned}
\overline{0} &= \{x \in \mathbb{Z} \,/ x \sim 0\} = \{x \in \mathbb{Z} \,/ x - 0 = km, k \in \mathbb{Z}\} = \{km / k \in \mathbb{Z}\},\\
\overline{1} &= \{x \in \mathbb{Z} \,/ x \sim 1\} = \{x \in \mathbb{Z} \,/ x - 1 = km, k \in \mathbb{Z}\} = \{km + 1 / k \in \mathbb{Z}\},\\
\overline{2} &= \{x \in \mathbb{Z} \,/ x \sim 2\} = \{x \in \mathbb{Z} \,/ x - 2 = km, k \in \mathbb{Z}\} = \{km + 2 / k \in \mathbb{Z}\},\\
&\ldots\ldots\ldots
\end{aligned}$$

Στο σύνολο $\mathbb{Z}_m$ ορίζουμε δύο πράξεις, την πρόσθεση και τον πολλαπλασιασμό κλάσεων, με τον εξής τρόπο:

$$\overline{x} + \overline{y} = \overline{x + y} \quad \text{και} \quad \overline{x} \cdot \overline{y} = \overline{x \cdot y}, \text{ για κάθε } x, y \in \mathbb{Z}_m.$$

Για παράδειγμα, στο σύνολο $\mathbb{Z}_6$ θα έχουμε

$$\overline{1} + \overline{3} = \overline{1 + 3} = \overline{4}, \text{ και } \overline{4} \cdot \overline{5} = \overline{4 \cdot 5} = \overline{20} = \overline{3 \cdot 6 + 2} = \overline{3 \cdot 6} + \overline{2} = \overline{2}.$$

Μπορούμε να δείξουμε ότι οι πράξεις αυτές είναι καλά ορισμένες. Προηγουμένως, όμως, αξίζει να δούμε γιατί χρειάζεται μια τέτοια απόδειξη.

Είναι γνωστό ότι οι κλάσεις $\overline{x}$ και $\overline{y}$ είναι υποσύνολα του $\mathbb{Z}$, και οι ακέραιοι x και y επιλέχθηκαν σαν αντιπρόσωποι των κλάσεων αυτών. Γνωρίζουμε, όμως, ότι οποιοδήποτε στοιχείο μιας κλάσης, μπορεί να θεωρηθεί αντιπρόσωπος της κλάσης αυτής. Έτσι, είναι δυνατόν να έχουμε

$$\left.\begin{array}{c} x \neq x_1 \text{ αλλά } \overline{x} = \overline{x_1} \\ y \neq y_1 \text{ αλλά } \overline{y} = \overline{y_1} \end{array}\right\} \tag{1.1}$$

Στην περίπτωση αυτή, οι πράξεις που ορίσαμε θα μας οδηγήσουν στα παρακάτω αποτελέσματα.

$$\left.\begin{array}{c} \overline{x} + \overline{y} = \overline{x + y} \text{ και } \overline{x_1} + \overline{y_1} = \overline{x_1 + y_1} \\ \overline{x} \cdot \overline{y} = \overline{x \cdot y} \text{ και } \overline{x_1} \cdot \overline{y_1} = \overline{x_1 \cdot y_1} \end{array}\right\} \tag{1.2}$$

Από τις σχέσεις (1.1) προκύπτει ότι τα πρώτα μέλη της πρόσθεσης και του πολλαπλασιασμού στις σχέσεις (1.2) είναι ίσα. Άρα θα πρέπει και τα αντίστοιχα δεύτερα μέλη να είναι επίσης ίσα, γεγονός που δεν φαίνεται αμέσως. Αυτό σημαίνει ότι πρέπει να δείξουμε ότι, όταν ισχύουν οι σχέσεις (1.1), θα ισχύουν και οι σχέσεις

$$\overline{x + y} = \overline{x_1 + y_1} \text{ και } \overline{x \cdot y} = \overline{x_1 \cdot y_1}.$$

Υποθέτουμε, λοιπόν, ότι ισχύουν οι σχέσεις (1.1). Τότε θα έχουμε

$$\overline{x} = \overline{x_1} \Rightarrow x \sim x_1 \Rightarrow x - x_1 = km \Rightarrow x = x_1 + km,$$
$$\overline{y} = \overline{y_1} \Rightarrow y \sim y_1 \Rightarrow y - y_1 = \lambda m \Rightarrow y = y_1 + \lambda m.$$

Χρησιμοποιώντας τις προηγούμενες ισότητες μπορούμε να πάρουμε

$$\overline{x+y} = \overline{(x_1 + km) + (y_1 + \lambda m)} = \overline{(x_1 + y_1) + (k+\lambda)m} = \overline{x_1 + y_1},$$

$$\overline{x \cdot y} = \overline{(x_1 + km) \cdot (y_1 + \lambda m)} = \overline{(x_1 \cdot y_1) + (ky_1 + \lambda x_1 + k\lambda m)m} = \overline{x_1 \cdot y_1}.$$

Αυτό σημαίνει ότι οι πράξεις της πρόσθεσης και του πολλαπλασιασμού που ορίσαμε είναι καλά ορισμένες, δηλαδή το αποτέλεσμα των πράξεων δεν εξαρτάται από την επιλογή των αντιπροσώπων των κλάσεων.

Οι δύο αυτές πράξεις έχουν την αντιμεταθετική και την προσεταιριστική ιδιότητα, όπως φαίνεται από τις παρακάτω ισότητες.

$$\overline{x} + \overline{y} = \overline{x+y} = \overline{y+x} = \overline{y} + \overline{x},$$
$$\overline{x} \cdot \overline{y} = \overline{x \cdot y} = \overline{y \cdot x} = \overline{y} \cdot \overline{x},$$

και

$$\begin{aligned}
\overline{x} + (\overline{y} + \overline{z}) &= \overline{x} + (\overline{y+z}) = \overline{x + (y+z)} = \overline{(x+y)+z} = \\
&= (\overline{x+y}) + \overline{z} = (\overline{x} + \overline{y}) + \overline{z}, \\
\overline{x} \cdot (\overline{y} \cdot \overline{z}) &= \overline{x} \cdot (\overline{y \cdot z}) = \overline{x \cdot (y \cdot z)} = \overline{(x \cdot y) \cdot z} = \\
&= (\overline{x \cdot y}) \cdot \overline{z} = (\overline{x} \cdot \overline{y}) \cdot \overline{z}.
\end{aligned}$$

Τέλος, το στοιχείο $\overline{0}$ είναι το μηδενικό στοιχείο της πρόσθεσης, ενώ το στοιχείο $\overline{1}$ είναι το μοναδιαίο στοιχείο του πολλαπλασιασμού, όπως προκύπτει από τις επόμενες σχέσεις, και την αντιμεταθετική ιδιότητα.

$$\overline{x} + \overline{0} = \overline{x+0} = \overline{x},$$
$$\overline{x} \cdot \overline{1} = \overline{x \cdot 1} = \overline{x}.$$

Αν, τώρα, $\overline{x}$ είναι τυχόν στοιχείο του $\mathbb{Z}_m$, τότε θα έχουμε

$$\overline{x} + \overline{m - x} = \overline{x + m - x} = \overline{m} = \overline{0}.$$

Δηλαδή το στοιχείο $\overline{m-x}$ είναι το αντίθετο του $\overline{x}$.

Από όλα τα προηγούμενα προκύπτει ότι, ***για κάθε φυσικό αριθμό*** $m > 1$***, το σύνολο*** $\mathbb{Z}_m$***, με πράξη την πρόσθεση, αποτελεί μια προσθετική, αντιμεταθετική ομάδα***.

Ως προς την πράξη του πολλαπλασιασμού, το σύνολο $\mathbb{Z}_m$ δεν μπορεί να αποτελεί ομάδα, διότι το στοιχείο $\overline{0}$ δεν έχει αντίστροφο. Μπορούμε, όμως, να αποδείξουμε ότι το σύνολο

$$\mathbb{Z}_m^* = \{\overline{x} \in \mathbb{Z}_m / (x, m) = 1\},$$

όλων των στοιχείων του $\mathbb{Z}_m$, των οποίων οι αντιπρόσωποι είναι πρώτοι με το δείκτη m, αποτελεί μια πολλαπλασιαστική, αντιμεταθετική ομάδα.

Αν $\overline{x}$ και $\overline{y}$ είναι δύο στοιχεία του συνόλου $\mathbb{Z}_m^*$, τότε θα ισχύουν

$$(x, m) = 1 \text{ και } (y, m) = 1.$$

Άρα θα ισχύει και η σχέση $(xy, m) = 1$, δηλαδή θα έχουμε $\overline{x} \cdot \overline{y} \in \mathbb{Z}_m^*$. Αυτό, βέβαια, σημαίνει ότι το σύνολο $\mathbb{Z}_m^*$ είναι κλειστό ως προς τον πολλαπλασιασμό. Επομένως, το μόνο που χρειάζεται να αποδείξουμε είναι ότι το αντίστροφο κάθε στοιχείου του $\mathbb{Z}_m^*$ είναι επίσης ένα στοιχείο του $\mathbb{Z}_m^*$.

Έστω, λοιπόν, $\overline{x}$ τυχόν στοιχείο του συνόλου $\mathbb{Z}_m^*$. Τότε ασφαλώς θα ισχύει $(x, m) = 1$, άρα θα υπάρχουν ακέραιοι a και b τέτοιοι, ώστε να ισχύει η σχέση $ax + bm = 1$. Επομένως θα έχουμε

$$\overline{1} = \overline{ax + bm} = \overline{ax} + \overline{bm} = \overline{a} \cdot \overline{x} + \overline{b} \cdot \overline{m} = \overline{a} \cdot \overline{x},$$

εφόσον ισχύει $\overline{m} = \overline{0}$. Αυτό σημαίνει ότι το στοιχείο $\overline{a}$ είναι το αντίστροφο του $\overline{x}$. Επιπλέον, θα ισχύει $\overline{a} \in \mathbb{Z}_m^*$, διότι $(a, m) = 1$, εφόσον υπάρχουν ακέραιοι x και b τέτοιοι, ώστε να ισχύει $ax + bm = 1$.

Άρα αποδείξαμε ουσιαστικά ότι, ***για κάθε φυσικό αριθμό*** $m > 1$***, το σύνολο*** $\mathbb{Z}_m^*$ ***αποτελεί μια πολλαπλασιαστική, αντιμεταθετική ομάδα***.

Είναι προφανές ότι, στην περίπτωση που ο δείκτης m είναι ένας πρώτος αριθμός, τότε το σύνολο $\mathbb{Z}_m^*$ είναι το σύνολο των μη μηδενικών στοιχείων του συνόλου $\mathbb{Z}_m$. Αυτό σημαίνει ότι το σύνολο $\mathbb{Z}_p^* = \mathbb{Z}_p - \{\overline{0}\}$ είναι μια πολλαπλασιαστική, αντιμεταθετική ομάδα, για κάθε πρώτο αριθμό p.▲

Το επόμενο είναι ένα παράδειγμα μιας ημιομάδας, η οποία δεν είναι ομάδα.

Παράδειγμα 1.1.4 Έστω S ένα σύνολο με περισσότερα από ένα στοιχεία. Στο S ορίζουμε μια πράξη $*$ με τον εξής τρόπο:

$$a * b = a, \text{ για κάθε } a \in S \text{ και } b \in S.$$

Επειδή $a * (b * c) = a * b = a$ και $(a * b) * c = a * c = a$, προκύπτει ότι το σύνολο S αποτελεί μια ημιομάδα, εφόσον ισχύει η προσεταιριστική ιδιότητα.

Θα δείξουμε ότι δεν υπάρχει μοναδιαίο στοιχείο. Πράγματι, αν υποθέσουμε ότι e είναι το μοναδιαίο στοιχείο του S, τότε το S θα περιέχει ένα τουλάχιστον στοιχείο $a \neq e$, εφόσον έχει περισσότερα από ένα στοιχεία. Επομένως, θα πρέπει να ισχύει $e * a = a = a * e$, πράγμα άτοπο, διότι σύμφωνα με τον ορισμό της πράξης έχουμε $e * a = e$. Αυτό σημαίνει ότι το S δεν μπορεί να έχει μοναδιαίο στοιχείο, οπότε δεν είναι μονοειδές, ούτε φυσικά ομάδα.▲

Ακολουθεί η ομάδα μεταθέσεων. Μια σημαντική ομάδα, όπως θα δούμε σύντομα.

Παράδειγμα 1.1.5 Έστω X ένα μη κενό σύνολο. Κάθε αμφιμονότιμη και επί συνάρτηση $f : X \longrightarrow X$ λέγεται ***μετάθεση*** του συνόλου X. Το σύνολο των μεταθέσεων του X συμβολίζεται με $S(X)$, δηλαδή

$$S(X) = \{f / f : X \longrightarrow X, \, f \text{ αμφιμονότιμη και επί}\}.$$

Στο σύνολο $S(X)$ ορίζουμε σαν πράξη τη σύνθεση συναρτήσεων, η οποία έχει την προσεταιριστική, αλλά όχι την αντιμεταθετική ιδιότητα. Επίσης, η ταυτοτική συνάρτηση $I_X : X \longrightarrow X$ είναι το μοναδιαίο στοιχείο της πράξης αυτής, και κάθε στοιχείο $f : X \longrightarrow X$ του $S(X)$ έχει αντίστροφο στοιχείο, που είναι η αντίστροφη συνάρτηση $f^{-1} : X \longrightarrow X$. Αυτό σημαίνει ότι το σύνολο $S(X)$ είναι μια ομάδα, με πράξη τη σύνθεση συναρτήσεων. Η ομάδα $S(X)$ λέγεται ***ομάδα μεταθέσεων*** του συνόλου X.

Ειδικότερα, στην περίπτωση που είναι $X = I_n = \{1, 2, \ldots, n\}$, τότε η ομάδα $S(X)$ συμβολίζεται με S_n, και λέγεται ***συμμετρική ομάδα*** των n στοιχείων.

Ένα τυπικό στοιχείο της ομάδας S_n, δηλαδή μια τυπική αμφιμονότιμη και επί συνάρτηση $\sigma : I_n \longrightarrow I_n$, θα είναι μια αντιστοιχία της μορφής

$$\begin{array}{rccccc} & 1 & 2 & 3 & \cdots & n \\ \sigma : & \downarrow & \downarrow & \downarrow & \cdots & \downarrow \\ & a_1 & a_2 & a_3 & \cdots & a_n \end{array}$$

όπου τα στοιχεία a_1, a_2, ..., a_n είναι τα στοιχεία 1, 2, 3, ..., n, με διαφορετική ενδεχόμενα διάταξη. Έτσι, για τα στοιχεία της ομάδας S_n θα χρησιμοποιούμε το συμβολισμό

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ a_1 & a_2 & a_3 & \cdots & a_n \end{pmatrix},$$

ο οποίος θα δείχνει ότι πρόκειται για τη συνάρτηση

$$\sigma : \{1, 2, \ldots, n\} \longrightarrow \{1, 2, \ldots, n\},$$

που απεικονίζει το 1 στο a_1, το 2 στο a_2, ..., το n στο a_n. Έτσι, μπορούμε να πούμε ότι η ομάδα S_n είναι το σύνολο

$$S_n = \left\{ \sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ a_1 & a_2 & a_3 & \cdots & a_n \end{pmatrix} / a_1, a_2, \ldots, a_n \in I_n \right\}.$$

Με τη νέα αυτή γραφή των στοιχείων της S_n κάθε στοιχείο προσδιορίζεται πλήρως από τη δεύτερη γραμμή του πίνακα, εφόσον η πρώτη είναι πάντοτε το πεδίο ορισμού της συνάρτησης, δηλαδή τα στοιχεία 1, 2, 3, ..., n. Η δεύτερη γραμμή αποτελείται και πάλι από τα στοιχεία 1, 2, 3, ..., n, χωρίς επαναλήψεις, και χωρίς παραλήψεις, με διαφορετική γενικά διάταξη. Επομένως, για να βρούμε το πλήθος των στοιχείων της S_n αρκεί να βρούμε τους διαφορετικούς τρόπους με τους οποίους μπορεί να συμπληρωθεί η δεύτερη γραμμή.

Η δεύτερη γραμμή έχει n θέσεις που πρέπει να συμπληρωθούν με τα στοιχεία του I_n. Έτσι, τη θέση a_1 μπορεί να καταλάβει ένα οποιοδήποτε στοιχείο του I_n, δηλαδή για τη θέση a_1 έχουμε n διαφορετικές επιλογές. Όμως, από τη στιγμή που θα επιλεγεί το στοιχείο που θα τοποθετηθεί στη θέση a_1, τότε για το στοιχείο a_2 θα υπάρχουν μόνο $n-1$ διαφορετικές επιλογές, εφόσον στη θέση a_2 δεν μπορεί να τοποθετηθεί το στοιχείο που κατέλαβε τη θέση a_1 (η συνάρτηση δεν θα ήταν αμφιμονότιμη). Άρα για τις θέσεις a_1 και a_2 θα έχουμε συνολικά $n(n-1)$ διαφορετικές επιλογές. Ασφαλώς, για τη θέση a_3 θα έχουμε $n-2$ διαφορετικές επιλογές, για τη θέση a_4 θα έχουμε $n-3$ διαφορετικές επιλογές κλπ. Επομένως, για να συμπληρωθούν όλες οι θέσεις της δεύτερης γραμμής θα έχουμε συνολικά $n(n-1)(n-2)\cdots 3\cdot 2\cdot 1 = n!$ διαφορετικές επιλογές. Αυτό σημαίνει ότι η ομάδα S_n περιέχει $n!$ στοιχεία.

Ένα στοιχείο $\sigma \in S_n$ είναι μια αμφιμονότιμη και επί συνάρτηση $\sigma : I_n \longrightarrow I_n$. Το στοιχείο αυτό μπορεί να γραφεί στην μορφή:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ a_1 & a_2 & a_3 & \cdots & a_n \end{pmatrix}, \tag{1.3}$$

όπου $a_i \in X = \{1, 2, 3, \ldots, n\}$ είναι το στοιχείο, στο οποίο η αμφιμονότιμη και επί συνάρτηση σ απεικονίζει το στοιχείο $i \in X$. Δηλαδή θα έχουμε

$$\sigma(i) = a_i, \text{ για κάθε } i = 1, 2, \ldots, n.$$

Προφανώς, η πράξη της ομάδας S_n είναι η σύνθεση συναρτήσεων. Θα χρησιμοποιήσουμε, όμως, το όνομα του πολλαπλασιασμού, όπως από την αρχή συμφωνήσαμε, δανειζόμενοι και την αντίστοιχη ορολογία. Έτσι, αν σ και τ είναι δύο στοιχεία της S_n το γινόμενο $\sigma\tau$, θα γράφουμε απλούστερα $\sigma\tau$ αντί της σύνθεσης $\sigma \circ \tau$, θα είναι η συνάρτηση

$$\sigma\tau : \{1, 2, \ldots, n\} \longrightarrow \{1, 2, \ldots, n\},$$

που ορίζεται από τη σχέση:

$$\sigma\tau(i) = \sigma(\tau(i)), \text{ για κάθε } i = 1, 2, \ldots, n.$$

Για παράδειγμα, αν

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \text{ και } \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

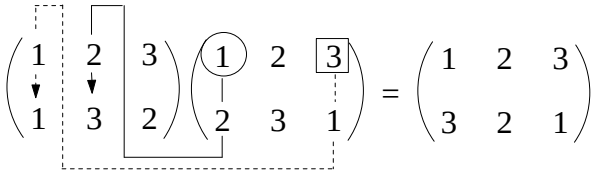
είναι δύο στοιχεία της ομάδας S_3, τότε το γινόμενο $\sigma\tau$ θα είναι

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

Πράγματι, εύκολα διαπιστώνεται ότι θα ισχύουν

$$\begin{aligned} \sigma\tau(1) &= \sigma(\tau(1)) = \sigma(2) = 3, \\ \sigma\tau(2) &= \sigma(\tau(2)) = \sigma(3) = 2, \text{ και} \\ \sigma\tau(3) &= \sigma(\tau(3)) = \sigma(1) = 1. \end{aligned}$$

Ένας εύκολος τρόπος για να βρούμε το γινόμενο μεταθέσεων περιγράφεται στο παρακάτω διάγραμμα. Στη διαδικασία αυτή ξεκινάμε πάντοτε από δεξιά προς τα αριστερά. Αν, για παράδειγμα, θέλουμε να βρούμε το αντίστοιχο του 1 ακολουθούμε τη διαδρομή $1 \longrightarrow 2 \longrightarrow 2 \longrightarrow 3$. Άρα το αντίστοιχο του 1 είναι το 3. Με τον ίδιο τρόπο βρίσκουμε και τα υπόλοιπα στοιχεία. Έτσι, για να βρούμε το αντίστοιχο του 3, ξεκινάμε από δεξιά προς τα αριστερά, και ακολουθούμε τη διαδρομή $3 \longrightarrow 1 \longrightarrow 1 \longrightarrow 1$. Οπότε το αντίστοιχο του 3 είναι το 1.



Είδαμε ότι ο συμβολισμός (1.3) σημαίνει ότι η συνάρτηση σ απεικονίζει το στοιχείο k στο στοιχείο a_k, δηλαδή έχουμε τη σχέση $\sigma(k) = a_k$, για κάθε $k \in I_n$. Επομένως, αν αλλάξουμε, με οποιοδήποτε τρόπο, τη διάταξη των κάθετων ζευγών $\{1, a_1\}$, $\{2, a_2\}$, $\ldots$, $\{n, a_n\}$, η αντιστοιχία

$$\begin{array}{ccccc} 1 & 2 & 3 & \cdots & n \\ \downarrow & \downarrow & \downarrow & \cdots & \downarrow \\ a_1 & a_2 & a_3 & \cdots & a_n \end{array}$$

που ορίζει η συνάρτηση σ δεν αλλάζει, δηλαδή η μετάθεση σ παραμένει αμετάβλητη. Για παράδειγμα, θα έχουμε

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 3 & 1 & 2 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 4 & 2 & 1 & 3 \\ 2 & 1 & 3 & 4 \end{pmatrix} = \cdots$$

Απλά συμφωνήσαμε η πρώτη γραμμή του πίνακα να βρίσκεται πάντοτε στη συνήθη διάταξη.

Η παρατήρηση αυτή μας οδηγεί σε δύο συμπεράσματα. Αν και περιγράψαμε προηγουμένως ένα τρόπο για να βρίσκουμε το γινόμενο μεταθέσεων, ας υποθέσουμε ότι θέλουμε να πολλαπλασιάσουμε τις μεταθέσεις

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \text{ και } \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}.$$

Αλλάζουμε τα κάθετα ζεύγη της μετάθεσης σ κατά τέτοιο τρόπο, ώστε η πρώτη γραμμή της σ να γίνει ίδια με τη δεύτερη γραμμή της τ, δηλαδή

$$\sigma = \begin{pmatrix} 4 & 2 & 1 & 3 \\ 2 & 1 & 3 & 4 \end{pmatrix}.$$

Τότε το γινόμενο $\sigma \cdot \tau$ θα είναι η μετάθεση, η οποία θα έχει σαν πρώτη γραμμή την πρώτη γραμμή της τ, και σαν δεύτερη γραμμή τη δεύτερη γραμμή της νέας μορφής της σ, δηλαδή

$$\sigma \cdot \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}.$$

Το δεύτερο συμπέρασμα αφορά την αντίστροφη μετάθεση. Ας υποθέσουμε ότι έχουμε τη μετάθεση σ που ορίζεται από τη σχέση (1.3). Είναι προφανές ότι, η αντίστροφη συνάρτηση της σ θα είναι συνάρτηση που απεικονίζει το a_1 στο 1, το a_2 στο 2, ..., το a_n στο n. Δηλαδή θα είναι η μετάθεση

$$\sigma^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}.$$

Πράγματι, χρησιμοποιώντας το προηγούμενο συμπέρασμα, εύκολα διαπιστώνεται ότι ισχύει

$$\begin{aligned} \sigma \cdot \sigma^{-1} &= \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ a_1 & a_2 & a_3 & \cdots & a_n \end{pmatrix} \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix} = \\ &= \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix} = \sigma_0, \end{aligned}$$

όπου σ_0 είναι η ταυτοτική μετάθεση, δηλαδή το μοναδιαίο στοιχείο της S_n. Για παράδειγμα, το αντίστροφο στοιχείο της μετάθεσης

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix},$$

θα είναι η μετάθεση

$$\tau^{-1} = \begin{pmatrix} 4 & 2 & 1 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}.$$

Όπως είδαμε η ομάδα S_n έχει $n!$ στοιχεία, επομένως η ομάδα S_3 έχει $3! = 6$ στοιχεία, και είναι η μικρότερη μη αντιμεταθετική ομάδα. Αν θέσουμε

$$\sigma_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$
$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \pi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

τότε, μετά από κάποιες πράξεις, μπορούμε να βρούμε ότι ο πίνακας της συμμετρικής

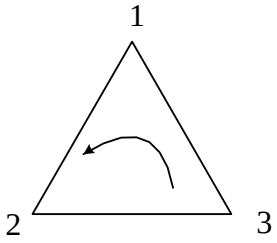
ομάδας S_3 θα είναι:

	σ_0	σ_1	σ_2	π_1	π_2	π_3
σ_0	σ_0	σ_1	σ_2	π_1	π_2	π_3
σ_1	σ_1	σ_2	σ_0	π_3	π_1	π_2
σ_2	σ_2	σ_0	σ_1	π_2	π_3	π_1
π_1	π_1	π_2	π_3	σ_0	σ_1	σ_2
π_2	π_2	π_3	π_1	σ_2	σ_0	σ_1
π_3	π_3	π_1	π_2	σ_1	σ_2	σ_0

Ο πίνακας της S_3 δεν είναι συμμετρικός ως προς την κύρια διαγώνιο, άρα η ομάδα S_3 δεν είναι αντιμεταθετική. Για παράδειγμα, βλέπουμε ότι $\pi_1\sigma_1 = \pi_2 \neq \pi_3 = \sigma_1\pi_1$.▲

Στην ομάδα S_3 μπορούμε να καταλήξουμε και με διαφορετικό τρόπο. Ας δούμε το επόμενο παράδειγμα.

Παράδειγμα 1.1.6 Θεωρούμε ένα ισόπλευρο τρίγωνο και αριθμούμε τις κορυφές του με τους αριθμούς 1, 2, 3.



Θεωρούμε επίσης τους παρακάτω μετασχηματισμούς του τριγώνου αυτού:

σ_0	είναι στροφή του τριγώνου περί το κέντρο του κατά	$0\,^\circ$
σ_1	είναι στροφή του τριγώνου περί το κέντρο του κατά	$120\,^\circ$
σ_2	είναι στροφή του τριγώνου περί το κέντρο του κατά	$240\,^\circ$
π_1	περιστροφή περί τη διχοτόμο της γωνίας 1 κατά	$180\,^\circ$
π_2	περιστροφή περί τη διχοτόμο της γωνίας 2 κατά	$180\,^\circ$
π_3	περιστροφή περί τη διχοτόμο της γωνίας 3 κατά	$180\,^\circ$

Κάθε ένας από τους μετασχηματισμούς αυτούς είναι μια συμμετρία του ισοπλεύρου τριγώνου. Αυτό σημαίνει ότι κάθε ένας από τους μετασχηματισμούς αυτούς στέλνει τις κορυφές του τριγώνου στις κορυφές του ιδίου τριγώνου και μόνο σε αυτές. Δηλαδή, κάθε ένας από τους παραπάνω μετασχηματισμούς είναι μια αμφιμονότιμη και

επί συνάρτηση από το σύνολο $\{1, 2, 3\}$ στον εαυτό του. Επομένως είναι μια μετάθεση του συνόλου $\{1, 2, 3\}$. Για παράδειγμα, ο μετασχηματισμός σ_2 είναι η συνάρτηση

$$\sigma_2 : \{1, 2, 3\} \longrightarrow \{1, 2, 3\},$$

που ορίζεται από τις σχέσεις $\sigma_2(1) = 3$, $\sigma_2(2) = 1$, $\sigma_2(3) = 2$, εφόσον απεικονίζει την κορυφή 1 στην 3, τη 2 στην 1, και την κορυφή 3 στη 2. Αυτό προκύπτει από το γεγονός ότι ο μετασχηματισμός σ_2 στρέφει το τρίγωνο κατά 240° προς τη κατεύθυνση που σημειώνεται στο σχήμα. Άρα ο μετασχηματισμός σ_2 είναι ουσιαστικά η μετάθεση

$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Γενικά, εύκολα διαπιστώνεται ότι κάθε μετασχηματισμός του τριγώνου είναι μια μετάθεση του συνόλου $\{1, 2, 3\}$, και κάθε μετάθεση του συνόλου $\{1, 2, 3\}$ αντιστοιχεί σε ένα μετασχηματισμό του τριγώνου. Για παράδειγμα ο μετασχηματισμός π_3, είναι η μετάθεση

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

Κάθε μετασχηματισμός είναι μια συνάρτηση, άρα μπορούμε να μιλάμε για σύνθεση συναρτήσεων. Η σύνθεση αυτή σαν σύνθεση αμφιμονότιμων και επί συναρτήσεων, θα είναι επίσης ένας μετασχηματισμός του ισοπλεύρου τριγώνου. Δηλαδή, στο σύνολο

$$D_3^* = \{\sigma_0, \sigma_1, \sigma_2, \pi_1, \pi_2, \pi_3\},$$

των συμμετριών του ισοπλεύρου τριγώνου ορίζεται μια πράξη. Για παράδειγμα, η σύνθεση $\sigma_2\pi_3$, των σ_2 και π_3, θα είναι ο μετασχηματισμός

$$\sigma_2\pi_3 : \{1, 2, 3\} \longrightarrow \{1, 2, 3\},$$

που ορίζεται από τις σχέσεις

$$\begin{aligned} \sigma_2\pi_3(1) &= \sigma_2(\pi_3(1)) = \sigma_2(2) = 1, \\ \sigma_2\pi_3(2) &= \sigma_2(\pi_3(2)) = \sigma_2(1) = 3, \\ \sigma_2\pi_3(3) &= \sigma_2(\pi_3(3)) = \sigma_2(3) = 2. \end{aligned}$$

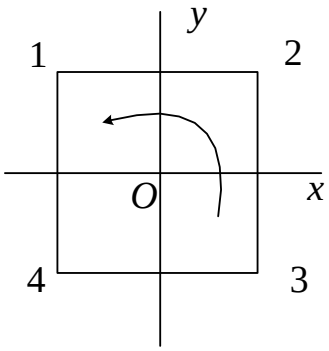
Ακόμη απλούστερα, χρησιμοποιώντας το γινόμενο μεταθέσεων θα έχουμε

$$\sigma_2\pi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \pi_1.$$

Εύκολα διαπιστώνεται ότι το σύνολο D_3^* εφοδιασμένο με την πράξη της σύνθεσης μετασχηματισμών αποτελεί μια ομάδα, της οποίας ο πίνακας είναι ακριβώς ίδιος με τον πίνακα της συμμετρικής ομάδας S_3. Αυτός, άλλωστε, είναι ο λόγος για τον οποίο χρησιμοποιήσαμε τα ίδια σύμβολα για τις δύο αυτές ομάδες.▲

Στο προηγούμενο παράδειγμα είδαμε ότι κάθε συμμετρία του ισοπλεύρου τριγώνου είναι ένα στοιχείο της S_3, και αντίστροφα. Όμως, δεν ισχύει το ίδιο για τις συμμετρίες του τετραγώνου, όπως θα δούμε στο επόμενο παράδειγμα.

Παράδειγμα 1.1.7 Θεωρούμε ένα τετράγωνο με κέντρο την αρχή του συστήματος συντεταγμένων και πλευρές παράλληλες προς τους άξονες.



Αριθμούμε τις κορυφές του με τους αριθμούς 1, 2, 3, 4. Θεωρούμε τώρα τους παρακάτω μετασχηματισμούς του τετραγώνου

I	είναι στροφή περί το κέντρο κατά	$0\,^\circ$
R	είναι στροφή περί το κέντρο κατά	$90\,^\circ$
R^2	είναι στροφή περί το κέντρο κατά	$180\,^\circ$
R^3	είναι στροφή περί το κέντρο κατά	$270\,^\circ$
T_x	είναι περιστροφή περί τον άξονα Ox κατά	$180\,^\circ$
T_y	είναι περιστροφή περί τον άξονα Oy κατά	$180\,^\circ$
T_{13}	είναι περιστροφή περί τη διαγώνιο $1, 3$ κατά	$180\,^\circ$
T_{24}	είναι περιστροφή περί τη διαγώνιο $2, 4$ κατά	$180\,^\circ$

Προφανώς, κάθε ένας από τους μετασχηματισμούς αυτούς είναι μια αμφιμονότιμη και επί συνάρτηση από το σύνολο των κορυφών του τετραγώνου στον εαυτό του. Δηλαδή θα είναι μια μετάθεση του συνόλου $\{1, 2, 3, 4\}$. Για παράδειγμα, ο μετασχηματισμός R^2, που στρέφει το τετράγωνο κατά $180\,^\circ$ προς την κατεύθυνση που σημειώνεται στο σχήμα, θα απεικονίσει την κορυφή 1 στην 3, τη 2 στην 4, την 3 στην 1 και την 4 στην κορυφή 2. Δηλαδή, πρόκειται για τη συνάρτηση

$$R^2 : \{1, 2, 3, 4\} \longrightarrow \{1, 2, 3, 4\},$$

που ορίζεται από τις σχέσεις $R^2(1) = 3$, $R^2(2) = 4$, $R^2(3) = 1$, $R^2(4) = 2$. Άρα ο μετασχηματισμός R^2 είναι η μετάθεση

$$R^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}.$$

Με εντελώς ανάλογο τρόπο, μπορούμε να βρούμε ότι ο μετασχηματισμός T_y είναι η συνάρτηση

$$T_y : \{1, 2, 3, 4\} \longrightarrow \{1, 2, 3, 4\},$$

που ορίζεται από τις σχέσεις $T_y(1) = 2$, $T_y(2) = 1$, $T_y(3) = 4$ και $T_y(4) = 3$. Δηλαδή ο μετασχηματισμός T_y είναι η μετάθεση

$$T_y = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

Επομένως κάθε ένας μετασχηματισμός του τετραγώνου περιγράφεται με μια μετάθεση του συνόλου $\{1, 2, 3, 4\}$. Όμως, σε αντίθεση με τους μετασχηματισμούς του ισοπλεύρου τριγώνου, κάθε μετάθεση του συνόλου $\{1, 2, 3, 4\}$ δεν ορίζει ένα μετασχηματισμό του τετραγώνου. Για παράδειγμα, η μετάθεση

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$$

δεν μπορεί να ορίζει μετασχηματισμό του τετραγώνου, αφού αφήνει σταθερές τις κορυφές 1, 2 και εναλλάσσει τις κορυφές 3 και 4, δηλαδή καταστρέφει το σχήμα.

Φυσικά, όπως και στην περίπτωση των μετασχηματισμών του τριγώνου, μπορούμε να μιλάμε για σύνθεση μετασχηματισμών. Το αποτέλεσμα μπορεί να βρεθεί