ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ

Αναπαραστάσεις του Magnus και εφαρμογές

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ ΕΙΔΙΚΕΥΣΗΣ ΣΤΑ ΘΕΩΡΗΤΙΚΑ ΜΑΘΗΜΑΤΙΚΑ

Σωτηριος Δ. Χασαπης

Επιβλέπων: Ευαγγελος Ραπτης

2008

Περιεχόμενα

Τα θέματα που θα ασχοληθούμε :

- Αναπαράσταση του Magnus μίας ελεύθερης ομάδας σε ένα δακτύλιο δυναμοσειρών.
- Εφαρμογές της αναπαράστασης στη συνδυαστική θεωρία ομάδων.
- Αναπαράσταση Magnus για ομάδες πλεξιδίων Artin.
- Πλεξίδια και κρυπτογραφία (περιγραφή).
- Εφαρμογή δακτυλίου δυναμοσειρών, μέσω της αναπαράστασης που εισήγαμε παραπάνω στην κρυπτογραφία.

Κεφάλαιο 1

Εισαγωγή

1.1 Πρόλογος

Ο Emile Artin το 1925 στο [2] εισήγε τα πλεξίδια(braids) ως μαθηματικά αντικείμενα, καταρχήν διαισθητικά - γεωμετρικά, όπως συμβαίνει με τις περισσότερες έννοιες και αργότερα με αυστηρότητα και πλήρη εγκυρότητα, όπως ο ίδιος μαρτυρά στο [3] το 1947. Προφανώς, κανείς δεν μπορούσε να προβλέψει την ανάπτυξη που θα είχε η ιδέα του αυτή με ευρύτατη χρήση σε θεωρία κόμπων(knot theory), ομάδες Artin και βέβαια πρόσφατα στην κρυπτογραφία. Μία σημαντική οπτική των ομάδων πλεξιδίων υλοποιείται μέσω μίας κλάσης αναπαραστάσεων που εισήχθηκαν από τον W.Magnus το 1939 και φέρουν το όνομά του. Σημαντικότατη τέτοιου τύπου αναπαράσταση είναι αυτή του Burau (1936), η οποία είναι πιστή αναπαράσταση της ομάδας πλεξιδίων $\mathcal{B}_n$ για $n \leq 3$, αλλά αποδείχθηκε πρόσφατα ότι δεν είναι πιστή για $n \geq 9$ Moody(1991)[25], $n \geq 6$ Long-Paton (1993)[20] και $n = 5$ Bigelow(1999) [7]. Η χρήση των πλεξιδίων στην κρυπτογραφία πρωτοεμφανίστηκε στα [1], [19],το

1999 και 2000 αντίστοιχα, αλλά τείνει να αποδειχθεί ανεπαρκής, ως προς την ασφάλεια που μπορεί να παρέχει(βλ. [26]).

Εντούτοις, οι βασικές ιδέες που χρησιμοποιούνται στην κρυπτογραφία με χρήση ομάδων πλεξιδίων, ανήκουν στον πυρήνα μίας πρόσφατα αναπτυχθήσας κατεύθυνσης τη λεγόμενη :

μη μεταθετική αλγεβρική κρυπτογραφία.

Αυτή πιστεύεται ότι πρόκειται να είναι το μέλλον στην ασφαλή κρυπτογράφηση για τη μεταφορά δεδομένων, λαμβάνοντας υπόψη ότι η συνεχώς αυξανόμενη υπολογιστική δύναμη θα ωθήσει στη χρήση θεωρητικού υποβάθρου μη ικανού να αντιμετωπιστεί από έναν υπολογιστή. Μία αναδειχθείσα, τελευταία, βάση ενός τέτοιου συστήματος (Baumslag 2007,[5]) είναι ο

δακτύλιος των δυναμοσειρών
σε n - πλήθος μη μετατιθέμενων μεταβλητών

με χρήση μίας αναπαράστασης της ελεύθερης ομάδας σε n γεννήτορες σε αυτόν. Η αναπαράσταση αυτή, που εισήχθηκε αρχικά από τον Magnus το 1935 στο [21], είναι αντίστοιχη της αναπαράστασης του Magnus για ομάδες πλεξιδίων που αναφέραμε παραπάνω και αναδιαμορφώθηκε από τον Magnus το 1973 στο [22].

Η χρήση και οι εφαρμογές αυτής της αναπαράστασης του Magnus υπήρξαν σημαντικότατες διαχρονικά, τόσο σε θεωρητικό, όσο και σε

πρακτικό επίπεδο. Η παρούσα εργασία ξεκινά με αυτήν την αναπαράσταση στο κεφάλαιο: 3. Ακολουθεί μία σύντομη αναφορά στη χρήση της γενικότερα σε προβλήματα συνδυαστικής θεωρίας ομάδων στο κεφάλαιο: 4, ενώ κλείνουμε με χρήση της προσαρμοσμένης αυτής αναπαραστάσης στην κρυπτογραφία στο κεφάλαιο: 6. Ενδιάμεσα, στο κεφάλαιο: 5, παρουσιάζουμε τις βασικές ιδιότητες των ομάδων πλεξιδίων του Artin και της αντίστοιχης αναπαράστασης του Magnus σε αυτά, όπως περιγράφηκε προηγουμένως.

1.2 Βασικές έννοιες

Η άλγεβρα επί ενός μεταθετικού δακτυλίου R (όλοι οι δακτύλιοι θα θεωρούνται με μονάδα) είναι γενίκευση της έννοιας της άλγεβρας επί ενός σώματος K, όπου το σώμα αντικαθίσταται από ένα μεταθετικό δακτύλιο R.

Ορισμός. 1.2.1 .

Έστω R μεταθετικός δακτύλιος. Μία R-άλγεβρα είναι ένα σύνολο A (μη κενό) με δομή δακτυλίου:

$$
\begin{aligned}
+ : A \times A \mapsto A,\ (R,+) \qquad & \text{είναι αβελιανή ομάδα} \\
\cdot : A \times A \mapsto A,\ (R,\cdot\,) \qquad & \text{είναι μονοειδές} \\
a(b+c) = ab + ac \qquad & \text{επιμεριστική ιδιότητα}
\end{aligned}
$$

και αριστερού R-προτύπου[1]:

$$
\begin{aligned}
(R,+) \qquad & \text{αβελιανή ομάδα} \\
R \times A \to A \qquad & \text{βαθμωτός πολλαπλασιασμός} \\
(r,m) \mapsto r \cdot m & \\
r \cdot (x+y) = rx + ry \qquad & \text{επιμεριστική} \\
(r+s) \cdot x = rx + ry \qquad & \text{επιμεριστική} \\
(rs)x = r(sx) \qquad & \text{R - προσεταιριστική} \\
1_R \cdot x = x \qquad & \text{μονάδα δακτυλίου}
\end{aligned}
$$

[1] Αντίστοιχα ορίζεται και για δεξί.

ώστε ο πολλαπλασιασμός του δακτυλίου να είναι R-διγραμμική απεικόνιση:

$$r(xy) = (rx)y = x(ry), r, s \in R,\ x, y \in A$$

Παράδειγμα 1.2.2 .

Κάθε δακτύλιος R είναι προσθετικά μία αβελιανή ομάδα και κατά συνέπεια ένα $\mathbb{Z}$- πρότυπο. Οπότε έχουμε ότι ο R είναι και μία $\mathbb{Z}$-άλγεβρα.

Παράδειγμα 1.2.3 .

Έστω G μία πολλαπλασιαστική ομάδα και R ένας μεταθετικός δακτύλιος με μονάδα.

Ο ομαδοδακτύλιος RG ορίζεται να έχει στοιχεία της μορφής:

$$\sum a_g g,\ a_g \in R, g \in\ G, a_g \neq 0 \text{ για πεπερασμένο πλήθος } g \in G$$

και έχει δομή δακτυλίου με πράξεις που ορίζονται ως εξής:

$$\sum a_g g + \sum b_g g = \sum (a_g + b_g) g \qquad \text{πρόσθεση} \quad (1.1)$$

$$\sum a_g g \cdot \sum b_h h = \sum_g \sum_h (a_g b_h) gh \qquad \text{πολλαπλασιασμός} \quad (1.2)$$

Τότε ο ομαδοδακτύλιος RG είναι μία R - άλγεβρα με δομή R-προτύπου:

$$r \sum r_i g_i = \sum (r \cdot r_i) g_i, \qquad r, r_i \in R, g_i \in G$$

Ορισμός. 1.2.4 .

Ομομορφισμός δύο αλγεβρών A,B είναι ένας R- γραμμικός ομομορφισμός δακτυλίων, ώστε:

$$\begin{aligned} \varphi : A &\rightarrow B \\ \varphi(rx) &= r\varphi(x) \\ \varphi(x+y) &= \varphi(x)+\varphi(y) \\ \varphi(xy) &= \varphi(x)\varphi(y) \\ \varphi(1_A) &= 1_B,\ x,y \in A,\ r \in R \end{aligned}$$

Κεφάλαιο 2

Ελεύθερα παραγόμενες άλγεβρες

2.1 Βασικές έννοιες

Στο εξής θεωρούμε μία ακεραία περιοχή R με $1(\neq 0)$, την οποία θα ονομάζουμε δακτύλιο συντεταγμένων. Οι άλγεβρες M θα είναι R-πρότυπα με εσωτερικό πολλαπλασιασμό:

$$(r_1u)(r_2v) = (r_1r_2)(uv)$$

$$1u = u$$

$$(r_1 + r_2)u = r_1u + r_2u$$

$$r(u + v) = ru + rv,\ \forall u, v \in M, r_1, r_2 \in R$$

2.2 Η άλγεβρα $A_0(R, r)$

Έστω $X = \{x_1, x_2, .., x_r\} \neq \emptyset$, το οποίο θα ονομάζουμε σύνολο μεταβλητών. Ορίζουμε την προσεταιριστική R - άλγεβρα με στοιχεία βάσης του X, τα μονώνυμα:

$$x_{n_1}^{e_1}x_{n_2}^{e_2}\ldots x_{n_k}^{e_k}, \text{όπου } n_i \in \{1, 2, ..., r\}, n_i \neq n_{i+1},\ e_i, k \in \mathbb{N}$$

η οποία είναι το σύνολο όλων των πεπερασμένων αθροισμάτων αυτών των μονωνύμων. Σημειώνουμε ότι οι μεταβλητές x_i δε μετατίθενται.

Ορίζουμε ως μονάδα της άλγεβρας τη μονάδα του δακτυλίου R και γράφουμε συμβατικά:

$$1 = x_i^0, \ \forall \ i \in \{1, 2, ..., r\}$$

Βάση της άλγεβρας το σύνολο: $\{x_1, x_2, ..., x_r\}$ με συντελεστές από τον R και πράξεις:

πολλαπλασιασμός στοιχείων βάσης: ανηγμένη παράθεση

πολλαπλασιασμός αθροισμάτων: $u(v + w) = uv + uw$

$$(r_1 u)(r_2 v) = (r_1 r_2)(uv)$$

Ορισμός. 2.2.1 .

Η $A_0(R, r)$ λέγεται ελεύθερα παραγόμενη προσεταιριστική άλγεβρα τάξης r επί του R και το σύνολο $\{x_1, x_2, ..., x_r\}$ σύνολο ελευθέρων γεννητόρων.

Ορισμός. 2.2.2 .

Ονομάζουμε ομογενή συνιστώσα βαθμού ν ενός στοιχείου της $A_0(R, r)$ ένα άθροισμα μονωνύμων καθένα εκ των οποίων έχει άθροισμα βαθμών των παραγόντων του ίσο με ν.

Παράδειγμα 2.2.3 .

Αν θεωρήσουμε την άλγεβρα $A_0(\ \mathbb{Z}, 2)$ με βάση της άλγεβρας το σύνολο ελευθέρων γεννητόρων: $\{x, y\}$ τότε τα ομογενή μονώνυμα

βαθμού 2 θα είναι τα εξής: x^2, xy, y^2, yx. Τα στοιχεία της θα είναι $\mathbb{Z}$-αθροίσματα των στοιχείων της βάσης. Οι ομογενείς συνιστώσες του στοιχείου $x^3 + xy^2 - 4x + 1$ είναι:

- Βαθμού 0 : 1
- Βαθμού 1 : $-4x$
- Βαθμού 3 : $x^3 + xy^2$

Παράδειγμα 2.2.4 .

Η άλγεβρα $A_0(\mathbb{Z}, 1)$ έχει μία μεταβλητή και συντελεστές ακεραίους, είναι λοιπόν ο δακτύλιος των πολυωνύμων επί του $\mathbb{Z}$: $\mathbb{Z}[x]$.

2.3 Οι άλγεβρες $A_0(R,\infty)$ και $A(R,r)$

Η άλγεβρα $A_0(R,\infty)$ είναι η ελεύθερη προσεταιριστική άλγεβρα, η οποία παράγεται από αριθμήσιμο πλήθος μεταβλητών: x_ρ, $\rho = 1,2,3,....$ Για παράδειγμα ένα στοιχείο αυτής της άλγεβρας θα μπορούσε να είναι το εξής:

$$1 + x_1 + x_7 + x_2x_3 + x_2x_1$$

Επειδή τα στοιχεία της $A_0(R,\infty)$ είναι πεπερασμένα αθροίσματα, σε άπειρες μεταβλητές, τότε κάθε στοιχείο της θα περιέχεται σε μία υπάλγεβρα $A_0(R,r)$ για κάποιο r.

Θεωρούμε τώρα την άλγεβρα $A(R,r)$ που προκύπτει από την $A_0(R,r)$, αν επιτρέψουμε και άπειρα αθροίσματα στοιχείων. Πρόκειται για το δακτύλιο των τυπικών δυναμοσειρών σε r το πλήθος μη μετατιθέμενες μεταβλητές. Τότε κάθε στοιχείο $u \in A(R,r)$ θα γράφεται στη μορφή: $u = \sum_{n=0}^{\infty} u_n$, όπου u_n ομογενής όρος βαθμού n της $A_0(R,r)$.

Παράδειγμα 2.3.1 .

Έστω $u \in A(R,r)$ τότε θα μπορούσε να είναι:

$$u = \underbrace{x_1x_2^3x_4 + x_4^5}\ \underbrace{+x_3^7}\qquad \underbrace{+x_1^7x_4} + \ldots$$

ομογενής συνιστώσα: βαθμού 5 βαθμού 7 βαθμού 8

Πράξεις στην άλγεβρα $A(R,r)$

Έστω $u=\sum_{n=0}^{\infty}\lambda_n u_n\ ,\lambda_n\in R,\ u_n$ μονώνυμο r - μεταβλητών και $v=\sum_{n=0}^{\infty}\varkappa_n v_n\ ,\varkappa_n\in R,\ v_n$ μονώνυμο r - μεταβλητών

$$\text{πρόσθεση δακτυλίου: } u+v=\sum_{n=0}^{\infty}\lambda_n u_n+\varkappa_n v_n$$

$$\text{πολλαπλασιασμός προτύπου: } \lambda\cdot v=\sum_{n=0}^{\infty}\lambda\lambda_n u_n$$

$$\text{πολλαπλασιασμός δακτυλίου: } u\cdot v=\sum_{n=0}^{\infty}c_n a_n$$

$$\text{όπου: } c_n a_n=\sum_{i+j=n}\lambda_i\varkappa_j u_i v_j$$

Κεφάλαιο 3

Απεικονίζοντας μία ελεύθερη ομάδα τάξης r στην $A(\mathbb{Z}, r)$

3.1 Εισαγωγή

Η προσεταιριστική $\mathbb{Z}$- άλγεβρα $A_0(\mathbb{Z}, r)$ στις μη μετατιθέμενες μεταβλητές $x_1, x_2, ..., x_r$ αποτελείται από πολυώνυμα των μεταβλητών αυτών με ακεραίους συντελεστές. Οπότε μπορούμε στην A_0 να θεωρήσουμε και τα στοιχεία που προκύπτουν από αντικαταστάσεις ενός στοιχείου σ' ένα άλλο (υπενθυμίζουμε ότι στην $A_0(\mathbb{Z}, r)$ έχουμε μόνο πεπερασμένα αθροίσματα μονωνύμων).

Παράδειγμα 3.1.1 .

Έστω $P(x_\rho) = x_1x_2^2 + x_2x_3x_1$ και $B_1(x_\rho), B_2(x_\rho), B_3(x_\rho) \in A_0$, τότε θα είναι και

$$P(B_\rho) = B_1B_2^2 + B_2B_3B_1 \in A_0$$

Όμως η ίδια αντικατάσταση δεν μπορεί να γίνει στην άλγεβρα $A(\mathbb{Z}, r)$, δηλαδή την προσεταιριστική $\mathbb{Z}$- άλγεβρα των τυπικών δυναμοσειρών

στις μη μετατιθέμενες μεταβλητές $x_1, x_2, ..., x_r$ με ακεραίους συντελεστές και αυτό διότι μετά την αντικατάσταση μπορεί να προκύψει και στοιχείο που δεν ανήκει στην άλγεβρα επί του $\mathbb{Z}$. Ας δούμε το επόμενο:

Παράδειγμα 3.1.2 .

Έστω το στοιχείο της $A(\mathbb{Z}, r)$:

$$P(x_1) = 1 + x_1 + x_1^2 + \ldots + x_1^n + \ldots$$

τότε θα έχουμε ότι:

$$P(2) = 1 + 2 + 2^2 + \ldots + 2^n + \ldots$$

το οποίο δεν είναι ένα στοιχείο της άλγεβρας $A(\mathbb{Z}, r)$ αφού πρόκειται για στοιχείο που δεν είναι στο δακτύλιο συντεταγμένων $\mathbb{Z}$. Πότε, λοιπόν, ένα στοιχείο που προκύπτει από αντικατάσταση θα είναι και στοιχείο της άλγεβρας;

3.2 Αναπαράσταση του Magnus

Στη συνέχεια θα οδηγηθούμε στη μελέτη μίας αναπαράστασης της παραπάνω άλγεβρας.

Λήμμα 3.2.1 .

Έστω $Q_1(x_\rho), Q_2(x_\rho), ...Q_r(x_\rho) \in A(\ \mathbb{Z}, r)$ με μηδενικό σταθερό όρο, τότε η απεικόνιση:

$$x_\rho \rightarrow\ Q_\rho,\ \rho = 1, 2, ..., r$$

ορίζει ομομορφισμό της $\mathbb{Z}$- άλγεβρας A στον εαυτό της.

Απόδειξη

Άμεση από τις ιδιότητες.

□

Αυτό το λήμμα μας επιτρέπει να δείξουμε ότι η $A(\ \mathbb{Z}, r)$ περιέχει μία μεγάλη πολλαπλασιαστική ομάδα, στην οποία θα βρούμε μία χρήσιμη αναπαράσταση της ελεύθερης ομάδας τάξης r.

Λήμμα 3.2.2 .

Το σύνολο M $\subset$ $A(\mathbb{Z}, r)$ όλων των στοιχείων της $A(\mathbb{Z}, r)$ με σταθερό όρο 1 είναι πολλαπλασιαστική ομάδα, όπου κάθε στοιχείο: $g = 1 + h$ έχει αντίστροφο το εξής στοιχείο:

$$g^{-1} = 1 - h + h^2 - h^3 + ... + (-1)^n h^n + ... \qquad (3.1)$$

Απόδειξη

Δύο στοιχεία του M όταν πολλαπλασιαστούν μεταξύ τους θα δώσουν σταθερό όρο 1, οπότε το M είναι κλειστό ως προς τον πολλαπλασιασμό. Ακόμα, η προσεταιριστική ιδιότητα έπεται άμεσα από τον προσεταιρισμό του πολλαπλασιασμού στην $A(\mathbb{Z}, r)$ και μοναδιαίο στοιχείο είναι το 1 $\in$ M. Τώρα, θα δείξουμε ότι το στοιχείο: $g = 1 + h$ έχει αντίστροφο στοιχείο το g^{-1}, όπως αυτό περιγράφεται στη σχέση: (3.1).

Πράγματι, θεωρούμε το στοιχείο:

$$Q(x_1) = 1 - x_1 + x_1^2 - x_1^3 + \ldots + (-1)^n x_1^n + \ldots$$

όμως τότε έχουμε:

$$\begin{aligned}(1 + x_1)Q(x_1) = & \\ &= 1 - \cancel{x_1} + \cancel{x_1^2} - \cancel{x_1^3} + \ldots + \cancel{(-1)^n x_1^n} + \ldots \\ &+ \cancel{x_1} - \cancel{x_1^2} + \cancel{x_1^3} - \cancel{x_1^4} + \ldots \cancel{(-1)^{n+1} x_1^n} + \ldots \\ &= 1\end{aligned}$$

Δηλαδή δείξαμε ότι: $(1 + x_1)Q(x_1) = 1$, τότε όμως από Λήμμα

(3.2.1) έπεται ότι:

$$(1+h)Q(h) = 1 \Rightarrow \ g \cdot g^{-1} = 1$$

Συνεπώς, κάθε στοιχείο του M έχει αντίστροφο στο M, οπότε έπεται το ζητούμενο. $\square$

Στη συνέχεια θα δούμε τη διατύπωση του βασικού θεωρήματος από το οποίο θα οδηγηθούμε στη ζητούμενη αναπαράσταση της ελεύθερης ομάδας $F(r)$ με διάσταση r.

Θεώρημα 3.2.3 *(Αναπαράστασης του Magnus,* **1935***)* .

Έστω η άλγεβρα $A(\ \mathbb{Z}, r)$, η οποία παράγεται ελεύθερα από τα στοιχεία $x_1, x_2, \ldots, x_r$, τότε τα στοιχεία:

$$\alpha_i = 1 + x_i, \ i = 1, \ldots, r \tag{3.2}$$

της άλγεβρας $A(\ \mathbb{Z}, r)$ είναι γεννήτορες μίας ελεύθερης ομάδας $F(r)$, η οποία έχει διάσταση r.
Επιπλέον, κάθε στοιχείο της ομάδας έχει αντίστροφο:

$$\alpha_i^{-1} = 1 - x_i + x_i^2 - x_i^3 + \ldots + (-1)^n x_i^n + \ldots, \ i = 1, \ldots, r \tag{3.3}$$

Απόδειξη

Στο Λήμμα (3.2.2) αποδείχτηκε ότι τα στοιχεία της $A(\ \mathbb{Z}, r)$, τα οποία έχουν μοναδιαίο σταθερό όρο αποτελούν ομάδα. Οπότε αρκεί να δείξουμε ότι μία ανηγμένη λέξη στα στοιχεία: $\alpha_i = 1 + x_i,\ i = 1, \ldots, r$ είναι 1, αν και μόνο αν είναι η κενή λέξη.

Έστω, λοιπόν, η λέξη:

$$w = \alpha_{\varkappa_1}^{\varepsilon_1}\alpha_{\varkappa_2}^{\varepsilon_2}\ldots\alpha_{\varkappa_\lambda}^{\varepsilon_\lambda},\ \text{όπου}\ \alpha_{\varkappa_i} \in \{\alpha_1, \alpha_2, ..., \alpha_r\},\ \alpha_{\varkappa_i} \neq \alpha_{\varkappa_{i+1}},\ \varepsilon_i \in\ \mathbb{Z}.$$

Ισχυρισμός: $\boxed{\alpha_i^n = 1 + nx_i + x_i^2h(x_i),\quad n \in\ \mathbb{N}}$, όπου $h(x_i)$ είναι τυπική δυναμοσειρά του x_i.

Θα δείξουμε τον ισχυρισμό με επαγωγή: Για $n = 1$ συμβαίνει:

$$\alpha_i = 1 + x_i + x_i^2h(x_i),$$

το οποίο ισχύει για $h(x_i) = 0$. Ακόμα έχουμε:

$$\alpha_i^{n+1} = \alpha_i^n \cdot \alpha_i =$$

$$(1 + nx_i + x_i^2h(x_i))(1 + x_i) =$$

$$1 + nx_i + x_i^2h(x_i) + x_i + nx_i^2 + x_i^3h(x_i) =$$

$$1 + (n+1)x_i + \boxed{nx_i^2 + x_i^2h(x_i) + x_i^3h(x_i)}\ \in A(\ \mathbb{Z}, r)$$

Οπότε συμπεραίνουμε ότι:

$$w = \alpha_{\varkappa_1}^{\varepsilon_1}\alpha_{\varkappa_2}^{\varepsilon_2}\ldots\alpha_{\varkappa_\lambda}^{\varepsilon_\lambda} =$$

$$[(1 + \varepsilon_1x_{\varkappa_1} + x_{\varkappa_1}^2h(x_{\varkappa_1})]\ldots[(1 + \varepsilon_\lambda x_{\varkappa_\lambda} + x_{\varkappa_\lambda}^2h(x_{\varkappa_\lambda})]$$

όπου περιέχεται και το μονώνυμο $\varepsilon_1 \dots \varepsilon_\lambda x_{\varkappa_1} \dots x_{\varkappa_\lambda}$ βαθμού λ και μήκους λ, αφού $\varepsilon_1 \dots \varepsilon_\lambda \neq 0$. Συνεπώς, είναι: $w \neq 1$, οπότε έπεται το ζητούμενο. $\square$

Θα δούμε τώρα κάποια αποτελέσματα που απορρέουν από το θεώρημα (3.2.3).

Ορισμός. 3.2.4 .

Μία υποομάδα $K < G$ καλείται χαρακτηριστική στη G, αν είναι κλειστή ως προς τους αυτομορφισμούς της G, δηλαδή: $\theta(K) \subset K$, $\forall\, \theta \in Aut(G)$. Η K καλείται πλήρως αναλλοίωτη αν είναι κλειστή ως προς τους ενδομορφισμούς της G.

Αν $F(r)$ είναι ελεύθερη ομάδα με r γεννήτορες τότε συμβολίζουμε με:

$$D_n(F) = \{c_n \in F(r) : c_n = 1 + h_n(x_1, \dots, x_r)\}$$

όπου $h_n \in A(\mathbb{Z}, r)$ με κανένα όρο βαθμού μικροτέρου του n. Δηλαδή ισχύει ότι: $h_n \in X^n$.

Θεώρημα 3.2.5 .

Η $D_n(F)$ είναι μία αναλλοίωτη υποομάδα της $F(r)$. Επιπλέον, η τομή όλων των $D_n(F)$ είναι τετριμμένη.

Πρόταση 3.2.6 .

Η ομάδα πηλίκο: $D_n(F)/D_{n+1}(F)$ για $F(r),\ r < \infty$ είναι πεπερασμένα παραγόμενη ελεύθερη αβελιανή ομάδα.

Η αναπαράσταση του Magnus που παρουσιάσαμε στο θεώρημα (3.2.3) δημοσιεύθηκε το 1935 στο [21] *Beziehungen zwischen Gruppen und Idealen in einem speziellen Ring, Mathematische Annalen, 111, 1935* γερμανική έκδοση του Annals of Mathematics. Η πρόσβαση στη γερμανική βιβλιογραφία κατέστη εφικτή μέσω της ηλεκτρονικής ιστοσελίδας:

`http://gdz.sub.uni-goettingen.de`

όπου κρατείται αρχείο και παρουσιάζονται χειρόγραφα και δημοσιεύσεις μαθηματικών κειμένων, ηλεκτρονικά, ενώ ταυτόχρονα είναι δωρεάν διαθέσιμα για ακαδημαϊκή χρήση. Η συλλογή εκτεινόταν την ημέρα συγγραφής της παρούσας σε περίπου πέντε εκατομύρια ψηφιοποιημένες σελίδες.

Εδώ η παρουσίαση έχει γίνει με πηγή το [23]: *Combinatorial Group Theory*, Magnus, Karrass, Solitar, 1968.

Κεφάλαιο 4

Εφαρμογές της αναπαράστασης του Magnus

4.1 Εισαγωγή

Η αναπαράσταση του Magnus έχει χρησιμοποιηθεί ευρύτατα στη θεωρία ομάδων, όπως θα δούμε παρακάτω και υπήρξε ιδιαιτέρως χρήσιμο εργαλείο σε πολλές περιπτώσεις. Μετατροπές της βρίσκουν εφαρμογή και σε σύγχρονες μεθόδους κρυπτογράφησης όπως περιγράφονται στο κεφάλαιο 6.

4.2 Hopfian ομάδες

Ορισμός. 4.2.1 *(Hopfian ομάδες)* .

Μία ομάδα G καλείται Hopfian αν δεν είναι ισόμορφη με ένα γνήσιο πηλίκο. Δηλαδή δεν υπάρχει $N \lhd G$, ώστε: $G \cong G/N$.

Παρατήρηση - Σχόλιο 4.2.2 .

Ισοδύναμα με τον ορισμό (4.2.1) μπορούμε να πούμε ότι αρκεί κάθε

επιμορφισμός: $G \rightarrow\ G$ να είναι και ισομορφισμός.

Παράδειγμα 4.2.3 .

1) Κάθε πεπερασμένη ομάδα είναι Hopfian. Διότι, αν

$$|G| = n, N \lhd G,\ |N| \mid |G| \text{ με: } |G/N| = k$$

και

$$G \cong G/N \Rightarrow\ |G| = |G/N| \Rightarrow\ n = k < n,\ \text{άτοπο.}$$

2) Κάθε απλή ομάδα είναι Hopfian, αφού δεν έχει γνήσιες κανονικές υποομάδες.

3) Μία ελεύθερη ομάδα απείρου διαστάσεως ΔΕΝ είναι Hopfian.

Διότι, έστω: $F = \langle x_1, x_2, \ldots \mid - \rangle$ και ο ομομορφισμός:

$$\varphi : x_1 \rightarrow 1$$

$$x_2 \rightarrow x_1$$

$$x_3 \rightarrow x_2$$

$$\vdots$$

είναι επιμορφισμός και $x_1 \in \ker \varphi$, οπότε δεν είναι ισομορφισμός.

4) ΔΕΝ είναι κάθε πεπερασμένα παραγόμενη ομάδα Hopfian. Συγκεκριμένα, υπάρχει πεπερασμένα παραγόμενη ομάδα G, η οποία ΔΕΝ είναι Hopfian, όπως βλέπουμε στο επόμενο:

Παράδειγμα 4.2.4 *(Ομάδες Baumslag - Solitar).*

Οι $G(k,l) =< t, a | ta^k t^{-1} = a^l >$ είναι πεπερασμένα παριστώμενες ομάδες, αλλά ΔΕΝ είναι Hopfian, αν και μόνο, αν το σύνολο των πρώτων διαιρετών του k είναι διαφορετικό του συνόλου διαιρετών του l και $|k| \neq 1, |l| \neq 1$.

Απόδειξη

(σκιαγράφηση) Έστω p πρώτος ,$p \neq 1,\ p \mid k,\ (p,l) = 1$ και ορίζουμε την απεικόνιση:

$$\begin{array}{rccc} \psi: & G(k,l) & \rightarrow & G(k,l) \\ & t & \rightarrow & t \\ & a & \rightarrow & a^p \end{array}$$

είναι ομομορφισμός ομάδων.

Θεωρούμε, τώρα το μεταθέτη:

$$[ta^m t^{-1}, a] = ta^{-m}t^{-1}a^{-1}ta^m t^{-1}a \neq 1$$

από Λήμμα Britton, ισχύει ότι:

$$\psi([ta^m t^{-1}, a]) = [ta^{pm}t^{-1}, a^p] = [a^l, a^p] = 1.$$

Δηλαδή ο μεταθέτης $[ta^m t^{-1}, a]$ είναι ένα μη τετριμμένο στοιχείου που ανήκει στον πυρήνα $\ker\psi$. Συνεπώς, ο ψ δεν είναι ισομορφισμός, άρα η ομάδα δεν είναι Hopfian. $\square$

Πόρισμα 4.2.5 *(Nielsen)* .

Μία πεπερασμένα παραγόμενη ελεύθερη ομάδα είναι Hopfian.

Εδώ παρουσιάζουμε μία απόδειξη αυτού με χρήση του παρακάτω:

Πόρισμα 4.2.6 .

Αν F_n ο n-οστός όρος της κατώτερης κεντρικής σειράς για την $F(r)$, τότε η $D_n(F)$ περιέχει την F_n.

Από θεώρημα: (3.2.5) έχουμε ότι η τομή όλων των $D_n(F)$ είναι τετριμμένη, οπότε από το προηγούμενο πόρισμα το ίδιο θα συμβαίνει και για την τομή των όρων της κατώτερης κεντρικής σειράς F_n, δηλαδή η ομάδα είναι προσεγγιστικά μηδενοδύναμη. Είναι και από υπόθεση πεπερασμένα παραγόμενη, οπότε είναι Hopfian, διότι ισχύει ότι κάθε πεπερασμένα παραγόμενη προσεγγιστικά μηδενοδύναμη ομάδα είναι Hopfian *βλ: [23], θεώρημα 5.5.*

Κεφάλαιο 5

Πλεξίδια(braids)

5.1 Εισαγωγή

Τα πλεξίδια (Braids) εισήχθηκαν ως μαθηματικά αντικείμενα από τον Emile Artin το 1925 (*Artin E., Theorie der Zopfe, Hamburg Abh. 4*, [2]), όπου όμως οι περισσότερες αποδείξεις του είναι διαισθητικές κυρίως και σε ορισμένα σημεία ελλιπείς. Η έννοια των πλεξιδίων εισήχθηκε όταν μία υφαντουργική εταιρεία ζήτησε κάποιες εφαρμογές από τον Artin τη δεκαετία του 1920. Οι αναφορές εδώ αφορούν στο μεταγενέστερο άρθρο του το 1947: *Artin, Theory of braids*, [3], όπου γίνεται μία πληρέστερη παρουσίαση του αντικειμένου.

5.2 Γεωμετρία των πλεξιδίων

Στο εξής θα συμβολίζουμε με $\mathcal{E}^3$ τον 3-διάστατο Ευκλείδιο χώρο και $\mathcal{E}_0^2, \mathcal{E}_1^2$ τα παράλληλα επίπεδα από τα $z = 0, z = 1$ αντίστοιχα.

Θεωρούμε ακόμα τα εξής n σημεία σε καθένα από τα δύο επίπεδα:

$$P_i = (i, 0, 1),\ Q_i = (i, 0, 0),\ i = 1, 2, \ldots, n$$

τα οποία ανήκουν στην ευθεία $y = 0$ καθενός από τα δύο επίπεδα.

Ορισμός. 5.2.1 *(Πλεξίδιο).*

Ένα πλεξίδιο με n - νήματα (n-πλεξίδιο) αποτελείται από ένα σύστημα n τόξων α_i (τα νήματα του πλεξιδίου), ώστε κάθε α_i συνδέει ένα σημείο P_i του ενός επιπέδου με ένα σημείο $Q_{\pi(i)}$ του άλλου επιπέδου, όπου $\pi \in\ S_n$, ώστε:

α. Κάθε τόξο α_i τέμνει ακριβώς μία φορά το επίπεδο: $z = t, \forall t \in [0, 1]$.

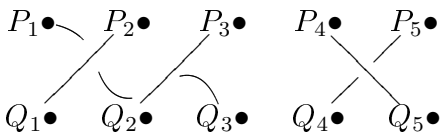
β. Τα τόξα $\alpha_1, \alpha_2, ..., \alpha_n$ τέμνουν το $z = t$ σε n διακεκριμμένα σημεία $\forall t \in [0, 1]$.

Δηλαδή, το τόξο α_i φθίνει γνήσια από το σημείο $P_i \to Q_{\pi(i)}$.

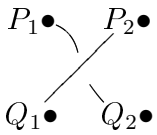
Ορισμός. 5.2.2 .

Η μετάθεση π καλείται μετάθεση του πλεξιδίου. Αν είναι τετριμμένη τότε καλείται γνήσιο(pure) ή χρωματισμένο πλεξίδιο(coloured).

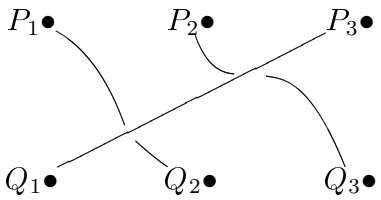
Παράδειγμα 5.2.3 *(Παραδείγματα πλεξιδίων).*



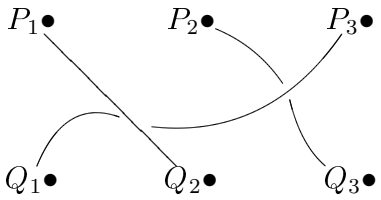
Σχήμα 5.1: *5 - πλεξίδιο*



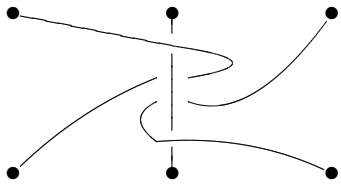
Σχήμα 5.2: *2 - πλεξίδιο*



Σχήμα 5.3: *3 - πλεξίδιο*



Σχήμα 5.4: *3 - πλεξίδιο*



Σχήμα 5.5: *Γνήσιο 3 - πλεξίδιο*

Παρατήρηση - Σχόλιο 5.2.4 .

Στα πλεξίδια των (5.3),(5.4)αντιστοιχεί η ίδια μετάθεση $\pi = (123)$. Όμως αυτά είναι διαφορετικά μεταξύ τους. Δηλαδή, η μετάθεση ενός πλεξιδίου δεν το καθορίζει μονοσήματα.

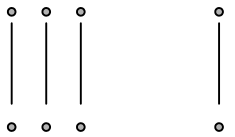
5.3 Ομάδες Πλεξιδίων

5.3.1 Γεωμετρική θεώρηση ομάδων πλεξιδίων

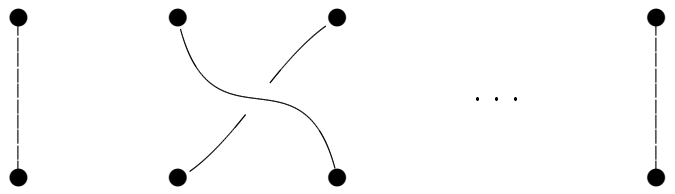
Έστω α, β δύο n - πλεξίδια θα ορίσουμε ως πράξη σ' αυτά $\alpha \cdot \beta$ το n - πλεξίδιο που προκύπτει αν στο τέλος του α ενώσουμε το β. Η πράξη αυτή καλείται σύνθεση πλεξιδίων και προσάπτει δομή ομάδας στο σύνολο των n - πλεξιδίων.

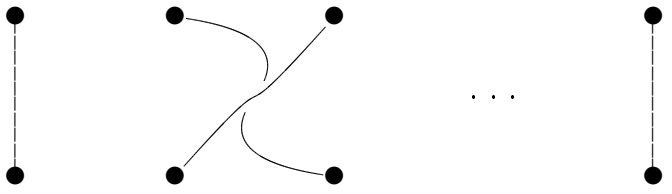
Παράδειγμα 5.3.1 *(Παραδείγματα πλεξιδίων και πράξεων).*

- Ταυτοτικό στοιχείο ως προς την πράξη της σύνθεσης αποτελείται από n πλήθος νήματα παράλληλα και χωρίς διασταυρώσεις, όπως στο σχήμα:



- Αντίστροφο στοιχείο β^{-1} είναι η ανάκλαση του β ως προς το επίπεδο των κάτω σημείων:

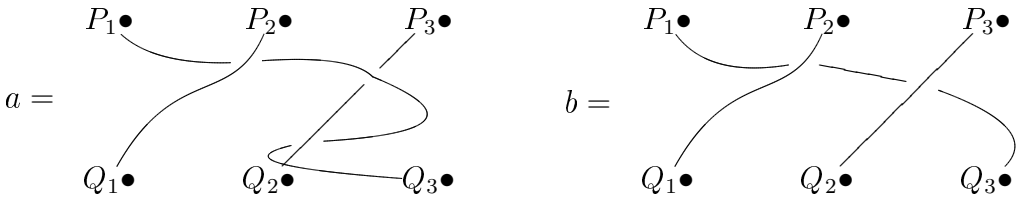
$b =$ 

$b^{-1} =$ 

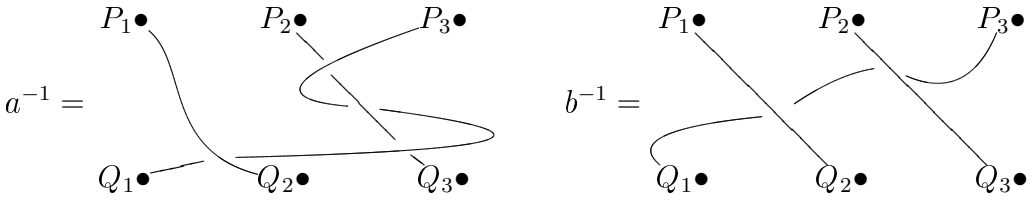
Ορισμός. 5.3.2 .

Συμβολίζουμε με $\mathcal{B}_n$ την ομάδα πλεξιδίων με n το πλήθος νήματα. Η υποομάδα $\mathcal{PB}_n$ της $\mathcal{B}_n$ αποτελούμενη από τα πλεξίδια με τετριμμένη μετάθεση καλείται υποομάδα γνησίων πλεξιδίων(pure) ή ακόμα και χρωματισμένη (coloured) ομάδα πλεξιδίων.

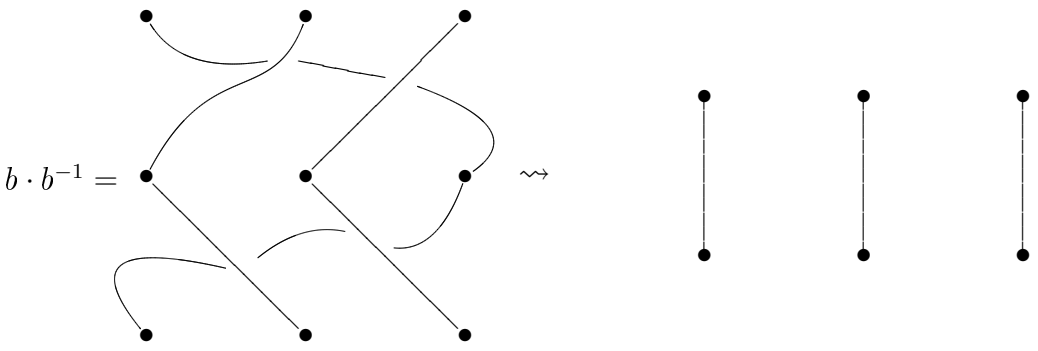
Ορισμένα παραδείγματα πλεξιδίων:



Σχήμα 5.6: *3-πλεξίδια με μετάθεση (132)*

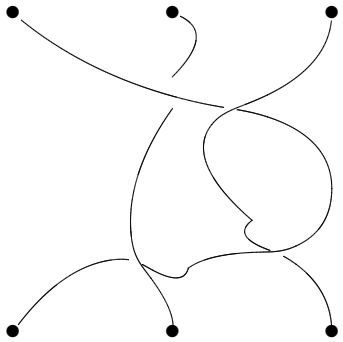


Σχήμα 5.7: *3-πλεξίδια με μετάθεση (312)*



Σχήμα 5.8: *Σύνθεση αντιστρόφων πλεξιδίων*

Παρατηρούμε ότι δεν αρκεί μόνο η μετάθεση ενός πλεξιδίου για να περιγραφεί αυτό πλήρως, αφού τα a, b παραπάνω έχουν τον ίδιο τύπο μετάθεσης, αλλά είναι διαφορετικά. Δηλαδή, αποτελεί ουσιαστικό ποιοτικό γνώρισμα ενός πλεξιδίου, ο τρόπος με τον οποίο τα νήματα του

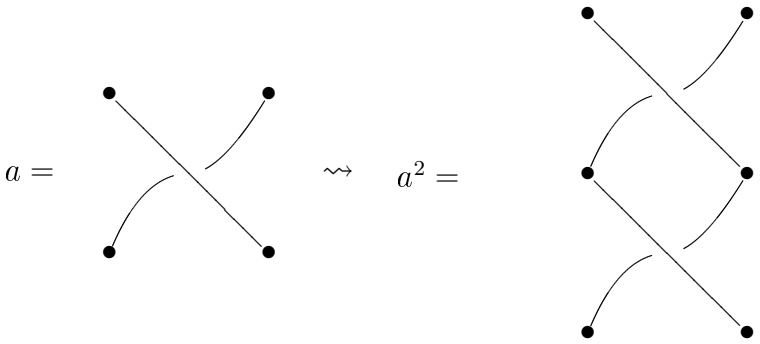


Σχήμα 5.9: *Γνήσιο πλεξίδιο(με τετριμμένη μετάθεση)*

πλεξιδίου περιελίσσονται μεταξύ τους. Αυτό καθίσταται σαφές και με το παρακάτω παράδειγμα.

Παράδειγμα 5.3.3 *(Πλεξίδια άπειρης τάξης).*

Συνθέτοντας πλεξίδια με τον εαυτό τους υπάρχει η δυνατότητα να λάβουμε το ταυτοτικό πλεξίδιο, τότε ονομάζουμε κατά φυσιολογικό τρόπο τάξη του πλεξιδίου το πλήθος των φορών που συνθέσαμε το εν λόγω πλεξίδιο με τον εαυτό του για να λάβουμε το ταυτοτικό πλεξίδιο.



Σχήμα 5.10: *2-πλεξίδιο με μετάθεση (12) άπειρης τάξης*

Κάθε φορά που συνθέτουμε το α με τον εαυτό του, τα νήματα διαπλέκονται κατά μία φορά περισσότερο μεταξύ τους.

Πάντως, έχει αποδειχθεί το εξής θεώρημα σχετικά με τις ομάδες πλεξιδίων:

Θεώρημα 5.3.4 .

Οι ομάδες πλεξιδίων $B_n,\ n = 2, 3, \ldots$ είναι όλες ελεύθερες στρέψης[1].

Απόδειξη

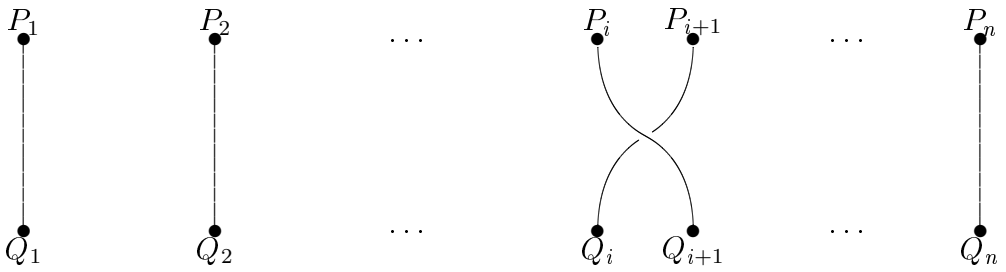
Για μία σύντομη και κομψή απόδειξη βλ. [11]. Για μία παλαιότερη απόδειξη με χρήση λιγότερων εργαλείων: [10] $\square$

[1] Δηλαδή δεν περιέχουν στοιχείο πεπερασμένης τάξης εκτός του ταυτοτικού.

5.3.2 Παράσταση του Artin

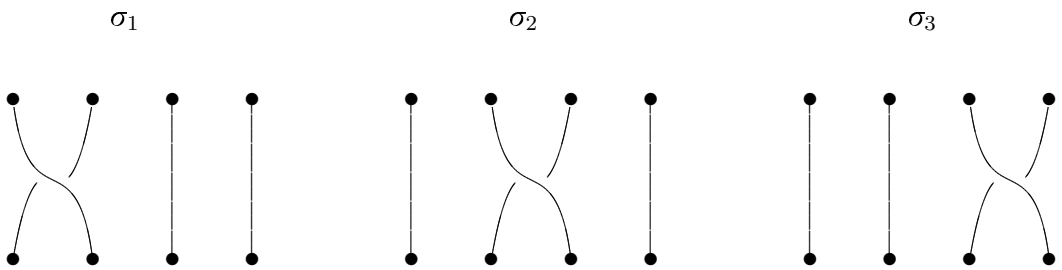
Ορισμός. 5.3.5 *(Στοιχειώδες πλεξίδιο).*

Ονομάζουμε στοιχειώδες πλεξίδιο σ_i το (γεωμετρικό) n - πλεξίδιο που σχηματίζεται αν διαπλέξουμε το i-οστό νήμα πάνω από το $(i+1)$-οστό νήμα όπως φαίνεται στο παρακάτω σχήμα:



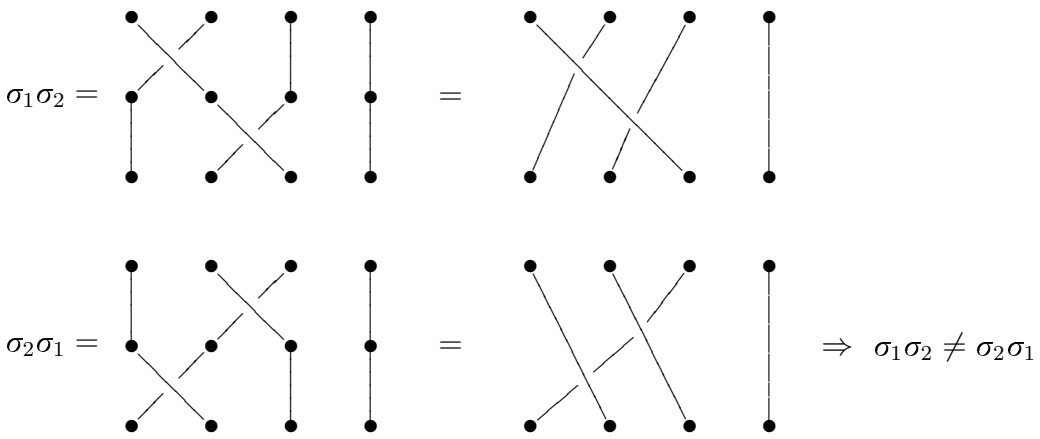
Σχήμα 5.11: *Στοιχειώδες πλεξίδιο*

Στην B_4 θεωρούμε τα στοιχειώδη πλεξίδια:

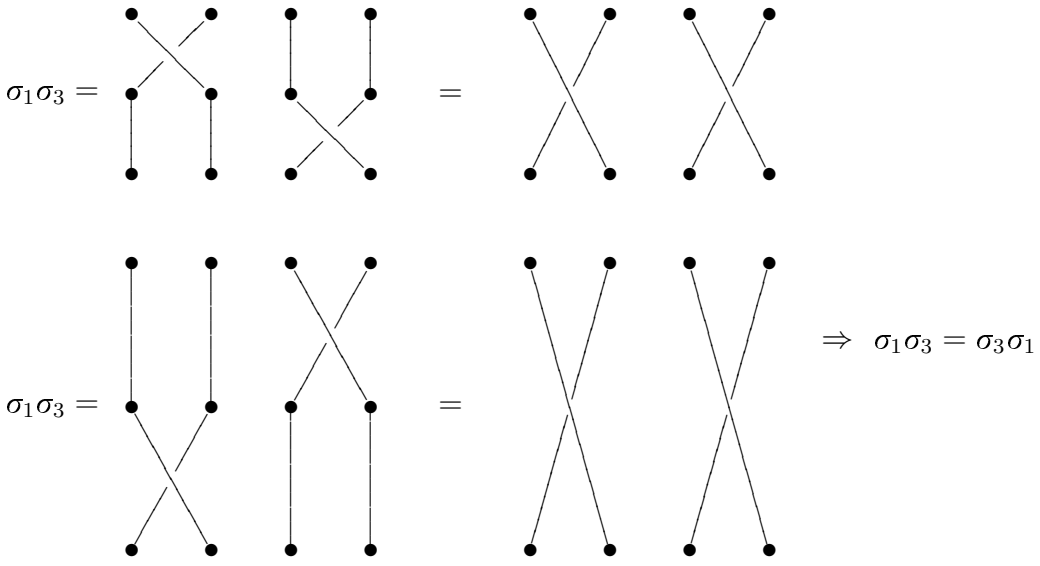


Σχήμα 5.12: *Στοιχειώδη πλεξίδια της* $\mathcal{B}_4$

Γενικά, τα στοιχειώδη πλεξίδια δε μετατίθενται(βλ.σχήμα 5.13). Όμως, ισχύει ότι στοιχειώδη πλεξίδια με δείκτες που διαφέρουν περισσότερο



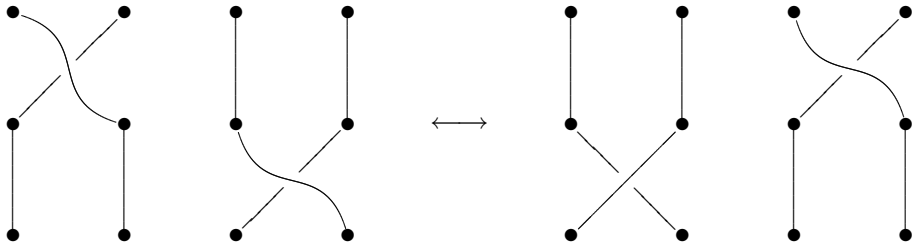
Σχήμα 5.13: *Διαδοχικά στοιχειώδη πλεξίδια δε μετατίθενται*



Σχήμα 5.14: *Πράξεις στοιχειωδών πλεξιδίων*

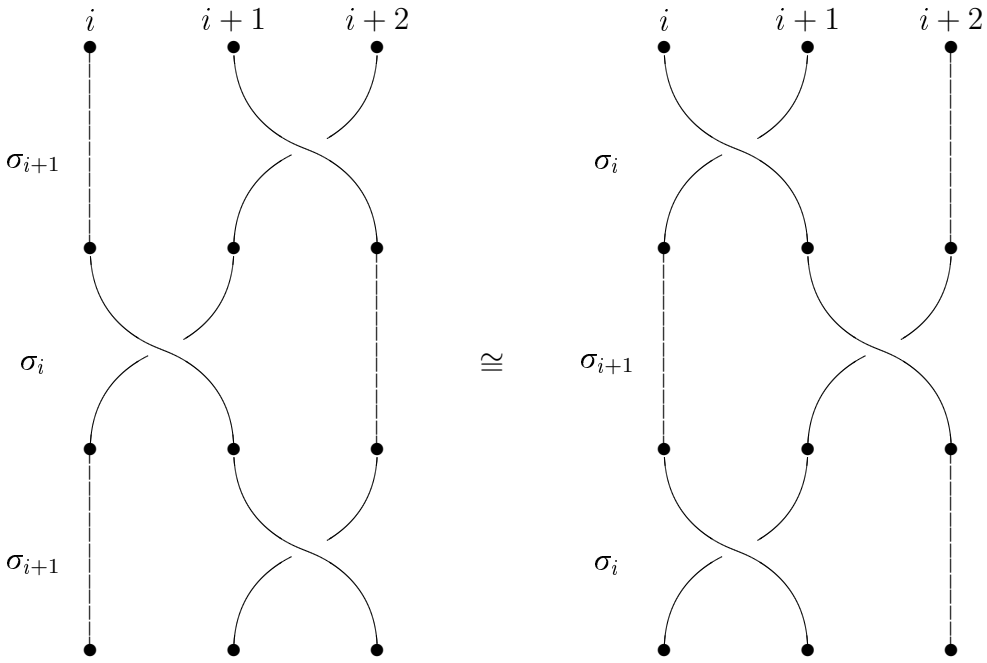
από 1 μετατίθενται μεταξύ τους(βλ. σχήμα 5.15).

Επιπλέον, ισχύει η εξής σχέση:



Σχήμα 5.15: *Τα στοιχειώδη πλεξίδια μετατίθενται αν οι δείκτες τους διαφέρουν περισσότερο από 1.*

$$\boxed{\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}}$$



Σχήμα 5.16: $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$

Παρόλα αυτά οι δύο αυτές σχέσεις που είδαμε δεν αρκούν για να περιγράψουν πλήρως την ομάδα των πλεξιδίων $\mathcal{B}_n$. Αυτό πιστοποιείται και από το επόμενο θεώρημα του Artin:

Θεώρημα 5.3.6 *(Artin[1925]).*

$\mathcal{B}_n \cong \langle \sigma_1, \sigma_2, \ldots, \sigma_{n-1} : \sigma_i\sigma_j = \sigma_j\sigma_i,\ |i-j| > 1,\ \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \rangle$

Θεώρημα 5.3.7 *Θεώρημα αναπαράστασης του Artin* .

Η ομάδα πλεξιδίων $\mathcal{B}_n$ δέχεται μία πίστη αναπαράσταση ως ομάδα των αυτομορφισμών της ελεύθερης ομάδας $F_n =< x_1, \ldots, x_n >$ διάστασης n. Η αναπαράσταση επάγεται από την απεικόνιση ψ της $\mathcal{B}_n$ στην $AutF_n$, η οποία ορίζεται ως εξής:

$$\begin{aligned}
\psi : \ & \mathcal{B}_n \to Aut(F_n) \\
& \sigma_i \to \psi(\sigma_i) : \quad F_n \to F_n \\
& \qquad\qquad\qquad\quad x_i \to x_i x_{i+1} x_i^{-1} \\
& \qquad\qquad\qquad\quad x_{i+1} \to x_i \\
& \qquad\qquad\qquad\quad x_j \to x_j, \ \alpha\nu \ j \neq i, i+1
\end{aligned}$$

Ο περιορισμός της ψ στην υποομάδα των γνησίων πλεξιδίων $\mathcal{PB}_n$ γίνεται:

$$\begin{aligned}
\psi : \ & \mathcal{PB}_n \to Aut(F_n) \\
& A_{rs} \to \psi(A_{rs}) : \quad F_n \to F_n \\
& \qquad\qquad\qquad\quad x_i \to x_i, \ \alpha\nu \ s < i \ \acute{\eta} \ \alpha\nu \ i < r \\
& \qquad\qquad\qquad\quad x_i \to x_r x_i x_r^{-1} \ \alpha\nu \ s = i \\
& \qquad\qquad\qquad\quad x_i \to x_i x_s x_i x_s^{-1} x_i^{-1} \ \alpha\nu \ r = i \\
& \qquad\qquad\qquad\quad x_i \to x_r x_s x_r^{-1} x_s^{-1} x_i x_s x_r x_s^{-1} x_r^{-1}, \ \alpha\nu \ r < i < s
\end{aligned}$$

Απόδειξη

Βλ. [10] $\square$

5.4 Αναπαραστάσεις ομάδων πλεξιδίων

Μία παραγώγιση $\mathcal{D} : \mathbb{Z}G \to \mathbb{Z}G$ είναι μία απεικόνιση με τις ιδιότητες:

$$\alpha)\mathcal{D}(u+v) = \mathcal{D}u + \mathcal{D}v \qquad \text{γραμμική} \qquad (5.1)$$

$$\beta)\mathcal{D}(u \cdot v) = \mathcal{D}uo(v) + u \cdot \mathcal{D}v \qquad u, v \in \mathbb{Z}G \qquad (5.2)$$

Άμεσα προκύπτουν οι εξής ιδιότητες:

1. $\mathcal{D}(\mathrm{gh}) = \mathcal{D}\mathrm{g} + \mathrm{g}\,\mathcal{D}\mathrm{h}\ , \qquad g, h \in G$
2. $\mathcal{D}\mathrm{a} = 0, \qquad \forall a \in \mathbb{Z}$
3. $\mathcal{D}(\sum a_g g) = \sum a_g \mathcal{D}(g)$
4. $\mathcal{D}(u_1 u_2 \dots u_n) = \sum_{i=1}^{n} u_1 u_2 \dots u_{i-1} \mathcal{D}u_i o(u_{i+1}) \dots o(u_n)$
5. $\mathcal{D}(g^{-1}) = -g^{-1}\mathcal{D}g, \qquad \forall g \in G$

Παρατήρηση - Σχόλιο 5.4.1 .

Οι παραγωγίσεις του $\mathbb{Z}$G σχηματίζουν ένα δεξί $\mathbb{Z}G$- πρότυπο, με πράξεις που ορίζονται ως εξής:

$$1.(\mathcal{D}_1 + \mathcal{D}_2)(u) = \mathcal{D}_1 u + \mathcal{D}_2 u$$

$$2.(\mathcal{D}u)v = \mathcal{D}(uv)$$

5.4.1 Παραγωγίσεις σε ελεύθερο ομαδοδακτύλιο

Έστω $F_n =< x_1, x_2, \ldots, x_n >$ ελεύθερη ομάδα[2] διάστασης n. Ένα στοιχείο του ελεύθερου ομαδοδακτυλίου $\mathbb{Z}F_n$ είναι ένα πολυώνυμο

$$f(x) = \sum a_u u, u \in F_n, a_u \in \mathbb{Z} \text{ με πεπερασμένο πλήθος } a_u \neq 0.$$

Αν $\varphi : F_n \to G$ ομομορφισμός ομάδων τότε επάγεται ένας ομομορφισμός δακτυλίων:

$$\varphi : \mathbb{Z}F_n \to \mathbb{Z}G$$
$$f(x) = \sum a_u u \to \sum a_u \varphi(u)$$

Ειδικότερα, ο ομομορφισμός $o : F_n \to 1$ επάγει τον ομομορφισμό:

$$o : \mathbb{Z}F_n \to \mathbb{Z}$$
$$\sum a_u u \to \sum a_u o(u) = \sum a_u$$

Θεώρημα 5.4.2 *(Παράγωγος ως προς x_i).*

Σε κάθε γεννήτορα x_j της F_n αντιστοιχεί μία παραγώγιση:

$$f(x) \to D_j f(x) = f_{x_j}(x) = \frac{\partial f(x)}{\partial x_j} \tag{5.3}$$

η οποία καλείται μερική παράγωγος ως προς x_j, με την ιδιότητα:

$$\frac{\partial x_k}{\partial x_j} = \delta_{j,k} = \begin{cases} 1, \alpha\nu\ k = j, \\ 0, \alpha\nu\ k \neq j \end{cases} \tag{5.4}$$

Επιπλέον, υπάρχει μοναδική παραγώγιση $f(x) \mapsto f'(x)$ που απεικονίζει τα $x_1, x_2, \ldots$ στα δεδομένα στοιχεία $h_1(x), h_2(x), \ldots \in \mathbb{Z}F_n$ και

[2] Η βάση της ομάδας μπορεί να μην είναι ούτε αριθμήσιμη.

δίνεται από τη σχέση:

$$f'(x) = \sum \frac{\partial(f(x))}{\partial x_j} \cdot h_j(x) \tag{5.5}$$

Πρόταση 5.4.3 *(Θεμελιώδης σχέση του ελεύθερου λογισμού).*

Έστω $f(x) \in \mathbb{Z}F_n$. Τότε ισχύει ότι:

$$f(x) = f(1) + \sum_j \frac{\partial(f(x))}{\partial x_j} (x_j - 1) \tag{5.6}$$

$$\sum_j \frac{\partial(f(x))}{\partial x_j} (x_j - 1) = f(x) - f(1) \tag{5.7}$$

5.4.2 Αναπαραστάσεις του Magnus

Έστω S_n η ελεύθερη ημιομάδα με βάση $s_1, s_2, \ldots, s_n$ και R δακτύλιος. Θεωρούμε τον ημιομαδοδακτύλιο $A_0(R, S_n)$ με στοιχεία πολυώνυμα στις μη μετατιθέμενες μεταβλητές s_i με συντελεστές από τον R. Αν F_n η ελεύθερη ομάδα με βάση $x_1, x_2, \ldots, x_n$ ορίζουμε μία απεικόνιση:

$$r : F_n \to M_2[A_0(\mathbb{Z}F_n, S_n)]$$
$$w \mapsto [w] = \begin{pmatrix} w & \sum_{j=1}^{n} \frac{\partial(w)}{\partial x_j}\, s_j \\ 0 & 1 \end{pmatrix}$$

Εφόσον όμως: $\frac{\partial(x_i)}{\partial x_j} = \delta_{ij}$ έπεται ότι:

$$\sum_{j=1}^{n} \frac{\partial(x_i)}{\partial x_j}\, s_j = \sum_{j=1}^{n} \delta_{ij} s_j = s_i \Rightarrow$$
$$x_i \mapsto r(x_i) = [x_i] = \begin{pmatrix} x_i & s_i \\ 0 & 1 \end{pmatrix}$$

Συνεπώς, έπεται άμεσα ότι, αν: $w, v \in F_n$ τότε:

$$[wv] = [w][v]$$

από ιδιότητες της παραγώγισης(βλ. 5.1).

Συνεπώς, η απεικόνιση $w \mapsto [w]$ είναι μία αναπαράσταση της F_n, η οποία καλείται αναπαράσταση Magnus της F_n.

Ένα βασικό μειονέκτημα αυτής της αναπαράστασης είναι ότι περιέχει στον πίνακά της την αρχική λέξη w, γεγονός που την καθιστά όχι ιδιαίτερα χρήσιμη. Αυτό μπορεί να ξεπεραστεί, θεωρώντας έναν ομομορφισμό φ που δρα στην ελεύθερη ομάδα F_n και την εξής απεικόνιση:

$$w \mapsto \varphi([w]) = \begin{pmatrix} \varphi(w) & \sum_{j=1}^{n} \varphi(\frac{\partial(w)}{\partial x_j}\ )s_j \\ 0 & 1 \end{pmatrix} \tag{5.8}$$

Ορισμός. 5.4.4 *(Αναπαράσταση φ του Magnus).*

Η αναπαράσταση που ορίστηκε στην (5.8) καλείται αναπαράσταση φ του Magnus.

Θεώρημα 5.4.5 .

Ο πυρήνας της φ - αναπαράστασης του Magnus είναι η υποομάδα των μεταθετών του $\ker \varphi$.

Παρατήρηση - Σχόλιο 5.4.6 .

Η αναπαράσταση του προηγουμένου πορίσματος μπορεί να θεωρηθεί ότι είναι αντίστοιχη της αναπαράστασης του Magnus της F_n στην $A_0(\mathbb{Z}, S_n)$(βλ.3.2.3) στους πίνακες.

Στόχος μας με την εισαγωγή των αναπαραστάσεων του Magnus δεν ήταν μόνο η μελέτη των ομάδων πηλίκο της F_n, αλλά κυρίως η σύνδεσή τους με τη μελέτη υποομάδων της ομάδας αυτομορφισμών $Aut(F_n)$ της F_n, όπως οι $\mathcal{B}_n$ και $\mathcal{PB}_n$.

Έστω φ ομομορφισμός που δρα στην F_n και A_φ ομάδα αυτομορφισμών της F_n με την ιδιότητα:

$$\varphi(x) = \varphi(\alpha(x)), \forall x \in F_n,\ \alpha \in A_\varphi \tag{5.9}$$

Αν για παράδειγμα επιλέξουμε ως φ τον αβελιανοποιητή, θα μπορούσαμε να επιλέξουμε A_φ να είναι η υποομάδα εκείνων των αυτομορφισμών της F_n που απεικονίζει κάθε στοιχείο σε ένα συζυγές του. Τότε κάθε υποομάδα της $AutF_n$ που επάγει τον ταυτοτικό αυτομορφισμό της ομάδας πηλίκο F_n/F_n' θα ήταν δεκτή.

5.4.3 Η αναπαράσταση Burau (1936), [12]

Από το (5.3.7) έχουμε ότι η $\mathcal{B}_n$ έχει μία πιστή αναπαράσταση ως

ομάδα των δεξιών αυτομορφισμών της ελεύθερης ομάδας F_n διάστασης n. Δηλαδή μπορούμε να βλέπουμε την $\mathcal{B}_n$ ως υποομάδα της $AutF_n$. Συγκεκριμένα, επιλέγουμε γεννήτορες της $\mathcal{B}_n$ με τους αυτομορφισμούς του θεωρήματος (5.3.7).

Ορισμός. 5.4.7 *Αναπαράσταση Burau.*

Έστω $\mathbb{Z} =< a >$ μία άπειρη κυκλική ομάδα και

$$\psi : F_n \rightarrow \mathbb{Z} \tag{5.10}$$

$$x_i \rightarrow a,\ 1 \leq i \leq n \tag{5.11}$$

τότε ικανοποιείται η προϋπόθεση (5.9)

$$\psi(\sigma_i(x_j)) = \psi(x_j)\ \forall\ (i,j),$$

οπότε υπάρχει μία αναπαράσταση Magnus της $\mathcal{B}_n$ με πίνακα που αντιστοιχεί στο γεννήτορα σ_i της $\mathcal{B}_n$ τον:

$$||\sigma_i||^{\psi} = \left(\begin{array}{c|ccc} I_{i-1} & 0 & 0 & 0 \\ \hline 0 & 1-a & a & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & I_{n-i-1} \end{array}\right) \tag{5.12}$$

όπου I_k αντιστοιχεί στον $k \times k$ μοναδιαίο πίνακα.

Παρατήρηση - Σχόλιο 5.4.8 .

Η αναπαράσταση αυτή εισήχθηκε από τον Burau το 1936 στο [12]. Για μεγάλο διάστημα γνωρίζαμε ότι η αναπαράσταση Burau είναι πιστή για $n \leq 3$ και ήταν υποψήφια για μία πιστή γραμμική αναπαράσταση της $\mathcal{B}_n$, $\forall\ n$. Όμως το 1991 ο Moody [25] απέδειξε ότι για $n > 9$ η αναπαράσταση Burau δεν είναι πιστή. Αργότερα οι Long και Paton [20] απέδειξαν ότι δεν είναι πιστή[3] για $n \geq 6$ και ο Bigelow [7] για $n \geq 5$. Πάντως ο Bigelow απέδειξε το 2001 [8] τη γραμμικότητα της $\mathcal{B}_n$.

[3] Το ζήτημα για n=4 παρέμενε ανοικτό έως τουλάχιστον το 2005

5.5 Πλεξίδες και κρυπτογραφία δημοσίου κλειδιού

Οι ομάδες πλεξιδίων διαθέτουν κάποιες συγκεκριμένες δομικές ιδιότητες, οι οποίες χρησιμοποιήθηκαν για τη δημιουργία μίας νέας μεθόδου κρυπτογράφησης δεδομένων (βλ και κεφάλαιο 6). Εν συντομία το πρόβλημά μας είναι να κρυπτογραφήσουμε ένα μυστικό μήνυμα σε έναν κώδικα και με τέτοιο τρόπο, ώστε να μπορεί αφενός να μεταφερθεί μέσω ενός συστήματος επικοινωνιών ευρείας πρόσβασης, όπως το διαδίκτυο, αφετέρου να αποκωδικοποιείται από τον παραλήπτη με χρήση κάποιου είδους πληροφορίας (μυστικό κλειδί) που είναι γνωστό μόνο σε αποστολέα και παραλήπτη. Το ζήτημα, λοιπόν, είναι να βρεθεί ένα ιδιωτικό κλειδί, γνωστό μόνο σε αποστολέα και παραλήπτη, που τότε θα είναι σε θέση να ανταλλάξουν πληροφορίες μέσω ενός μη ασφαλούς καναλιού επικοινωνίας. Τα τελευταία χρόνια έχει γίνει πολύ δουλειά σχετική, στηριγμένη στην υπόθεση ότι το πρόβλημα της λέξης αυξάνεται πολυωνυμικά καθώς ο δείκτης των πλεξιδίων B_n αυξάνεται, ενώ δε συμβαίνει το ίδιο για το πρόβλημα της συζυγίας. Έτσι, ενώ και τα δύο προβλήματα (λέξης και συζυγίας) είναι πλήρως λυμένα για ομάδες πλεξιδίων, εντούτοις υπάρχει η υπόθεση της διαφορετικότητάς τους ως προς την πολυπλοκότητα.

Έτσι, μία γενίκευση του προβλήματος του διακριτού λογαρίθμου σε ομάδες γενικά αποτελεί το πρόβλημα της συζυγίας, δηλαδή, δοθέντων δύο στοιχείων α, β μίας ομάδας G να βρεθεί ένα στοιχείο x, ώστε να

ισχύει: $xax^{-1} = b$. Η υπολογιστική δυσκολία του συγκεκριμένου προβλήματος για τις ομάδες πλεξιδίων ήταν αυτή που ώθησε τη χρήση τους σε κρυπτοσυστήματα ομάδων. Εντούτοις, τελευταία φαίνεται ότι η χρήση του προβλήματος αυτού σε ομάδες πλεξιδίων μπορεί να μην παρέχει την απαιτούμενη ασφάλεια για μία ευρεία χρήση (βλ.[29]). Σήμερα η έρευνα έχει στραφεί προς δύο κατευθύνσεις. Αφενός στην αναζήτηση ενός διαφορετικού προβλήματος στη συνδυαστική θεωρία ομάδων ικανής πολυπλοκότητας, ώστε να μπορεί να αποτελέσει τη βάση ενός νέου κρυπτοσυστήματος. Αφετέρου, στη χρήση ομάδων, πλην των πλεξιδίων, οι οποίες να μπορούν να αποτελούν ασφαλή βάση για χρήση, μέσω του προβλήματος συζυγίας, στην καθημερινή πραγματικότητα.

Κεφάλαιο 6

Εφαρμογές στην Κρυπτογραφία

6.1 Εισαγωγή

Η μέθοδος κρυπτογράφησης με χρήση δημοσίου κλειδιού είναι ευρέως διαδεδομένη και χρησιμοποιείται τις τελευταίες δεκαετίες. Η βασική απαίτηση αφορά την ασφαλή μεταφορά μίας πληροφορίας μέσω κάποιου δικτύου επικοινωνιών ελεύθερης πρόσβασης (διαδίκτυο, τηλεφωνικό δίκτυο, κλπ).

Η κύρια ιδέα έγκειται στην κρυπτογράφηση των προς μεταφορά δεδομένων με χρήση ενός κλειδιού το οποίο είναι γνωστό σε αποστολέα, που κρυπτογραφεί την πληροφορία και σε παραλήπτη, ο οποίος αποκρυπτογραφεί την πληροφορία. Όλες οι λύσεις του προβλήματος αυτού υποκρύπτουν την ιδέα της χρήσης προβλημάτων τα οποία επιδέχονται ακριβείς λύσεις - γνωστές σε αποστολέα και παραλήπτη - αλλά κάποιος που απλώς παρακολουθεί, ακόμα κι αν έχει όλα τα δεδομένα, δεν δύναται να βρει αυτή τη λύση. Η μέχρι πριν λίγα χρόνια χρήση των διαφόρων σχετικών μεθόδων, όπως ο αλγόριθμος RSA, Diffie -

Hellman [13], μέθοδοι ελλειπτικών καμπυλών εξαρτώνται από τη δομή αβελιανών ομάδων. Από την άλλη πλευρά η διαρκής ενδυνάμωση της ισχύος των σύγχρονων υπολογιστών έχει καταστήσει τέτοιες μεθόδους θεωρητικά τουλάχιστον ανασφαλείς. Προς τούτο, λοιπόν, έχουν γίνει προσπάθειες για την ανάπτυξη μεθόδων διαφορετικής φιλοσοφίας που θα είναι θεωρητικά ασφαλέστερες.

Η ιδέα που θα εξετάσουμε στο παρόν στηρίζεται σε μη μεταθετικές δομές ως βάση για την κρυπτογράφηση και γενικώς καλείται μη μεταθετική αλγεβρική κρυπτογραφία. Σε αυτήν την κατεύθυνση έχει γίνει χρήση τελευταία και των ιδιοτήτων των ομάδων πλεξιδίων του Artin με χρήση του προβλήματος της συζυγίας -όπως περιγράφηκε προηγουμένως- που ώθησε στην ανάπτυξη της κρυπτογραφίας με ομάδες πλεξιδίων(βλ. [1] και [19]). Εντούτοις αυτή τελευταία τείνει να αποδειχθεί ανεπαρκής, αφού έχουν βρεθεί διάφορες σημαντικές αδυναμίες. Πάντως οι βασικές ομαδοθεωρητικές ιδέες που χρησιμοποιούνται στην κρυπτογραφία μέσω ομάδων πλεξιδίων είναι σημαντικές και αυτές θα χρησιμοποιούνται και στη μέθοδο του [5] που θα δούμε. Διευρύνεται το σύνολο των μη μεταθετικών αλγεβρικών αντικειμένων που χρησιμοποιούνται στην κρυπτογραφία με τη διερεύνηση διαφορετικών μεθόδων χρήσης του δακτυλίου των τυπικών δυναμοσειρών $R << x_1, \ldots, x_n >>$ στις μη μετατιθέμενες μεταβλητές $x_1, \ldots, x_n$ ως βάσης για την ανάπτυξη κρυπτοσυστημάτων. Ειδικότερα γίνεται χρήση του αποτελέσματος (3.2.3) όπου μία πεπερασμένα παραγόμενη ελεύθερη

ομάδα F έχει μία πιστή αναπαράσταση σε ένα πηλίκο του δακτυλίου των τυπικών δυναμοσειρών στις μη μετατιθέμενες μεταβλητές.

6.2 Τυπικές δυναμοσειρές και η αναπαράσταση του Magnus

Θεωρούμε το δακτύλιο των τυπικών δυναμοσειρών επί του δακτυλίου R :

$$A(R,n) = R\langle\langle x_1, \ldots, x_n\rangle\rangle.$$

Γενικά, αρκεί να χρησιμοποιήσουμε ως δακτύλιο $R = \mathbb{Q}$. Οπότε θεωρούμε: $H = \mathbb{Q}\langle\langle x_1, \ldots, x_n\rangle\rangle = A(\mathbb{Q}, n)$. Πρώτο χρήσιμο εργαλείο αποτελεί μία πιστή αναπαράσταση μίας πεπερασμένα παραγόμενης ελεύθερης ομάδας σ' ένα πηλίκο της H, η οποία αναπτύχθηκε από τον Magnus. Για $n \geq 2$ υπάρχουν ελεύθερες υποομάδες κάθε διάστασης σε αυτό το πηλίκο της H. Ιδιαιτέρως κάποιες επιπρόσθετες σχέσεις μπορούν να δώσουν αναπαραστάσεις ελευθέρων μηδενοδύναμων ομάδων.

6.2.1 Η αναπαράσταση του Magnus

Εδώ γενικεύεται η ιδέα που παρουσιάστηκε στο (3.2.3). Έστω $d > 1, d \in \mathbb{Z}$ και ισχύουν επιπλέον οι σχέσεις:

$$x_1^d = x_2^d = \ldots = x_n^d = 0 \text{ στην } H = \mathbb{Q}\langle\langle x_1, \ldots, x_n \rangle\rangle.$$

Ονομάζουμε $\overline{H}$ το πηλίκο που προκύπτει. Τα στοιχεία του πηλίκου $\overline{H}$ είναι πολυώνυμα βαθμού $< d$ στις μη μετατιθέμενες μεταβλητές $x_1, x_2, \ldots, x_n$. Η πιστή αναπαράσταση μίας ελεύθερης ομάδας δίνεται από τα μονώνυμα:

$$\alpha_1 = 1 + x_1, \alpha_2 = 1 + x_2, \ldots, \alpha_n = 1 + x_n$$

Στην H έχουμε ότι:

$$\frac{1}{1+x_i} = 1 - x_i + x_i^2 - x_i^3 + \ldots \qquad \text{Βλέπε: (3.2.2)}$$

Οπότε κάθε α_i είναι αντιστρέψιμο στοιχείο στην H και κατά συνέπεια στην $\overline{H}$ όπου όμως θα είναι βαθμού $< d$, δηλαδή θα έχουμε ότι:

$$\frac{1}{1+x_i} = 1 - x_i + x_i^2 - x_i^3 + \ldots + (-1)^{d-1} x_i^{d-1}$$

Συνεπώς κάθε $\alpha_i = 1 + x_i \in U(\overline{H})$ την ομάδα των μονάδων της $\overline{H}$ [1].

Παρατήρηση - Σχόλιο 6.2.1 .

Αν ο ακέραιος d που αποτελεί την ορίζουσα δύναμη διατηρηθεί μυστικός, τότε τα αντίστροφα στοιχεία είναι άγνωστα.

[1] Ομάδα μονάδων της H ονομάζουμε τα στοιχεία που αντιστρέφονται στην H.

Θεώρημα 6.2.2 *(Magnus).*

Τα στοιχεία:

$$\alpha_1 = 1 + x_1, \ldots, \alpha_n = 1 + x_n$$

παράγουν ελεύθερα μία υποομάδα της $U(\overline{H}\ )$. Συνεπώς η απεικόνιση:

$$y_1 \longrightarrow \alpha_1$$

$$y_2 \longrightarrow \alpha_2$$

$$\vdots$$

$$y_n \longrightarrow \alpha_n$$

ορίζει μία πιστή αναπαράσταση της ελεύθερης ομάδας με γεννήτορες $y_1, \ldots, y_n$ στην $\overline{H}$.

Η απόδειξη της πιστότητας της αναπαράστασης[2] του Magnus μας οδηγεί σε διάφορους αλγορίθμους για χρήση της εικόνας στο δακτύλιο δυναμοσειρών. Θα γίνει χρήση αυτών στο κρυπτοσύστημα που αναπτύσσεται. Στο εξής συμβολίζουμε με:

$$\boxed{\overline{F} =< \alpha_i, i \in \ I >\leq \overline{H}}$$

Ο πρώτος αλγόριθμος είναι μία μέθοδος , δοθέντος ενός πολυωνύμου στην $\overline{H}$ που γράφεται σε πολυωνυμική μορφή και είναι στην $\overline{F}$, για να γραφεί στη μοναδική του διάσπαση σε ελεύθερες ομάδες. Δηλαδή δοθέντος ενός πολυωνύμου $f(x_1, x_2, \ldots, x_n)$ στις μη μετατιθέμενες μεταβλητές $x_1, x_2, \ldots, x_n$ που είναι στην $\overline{F}$ το ξαναγράφουμε ως

[2] Μία αναπαράσταση φ καλείται πιστή, αν $\ker \varphi = 1$

$f = W(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Γενικά δεν υπάρχει αλγόριθμος παραγοντοποίησης στην $\overline{H}$. Για κάθε μονώνυμο $x_{i_1}x_{i_2}\ldots x_{i_k} \in \overline{H}$ ονομάζουμε το k μήκος του μονωνύμου σε αναλογία με το μήκος μίας λέξης σε μία ελεύθερη ομάδα.

Θεώρημα 6.2.3 *(Αλγόριθμος εύρεσης ελεύθερης διάσπασης σε ελεύθερες ομάδες στοιχείων της $\overline{F}$).*

Έστω $f = f(x_1, x_2, \ldots, x_n) \in \overline{H} \Rightarrow \ f \in \overline{F}$. Υπάρχει ένας αλγόριθμος με τον οποίο ξαναγράφουμε την f με τη βοήθεια των ελευθέρων γεννητόρων $\alpha_1, \ldots, \alpha_n$, δηλαδή: $f = W(\alpha_1, \ldots, \alpha_n)$.

Βήμα 1ο : Επισημαίνουμε στο πολυώνυμο f το μονώνυμο μεγίστου μήκους που εμφανίζεται: $nx_{i_1}\ldots x_{i_k}$ μεγίστου μήκους με $n \in \mathbb{Z}-\{0\}$ όπου κάθε μεταβλητή του f εμφανίζεται στο μονώνυμο αυτό με δύναμη 1. Το κ δίνει το μήκος της λέξης που αντιστοιχεί στην ελεύθερη ομάδα. Επιπλέον, η λέξη αυτή πρέπει να έχει τη μορφή: $\alpha_{i_1}^{n_1}\ldots\alpha_{i_k}^{n_k}$ όπου n_i διαιρέτης του n.

Βήμα 2ο : Για κάθε διαιρέτη του $n_i \in \ \mathbb{Z}$ του n υπολογίζουμε το πολυώνυμο:

$$(1 + x_i)^{-n_1} f.$$

Σε ένα ακριβώς τέτοιο γινόμενο το μέγιστο μήκος θα είναι κ-1 και θα υπάρχει μοναδικό μονώνυμο μήκους κ-1, το οποίο θα περιέχει κάθε

μεταβλητή του f εκτός ίσως του x_{i_1} με δύναμη 1. Τότε θα έχουμε:

$$\boxed{f = (1 + x_{i_1})^{n_1} f_1,\ f_1 \in \overline{F}}$$

Βήμα 3ο : Συνεχίζουμε τη διαδικασία με αυτόν τον τρόπο μέχρι να φτάσουμε στη μονάδα, οπότε θα έχουμε λάβει τη διάσπαση στην ελεύθερη ομάδα να είναι της μορφής:

$$\boxed{f = (1 + x_{i_1})^{n_1} \dots 1 + x_{i_k})^{n_k} = \alpha_{i_1}^{n_1} \dots a_{i_k}^{n_k}}$$

Με μία αλλαγή αυτού του αλγορίθμου μπορούμε να προσδιορίζουμε πότε ένα στοιχείο της $\overline{H} \in \overline{F}$. Η απόδειξη του είναι παρόμοια:

Θεώρημα 6.2.4 *(Αλγόριθμος υπολογισμού αν το $f \in \overline{H}$ είναι $f \in \overline{F}$).*

Έστω $f = f(x_1, \dots, x_n) \in \overline{H}$, τότε υπάρχει αλγόριθμος που αποφασίζει αν $f \in \overline{F}$ και δίνει γραφή του f με τη βοήθεια των: $\alpha_i = 1 + x_i, i = 1, ..., n$.

Βήμα 1ο : Αν ο σταθερός όρος του $f \neq 1$, τότε: $f \notin \overline{F}$. Ακόμα, αν το f έχει μη ακέραιους συντελεστές, τότε $f \notin \overline{F}$.

Βήμα 2ο : Έστω ότι δεν έχουμε απόφαση από το προηγούμενο βήμα. Αν το f δεν περιέχει μοναδικό μονώνυμο $nx_{i_1}, ..., x_{i_k}$ μεγίστου μήκους για $n \in \mathbb{Z} - 0$ και περιέχει όλες τις μεταβλητές του f σε δύναμη εκθέτη 1, τότε έχουμε ότι: $f \notin \overline{F}$.

Βήμα 3ο : Έστω ότι δεν έχουμε απόφαση από το προηγούμενο βήμα. Αν το f περιέχει μονώνυμο του βήματος 2: $nx_{i_1}, ..., x_{i_k}$ μεγίστου μήκους για $n \in \mathbb{Z} - 0$, τότε αν $f \in \overline{F}$ ο k δίνει το μήκος της

αντίστοιχης λέξης στην ελεύθερη ομάδα, η οποία θα έχει τη μορφή:

$$\alpha_{i_1}^{n_1} \dots a_{i_k}^{n_k}, \text{ όπου: } n_i | n$$

Βήμα 4ο : Για κάθε διαιρέτη n_i του n σχηματίζουμε διαδοχικά το πολυώνυμο $(1 + x_{i_1})^{-n_1}$. Αν σε ένα τέτοιο γινόμενο το μέγιστο μήκος είναι $k - 1$ και δεν υπάρχει νέο μονώνυμο με τα προηγούμενα χαρακτηριστικά, τότε: $f \notin \overline{F}$.

Βήμα 5ο : Αν προκύψει η μονάδα, τότε $f \in \overline{F}$ και η διαδικασία δίνει τη διάσταση σε ελεύθερο γινόμενο του f.

Για κάποιες εφαρμογές στην κρυπτογραφία θα χρησιμοποιήσουμε ολόκληρη την ομάδα των αντιστρεψίμων στοιχείων $U(\overline{H}\ )$ της

$$\overline{H}\ = \langle\langle x_1, x_2, ..., x_n \rangle\rangle / < x_i^d = 0,\ i = 1, 2, ..., n >,$$

η οποία επί του $\mathbb{Q}$ είναι εκείνα τα πολυώνυμα με μη μηδενικό σταθερό όρο.

Θεώρημα 6.2.5 .

Η ομάδα των μονάδων $U(\overline{H}\ )$ επί του $\mathbb{Q}$ αποτελείται από εκείνα ακριβώς τα πολυώνυμα με μη μηδενικό σταθερό όρο.

Απόδειξη

Έστω ότι η ορίζουσα δύναμη $d > 1$ και $p(x) \in \overline{H}$ με μη μηδενικό σταθερό όρο. Τότε το $p(x)$ είναι σχετικά πρώτο με τα πολυώνυμα x_i^d, οπότε είναι αντιστρέψιμο. $\square$

Επισημαίνουμε ότι για τον πολλαπλασιασμό στην $\overline{H}$ δεν υπάρχει αλγόριθμος παραγοντοποίησης. Εντούτοις, αν $f \in \overline{H}$ είναι γνωστό και $g = fe,\ e \in \overline{F}$ είναι επίσης γνωστό, τότε μπορούμε να προσδιορίσουμε το e, διότι, αν τα e, fe είναι γνωστά τότε στο fe υπάρχει μοναδικό μονώνυμο που επεκτείνει τα μονώνυμα του f όπως και στο θεώρημα (6.2.3). Αναγνωρίζοντας αυτό το μονώνυμο μπορούμε να βρούμε την ελεύθερη διάσπαση του e.

6.3 Κρυπτοσυστήματα με χρήση δακτυλίων τυπικών δυναμοσειρών.

6.3.1 Κρυπτοσυστήματα σε μη αβελιανές ομάδες

Έστω G μία πεπερασμένα παριστώμενη ομάδα, για παράδειγμα ως ομάδα πινάκων. Η βασική επιθυμητή ιδιότητα της G είναι να διαθέτει δύο μεγάλες υποομάδες A_1, A_2 των οποίων τα στοιχεία μετατίθενται μεταξύ τους. Εναλλακτικά θα μπορούσε να χρησιμοποιηθεί μία μεγάλη αβελιανή υποομάδα της G. Όταν γράφουμε μεγάλη εννοούμε ότι είναι δύσκολο να προσδιοριστεί αν ένα τυχαίο στοιχείο της G ανήκει στην A_1 ή στην A_2 (ή στην A) και επιπλέον αυτές οι υποομάδες είναι αρκετά μεγάλες, ώστε να μπορούν να επιλεχθούν στοιχεία με τυχαίο τρόπο από αυτές.

Αν υποθέσουμε τώρα ότι μία πηγή B θέλει να επικοινωνήσει με ένα δέκτη A, μέσω ενός μη ασφαλούς καναλιού (πχ διαδίκτυο). Αρχικά, γίνεται κωδικοποίηση του μηνύματος μέσα στην πεπερασμένα γεννόμενη ομάδα G, με τις ιδιότητες που περιγράφηκαν παραπάνω. Οι δύο υποομάδες A_1, A_2, των οποίων τα στοιχεία μετατίθενται κρατούνται μυστικές από πηγή και δέκτη. Μάλιστα υποθέτουμε ότι η πηγή B γνωρίζει μόνο την υποομάδα A_1 και ο δέκτης A γνωρίζει μόνο την υπομάδα A_2.

Αν η πηγή B θέλει να στείλει το μήνυμα $M \in G$(κωδικοποιημένο στην ομάδα G), στο δέκτη A, επιλέγει τυχαία δύο στοιχεία $B_1, B_2 \in A_1$ και στέλνει στο δέκτη το μήνυμα: $\beta_1 M \beta_2$. Ο δέκτης A επιλέγει δύο

τυχαία στοιχεία $\gamma_1, \gamma_2 \in A_2$ και επιστρέφει το μήνυμα $\gamma_1\beta_1 M\beta_2\gamma_2$ στον B. Αυτά τα μηνύματα εμφανίζονται στην αναπαράσταση της G, για παράδειγμα ως πίνακες ή ανηγμένες λέξεις, οπότε δεν εμφανίζονται ως μία απλή διαδοχή γραμμάτων. Τώρα, εφόσον τα στοιχεία των A_1, A_2 μετατίθενται ισχύει ότι:

$$\gamma_1\beta_1 M\beta_2\gamma_2 = \beta_1\gamma_1 M\gamma_2\beta_2$$

Όμως η πηγή B γνωρίζει τα στοιχεία β_1, β_2 καθώς επίσης και τα αντίστροφά τους, οπότε πολλαπλασιάζοντας με τα αντίστροφα δημιουργεί το μήνυμα $\gamma_1 M\gamma_2$ το οποίο αποστέλλει εκ νέου στο δέκτη A. Αυτός με τη σειρά του γνωρίζει τα στοιχεία γ_1, γ_2, οπότε, πολλαπλασιάζοντας με τα αντίστροφά τους λαμβάνει αυτούσιο το μήνυμα M. Προφανώς, για κάθε μήνυμα πηγή και δέκτης μπορούν να χρησιμοποιούν διαφορετικά στοιχεία των ομάδων A_1, A_2. Σχηματικά έχουμε το εξής:

$$M \overset{B:\ \beta_1,\beta_2\in A_1}{- - \text{--} \rightarrow} \alpha_1 M\alpha_2 \overset{A:\ \gamma_1,\gamma_2\in A_2}{- - \text{--} \rightarrow}$$

$$\gamma_1\beta_1 M\beta_2\gamma_2 = \beta_1\gamma_1 M\gamma_2\beta_2$$

$$\overset{B:\ \gamma_1^{-1},\beta_2^{-1}\in A_1}{- - \text{--} \rightarrow} \gamma_1 M\gamma_2 \overset{A:\ \gamma_1^{-1}\gamma_2^{-1}}{=} M$$

Αυτή η μέθοδος αποτελεί μία γενίκευση της μεθόδου των Anshel,Anshel, Goldfeld και Ko-Lee (βλ.[1]), οι οποίοι χρησιμοποίησαν ομάδες πλεξιδίων ως βάση. Στη συνέχεια βλέπουμε μία εφαρμογή της μεθόδου με χρήση του δακτυλίου των δυναμοσειρών σε μη μετατιθέμενες μεταβλητές.

6.3.2 Κρυπτοσυστήματα με το δακτύλιο $A(\mathbb{Q}, n)$.

Υποθέτουμε ότι έχουμε ένα δακτύλιο R με μεγάλη ομάδα αντιστρεψίμων στοιχείων $U(R)$. Ομοίως με πριν με τον όρο "μεγάλη" εννοούμε ότι περιέχει μία μη αβελιανή ελεύθερη υποομάδα, ώστε να είναι δυνατή η τυχαία επιλογή στοιχείων από την $U(R)$. Επιπλέον υποθέτουμε ότι δεν υφίσταται αλγόριθμος παραγοντοποίησης στον R.

Αν η πηγή B θέλει να στείλει ένα μήνυμα r στο δέκτη A γίνεται κωδικοποίηση μέσα στο δακτύλιο R, οπότε τα στοιχεία του δακτυλίου αναπαριστούν μηνύματα, δηλαδή $r \in R$. Ο B επιλέγει ένα στοιχείο $e \in U(R)$ και αποστέλλει το μήνυμα: re. Ο δέκτης A επιλέγει ένα άλλο στοιχείο $f \in U(R)$ και επαναστέλλει το μήνυμα fre στην πηγή B. Ο B γνωρίζει το στοχείο e^{-1}, οπότε το εφαρμόζει και στέλνει στον A το μήνυμα $free^{-1} = fr$. Τελικά ο A εφαρμόζοντας και αυτός το γνωστό του στοιχείο f^{-1} έχει $f^{-1}fr = r$ αποκωδικοποιημένο το μήνυμα r.

Σχηματικά η αναπαράσταση της διαδικασίας είναι:

$$r \overset{B:\ e\in U(R)}{- - -\!-\!-\rightarrow} re \overset{A:\ f\in U(R)}{- - -\!-\!-\rightarrow} fre \overset{B:\ e^{-1}\in U(R)}{- - -\!-\!-\rightarrow} free^{-1} = fr \overset{A:\ f^{-1}}{=} f^{-1}fr =$$

Αυτή η μέθοδος μπορεί να εφαρμοστεί, χρησιμοποιώντας ως δακτύλιο τον: $R = \overline{H}$. Η ορίζουσα δύναμη $d > 0$ μένει μυστική, ανάμεσα σε αποστολέα και παραλήπτη. Η κρυπτογράφηση γίνεται σε ένα πολυώνυμο με μη μετατιθέμενες μεταβλητές και μπορεί να υλοποιηθεί με διάφορους τρόπους. Για παράδειγμα αν οι συντελεστές του πολυωνύ-

μου είναι ρητοί, τότε μπορούμε να κωδικοποιήσουμε το αλφάβητο με ρητούς αριθμούς, οπότε το μήνυμα να διαβαζεται μέσω των συντελεστών αυτών.

Συγκεκριμένα, αν θεωρήσουμε ότι ο αποστολέας θέλει να στείλει το μήνυμα $T \in \mathbb{Q}[[x_1, ..., x_n]]$, όπου $x_i^d = 0, \forall i$. Στη συνέχεια θεωρούμε ένα πολυώνυμο $S \in \mathbb{Q}[[x_1, ..., x_n]]$ με μονώνυμα βαθμού μεγαλύτερου του d μόνο. Αν $R = T + S$ και ο Β επιλέξει ένα στοιχείο $W \in U(\overline{H})$, τότε στέλνει το μήνυμα RW, γνωρίζοντας το αντίστροφο στοιχειο W^{-1}. Κατά τη σειρά της διαδικασίας που περιγράψαμε προηγουμένως ο Α επιλέγει ένα άλλο στοιχείο $V \in U(\overline{H})$ και στέλνει πίσω το μήνυμα VRW. Ο Β πολλαπλασιάζει με W^{-1} και στέλνει το VR, οπότε ο Α μπορεί να αποκωδικοποιήσει και να λάβει το R. Εφόσον, όμως και ο Α γνωρίζει την ορίζουσα δύναμη $d > 0$ μπορεί να απαλείψει από το $R = T + S$ όλα τα μονώνυμα με βαθμό μεγαλύτερο και να λάβει πλήρως το αρχικό μήνυμα T.

Ένας υποκλοπέας θα έπρεπε να γνωρίζει τόσο τον παράγοντα RW όσο και την ορίζουσα δύναμη d.

Παράδειγμα 6.3.1 *(Παράδειγμα υλοποίησης).*

Επιλέγουμε ως δακτύλιο υλοποίησης $R = \overline{H} = H/\langle x_i^2 = 0, i = 1, 2, \ldots\rangle$, όπου: $H = \mathbb{Q}\langle\langle x_1, x_2, \ldots\rangle\rangle$. Θεωρούμε ότι τα γράμματα του ελληνικού αλφαβήτου α, β αντιστοιχούνται σε ρητούς ως εξής:

$$\alpha \rightarrow \frac{1}{2}$$
$$\beta \rightarrow \frac{1}{3}$$

Επιπλέον, θεωρούμε ότι θέλουμε να αποστείλουμε το μήνυμα: "αβ". Τότε μπορούμε να ορίσουμε ως διάταξη των γραμμάτων αυτή που καθορίζεται από την διάταξη των μεταβλητών του δακτυλίου των δυναμοσειρών, δηλαδή θεωρούμε ότι το μήνυμα "αβ" υλοποιείται από:

$$T = \frac{1}{2}\, x_1 + \frac{1}{3} x_2$$

όπου η λεξικογραφική διάταξη για παράδειγμα των μεταβλητών του δακτυλίου των δυναμοσειρών μας δίνει και τη διάταξη των γραμμάτων. Θεωρούμε ακόμα έναν παράγοντα "θορύβου" $S = x_1^3$, ο οποίος βεβαίως πρέπει να περιέχει μονώνυμα με δυνάμεις μεγαλύτερες της ορίζουσας δύναμης $d = 2$, όπως έχει επιλεχθεί στο συγκεκριμένο παράδειγμα. Τότε το αρχικό μήνυμα που θα αποσταλεί θα είναι:

$$R = T + S = \frac{1}{2}\, x_1 + \frac{1}{3} x_2 + x_1^3$$

Ο αρχικός αποστολέας του μηνύματος επιλέγει ένα αντιστρέψιμο στοιχείο του δακτυλίου για παράδειγμα το:

$$W = 1 + x_1, W^{-1} = 1 - x_1$$

και αποστέλει το μήνυμα:

$$RW = (\frac{1}{2}x_1 + \frac{1}{3}x_2 + x_1^3)(1 + x_1) = \frac{1}{2}x_1 + \frac{1}{3}x_2 + x_1^3 + \frac{1}{2}x_1^2 + \frac{1}{3}x_2x_1 + x_1^4 =$$
$$= x_1^4 + x_1^3 + \frac{1}{2}x_1^2 + \frac{1}{3}x_2x_1 + \frac{1}{2}x_1 + \frac{1}{3}x_2$$

Ο παραλήπτης επιλέγει με τη σειρά του ένα αντιστρέψιμο στοιχείο του δακτυλίου για παράδειγμα το:

$$V = 1 + x_2, V^{-1} = 1 - x_2$$

και αποστέλει το μήνυμα:

$$VRW = (1 + x_2)(x_1^4 + x_1^3 + \frac{1}{2}x_1^2 + \frac{1}{3}x_2x_1 + \frac{1}{2}x_1 + \frac{1}{3}x_2) =$$
$$= x_1^4 + x_1^3 + \frac{1}{2}x_1^2 + \frac{1}{3}x_2x_1 + \frac{1}{2}x_1 + \frac{1}{3}x_2 + x_2x_1^4 + x_2x_1^3 + \frac{1}{2}x_2x_1^2$$
$$+ \frac{1}{3}x_2^2x_1 + \frac{1}{2}x_2x_1 + \frac{1}{3}x_2^2$$

Ο αποστολέας του αρχικού μηνύματος πολλαπλασιάζει από δεξιά με το αντίστροφο του στοιχείου που είχε χρησιμοποιησεί και αποστέλει το μήνυμα:

$$VRWW^{-1} =$$
$$= x_1^4 + x_1^3 + \frac{1}{2}x_1^2 + \frac{1}{3}x_2x_1 + \frac{1}{2}x_1 + \frac{1}{3}x_2 + x_2x_1^4 + x_2x_1^3 + \frac{1}{2}x_2x_1^2 + \frac{1}{3}x_2^2x_1$$
$$+ \frac{1}{2}x_2x_1 + \frac{1}{3}x_2^2 - x_1^5 - x_1^4 - \frac{1}{2}x_1^3 - \frac{1}{3}x_2x_1^2 - \frac{1}{2}x_1^2 - \frac{1}{3}x_2x_1 - x_2x_1^5 - x_2x_1^4$$
$$- \frac{1}{2}x_2x_1^3 - \frac{1}{3}x_2^2x_1^2 - \frac{1}{2}x_2x_1^2 - \frac{1}{3}x_2^2x_1 \Rightarrow$$
$$VR =$$
$$\frac{1}{2}x_1^3 + \frac{1}{2}x_1 + \frac{1}{3}x_2 + \frac{1}{2}x_2x_1^3 + \frac{1}{2}x_2x_1 + \frac{1}{3}x_2^2 - x_1^5 - \frac{1}{3}x_2x_1^2 - x_2x_1^5 - \frac{1}{3}x_2^2x_1^2$$

Τελικά, ο παραλήπτης πολλαπλασιάζει από αριστερά με το αντίστροφο του στοιχείου που είχε επιλέξει:

$$
\begin{aligned}
&V^{-1}VR = \\
&(1-x_2)(\frac{1}{2}x_1^3+\frac{1}{2}x_1+\frac{1}{3}x_2+\frac{1}{2}x_2x_1^3+ \\
&\frac{1}{2}x_2x_1+\frac{1}{3}x_2^2-x_1^5-\frac{1}{3}x_2x_1^2-x_2x_1^5-\frac{1}{3}x_2^2x_1^2) \\
&=\frac{1}{2}x_1^3+\frac{1}{2}x_1+\frac{1}{3}x_2+\frac{1}{2}x_2x_1^3+\frac{1}{2}x_2x_1+ \\
&\frac{1}{3}x_2^2-x_1^5-\frac{1}{3}x_2x_1^2-x_2x_1^5-\frac{1}{3}x_2^2x_1^2 \\
&-\frac{1}{2}x_2x_1^3-\frac{1}{2}x_2x_1-\frac{1}{3}x_2^2-\frac{1}{2}x_2^2x_1^3\frac{1}{2}x_2^2x_1- \\
&\frac{1}{3}x_2^3+x_2x_1^5+\frac{1}{3}x_2^2x_1^2+x_2^2x_1^5+\frac{1}{3}x_2^3x_1^2 \\
&=\frac{1}{2}x_1^3-x_1^5-\frac{1}{3}x_2x_1^2-\frac{1}{2}x_2^2x_1^3-\frac{1}{2}x_2^2x_1 \\
&-\frac{1}{3}x_2^3+x_2^2x_1^5+\frac{1}{3}x_2^3x_1^2+\frac{1}{2}x_1+\frac{1}{3}x_2
\end{aligned}
$$

Και απαλείφοντας τα στοιχεία με δύναμη μεγαλύτερη του 2 λαμβάνει:

$$R = \frac{1}{2}x_1 + \frac{1}{3}x_2$$

Βιβλιογραφία

[1] I. Anshel, M. Anshel και D. Goldfeld, *An algebraic method for public key cryptography*, Math research letters 6 , No. 3-4, 1999.

[2] E. Artin, *Theorie der Zopfe*, Hamburg Abh. 4, pp. 47-72.

[3] E. Artin, *Theory of Braids*, The anals of mathematics, 2nd ser., Vol. 48, No. 1. (Jan 1947), pp 101-126, `http://links.jstor.org/`

[4] Gilbert Baumslag, *Topics in Combinatorial Group Theory*, Birkhauser, 1993.

[5] Gilbert Baumslag, B. Fine και X.Xu, *Cryptosystems Using Linear Groups*, Appl. Alg. in Engineering, Communication and Computing, 17, 2006, p.p.205-217.

[6] Gilbert Baumslag, Yegor Brukhov, B. Fine και G.Rosenberger, *Encryption Methods using Formal Power Series Rings*, Centre de Recerca Matematica(CRM), Catalan, December 2007.

[7] S. Bigelow, *The Burau representation of the braid group B_n is not faithful for n=5*, Geometry and Topology 3, 1999, 397-404 .

[8] S. Bigelow, *Braid groups are linear*,Journal of American Mathematical Society 14, No. 2, 2001, 471-486.

[9] Joan S. Birman, *On Braid Groups*, Communications on Pure and Applied Mathematics 22:41-72, Quart. J. Math. Oxford. 20, 1969.

[10] Joan S. Birman , *Braids, Links and Mapping Class Groups*, Annals of Mathematics Studies, volume 82, Princeton University Press, 1974.

[11] Joan S. Birman και Tara E. Brendle, *Braids: A Survey*, 2004.

[12] W. Burau, *Uber Zopfgruppen und gleischsinning verdrillte Verkettungen*, Abh. Math. Sem. Ham. II, 171-178, 1936.

[13] W. Diffie και M. Hellman, *New directions in cryptography*, IEEE Trans. in Information Theory, No. 6, Ιούνιος 1977.

[14] Edward Fadell και Lee Neuwirth, *Configuration spaces*, Mathematica Scandinavia 10: 111-118, 1962.

[15] Ralph H. Fox, *Free Differential Calculus I: Derivation in the Free Group Ring*, The Annals of Mathematics, 2nd Ser., Vol. 57, No.3 (May, 1953), pp.547-560, `http://links.jstor.org/`

[16] Ralph H. Fox, *Free Differential Calculus II: The Isomorphism Problem of Groups*, The Annals of Mathematics, 2nd Ser., Vol. 59, No.2 (May, 1954), pp.196-210, `http://links.jstor.org/`

[17] Allen Hatcher, *Algebraic Topology*, Cambridge University Press, 2002.

[18] Nicholas Jackson, *Notes on braid groups*, 2004.

[19] K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Han, J. Kang και C. Park, *New public key cryptosystems using braid groups*, Lecture notes in Computer Science, Springer, Berlin 2000.

[20] D. Long και M. Paton, *The Burau representation of the braid group $\mathcal{B}_n$ is not faithful for $n \geq 6$*, Topology 32,1993, pp.439-447.

[21] W. Magnus , *Beziehungen zwischen Gruppen und Idealen in einem speziellen Ring*, Springer, Mathematische Annalen 111, 1935, pp.259-281.

[22] W.Magnus, *Rational Representations of Fuchsian Groups and Non-Parabolic Subgroups of the Modular Group*, Nachrichten der Akad Gottingen, 1973, pp. 179-189

[23] W. Magnus και A. Karrass και D. Solitar, *Combinatorial Group Theory*, Dover Publications, 2η έκδοση, εκτύπωση 2004.

[24] Charles F. Miller III, *Combinatorial Group Theory*, University of Melbourne, 1996-2004, `www.ms.unimelb.edu.au/~cfm`.

[25] J. Moody, *The Burau representation of the braid group $\mathcal{B}_n$ is not faithful for large n*, Bull. Amer. Math. Soc. 25,1991, pp.379-384.

[26] A. G. Myasnikov, V. Shpilrain and A.Ushakov, *A practical attack on some braid group based cryptographic protocols*, in CRYPTO 2005, Lecture Notes Comp. Sc. 3621 (2005),pp. 86-96.

[27] Derek J.S. Robinson, *A Course in the Theory of Groups*, Springer, 2η έκδοση, 1996.

[28] Colin Rourke και Sofia Lambropoulou , *Markov's theorem in 3-manifolds*, Topology and its Applications, 78:95-122, 1997.

[29] Vladimir Shpilrain και Gabriel Zapata, *Combinatorial Group Theory and Public Key Cryptography*, Cryptology ePrint Archive, Report 2004/242 , 2004, `http://eprint.iacr.org/`.

Ευχαριστίες

Τέλος, θα ήθελα να ευχαριστήσω όλους τους καθηγητές μου, ειδικότερα του τμήματος μαθηματικών, που συνετέλεσαν, ο καθένας με τον τρόπο του, είτε το γνωρίζουν, είτε όχι, σε αυτήν την εργασία. Ιδιαιτέρως, τους κυρίους Δ.Βάρσο και Δ.Λάππα για τη συμβολή τους και τις παρατηρήσεις τους ως μέλη της τριμελούς επιτροπής και τον επιβλέποντα καθηγητή κ. Ε.Ράπτη για την άψογη συνεργασία μας, με ό,τι συμπεριλαμβάνει αυτό. Φυσικά, δε θα μπορούσα να ξεχάσω τους συναδέλφους μου, την ομάδα 42, τους φίλους και την οικογένειά μου που με υποφέρουν όλον αυτόν τον καιρό. Αφιερώνω ειδικά στη μνήμη του Πατέρα μου που χάθηκε στην έναρξη του παρόντος κύκλου σπουδών το Σεπτέμβρη του 2004.

Κερατσίνι,

Φεβρουάριος 2008,

Σωτήριος Δ. Χασάπης.