ΚΕΦΑΛΑΙΟ 8: Εφαρμογή: Το θεώρημα του Burnside

Θα αποδείξουμε εδώ ότι κάθε ομάδα τάξης $p^a q^b$ (p, q πρώτοι) είναι επιλύσιμη. Το θεώρημα αυτό αποδείχτηκε από τον Burnside το 1904 ο οποίος χρησιμοποίησε τη νέα τότε θεωρία αναπαραστάσεων ομάδων που αναπτύχθηκε από τον Frobenius. Για σχεδόν 70 χρόνια δεν υπήρχε απόδειξη που να αποφεύγει χαρακτήρες και αναπαραστάσεις. Τελικά βρέθηκε μια ομαδοθεωρητική απόδειξη το 1972 από τον J. Thompson (Fields Medal) η οποία είναι μακροσκελής και δύσκολη. Αργότερα βρέθηκαν πιο σύντομες αποδείξεις.

8.1. Αλγεβρικοί Ακέραιοι.

Ξεκινάμε με ορισμένα στοιχεία που αφορούν αλγεβρικούς ακεραίους. Ένας αριθμός $a \in \mathbf{C}$ ονομάζεται **αλγεβρικός ακέραιος** αν είναι ρίζα ενός μονικού πολυωνύμου $p(x) \in \mathbf{Z}[x]$. Το σύνολο των αλγεβρικών ακεραίων συμβολίζεται με O και ο σκοπός μας είναι να δείξουμε ότι το O είναι υποδακτύλιος του $\mathbf{C}$ (δες για παράδειγμα τις σημειώσεις του γράφοντος, "Μεταθετική Άλγεβρα και Εφαρμογές", Αθήνα 1999, § 7.2).

8.1.1 Πρόταση. *Έστω $R \subseteq S$ δακτύλιοι και $s \in S$. Τότε τα παρακάτω είναι ισοδύναμα*

(i) το s είναι ακέραιο πάνω από το R (δηλαδή εξ ορισμού είναι ρίζα μονικού πολυωνύμου $p(x) \in R[x]$)

(ii) ο υποδακτύλιος $R[s]$ του S είναι πεπερασμένα παραγόμενο R-πρότυπο

(iii) υπάρχει υποδακτύλιος R' του S έτσι ώστε $R[s] \subseteq R'$ και το R' είναι πεπερασμένα παραγόμενο R-πρότυπο

(iv) υπάρχει πιστό $R[s]$-πρότυπο που είναι πεπερασμένα παραγόμενο R-πρότυπο.

Απόδειξη: (i)$\Rightarrow$(ii) Ως R-πρότυπο το $R[s]$ παράγεται από τα $1, s, s^2, \ldots$

Από την υπόθεση έχουμε

$$s^n + r_{n-1}s^{n-1} + \ldots + r_0 = 0$$

για κάποια $r_i \in R$. Άρα $s^n = -r_{n-1}s^{n-1} - \ldots - r_0$ και $s^{n+k} = -r_{n-1}s^{n+k-1} - \ldots - r_0 s^k$,

οπότε μια προφανής επαγωγή στο k δείχνει ότι το s^{n+k} είναι R-γραμμικός συνδυασμός των $1, s, ..., s^{n-1}$.

(ii) $\Rightarrow$ (iii) Προφανές

(iii) $\Rightarrow$ (iv) Το R' είναι πιστό $R[s]$-πρότυπο

(iv) $\Rightarrow$ (i) Έστω M πιστό $R[s]$-πρότυπο που παράγεται από $m_1, ..., m_n$.

Υπάρχουν $r_{ij} \in R$ με

$$sm_1 = r_{11}m_1 + r_{12}m_2 + ... + r_{1n}m_n$$
$$\dots$$
$$sm_n = r_{n1}m_1 + r_{n2}m_2 + ... + r_{nn}m_n,$$

οπότε

$$0 = (r_{11} - s)m_1 + r_{12}m_2 + ... + r_{1n}m_n$$
$$\dots$$
$$0 = r_{n1}m_1 + r_{n2}m_2 + ... + (r_{nn} - s)m_n.$$

Έστω A ο $n \times n$ πίνακας των συντελεστών των m_i στο τελευταίο σύστημα. Γράφουμε αυτό ως

$$0 = A \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}$$

οπότε

$$0 = (adjA)A \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}.$$

Αλλά $(adjA)A = (\det A)I_n$, όπου I_n είναι ο ταυτοτικός $n \times n$ πίνακας, όπως θυμόμαστε από τη Γραμμική Άλγεβρα. (Η απόδειξη που δίνεται εκεί ισχύει και για μεταθετικούς δακτυλίους στη θέση σωμάτων). Άρα

$$(\det A)m_i = 0, \qquad i = 1, ..., n.$$

Επειδή το M είναι πιστό $R[s]$-πρότυπο και τα m_i παράγουν το M παίρνουμε

$$\det A = 0.$$

Το ανάπτυγμα της ορίζουσας $\det A$ δίνει τη ζητούμενη σχέση.

8.1.2 Πόρισμα. *Έστω $R \subseteq S$ δακτύλιοι και $s_1, ..., s_n \in S$ στοιχεία ακέραια πάνω από*

το R. Τότε ο δακτύλιος $R[s_1,...,s_n]$ *είναι πεπερασμένα παραγόμενο R-πρότυπο.*

Απόδειξη: Για $n=1$ δες την προηγούμενη πρόταση. Για $n>1$ γράφουμε

$$R[s_1,...,s_{n-1}] = R[s_1,...,s_{n-1}][s_n].$$

Το $R[s_1,...,s_{n-1}]$ είναι πεπερασμένα παραγόμενο *R*-πρότυπο από την υπόθεση της επαγωγής. Το $R[s_1,...,s_{n-1}][s_n]$ είναι πεπερασμένα παραγόμενο $R[s_1,...,s_{n-1}]$ πρότυπο (αφού το s_n είναι ακέραιο πάνω από το *R*). Συνεπώς το $R[s_1,...,s_n]$ είναι πεπερασμένα *R*-πρότυπο.

■

8.1.3 Πόρισμα. *Το σύνολο* O *είναι υποδακτύλιος του* $\mathbf{C}$**.**

Απόδειξη: Έστω $a,b \in \mathsf{O}$. Ο δακτύλιος $\mathbf{Z}[a,b]$ είναι πεπερασμένα παραγόμενο **Z**-πρότυπο από το πόρισμα 8.1.2 για $R=\mathbf{Z}$ και $S=\mathsf{O}$. Από την πρόταση 7.4.1 (iii) συμπεραίνουμε ότι $a-b \in \mathsf{O}$ και $ab \in \mathsf{O}$.

■

8.1.4 Πρόταση. $\mathsf{O} \cap \mathbf{Q} = \mathbf{Z}$.

Απόδειξη: Έστω $a/b \in \mathbf{Q}$ με $a,b \in \mathbf{Z}$, μ.κ.δ. $(a,b)=1$. Αν $a/b \in \mathsf{O}$ τότε έχουμε μια σχέση της μορφής

$$(a/b)^n + a_{n-1}(a/b)^{n-1} + ... + a_0, \quad a_i \in \mathbf{Z}$$

οπότε

$$a^n + a_{n-1}ba^{n-1} + ... + a_0 b^n = 0$$

πράγμα που δίνει ότι το *b* διαιρεί το a^n. Άρα $b=\pm 1$, οπότε $a/b \in \mathbf{Z}$. Η άλλη σχέση $\mathbf{Z} \subseteq \mathsf{O} \cap \mathbf{Q}$ είναι προφανής.

■

Επιστρέφουμε τώρα σε χαρακτήρες.

8.1.5 Πρόταση. *Έστω* χ *χαρακτήρας της G. Τότε για κάθε* $g \in G$*, το* $\chi(g)$ *είναι αλγεβρικός ακέραιος.*

Απόδειξη: Κάθε ρίζα της μονάδας είναι αλγεβρικός ακέραιος ως ρίζα του $x^m - 1$. Γνωρίζουμε ότι το $\chi(g)$ είναι άθροισμα ριζών της μονάδας, οπότε το ζητούμε

προκύπτει από το πόρισμα 8.1.3.

■

Κατά συνέπεια οι μόνοι ρητοί αριθμοί που εμφανίζονται στον πίνακα χαρακτήρων της G είναι οι ακέραιοι.

8.2. Θεώρημα του Burnside.

8.2.1 Λήμμα. *Έστω V ανάγωγο $\mathbf{C}[G]$-πρότυπο και $z \in C(\mathbf{C}[G])$. Τότε υπάρχει $\lambda \in \mathbf{C}$ με την ιδιότητα $zv = \lambda v$ για κάθε $v \in V$.*

Απόδειξη: Επειδή $z \in C(\mathbf{C}[G])$, η συνάρτηση $f : V \ni v \mapsto zv \in V$ είναι $\mathbf{C}[G]$-ομομορφισμός. Επειδή το $\mathbf{C}$ είναι αλγεβρικά κλειστό η f έχει μη ιδιοτιμή, έστω λ. Άρα $f(v) = \lambda v$ για κάποιο $\lambda \in \mathbf{C}$, $v \in V$, $v \neq 0$. Συνεπώς ο ομομορφισμός $f - \lambda 1_V$ έχει μη μηδενικό πυρήνα. Αφού το V είναι ανάγωγο, παίρνουμε $Ker(f - \lambda 1_V) = V$, δηλαδή $f(v) = \lambda v$ για κάθε $v \in V$.

■

8.2.2 Πρόταση. *Έστω χ ανάγωγος χαρακτήρας της G και $g \in G$. Τότε ο αριθμός*

$$\lambda = \frac{|G|}{|C(g)|}\frac{\chi(g)}{\chi(1)}$$

είναι αλγεβρικός ακέραιος.

Απόδειξη: Έστω $V \subseteq \mathbf{C}[G]$ ανάγωγο $C[G]$-πρότυπο με χαρακτήρα χ και έστω $\overline{C}$ το άθροισμα των συζυγών του g. Τότε

$$\overline{C}v = \lambda v \text{ για κάθε } v \in V. \qquad (2)$$

Πράγματι, αφού $\overline{C} \in C(\mathbf{C}[G])$ (δες τη συζήτηση πριν την πρόταση 7.1.6) συμπεραίνουμε από το λήμμα 8.2.1 ότι υπάρχει $\mu \in \mathbf{C}$ με $\overline{C}v = \mu v$ για κάθε $v \in V$. Λαμβάνοντας ίχνη η τελευταία σχέση δίνει $\sum \chi(g') = \mu\chi(1)$, όπου το g' διατρέχει τα συζυγή στοιχεία του g. Επειδή $\chi(g') = \chi(g)$ και το πλήθος των g' είναι $|G|/|C(g)|$ παίρνουμε

$$\mu = \frac{|G|}{|C(g)|}\frac{\chi(g)}{\chi(1)}.$$

Θεωρούμε τώρα τη γραμμική απεικόνιση

$$f : \mathbf{C}[G] \ni z \mapsto \overline{C}z \in \mathbf{C}[G].$$

Ο πίνακας της f ως προς τη βάση $G = \{g_1,...,g_n\}$ έχει στοιχεία ακέραιους αριθμούς. Κάθε ιδιοτιμή ενός τέτοιου πίνακα είναι αλγεβρικός ακέραιος. Από το (2), το λ είναι ιδιοτιμή της f, και άρα το λ είναι αλγεβρικός ακέραιος.

■

Από την προηγούμενη πρόταση ο αριθμός

$$\frac{|G|}{|C(g)|}\frac{\chi(g)}{\chi(1)}$$

είναι αλγεβρικός ακέραιος. Έστω ότι μκδ $\left(\frac{|G|}{|C(g)|}, \chi(1)\right) = 1$. Τότε $a\frac{|G|}{|C(g)|} + b\,\chi(1) = 1$ για κάποιο $a, b \in \mathbf{Z}$, οπότε

$$\frac{\chi(g)}{\chi(1)} = a\frac{|G|}{|C(g)|}\frac{\chi(g)}{\chi(1)} + b\,\chi(g)$$

που είναι αλγεβρικός ακέραιος (πόρισμα 8.1.3).

8.2.4 Πόρισμα. *Με τους προηγούμενους συμβολισμούς, έστω μ.κ.δ* $\left(\frac{|G|}{|C(g)|}, \chi(1)\right) = 1$.

Τότε ο $\chi(g)/\chi(1)$ *είναι αλγεβρικός ακέραιος.*

■

Ερχόμαστε τώρα στο τελευταίο προπαρασκευαστικό αποτέλεσμα που αποτελεί το κλειδί για τα θεωρήματα που ακολουθούν. Εδώ θα χρησιμοποιήσουμε λίγη θεωρία Galois. Με $C(\rho(G))$ συμβολίζουμε παρακάτω το κέντρο της ομάδας $\rho(G)$.

8.2.5 Πόρισμα. *Με τους προηγούμενους συμβολισμούς, έστω μ.κ.δ* $\left(\frac{|G|}{|C(g)|}, \chi(1)\right) = 1$.

Έστω $\rho : G \to GL_n(\mathbf{C})$ *αναπαράσταση με χαρακτήρα χ. Τότε*

$$\acute{\eta}\ \rho(g) \in C(\rho(G)) \quad \acute{\eta}\ \chi(g) = 0.$$

Απόδειξη: Επειδή το $\chi(g)$ είναι αθροισμα ριζών της μονάδας (πλήθους $\chi(1)$) η τριγωνική ανισότητα δίνει

$$\left|\frac{\chi(g)}{\chi(1)}\right| \le 1.$$

Αν ισχύει ισότητα, τότε αυτές οι ρίζες της μονάδας είναι ίσες μεταξύ τους (γιατί;)

Ισχυριζόμαστε ότι $\rho(g) \in C(\rho(G))$. Πράγματι, έστω m η τάξη του g. Τότε $\rho(g)^m = I$, οπότε το ελάχιστο πολυώνυμο του πίνακα $\rho(g)$ διαιρεί το $x^m - 1$ και κατά συνέπεια έχει διακεκριμένες ρίζες. Άρα ο $\rho(g)$ είναι διαγωνίσιμος, και συνεπώς όμοιος με έναν πίνακα της μορφής ωI (γιατί οι ιδιοτιμές του $\rho(g)$ ταυτίζονται). Άρα $\rho(g) = \omega I$ που ανήκει στο κέντρο της $GL_n(\mathbf{C})$.

Έστω τώρα ότι $\left|\frac{\chi(g)}{\chi(1)}\right| < 1$. Θέτουμε $a = \frac{\chi(g)}{\chi(1)}$. Έστω ε μια πρωταρχική m-ρίζα της μονάδας, όπου m είναι η τάξη του g, και $K = \mathbf{Q}(\varepsilon)$ οπότε $a \in K$. Για κάθε $\sigma \in Gal(K/\mathbf{Q})$, ισχύει $\sigma(a) \le 1$, γιατί

$$\sigma(a) = \frac{1}{\chi(1)}\sigma(\chi(g)) = \frac{1}{\chi(1)}(\omega_1 + ... + \omega_{\chi(1)})$$

όπου κάθε ω_i είναι ρίζα της μονάδας. Συνεπώς η υπόθεση δίνει

$$\left|\prod_{\sigma \in Gal(K,\mathbf{Q})} \sigma(a)\right| < 1.$$

Επειδή το a είναι αλγεβρικός ακέραιος (πόρισμα 8.2.4), κάθε $\sigma(a)$ είναι αλγεβρικός ακέραιος και άρα το $b = \prod_{\sigma \in Gal(K,\mathbf{Q})} \sigma(a)$ είναι αλγεβρικός ακέραιος. Από την άλλη μεριά, το b είναι ρητός αριθμός, γιατί $\sigma(b) = b$ για κάθε $\sigma \in Gal(K,\mathbf{Q})$. Επομένως (πρόταση 8.1.4) $b \in \mathbf{Z}$. Αφού $|b| < 1$ παίρνουμε $b = 0$. Δηλαδή $\sigma(a) = 0$ για κάποιο σ, που δίνει βέβαια $a = 0$.

■

Σημείωση: Στην προηγούμενη απόδειξη θα μπορούσαμε να πάρουμε στη θέση του K οποιαδήποτε επέκταση του Galois που περιέχει το ε.

8.2.6 Θεώρημα *(Burnside). Έστω G πεπερασμένη ομάδα και C μια κλάση συζυγίας της G με* $|C| = p^m$, *p πρώτος* $m > 0$. *Τότε υπάρχει μη τετριμμένη ανάγωγη αναπαράσταση ρ της G με την ιδιότητα το* $\rho(C) \subseteq C(\rho(G))$. *Συνεπώς η G δεν είναι απλή.*

Απόδειξη: Έστω χ_{reg} ο χαρακτήρας του κανονικού $\mathbf{C}[G]$-προτύπου και $g \in G$, $g \neq 1$. Τότε (λήμμα 7.2.3)

$$0 = \chi_{reg}(g) = \chi_1(1)\chi_1(g) + ... + \chi_s(1)\chi_s(g) = 1 + \chi_2(1)\chi_2(g) + ... + \chi_s(1)\chi_s(g),$$

όπου χ_1 είναι ο χαρακτήρας της τετριμμένης αναπαράστασης. Γράφουμε την προηγούμενη σχέση ως

$$\sum_{i=2}^{s} \chi_i(g)\frac{\chi_i(1)}{p} = -\frac{1}{p}.$$

Επειδή το $-\frac{1}{p}$ δεν είναι αλγεβρικός ακέραιος (πρόταση 8.1.4), για κάποιο $i \geq 2$ το $\chi_i(g)\chi_i(1)/p$ δεν είναι αλγεβρικός ακέραιος (πόρισμα 8.1.3). Επειδή το $\chi_i(g)$ είναι αλγεβρικός ακέραιος (πρόταση 8.1.5), το $\chi_i(1)/p$ δεν είναι. Δηλαδή το p δεν διαιρεί το $\chi(1)$. Άρα

$$\chi_i(g) \neq 0 \quad \text{και} \quad p \quad \text{δεν διαιρεί το} \quad \chi_i(1).$$

Άρα $\mu.\kappa.\delta(|C|, \chi_i(1)) = 1$. Τότε το πόρισμα 8.2.5 δίνει ότι το $\rho(g)$ ανήκει στο κέντρο της $\rho(G)$ για κάθε $g \in C$, όπου ρ είναι η ανάγωγη αναπαράσταση με χαρακτήρα χ_i.

Θα δείξουμε τέλος ότι η G δεν είναι απλή. Έστω $H = Ker\rho$, που είναι μια κανονική υποομάδα της G. Αφού η ρ δεν είναι η τετριμμένη αναπαράσταση έχουμε $H \neq G$. Αν ισχύει $H = 1$, τότε $G \cong \rho(G)$ και το κέντρο της $\rho(G)$ είναι μη τετριμμένο αφού περιέχει το σύνολο $\rho(C)$, όπως δείξαμε πριν. Αν $C(\rho(G)) = \rho(G)$ τότε η G είναι αβελιανή, και αφού η τάξη της δεν είναι πρώτος (γιατί $|C| = p^m$, $m < 0$) η G δεν είναι απλή. Αν $C(\rho(G)) \neq \rho(G)$, τότε το $C(\rho(G))$ είναι μια γνήσια μη τετριμμένη κανονική υποομάδα της $\rho(G)$, δηλαδή η $\rho(G)$ δεν είναι απλή.

■

Θυμίζουμε ότι μια ομάδα G ονομάζεται επιλύσιμη αν υπάρχουν υποομάδες της G

$$1 = G_0 < G_1 < \ldots < G_r < G$$

έτσι ώστε κάθε G_i είναι κανονική στη G_{i+1} και κάθε πηλίκο G_{i+1}/G_i είναι κυκλική τάξης πρώτου αριθμού. Ως απλές ασκήσεις αφήνουμε τις εξής παρατηρήσεις: 1) Αν η υποομάδα H της G είναι κανονική με την ιδιότητα η H και η G/H είναι επιλύσιμες, τότε η G είναι επιλύσιμη. 2) Κάθε ομάδα τάξης p^a, p πρώτος, $a > 0$ δεν είναι απλή (υπόδειξη: $C(G) \neq 1$). Ερχόμαστε τώρα στο δεύτερο φημισμένο θεώρημα του Burnside.

8.2.7 Θεώρημα (Burnside). *Κάθε ομάδα τάξης* $p^a q^b$, *όπου* p,q *είναι πρώτοι αριθμοί, είναι επιλύσιμη.*

Απόδειξη: Επαγωγή στο $a+b$. Το θεώρημα είναι προφανές για $a+b=1$ οπότε υποθέτουμε ότι $a+b \geq 2$. Θα δείξουμε πρώτα ότι η G δεν είναι απλή.

Αν $a=0$ ή $b=0$, τότε η G δεν είναι απλή από την παρατήρηση 2 που επισημάναμε πριν το θεώρημα. Έστω $a,b>1$. Έστω Q μια q-Sylow υποομάδα της G, οπότε $|Q|=q^b$. Τότε $C(Q)\neq 1$, από την παρατήρηση 2. Έστω $g\in C(Q),\ g\neq 1$. Τότε $Q\subseteq C_G(g)$ και άρα ο πληθάριθμος της συζυγούς κλάσεως του g, έστω C, είναι

$$|C|=[G:C_G(g)]=p^r$$

για κάποιο r. Αν $r=0,$ τότε $g\in C(G)$, οπότε η G δεν είναι απλή, αφού $<g>$ είναι γνήσια μη τετριμμένη κανονική υποομάδα της G. Αν $r\neq 0$, τότε η G δεν είναι απλή από το θεώρημα 8.2.6.

Έχοντας αποδείξει ότι η G δεν είναι απλή, μια προφανής επαγωγή στο $a+b$ βασιζόμενη στην παρατήρηση 1 δίνει το αποτέλεσμα.

■

Όπως έχουν τονίσει ήδη, υπάρχουν αποδείξεις του θεωρήματος 8.2.7 που αποφεύγουν χαρακτήρες. Το ίδιο όμως δεν συμβαίνει για το θεώρημα 8.2.6 μέχρι σήμερα.

Ασκήσεις

1. Κάθε μη αβελιανή απλή ομάδα ταξης ≤ 69 έχει ταξη 60 (Υπόδειξη: για να αποκλείσετε τις περιπτώσεις 30 και 42 εφαρμόστε τα θεωρήματα Sylow).

2. Κάθε μη αβελιανή απλή ομάδα δεν έχει αβελιανή υποομάδα δείκτη p^r, p πρώτος.

3. Έστω χ ανάγωγος χαρακτήρας της G. Τότε το $\chi(1)$ διαιρεί $|G|$. (Υπόδειξη: Έστω $g_1,...,g_s$ αντιπρόσωποι των κλάσεων συζυγίας. Από την πρόταση 8.2.2, ο αριθμός

$$\sum_{i=1}^{s}\frac{|G|}{|C(g_i)|}\frac{\chi(g_i)\overline{\chi(g_i)}}{\chi(1)}$$

είναι αλγεβρικός ακέραιος. Αυτός ισούται με $|G|/\chi(1)$, οπότε το ζητούμενο προκύπτει από την πρόταση 8.1.4).

4. Από τη στοιχειώδη θεωρία ομάδων γνωρίζετε ότι κάθε ομάδα τάξης p^2, p πρώτος, είναι αβελιανή. Δώστε μια άλλη απόδειξη (Υπόδειξη: προηγούμενη άσκηση και θεώρημα 7.1.8).

5. Έστω ομάδα G με την ιδιότητα τα στοιχεία g και g^{-1} είναι συζυγή για κάθε $g \in G$. Τότε ο πίνακας χαρακτήρων της G αποτελείται μόνο από ακεραίους αριθμούς. (Για παράδειγμα, οι συμμετρικές ομάδες S_n έχουν την προηγούμενη ιδιότητα).