אלגברה ב1

מאת

משה ירדן

תל אביב, תשס"ד

א. הגדרות החבורה

בסעיף זה נגדיר את מושג החֲבורה ונתן דֻגמאות לחבורות.

הגדרה: קבוצה לא ריקה G תקרא **חבורה** אם מתקַיְמים התנאים הבאים:

(א) לכל זוג סדור (a,b) של אברי G מתאים אבר אחד ויחד c של G. אנו רושמים $c=ab$ ואומרים ש c הוא המכפלה של a ו b.

(ב) מתקיֵם חק הצֵרוף: $a(bc)=(ab)c$.

(ג) קיָם אבר e ב G כך ש $ea=a$ לכל a ב G (e נקרא **אבר יחידה משמאל**).

(ד) לכל $a \in G$ קיָם $a' \in G$ כך ש $a'a=e$ (b נקרא **הָפְכִּי משמאל**). ∎

מסקנות מיָדיות.

(א) חֹק הצרוף המֻרחב.

(ב) $aa'=e$. כלומר, a' הנו גם הפכי מימין. לכן a' יקרֵא **הפכי** של a. ואכן, קיָם $a'' \in G$ כך ש $a''a'=e$. לכן $aa'=eaa'=a''a'aa'=a''a'=e$.

(ג) $ae=a$ לכל $a \in G$. כלומר, אבר יחידה משמאל כלומר, אבר יחידה משמאל הוא גם אבר יחידה מימין ולכן יקרא **אבר יחידה**. ואכן, $ae=aa'a=ea=a$.

(ד) קים ל G אבר יחידה יחיד. ואכן, אם e' הנו אבר יחידה נוסף, אזי $e=ee'=e'$.

(ה) קיָם ל a הפכי יחיד. ואכן, אם $a'a=e$ ו $a''a=e$, אזי $a'=a'(aa'')=(a'a)a''=a''$. נסמן את ההפכי של a ב a^{-1}.

(ו) $(ab)^{-1}=b^{-1}a^{-1}$.

חֲזָקות: החזקות של אבר $a \in G$ יֻגדרו באפן הבא: $a^0=e$, $a^{n+1}=a^na$, $a^{-n}=(a^n)^{-1}$. החזקות מקימות את התנאים הבאים:

(א) $a^ia^j=a^{i+j}$

(ב) $(a^i)^j=a^{ij}$

(ג) $a^ib^i=(ab)^i$ אם $ab=ba$ (בדרך כלל התנאי אינו נכון).

איזומורפיזם: העתקה חד חד ערכית α של חבורה G_1 על חבורה G_2 תקרא **איזומורפיזם** אם $\alpha(ab)=\alpha(a)\alpha(b)$ ו $\alpha(a^{-1})=\alpha(a)^{-1}$ לכל $a,b \in G_1$. ∎

חבורה חלופית: חבורה G תקֻנה **חִלופית** (או **אַבֵּלית**) אם $ab=ba$ לכל $a,b \in G$. במקרה זה משתמשים לעתים בכתיב חבורי וכותבים $a+b$ במקום ab. ∎

דֻגמאות לַחבורות:

(א) חבורת השלמים $\mathbb{Z}$.

(ב) החבורה החבורית F^+ והחבורה הכפלית $F^\times$ של שדה F.

(ג) החבורה הכפלית של המספרים הממשיים החיוביים $\mathbb{R}^\times_{>0}$. ההעתקה $x \mapsto e^x$ (e הנו בסיס הלוגרתמים הטבעיים) היא איזומורפיזם של $\mathbb{R}^+$ על $\mathbb{R}^\times_{>0}$.

(ד) החבורה הכפלית $\{\pm 1\}$.

(ה) חבורה מַעְגלית מסדר n: $\{e^{2\pi\sqrt{-1}k/n} \mid k \in \mathbb{Z}\}$.

(ו) חבורת המטריצות ההפיכות $\mathrm{GL}(n, F)$ מסדר $n \times n$ מעל שדה F. אם $n \geq 2$, חבורה זו אינה הפיכה.

(ז) חבורת התמורות $S(X)$ של קבוצה X.

(ח) חבורת התמורות S_n של הקבוצה $\{1, 2, \ldots, n\}$. זוהי **החבורה הסימטרית** S_n.

(ט) החבורה החפשית הנוצרת על ידי קבוצה X. ∎

ב. חבורות חלקיות

קבוצה חלקית H של חבורה G תקרא **חבורה חלקית** אם H היא חבורה ביחס לפעֻלת הכפל של G. במקרה זה נסמן $H \leq G$. אם בנוסף לכך $H \neq G$ נסמן $H < G$ ונאמר ש H היא תת חבורה **נאותה** של G.

למה ב.א: *קבוצה חלקית לא ריקה H של G היא חבורה חלקית אם ורק אם $ab \in H$ ו $a^{-1} \in H$ לכל $a, b \in H$.*

למה ב.ב: *אם $\{H_i \mid i \in I\}$ היא משפחה של חבורות חלקיות של חבורה G אזי $\bigcap_{i\in I} H_i$ היא חבורה חלקית של G.*

הלמה המתאימה ביחס לאחודים אינה נכונה. דֻגמה נגדית: $2\mathbb{Z}$ ו $3\mathbb{Z}$ הן חבורות חלקיות של $\mathbb{Z}$ אולם $2\mathbb{Z}\cup 3\mathbb{Z}$ אינה חבורה חלקית של $\mathbb{Z}$.

תהי S תת קבוצה של חבורה G. חתוך כל החבורות החלקיות של G המקיפות את S הוא חבורה חלקית של G הנקראת **החבורה הנוצרת על ידי** S. היא מסֻמנת ב $\langle S\rangle$. נסמן $S^{-1} = \{m^{-1} \mid m \in S\}$. אזי

$$\langle S\rangle = \{x_1, \ldots, x_n \mid x_i \in S \cup S^{-1}, \quad i = 1, \ldots, n\}$$

אם $S = \{a, b, \ldots, \ldots\}$, נסמן את $\langle S\rangle$ גם על ידי $\langle a, b, \ldots\rangle$. בפרט אם $a \in G$, אזי $\langle a\rangle$ היא החבורה המעגלית הנוצרת על ידי a: $\langle a\rangle = \{a^i \mid i \in \mathbb{Z}\}$. אם $\langle S\rangle = G$, נאמר ש S היא **מערכת יוצרים** של G.

תהי H תת חבורה של חבורה G. כל קבוצה מהצורה $gH = \{gh \mid h \in H\}$ תקרא **מחלקה שמאלית** של H ב G. אסף כל המחלקות השמאליות יסֻמן ב G/H.

למה ב.ג: *יהיו $G \leq H$ חבורות.*

(א) *לכל $g_1, g_2 \in G$ מתקיֵם $g_1H = g_2H$ או $g_1H \cap g_2H = \emptyset$.*

(ב) *נִתן להציג את G כאחוד זר של מחלקות שמאליות של H ב G: $G = \dot\bigcup_{g\in R} gH$ באשר R היא תת קבוצה של G הנקראת* **מערכת מיַצגים** *של G* **מודולו** *H.*

(ג) *אם H הִנה חבורה סופית, אזי $|gH| = |H|$ לכל $g \in G$.*

נסמן ב $|G|$ את העָצמה של G (= מספר אברי G במקרה ש G סופית). נסמן $(G : H) = |G/H|$ ונקרא ל $(G : H)$ **האִנְדֶקְס** של H ב G.

משפט ב.ד (לגרנז'): *תהי G חבורה סופית ו $H \leq G$. אזי $|G| = |H|(G : H)$. בפרט הסדר של חבורה חלקית של חבורה סופית מחלק את הסדר של החבורה.*

עבור תת קבוצות A ו B של G נסמן

$$.AB = \{ab \mid a \in A, \ b \in B\}$$

נשים לב לכך שגם אם A ו B הן תת חבורות, AB היא תת קבוצה של G ואינה בהכרח תת חבורה.

למה ב.ה: *תהיינה* A *ו* B *תת חבורות של חבורה סופית* G*. אזי*

$$|AB| = \frac{|A| \cdot |B|}{|A \cap B|}. \qquad (1)$$

הוכחה: ההַעְתקה $aB \mapsto a(A\cap B)$ מעתיקה את $A/A\cap B$ באֹפן חד חד ערכי על הקבוצה $\mathcal{A} = \{aB \mid a \in A\}$. נסמן $r = |\mathcal{A}|$. אזי, $r = |A/A \cap B| = \frac{|A|}{|A\cap B|}$. יהיו $a_1B, \dots, a_rB$ האברים השונים של $\mathcal{A}$. מלמה ב.ג(א) נובע ש $AB = \dot\bigcup_{i=1}^{r} a_iB$. לכן, $|AB| = r|B|$. מכאן נובעת הנֻסחה (1). ∎

ג. חבורות מַעְגליות

החבורה הפשוטה ביותר היא זו הנוצרת על ידי אבר אחד. חבורה כזו מכֻנה **מעגלית**. יהי g אבר בחבורה G. המספר הטבעי הקטן ביותר n שעבורו $g^n = e$ נקרא **הַסֵּדֶר** של g ומסֻמן ב $\mathrm{ord}(g)$. אם אין קים מספר כזה, כלומר $g^n \neq e$ לכל n, נסמן $\mathrm{ord}(g) = \infty$.

למה ג.א: *יהי g אבר בעל סדר סופי n בחבורה G. אזי:*

(א) $g^r = e$ *גורר* $n|r$.

(ב) $g^r = g^s$ *אם ורק אם* $r \equiv s \mod n$.

(ג) $\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}$.

(ד) $|\langle g \rangle| = \mathrm{ord}(g) = n$. *בפרט, הסדר של כל אבר בחבורה סופית מחלק את הסדר של החבורה.*

(ה) *לכל מספר שלם k מתקַיֵם* $\mathrm{ord}(g^k) = \frac{n}{\gcd(n,k)}$.

(ו) g^k *יוצר את* $\langle g \rangle$ *אם ורק אם* $\gcd(n,k) = 1$. *מספר היוצרים של* $\langle g \rangle$ *הנו* $\varphi(n)$.

למה ג.ב: *כל חבורה בעלת סדר ראשוני הנה מעגלית.*

למה ג.ג: *תהי $\langle g \rangle$ חבורה מעגלית בעלת סדר סופי n. לכל מחלק d של n קַיֶמֶת ל $\langle g \rangle$ בדיוק תת חבורה אחת מסדר d והיא $\langle g^{\frac{n}{d}} \rangle$. בפרט כל חבורה חלקית של $\langle g \rangle$ הנה מעגלית.*

הוכחה: תהי H תת חבורה לא טריביאלית של $\langle g \rangle$. יהי k המספר הטבעי הקטן ביותר כך ש $g^k \in H$. ממשפט החִלוק עם שארית נובע שאם $g^l \in H$, אזי $k|l$. לכן $H = \langle g^k \rangle$ הנה חבורה מעגלית. בפרט $g^n = e \in H$ ולכן, $k|n$. אם $d = |H|$, אזי $d = |H| = \mathrm{ord}(g^k) = \frac{n}{k}$. לכן, $k = \frac{n}{d}$ ו $H = \langle g^{\frac{n}{d}} \rangle$ נקבעת באפן יחיד על ידי סִדְרָהּ. ∎

למה ג.ד: *לכל n טבעי קַיֶמֶת חבורה מעגלית יחידה (עד כדי איזומורפיזם) מסדר n.*

למה ג.ה: *החבורה $\mathbb{Z}$ היא החבורה המעגלית האינסופית היחידה (עד כדי איזומורפיזם). החבורות החלקיות של $\mathbb{Z}$ הנן $n\mathbb{Z}$, באשר n עובר על כל המספרים השלמים האי שליליים.*

ד. חבורות נורמליות, הומומורפיזמים

אוטומורפיזם של חבורה G הוא איזומורפיזם של החבורה על עצמה. במלים אחרות, זוהי העתקה חד חד ערכית של G על עצמה השומרת על הכפל ועל פעֻלת ההִפוך. אסף כל האוטומורפיזמים של G יסֻמן ב $\mathrm{Aut}(G)$. אם $\alpha, \beta \in \mathrm{Aut}(G)$, אזי גם $\alpha \circ \beta$ ו α^{-1} הם אוטומורפיזמים של G. לכן, $\mathrm{Aut}(G)$ מהוָה חבורה ביחס לפעֻלת ההרכבה של האוטומורפיזמים.

יהיו a ו g אברים של חבורה G. נסמן

$$g^a = a^{-1}ga.$$

עבור a קבוע ההעתקה $g^a \mapsto g$ היא אוטומורפיזם של G הנקרא **האוטומורפיזם הפנימי של** G **המֻשרה על יד** a.

למה ד.א:

(א) $g^{ab} = (g^a)^b$.

(ב) $(gh)^a = g^a h^a$.

(ג) $(g^a)^{-1} = (g^{-1})^a$.

בַּחֲבורה חלופית כל אוטומורפיזם פנימי הוא הזהות. אם $\langle g \rangle$ הנה חבורה מעגלית מסדר n ו k הנו מספר טבעי הזר ל n, אזי ההעתקה $g^i \mapsto g^{ik}$ הנה אוטומורפיזם של $\langle g \rangle$ שאינו הזהות, בפרט הוא אינו פנימי. קבוצת כל האוטומורפיזמים הפנימיים של G מהוָה תת חבורה של $\mathrm{Aut}(G)$ המסֻמנת ב $\mathrm{Inn}(G)$.

על שני אברים g ו h של חבורה G יְאֻמַר שהם **צמודים זה לזה**, אם קיָם $a \in G$ כך ש $h = g^a$. יחס השקילות בחבורה הוא יחס שקילות. ביחס אליו מתפרקת החבורה לאחוד זר של מחלקות צמידות.

בין החבורות החלקיות של חבורה נתונה יש לחבורות הנשמרות על ידי כל האוטומורפיזמים הפנימיים חשיבות מיֻחדת. אלו הן בדיוק אותן תת החבורות העוברות ל 1 ב"הומומורפיזמים". אלו הן גם החבורות המשמשות לבניַּת חבורות מנה. כל המושגים אלו שזורים זה בזה ומהוִים את אבני היסוד של המשפטים היסודיים של תורת החבורות - משפטי האיזומורפיזמים.

נאמר על תת חבורה N של חבורה G שהיא **נורמלית** אם $N^g = N$ לכל $g \in G$. לחלופין, $gN = Ng$ לכל $g \in G$. במלים אחרות, לכל $g \in G$ ו $n \in N$ קיָם $n' \in N$ כך ש $ng = gn'$. אנו מסמנים $N \lhd G$.

לדֻגמה, כל תת חבורה של חבורה חלופית היא נורמלי. אם G היא חבורה, אזי G עצמה ותת החבורה $E = \{e\}$ הן תת חבורות נורמליות של G. אם N נורמלית ב G, אזי N נורמלית בכל תת חבורה של G המקיפה את N.

למה ד.ב: *תהי* N *תת חבורה נורמלית של חבורה* G*. אזי הנֻסחה*

$$(gN)(hN) = ghN$$

מגדירה פְּעֻלת כפל על הקבוצה G/N של המחלקות השמאליות של N ב G. תחת הגדרה זו הופכת G/N לחבורה הנקרֵאת **חבורת המנה של G מודולו** *N. אבר היחידה בחבורה זו הוא $eN = N$ והאבר ההָפכי נתן על ידי $(gN)^{-1} = g^{-1}N$.*

למה ד.ג: *אם $\{N_i \mid i \in I\}$ היא משפחה של חבורות חלקיות נורמליות של G אזי $\bigcap_{i\in I} N_i$ היא תת חבורה נורמלית של G.*

למה ד.ד: *תהיינה N ו A תת חבורות של חבורה G.*

(א) *אם $N \triangleleft G$, אזי $NA = AN$.*

(ב) *אם $NA = AN$ (ובפרט אם $N \triangleleft G$), אזי $NA = \langle N, A\rangle$.*

העתקה $\alpha\colon G \to H$ של חבורה G לתוך חבורה H נקראת **הומומורפיזם** אם $\alpha(g_1g_2) = \alpha(g_1)\alpha(g_2)$ לכל $g_1, g_2 \in G$. אם α על, כלומר אם $\alpha(G) = H$, נאמר ש α הוא **אפימורפיזם**. אם α חד חד ערכי, נאמר ש α הוא **מונומורפיזם** או גם **שִכּון**. לבסוף אומרים ש α הוא **אנדומורפיזם** אם α הוא הומומורפיזם של G לתוך עצמו.

למה ד.ה: *יהי $\alpha\colon G \to H$ הומומורפיזם. נסמן $\mathrm{Ker}(\alpha) = \{g \in G \mid \alpha(g) = e\}$.*

(א) *אם e הוא אבר היחידה של G, אזי $\alpha(e)$ הוא אבר היחידה של H.*

(ב) *$\alpha(g^{-1}) = \alpha(g)^{-1}$ לכל $g \in G$.*

(ג) *$\alpha(G)$ הוא תת חבורה של H.*

(ד) *$\mathrm{Ker}(\alpha)$ הוא תת חבורה נורמלית של G הנקראת הגרעין (Kernel) של α.*

(ה) *α חד חד ערכי אם ורק אם $\mathrm{Ker}(\alpha) = E$ הוא חבורת היחידה של G.*

משפט ד.ו (משפט האיזומורפיזם הראשון):

(א) *יהי K תת חבורה נורמלית של חבורה G. ההעתקה $\pi\colon G \to G/K$ המֻגדרת על ידי $\pi(g) = gK$ היא אפימורפיזם של G על G/K. אפימורפיזם זה נקרא* **העתקת המנה** *של G על G/K.*

(ב) *יהי $\alpha\colon G \to H$ אפימורפיזם. אזי $K = \mathrm{Ker}(\alpha)$ הוא תת חבורה נורמלית של G וההעתקה $\bar{\alpha}\colon G/K \to H$ המֻגדרת על ידי $\bar{\alpha}(gK) = \alpha(g)$ היא איזומורפיזם המקיֵם $\bar{\alpha} \circ \pi = \alpha$.*

דֻגמה ד.ז:

(א) לכל אבר $a \in G$ נסמן ב $\iota(a)$ את האוטומורפיזם הפנימי המֻשרה על ידי a. אזי ההעתקה $a \mapsto \iota(a^{-1})$ מהוָה אפימורפיזם של G על חבורת האוטומורפיזמים הפנימיים, $\mathrm{Inn}(G)$ של G. הגרעין של ι הוא המֶרכָּז של G. הוא מסֻמן ב $Z(G)$. לפי משפט האיזומורפיזם הראשון, $G/Z(G) \cong \mathrm{Inn}(G)$.

(ב) לכל n טבעי, $n\mathbb{Z}$ הנו תת חבורה נורמלית של $\mathbb{Z}$ בעלת אנדקס n. חבורת המנה $\mathbb{Z}/n\mathbb{Z}$ הנה חבורה מעגלית בת n אברים: $\mathbb{Z}/n\mathbb{Z} = \{i + n\mathbb{Z} \mid i = 0, 1, \ldots, n-1\}$. ∎

המכפלה הישרה של שתי חבורות G ו H הנה החבורה $G \times H$ שבה הכפל מֻגדר לפי מרכיבים: $(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2)$. אבר היחידה הנו (e_G, e_H) וההפוך נִתן על ידי $(g, h)^{-1} = (g^{-1}, h^{-1})$.

משפט ד.ח (משפט השאריות הסיני): *יהיו m ו n מספרים טבעיים זרים זה לזה.*

(א) *לכל $a, b \in \mathbb{Z}$ קיָם $x \in \mathbb{Z}$ כך ש $x \equiv a \mod m$ ו $x \equiv b \mod n$.*

(ב) $\varphi(mn) = \varphi(m)\varphi(n)$.

הוכחה: ההעתקה $x + mn \mapsto (x + mZ, x + nZ)$ היא הומומורפיזם $\varphi\colon \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. מהזרות של m ומ n נובע ש φ חד חד ערכית. הואיל ולשני האגפים אותו מספר אברים, נובע ש φ על. בפרט, עבור a, b שלמים קיָם $x \in \mathbb{Z}$ כך ש $x \equiv a \mod m$ ו $x \equiv b \mod n$.

כדי להוכיח את (ב) נשים לב לכך שכל החבורות הנ"ל הן למעשה חוגים וש φ הוא איזומורפיזם של חוגים. בתור שכזה מעתיק φ את חבורת האברים ההפיכים של אגף שמאל באפן חד חד ערכי על חבורות האברים ההפיכים באגף ימין. במלים אחרות: $(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$. לפי ההגדרה, $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$. לכן, $\varphi(mn) = \varphi(m)\varphi(n)$. ∎

משפט ד.ט (משפט האיזומורפיזם השני): *תהי N תת חבורה נורמלית של חבורה G ותהי A תת חבורה של G. אזי $A \cap N \lhd A$ ו $A/A \cap N \cong AN/N$.*

$$\begin{tikzcd}
 & A \arrow[r, dash] \arrow[d, dash] & AN \arrow[r, dash] \arrow[d, dash] & G \\
A_1 \arrow[r, dash] & A_1(A \cap N) \arrow[r, dash] \arrow[d, dash] & A_1N \arrow[d, dash] & \\
 & A \cap N \arrow[r, dash] & N &
\end{tikzcd}$$

אם A_1 היא תת חבורה של A אזי $A_1(A \cap N)/A \cap N$ עוברת באיזומורפיזם זה ל A_1N/N.

משפט ד.י (משפט האיזומורפיזם השלישי): *תהי N תת חבורה נורמלית של חבורה G.*

(א) *לכל תת חבורה A של G המקיפה את N נסמן $\bar{A} = A/N$. ההעתקה $\bar{A} \mapsto A$ מעתיקה את קבוצת כל החבורות החלקיות A של G המקיפות את N באפן חד חד ערכי על קבוצת כל החבורות החלקיות של $\bar{G}$ ומתקיֵם: $\overline{\bigcap_{i \in I} A_i} = \bigcap_{i \in I} \bar{A}_i$ ו $A_1 \le A_2$ אם ורק אם $\bar{A}_1 \le \bar{A}_2$.*

(ב) *אם $G \lhd M \lhd N$ אזי $M/N \lhd G/N$ וההעתקה $(gN)(M/N) \mapsto gM$, $g \in G$, הנה איזומורפיזם $G/M \cong (G/N)/(M/N)$.*

ה. מחלקות כפולות, מֶרְכָּז וּמְרַכֵּז

תְּהֶיֶינָה A ו B תת חבורות של G. לכל $g \in G$ הקבוצה $AgB = \{agb \mid a \in A,\ b \in B\}$ נקראת **מחלקה כפולה** של G ביחד ל A ו B. לכל $g \in G$ הקבוצה $g^{-1}Ag$ הנה חבורה. לכן, לפי למה ב.ה,

$$|AgB| = |g^{-1}AgB| = \frac{|g^{-1}Ag| \cdot |B|}{|g^{-1}Ag \cap B|} = \frac{|A| \cdot |B|}{|g^{-1}Ag \cap B|}. \tag{2}$$

למה ה.א: *תהיינה A ו B חבורות חלקיות של חבורה G. אזי:*

(א) *נִתָן להציג את G בתור אחוד זר:* $G = \bigcup_{i=1}^{k} Ag_iB$ כך $g_1 = 1$.

(ב) $|G| = \sum_{i=1}^{k} \frac{|A|\cdot|B|}{|g_i^{-1}Ag_i \cap B|}$.

בהנתן תת קבוצה S של G ואבר $a \in G$ נסמן

$$S^a = \{s^a \mid s \in S\}$$

נאמר ש S^a **צמודה** ל S על ידי a. אם H היא תת חבורה של G, אזי H^a היא תת חבורה של G וההעתקה $h \mapsto h^a$ הנה איזומורפיזם של H על H^a.

שוב, לתת קבוצה S של G נסמן

$$N_G(S) = \{a \in G \mid S^a = S\}.$$

זוהי תת חבורה של G הנקראת **המשַמֵּר** של S ב G. עוד נסמן

$$C_G(S) = \{a \in G \mid \forall s \in S\colon as = sa\}.$$

זוהי תת חבורה של $N_G(S)$ הנקראת **הרַכָּז** של S ב G. מן ההגדרות נובע שהרכז והמשמֵר של אבר מתלכדים זה עם זה: $C_G(g) = N_G(g)$. החבורה $Z(G) = C_G(G)$ נקראת **המרכָּז** של G. זוהי חבורת כל אברי G המתחלפים עם כל אברי G.

דוגמא ה.ב:

(א) המרכָּז של חבורה חלופית G הנו כל החבורה.

(ב) $Z(S_n) = 1$ לכל $n \geq 3$.

ואכן, יהי σ תמורה של $\{1, 2, \ldots, n\}$ שאינה הזהות. בלי הגבלת הכלליות $\sigma(1) = 2$. נתבונן בתמורה τ המְגדרת על ידי $\tau(1) = 3$, $\tau(2) = 2$, $\tau(3) = 1$ ו $\tau(i) = i$ לכל $i \geq 3$. אלו היה $\sigma\tau = \tau\sigma$, היינו מקבלים $\sigma(3) = \sigma(\tau(1)) = \tau(\sigma(1)) = \tau(2) = 2 = \sigma(1)$ בסתירה לחד חד ערכיות של σ. לכן $\sigma \notin Z(S_n)$, כנדרש.

(ג) $Z(\mathrm{GL}(n,K)) \cong K^\times$ לכל שדה K.

ואכן, חבורת האברים ההפיכים $R^\times$ של חוג R הנה חבורה. בפרט, $\mathrm{GL}(n,K)$ הנה חבורה האברים ההפיכים של חוג המטריצות $M_n(K)$. חוג זה איזומורפי לחוג האנדומורפיזמים $\mathrm{End}(K^n)$ של המרחב הוקטורי ה n־ממדי K^n. חבורת האברים ההפיכים של $\mathrm{End}(K^n)$ הנה אסף האוטומורפיזמים $\mathrm{Aut}(K^n)$ של K^n. לכן, האוטומורפיזם של חוגים $M_n(K) \to \mathrm{End}(K^n)$ משרֶה אוטומורפיזם של חבורות $\mathrm{GL}(n,K) \to \mathrm{Aut}(K^n)$. מספיק שנוכיח ש $Z(\mathrm{Aut}(K^n)) = 1$.

נתבונן ב $T \in Z(\mathrm{Aut}(K^n))$. יהי $v_1, \ldots, v_n$ בסיס של K^n. לכל i ו j השונים זה מזה נתבונן באוטומורפיזם היסודי E_{ij} המֻגדר על ידי

$$E_{ij}(v_i) = v_i + v_j$$
$$E_{ij}(v_k) = v_k \quad k \neq i$$

נרשֹם $Tv_i = \sum_{k=1}^n \alpha_{ik} v_k$ עם $\alpha_{ik} \in K$. אזי

$$TE_{ij}v_i = Tv_i + Tv_j = \sum_{k=1}^n \alpha_{ik} v_k + \sum_{k=1}^n \alpha_{jk} v_k$$
$$E_{ij}Tv_i = \sum_{k=1}^n \alpha_{ik} E_{ij} v_k = \alpha_{ii}(v_i + v_j) + \sum_{k \neq i} \alpha_{ik} v_k = \alpha_{ii} v_i + \sum_{k=1}^n \alpha_{ik} v_k$$

הואיל ו $TE_{ij} = E_{ij}T$, נקבל מהשואת האגפים הימניים של שני השויונים האחרונים ש $\alpha_{ii} v_j = \sum_{k=1}^n \alpha_{jk} v_k$. לכן, $\alpha_{jj} = \alpha_{ii}$ ו $\alpha_{jk} = 0$ לכל $j \neq k$. במלים אחרות, T אינה אלא הכפלה באבר α של $K^\times$. ההעתקה $\alpha \to T$ הנה איזומורפיזם של $\mathrm{Aut}(K^n)$ על $K^\times$. ∎

למה ה.ג: *תהי S תת קבוצה של חבורה G. אזי $(G : N_G(S))$ שוה למספר הקבוצות הצמודות ל S. בִיֶתר דיוק, ההעתקה $S^{g^{-1}} \mapsto gN_G(S)$ היא העתקה חד חד ערכית של קבוצת המחלקות השמאליות של $N_G(S)$ ב G על אסף הקבוצות הצמודות ל S.*

מסקנה ה.ד: *בחבורה סופית G מחלֵק מספר הקבוצות הצמודות ל S ב G את הסדר של G.*

ו. סדרות נורמליות

סדרה נורמלית של חבורה G היא סדרה (סופית) מהצורה

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_m = E \tag{1}$$

שבה $E = \{e\}$. נעיר שאין אנו דורשים ש $G_i \triangleleft G$ עבור $i \geq 2$. חבורות המנה G_i/G_{i+1} נקראות **גורמי הסדרה**.
על סדרה נורמלית נוספת,

$$G = H_1 \triangleright H_1 \triangleright \cdots \triangleright H_n = E \tag{2}$$

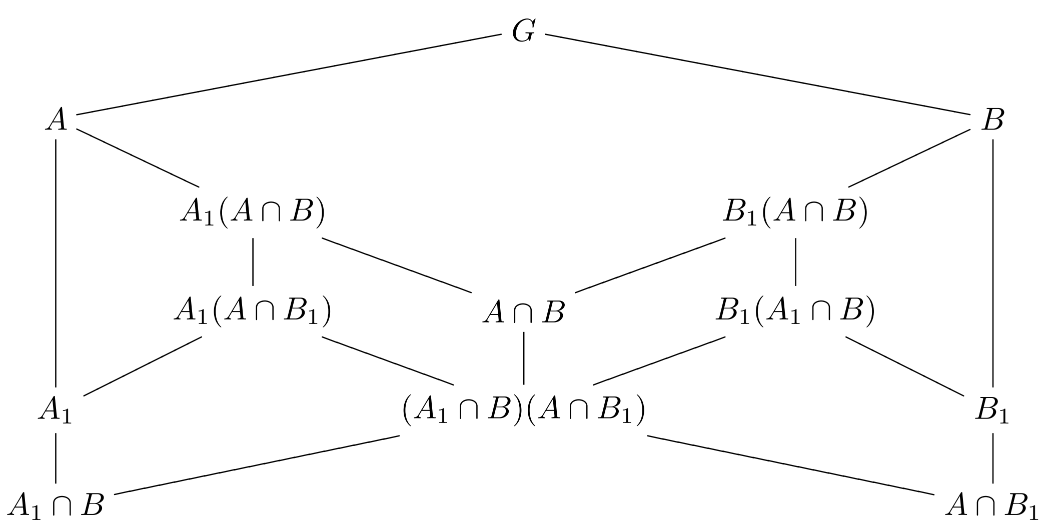
נאמר שהיא **שקולה** לסדרה (1) אם $m = n$ ואם קיֶמת תמורה π של הקבוצה $\{1, 2, \ldots, n\}$ כך ש

$$G_i/G_{i+1} \cong H_{\pi(i)}/H_{\pi(i)+1}$$

לכל $i \leq n-1$. הסדרה (2) תקרא **עִדּוּן** של הסדרה (1) אם כל ה G_i־ים מופיעים בין ה H_j־ים. נוכיח שלכל שתי סדרות נורמליות יש עדונים שקולים. לשם כך נביא את הלמה הבאה:

למה ו.א (Zassenhaus): *יהיו* $G \leq A \triangleleft A_1$ *ו* $G \leq B \triangleleft B_1$. *אזי* $A_1(A \cap B_1) \triangleleft A_1(A \cap B)$, $B_1(A \cap B) \triangleleft B_1(A_1 \cap B)$ *ו* $A_1(A \cap B)/A_1(A \cap B_1) \cong B_1(A \cap B)/B_1(A_1 \cap B)$.

הוכחה: נתבונן בתרשים החבורות הבא:



החבורות המופיעות בתרשים מקיְמות:

$$A_1(A \cap B_1) \cdot (A \cap B) = A_1(A \cap B)$$

$$A_1(A \cap B_1) \cap (A \cap B) = (A_1 \cap B)(A \cap B_1)$$

ולכן, לפי משפט האיזומורפיזם השני,

$$.A_1(A\cap B)/A_1(A\cap B_1)\cong(A\cap B)/(A_1\cap B)(A\cap B_1)$$

באפן סימטרי,

$$.(A\cap B)/(A_1\cap B)(A\cap B_1)\cong B_1(A\cap B)/B_1(A_1\cap B)$$

לכן, $A_1(A\cap B)/A_1(A\cap B_1)\cong B_1(A\cap B)/B_1(A_1\cap B)$, כנדרש. ∎

משפט ו.ב: (Schreier) *לכל שתי סדרות נורמליות של אותה החבורה קַיָמים עדונים השקולים זה לזה.*

הוכחה: תהְיֶינה

$$G=G_0\triangleright G_1\triangleright\cdots\triangleright G_m=E \tag{1}$$

$$G=H_0\triangleright H_1\triangleright\cdots\triangleright H_n=E \tag{2}$$

סדרות נורמליות של חבורה G. נסמן $G_{ij}=G_i(G_{i-1}\cap H_j)$, $i=0,\ldots,m$ ו $H_{ij}=H_j(H_{j-1}\cap G_i)$, $j=0,\ldots,n$. לפי למת Zassenhaus הסדרות הבאות נורמליות:

$$G_{i-1}=G_{i0}\triangleright G_{i1}\triangleright\cdots\triangleright G_{in}=G_i \qquad i=0,\ldots,m \tag{3}$$

$$H_{j-1}=H_{0j}\triangleright H_{1j}\triangleright\cdots\triangleright H_{mj}=H_j \qquad j=0,\ldots,n \tag{4}$$

הסדרה (3) מעדֶנת את (1) ואלו הסדרה (4) מעדנת את (2). בכל אחת מהסדרות יש $nm+1$ אברים ומתקיֵם $G_{i,j-1}/G_{ij}\cong H_{i-1,j}/H_{ij}$ לכל i ו j. במלים אחרות, הסדרות (3) ו (4) שקולות זו לזו. ∎

תהי H תת חבורה נורמלית של חבורה G. נאמר ש H **נורמלית מֵרבית** אם אין קיֶמת שום חבורה G_1 כך ש $H<G_1\triangleleft G$ ו $G_1\neq G$. **סדרת הֶרְכֵּב** (composition series) היא סדרה נורמלית ללא חזרות שאינה נִתֶנת לעדון נוסף. במלים אחרות, כל חבורה בסדרה הנה נורמלית מרבית בחבורה הקודמת לה. לבסוף נכנֶה חבורה G **פשוטה** (simple) אם אין לה שום חבורה חלקית נורמלית פרט ל E ולעצמה. לדֻגמה, כל חבורה מסדר ראשוני הנה פשוטה.

למה ו.ג: *התנאים הבאים על סדרה נורמלית* $G=G_0\triangleright G_1\triangleright\cdots\triangleright G_m=E$ *שקולים זה לזה:*

(א) *הסדרה הנה סדרת הרכב.*

(ב) G_{i+1} *נורמלית מרבית ב* G_i *עבור* $i=1,\ldots,m$.

(ג) G_i/G_{i+1} *היא חבורה פשוטה לא טריביאלית.*

הוכחה: יש להשתמש במשפט האיזומורפיזם השלישי. ∎

משפט ו.ד (Jordan-Hölder): *אם לחבורה G יש סדרת הרכֵּב, אזי כל שתי סדרות הרכב של G שקולות זו לזו.*

אם $G_0 \rhd G_1 \rhd \cdots \rhd G_m = E$ היא סדרת הרכב של G, אזי לפי משפט ז'ורדן־הלדר הגורמים G_i/G_{i+1} נקבעים עדי כדי איזומורפיזם ועד כדי סדר. הם נקראים **גורמי ההרכב** (composition factors) של G.

אנדוקציה על הסדר מראה שלכל חבורה סופית יש סדרת הרכב. לכן, לכל חבורה סופית יש גורמי הרכב מֻגדרים היטב. מצד שני, כל תת חבורה לא טריביאלית של $\mathbb{Z}$ הנה מהצורה $n\mathbb{Z}$ עבור מספר טבעי. היא מקיפה ממש את תת החבורה $2n\mathbb{Z}$. לכן, אין ל $\mathbb{Z}$ סדרת הרכב.

ז. חבורות פתירות

המושג של "חבורה פתירה" קשור לבעית פתירת משוואות בנעלם אחד מעל שדה בעזרת ארבעת פעֻלות החשבון והוצאות שרש. לפי משפט של גלואה, יש למשוואה פתרון כנ"ל אם ורק אם חבורת גלואה של המשוואה הנה "פתירה".

חבורה G תכֻנה **פתירה** (solvable) אם יש לה סדרה נורמלית שכל גורמיה חלופיים, כלומר אם קיֶמת סדרה מהצורה $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = E$ כך ש G_i/G_{i+1} חלופיים. בפרט, כל חבורה חלופית הנה פתירה.

נתבונן בשני אברים a ו b של חבורה G. נשים לב לכך ש $ab = ba$ אם ורק אם $a^{-1}b^{-1}ab = e$. באפן כללי נסמן

$$[a,b] = a^{-1}b^{-1}ab$$

ונקרא ל $[a,b]$ **המַחְלִיפָן** (commutator) של a ו b. כדי לסלק את חסר החִלופיות בחבורה עלינה לזהות את כל המחליפנים עם אבר היחידה. זאת נעשה באפן הבא:

נקרא לתת חבורה של G הנוצרת על ידי כל המחליפנים **חבורת המחליפן** של G. חבורה זו מסֻמנת ב G' (או גם ב $[G,G]$):

$$G' = \langle [a,b] \mid \ a,b \in G \rangle$$

אם α הנו אנדומורפיזם של G, אזי $\alpha[a,b] = [\alpha(a), \alpha(b)]$. בפרט נכונה נֻסחה זו עבור אוטומורפיזמים פנימיים. מכאן נובע ש G' נורמלית ב G. מההגדרה נובע שחבורת המנה G/G' חִלופית. יתר על כן, G' היא החבורה הנורמלית הקטנה ביותר של G עם מנה חלופית:

למה ז.א: *תהי H תת חבורה נורמלית של G. אזי G/H חלופית אם ורק אם H $G' \leq$.*

נגדיר את **חבורת המחליפן,** G^n, מסדר n של G באנדוקציה: $G^0 = G$, $G^{(1)} = G'$ ו $G^{(n+1)} = (G^{(n)})'$. סדרת המחליפנים $G \triangleright G^{(1)} \triangleright G^{(2)} \triangleright \cdots$ היא בודאי סדרה נורמלית שכל גורמיה חלופיים.

משפטון ז.ב: *G פתירה אם ורק אם קיָם n טבעי כך ש $G^{(n)} = E$.*

הוכחה: אם $G^{(n)} = E$, בודאי ש G פתירה. נניח אפוא ש $G = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_n \triangleright E$ היא סדרה נורמלית שגורמיה חלופיים. בפרט G/H_1 חלופית. לפי למה ז.א, $G' \leq H_1$. שוב, H_1/H_2 חלופית ולכן $H_1' \leq H_2$. לכן, $G'' \leq H_1' \leq H_2$. באנדוקציה מראים ש $G^{(n)} \leq H_n = E$. לכן, $G^{(n)} = E$. ∎

מהפתירות של חבורות מסֻימות אפשר ללמֹד על הפתירות של חבורות אחרות:

משפטון ז.ג: *תהי G חבורה.*

(א) *אם G פתירה, אזי כל חבורה חלקית של G וכל חבורת מנה של G פתירה.*

(ב) *אם $G \triangleleft N$ ואם N ו G/N פתירות, אזי גם G פתירה.*

(ג) אם $M, N \lhd G$ ואם G/M ו G/N פתירות, אזי גם $G/M \cap N$ פתירות. ∎

נזכיר כאן את המשפט הבא של Feit *ו* Thompson *שהוכיחו ב 1962 את המשפט הבא על פני 250 עמודים:*

משפט ז.ד: *כל חבורה סופית בעלת סדר אי זוגי פתירה.*

ח. חבורות סימטריות וחבורות חִלופין

חבורת התמורות S_n של הקבוצה $\{1,2,\ldots,n\}$ נקראת **חבורת הסימטריה** ממעלה n. חבורות חלקיות של S_n מופיעות כחבורות גלואה של פולינומים ממעלה n. בסעיף זה נלמד את תכונותיה הבסיסיות של החבורה S_n.

אבר π של S_n ירשֵם גם בצורה

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ 1^\pi & 2^\pi & \cdots & n^\pi \end{pmatrix}$$

אנו רואים את אברי S_n כפועלים מימין על הקבוצה $\{1,2,\ldots,n\}$, כמעריכים: התמונה של מספר i תחת π הנה תחת הסכם זה i^π. נדגים הסכם זה על ידי המכפלה הבאה:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix}=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \end{pmatrix}$$

אם $a_1,\ldots,a_m$ הם אברים שונים של הקבוצה $\{1,2,\ldots,n\}$, אזי ב $(a_1\,\cdots\,a_m)$ נסמן את התמורה π המֻגדרת באפן הבא: $a_i^\pi=a_{i+1}$, עבור $i=1,\ldots,m-1$, $a_m^\pi=a_1$ ו $a^\pi=a$ לכל $a\neq a_1,\ldots,a_m$. לתמורה זו נקרא **חִשוּק** (cycle) מארך m. לחשוק מארך 2 נקרא **חִלּוּף** (trasposition). חשוק מארך 1 הוא תמורת הזהות.

הבחירה שלנו לכתב את הפעֻלה של אברי S_n על המספרים כהעלאות בחזקה משתלבת יפה עם פעֻלת ההצמדה בחבורה S_n:

$$(a_1\,\cdots\,a_m)^\pi=(a_1^\pi\,\cdots\,a_m^\pi)$$

.

שני חשוקים $(a_1\,\cdots\,a_k)$ ו $(b_1\,\cdots\,b_m)$ **זרים זה לזה** אם $a_i\neq b_j$ לכל i ו j. חשוקים כאלו מתחלפים זה עם זה בכפל.

למה ח.א: *כל תמורה ב S_n נתנת להצגה כמכפלה של חשוקים זרים זה לזה. מכפלה זו היא יחידה עד כדי סדר הגורמים וגורמים טריביאליים מהצורה (a).*

למה ח.ב: *כל תמורה ב S_n הנה מכפלה של חלופים.*

הוכחה: מלמה ח.ב נובע שמספיק להוכיח שכל חשוק נתן להציג כמכפלה של חשוקונים. ואכן,

$$.(a_1\,\cdots\,a_m)=(a_1\,a_2)(a_1\,a_3)\cdots(a_1\,a_m)$$

נשים לב לכך שמספר החלופים המופיע באגף ימין של הזהות שוה ל $m-1$. בפרט מספר זה זוגי אם m אי זוגי והוא אי זוגי אם m זוגי. ∎

לכל תמורה π נסמן ב $p(\pi)$ את מספר הזוגות (i,j) המקימים $i^\pi>j^\pi$ ו $1\leq i<j\leq n$. התמורה π תקרֵא **זוגית** אם **אי זוגית** בהתאם לכך אם $p(\pi)$ זוגי או אי זוגי. נסמן $\mathrm{Sgn}(\pi)=(-1)^{p(\pi)}$.

למה ח.ג: $\mathrm{Sgn}(\pi\tau) = \mathrm{Sgn}(\pi) \cdot \mathrm{Sgn}(\tau)$ *לכל* $\pi, \tau \in S_n$.

הוכחה: אפשר להוכיח את הלמה באופן ישיר מההגדרה בעזרת קומבינטוריקה מסֻמּת. ההוכחה שנביא כאן יותר נאה אם כי היא משתמשת בחמר החורג במקצת מתורת החבורות.

יהיו $X_1, \dots, X_n$ משתנים. לכל $\pi \in S_n$ נתבונת בתמורה

$$X_i \mapsto X_{i^\pi}, \qquad i = 1, \dots, n$$

של משתנים אלו. נִתן להרחיב תמורה זו באפן יחיד לאוטומורפיזם של חוג הפולינומים $\mathbb{Z}[X_1, \dots, X_n]$. בפרט מתקיֵם $a^\pi = a$ לכל $a \in \mathbb{Z}$ ו $(f(\mathbf{X})g(\mathbf{X}))^\pi = f(\mathbf{X})^\pi g(\mathbf{X})^\pi$ עבור $f, g \in \mathbb{Z}[\mathbf{X}]$. נסמן

$$\Delta = \prod_{i<j}(X_i - X_j).$$

מההגדרה נובע ש $\Delta^\pi = \mathrm{Sgn}(\pi)\Delta$. לכן,

$$\Delta^{\tau\pi} = (\mathrm{Sgn}(\tau)\Delta)^\pi = \mathrm{Sgn}(\tau)\Delta^\pi = \mathrm{Sgn}(\tau)\mathrm{Sgn}(\pi)\Delta \tag{1a}$$

$$\Delta^{\tau\pi} = \mathrm{Sgn}(\tau\pi)\Delta \tag{1b}$$

השואת $(1a)$ ו $(1b)$ נותנת את הנֻסחה המבֻקשת. ∎

למה ח.ב אומרת שכל תמורה π נתנת להצגה כמכפלה של חִלופים. חִלוף הנו תמורה אי זוגית. מלמה ח.ג נובע אפוא ש π הוא תמורה זוגית כאשר מספר החשוקים המופיעים במכפלה הנ"ל זוגי. ההצגה של תמורה כמכפלה של חִלופים אינה יחידה אולם זוגיות מספר החִלופים במכפלה נקבעת באפן יחיד על ידי התמורה.

למה ח.ג אומרת גם שההעתקה $\pi \mapsto \mathrm{Sgn}(\pi)$ הוא אפימורפיזם של S_n על החבורה הכפלית $\{\pm 1\}$ בת שני אברים. גרעין העתקה זו הוא קבוצת כל התמורות הזוגיות. נסמנו ב A_n. זהו חבורה נורמלית ב S_n בעלת אנדקס 2 הנקראת **חבורת החִלופין** (alternative). חבורה זו מכילה בין היתר את כל החשוקים מארך 3. הלמה הבאה מקבילה ללמה ח.א ואומרת שהחשוקים מארך 3 יוצרים את A_n.

למה ח.ד: *כל תמורה זוגית ב* S_n *נתנת להצגה כמכפלה של חִלופים מארך* 3.

הוכחה: מספיק להוכיח שכל מכפלה של שני חִלופים נתנת להצגה כמכפלה של חשוקים מארך 3. ואכן, כל המקרים האפשריים מתמצים בשלש הדֻגמאות הבאות:

$$(1\,2)(1\,2) = (1)$$

$$(1\,2)(1\,3) = (1\,2\,3)$$

$$(1\,2)(3\,4) = (2\,3\,4)(1\,2\,3)$$

$\blacksquare$

הלמות הבאות יראו ש S_n רחוקה מלהיות חבורה פתירה. סדרת המחליפנים של S_n מסתיֶמת לאחר צעד אחד בלבד ב A_n:

למה ח.ה: *A_n הנה חבורת המחליפן של S_n.*

הוכחה: S_n/A_n בתור חבורה מסדר 2 הנה חלופית. לכן, לפי למה ז.א, $S_n' \leq A_n$. מצד שני, אם i,j,k הם שלשה מספרים שונים זה מזה, אזי

$$(i\,j\,k) = (i\,k)(i\,j)(i\,k)(i\,j).$$

אגף ימין שיך ל S_n'. מלמה ח.ד נובע ש $A_n \leq S_n'$. $\blacksquare$

למה ח.ו: *אם $n \geq 5$, אזי $A_n' = A_n$.*

הוכחה: ראשית נעיר שאם i,j,k,l הם מספרים שונים זה מזה, אזי

$$(i\,j)(k\,l) = (i\,l\,k)(i\,k\,j)(i\,k\,l)(i\,j\,k) \in A_n'$$

עלינו להראות שאם i,j,k הם מספרים שונים זה מזה, אזי $(i\,j\,k) \in A_n'$.

ואכן, מההנחה ש $n \geq 5$ נובע שקיָמים עוד מספרים l ו m שאינם גדולים מ n כך ש i,j,k,l,m שונים זה מזה. ואז $(i\,j\,k) = (j\,k)(i\,j) = (j\,k)(l\,m)\cdot(l\,m)(i\,j) \in A_n'$. $\blacksquare$

תוצאה ח.ז: *אם $n \geq 5$, אזי S_n ו A_n אינן פתירות.*

הוכחה: לפי למה ח.ו $S_n^{(k)} = A^n$ לכל $k \geq 1$. לכן, לפי משפטון ז.ב, S_n ו A_n אינן פתירות.

את התוצאה האחרונה נחַזק באפן נִכּר:

משפט ח.ח: *החבורה A_n פשוטה לכל $n \geq 5$.*

הוכחה: תהי N תת חבורה נורמלית לא טריביאלית של A_n. עלינו להוכיח ש $N = A_n$.

טַעֲנָה: *אם N מכילה חשוק מארך 3, אזי $N = A_n$.* ואכן, נניח בלי הגבלת הכלליות ש N מכילה את החשוק $\tau = (1\,2\,3)$. יהיו i,j,k מספרים שונים זה מזה. מלמה ח.ד נובע שמספיק להראות ש $(i\,j\,k) \in B$. ואכן נתבונן בתמורה

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots \\ i & j & k & l & m & \cdots \end{pmatrix}$$

שבה l ו m הם מספרים שונים זה מזה השונים גם מ i,j,k. בלי הגבלת הכלליות נוכל להניח ש π זוגית, אחרת נחליפה בתמורה

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots \\ i & j & k & l & m & \cdots \end{pmatrix} (l\, m) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots \\ i & j & k & m & l & \cdots \end{pmatrix}$$

שהיא זוגית. ואז $(i\, j\, k) = (1\,2\,3)^{\pi} \in N$, כי $A'_n \triangleleft n$.

שארית ההוכחה מבדילה עתה בין חמִשה מקרים:

מקרה א: *נניח שבין אברי N מצויה תמורה τ אשר בפרוקה למכפלה של חשוקים זרים מצוי חשוק שארכו לפחות 4.* נוכל להניח של τ יש הצורה $\tau = (1\,2\,3\,4\,a_5\ \cdots\ a_s)\kappa$, באשר κ הוא מכפלה של חשוקים הזרים לחשוק הראשון. יהי $\lambda = (1\,2\,3) \in A_n$. הוא מקַים $\tau^{-1}\tau^{\lambda} \in N$ $(1\,2\,4) =$. לכן, לפי הטענה, $N = A_n$.

מקרה ב: *בין אברי N מצויה תמורה τ שבפרוקה למכפלה של חשוקים זרים מופיע בדיוק אחד מארך 3, למשל $(1\,2\,3)$, וכל יתר החשוקים הם חלופים.* אזי, $(1\,3\,2) = (1\,2\,3)^2 = \tau^2$ (כל החלופים מצטמצמים) ולכן, לפי הטענה, $N = A_n$.

מקרה ג: *בין אברי N מצויה תמורה τ שבפרוקה למכפלה של חשוקים זרים מופיעים לפחות שני חשוקים מארך 3.* בלי הגבלת הכלליות $\tau = (1\,2\,3)(4\,5\,6)\kappa$, באשר κ היא מכפלה של חשוקים הזרים לשני החשוקים הראשונים. נסמן $\rho = (3\,4\,5)$. ואז $\tau\tau^{\rho} \in N$ $(1\,4\,3\,2\,6)\cdots =$. ממקרה א נובע ש $N = A_n$.

נותר לנו לטפל במקרים שכל אברי N מתפרקים למכפלה של חלופים. מספר האברים המופיעים בכל מכפלה כזו זוגי.

מקרה ד: *N מכילה אבר מהצורה $\tau = (1\,2)(3\,4)$.* נסמן $\alpha = (5\,2\,1)$ ונקבל $\tau\tau^{\alpha} \in N$ $(1\,2\,5) =$. לכן, לפי הטענה, $N = A_n$.

מקרה ה: *N מכילה אבר מהצורה $\tau = (1\,2)(3\,4)(5\,6)(7\,8)\kappa$, באשר κ הוא מכפלה של מספר זוגי של חלופים זרים של מספרים הגדולים או שוים ל 9.* נסמן $\beta = (2\,3)(4\,5)$. ואז $\tau\tau^{\beta} \in N$ $(1\,5\,4)(2\,3\,6) =$. לכן, לפי מקרה ג, $N = A_n$.

בזאת מִצינו את כל האפשרויות. ∎

בפרט קִבלנו ש A_5 היא חבורה פשוטה. הסדר של A_5 הוא 60. אפשר להוכיח ש A_5 היא החבורה הפשוטה הקטנה ביותר שאינה מעגלית.

ט. פעֻלה של חבורה על קבוצה

החבורה הסימטרית S_n פועלת על הקבוצה $\{1, 2, \ldots, n\}$ באפן כללי **פעֻלה** של חבורה G על קבוצה A היא העתקה $A \times G \to A$ כך שאם נרשׁם ב a^x את התמונה של הזוג (a, x) ($a \in A$ ו $x \in G$) ב A תחת העתקה זו יתקַימו הכללים הבאים:

(1) $a^{xy} = (a^x)^y$ ו $a^e = a$ לכל $x, y \in G$ ו $a \in A$.

כל $x \in G$ משרֶה העתקה $\tau_x \colon A \to A$ הפועלת מימין על אברי A באפן הבא: $a^{\tau_x} = a^x$ מתנאי (א) נובע ש $\tau_{xy} = \tau_x \tau_y$ ו $\tau_e = \mathrm{id}$. בפרט נקבל ש $\tau_x \tau^{x^{-1}} = \tau_{x^{-1}} \tau_x = \mathrm{id}$. לכן τ_x הוא תמורה של A. ההעתקה τ היא אפוא הומומורפיזם של G לתוך חבורת התמורות $S(A)$ של A. אנו אומרים ש τ היא **הצגה של** G **כחבורת תמורות** (permutation representation).

נאמר ש G פועלת על A **באפן נאֱמן** (או גם **נאֱמנה**) (faithfully) אם ההצגת התמורות τ דלעיל היא שכון. כלומר, $a^x = a$ לכל $a \in A$ גורר ש $x = e$.

דֻגמה ט.א:

(א) G פועלת על עצמה על ידי הצמדה. הגרעין של פעֻלה זו הוא המרכָּז של G.

(ב) G פועלת על עצמה על ידי כפל מימין. זוהי פעֻלה נאמנה המשכנת את G לתוך $S(G)$. בפרט, אם הסדר של G הוא n מקבלים בזה שכון של G לתוך S_n. אבחנה זו נקראת משפט Cayley.

(ג) כפל של סקלרים על מרחב וקטורי V אינו אלא פעֻלה נאמנה של החבורה החבורית F^+ של שדה F על V.

(ד) כפל מימין של מטריצות הפיכות מסדר $n \times n$ מעל שדה K על n־יות של אברי K מגדיר פעֻלה נאמנה של $\mathrm{GL}_n(K)$ על K^n.

(ה) אם H היא תת חבורה של חבורה G, אזי G פועלת על קבוצת המחלקות הימניות H/G על ידי כפל מימין. הגרעין של פעֻלה זו הוא $\bigcap_{g \in G} H^g$. ∎

נניח שוב ש G פועלת על קבוצה A ויהי $a \in A$. החבורה $G_a = \{x \in G \mid a^x = a\}$ נקראת **הַמְּשַׁמֵּר** (stabilizer) של a ב G. הנֻסחה הבאה מראה כיצד משתנה המשמֵר תחת הצמדה: $G_{a^y} = (G_a)^x$.

הקבוצה $a^G = \{a^x \mid x \in G\}$ נקראת **המסלול** (orbit) של a תחת G.

דגמה ט.ב:

(א) מעגל היחידה סביב הראשית פועל על $\mathbb{C}$ על ידי כפל מימין. המסלול של כל אבר z של $\mathbb{C}$ הנו מעגל היחידה ברדיוס $|z|$ מסביב לראשית.

(ב) $\mathbb{R}$ פועלת על $\mathbb{C}$ על ידי כפל מימין. המסלול של כל z ב $\mathbb{C}$ הנו הישר העובר דרך z והראשית. ∎

נקבע אבר $a \in A$. ההעתקה $G_a g \mapsto a^g$ מעתיקה את $G_a \backslash G$ באפן חד חד ערכי על G^a. העתקה זו מכבדת גם את הפעֻלה של G על שתי הקבוצות. אם G סופית, אזי

$$(G : G_a) = |a^G|. \tag{2}$$

בפרט הארך של המסלול מחלק את הסדר של החבורה. אם בנוסף לכך, A היא קבוצה סופית, היא מתפרקת למספר סופי של מסלולים זרים: $A = \dot{\bigcup}_{i \in I} a_i^G$. לכן, $|A| = \sum_{i \in I} |a_i^G|$. מ (2) נובע ש

$$|A| = \sum_{i \in I} (G : G_{a_i}). \tag{3}$$

במקרה הפרטי ש G היא חבורה סופית הפועלת על עצמה על ידי הצמדה, המסלולים הם מחלקות צמידות. הנֻסחה (3) מקבלת במקרה זה את הצורה $|G| = \sum_{c \in C} (G : G_c)$, באשר C היא קבוצת מיַצגים של מחלקות הצמידות של G ו $G_c = \{g \in G \mid\ c^g = g\}$. מחלקת צמידות מכילה אבר אחד אם רק אם אבר זה שיך למרכז של G. לכן,

$$|G| = |Z(G)| + \sum_{c \in C'} (G : G_c), \tag{4}$$

באשר C' היא קבוצת מיצגים של מחלקות צמידות של אברים שאינם במרכז G.

י. חבורות סילו

ראינו שאם G היא חבורה מעגלית מסדר n, אזי יש ל G תת חבורה מכל סדר d המחלק את n. לא כך הדבר בחבורות שאינן חלופיות. אולם אם d הנו החזקה הגדולה ביותר של מספר ראשוני המחלקת את n, יש ל G תת חבורה מסדר d. יתר על כן, תת חבורה זו נקבעת באפן יחיד עד כדי הצמדה. המשפטים המטפלים בתכונות אלו הוכחו על ידי המתמטקאי Sylow ונקראים על שמו.

יהיו p מספר ראשוני, G חבורה סופית ו P תת חבורה של G. נקרא ל P **חבורת סילו־**p של G אם $|P|$ הנו החזקה המרבית של p המחלקת את $|G|$. חבורה סופית H תקרא **חבורת־**p אם סדרה הוא חזקה של p. בפרט, כל חבורת סילו־p הנה חבורת־p.

תחילה נוכיח שלכל חבורה סופית G ולכל מספר ראשוני יש ל G חבורת סילו־p.

למה י.א: *תהי G חבורה חלופית סופית. אם p מחלק את $|G|$, אזי קיָם ל G אבר מסדר p.*

הוכחה: נניח בשלילה שאין קים אבר כזה. תהי H תת חבורה של G בעלת סדר מרַבִּי הזר ל p. הואיל ו p מחלק את $|G|$, החבורה H חלקית ממש ל G. נבחר $g \in G \smallsetminus H$. אזי $H < \langle H, g\rangle$ ולכן $p|\#\langle H, g\rangle$. מהחלופיות של G ומלמה ב.ה נובע ש $|\langle H, g\rangle| = |H \cdot \langle g\rangle| = \frac{|H|\cdot|\langle g\rangle|}{|H\cap\langle g\rangle|}$. לכן, $p|\mathrm{ord}(g)$. ∎

תוצאה י.? תכליל את למה י.א לחבורות סופיות כלשהן. לפני שאנו מגיעים לתוצאה הזו, נוכיח את הקיום של חבורות סילו:

משפט י.ב (המשפט הראשון של סילו): *תהי G חבורה סופית ויהי p מספר ראשוני. אזי קיֶמת ל G תת חבורה סילו־p.*

הוכחה: נוכיח את המשפט באנדוקציה על הסדר של G. יהי $|G| = mp^n$ באשר $p \nmid m$. בלי הגבלת הכלליות נוכל להניח ש $n \geq 1$ (אחרת החבורה הטריביאלית היא חבורת סילו־p).

אם קיֶמת ל G תת חבורה נאותה H בעלת אנדקס זר ל p, אזי יש ל H חבורת סילו־p (לפי הנחת האִנדוקציה). תת חבורה זו תהיה גם חבורת סילו־p של G.

נניח אפוא ש $p|(G:H)$ לכל תת חבורה נאותה H של G. בפרט אם $x \notin Z(G)$, אזי $G_x < G$ ולכן, $p|(G:G_x)$. מנֻסחה (4) של סעיף ט,

$$|G| = |Z(G)| + \sum_{x\in C'} (G:G_x) ,$$

נובע ש p מחלק את $|Z(G)|$. למה י.א נותנת תת חבורה A של $Z(G)$ מסדר p. בתור תת חבורה של המרכז, A נורמלית ב G. כמו כן, $|G/A| = mp^{n-1}$. לפי הנחת האנדוקציה קיֶמת ל G/A חבורת סילו־p שנסמנה ב $\bar{P}$. סדרה יהיה כמובן p^{n-1}. תהי P התמונה ההפוכה של $\bar{P}$ ב G תחת העתקת המנה $G/AG \to$. אזי $|P| = p^n$. במלים אחרות, P היא חבורת סילו־p של G. ∎

המשפט הבא נותן מידע על קבוצת חבורות סילו־p של חבורה סופית:

משפט י.ג (המשפט השני של סילו): *תהי G חבורה סופית.*

(א) *כל חבורת־p חלקית H של G מוכלת בחבורת סילו־p של G.*

(ב) *כל חבורת סילו־p של G צמודות זו לזו.*

(ג) *מספר חבורות סילו־p של G חופף ל 1 מודולו p.*

הקדמה להוכחה: נסמן ב S את קבוצת כל חבורות סילו־p של G. לפי משפט סילו הראשון, S אינה ריקה. נִתן ל G לפעל על קבוצה זו על ידי הצמדה. תהי P אחת מחבורות סילו־p. נתבונן במשָׁמֵר $G_P = \{g \in G \mid P^g = P\}$ ובמסלול $P^G = \{P^x \mid x \in G\}$ של P. לפי נֻסחה (2) של סעיף ט, $|P^G| = (G : G_P)$. בנוסף לזה, $P \le G_P$. לכן, $|P^G|$ אינו מתחלק ב p.

תהי עתה H חבורת־p חלקית של G. אזי H פועלת על P^G על ידי הצמדה. P^G מתפרק תחת פעֻלה זו לאחוד של מסלולים זרים: $P^G = \dot\bigcup_{i\in I} P_i^H$. בהתאם לכך,

$$|P^G| = \sum_{i\in I} |P_i^H| = \sum_{i\in I} (H : H_{P_i}). \qquad (1)$$

טענה: *לכל חבורה P' ב P^G שקול השויון $H_{P'} = H$ להכלה $H \le P'$.* ואכן, אם $H \le P'$ אזי $(P')^h = P'$ לכל $h \in H$, כלומר, $H \le P'$.

להפך, אם $(P')^h = P'$, אזי $\langle H, P'\rangle = HP'$. לכן, לפי למה ב.ה, $|\langle H, P'\rangle| = \frac{|H|\cdot|P'|}{|H\cap P'|}$ הוא חזקה של p. הואיל ו P' היא חבורת סילו־p של G, נובע מכאן ש $\langle H, P'\rangle = P'$, בפרט $H \le P'$.

הוכחת (א): הואיל ו H היא חבורת־p, האנדקס $(H : H_{P_i})$ הנו חזקת של p. הואיל ו p אינו מחלק את $|P^G|$ (לפי הפסקה הראשונה של ההוכחה), קיָם, לפי (1), $i \in I$ כך ש $H = H_{P_i}$. מהטענה נובע ש $H \le P_i$, כמבֻקש.

הוכחת (ב): נבחר עתה את H כאחת מחבורות סילו־p של G. בהוכחת (א) הראינו ש H מוכלת בחבורה P_i הצמודה ל P. לפי ההגדרה, $|H| = |P_i|$ ולכן $H = P_i$. במלים אחרות, H צמודה ל P.

הוכחת (ג): נבחר את H כ P. בלי הגבלת הכלליות נוכל להניח שקים $j \in I$ כך ש $P = P_j$. לפי הטענה, $P_{P_i} = P$ אם ורק אם $P_i = P$. במלים אחרות, $(P : P_P) = 1$ ו $(P : P_{P_i})$ מתחלק ב p לכל $i \neq j$. לכן, לפי (1),

$$|P^G| = \sum_{i\in I}(P : P_{P_i}) = 1 + \sum_{i\neq j}(P : P_{P_i}) \equiv 1 \mod p$$

כפי שטָעַנּוּ. ∎

בדֻגמה ה.ב ראינו שהמרכז של S_n טריביאלי. בחבורות p אין הדבר כך:

למה י.ד: *תהי G חבורת־p ותהי N חבורה נורמלית לא טריביאלית של G. אזי החתוך $N \cap Z(G)$ אינו טריביאלי. בפרט המרכז של G אינו טריביאלי.*

הוכחה: נִתן ל G לפעל על N על ידי הצמדה. יהיו $a_1, \ldots, a_r$ מיַצגים של מסלולֵי־G של N, באשר $a_1 = e$. לפי נֻסחה (3) של סעיף ט, $|N| = \sum_{i=1}^r (G : G_{a_i})$, באשר $G_{a_i} = \{g \in G \mid a_i^g = a_i\}$. בפרט $G_{a_1} = G_e = G$ ולכן $(G : G_{a_1}) = 1$. הואיל ו G הנָה חבורת־p, כל אחד מהאנדקסים $(G : G_{a_i}) = p^{k_i}$ הוא חזקה של p. אלו היו k_i גדולים מ 0 עבור, $i = 2, \ldots, r$, היינו מקבלים ש $|N| \equiv 1 \mod p$, בסתירה לכך ש $|N|$ הוא חזקה לא טריביאלית של p. לכן, קים $i \geq 1$ כך ש $(G : G_{a_i}) = 1$, כלומר $G = G_{a_i}$. האבר a_i הנו אבר לא טריביאלי של $N \cap Z(G)$, כמבֻקש. ∎

תוצאה י.ה (משפט קושי): *אם p מחלק את הסדר של חבורה G, אזי יש ב G אבר x מסדר p.*

הוכחה: המשפט הראשון של סילו נותן ל G חבורת סילו לא טריביאלית P. לפי משפט י.ד, $Z(P)$ אינו טריביאלי. הואיל ו $Z(P)$ היא חבורת־p חלופית, יש לה לפי למה י.א, אבר x מסדר p. ∎

תוצאה י.ו: *תהי G חבורת־p לא טריביאלית. אזי קַיֶמת לה סדרה נורמלית $G = G_n \triangleright G_n \triangleright G_{n-1} \triangleright \cdots \triangleright G_0 = E$ שכל גורמיה מעגליים מסדר p. יתר על כן, $G_i/G_{i-1} \leq Z(G/G_{i-1})$ לכל $i = 1, \ldots, n$.*

תוצאה י.ז: *כל חבורה מסדר p^2 הנה חלופית.*

הוכחה: תהי P חבורה מסדר p^2. מספיק להתבונן במקרה ש P אינה מעגלית. במקרה זה הסדר של כל אבר השונה מ e הוא p. נבחר אבר a שונה מ e ב $Z(P)$ (משפט י.ד). ונבחר $b \in G \smallsetminus P$. אזי $G = \langle a, b \rangle$ ו $ab = ba$. לכן, P חלופית. ∎

תוצאה י.ח: *יהיו p ו q מספרים ראשוניים. אזי כל חבורה G מסדר pq פתירה.*

הוכחה: מתוצאה י.ז נובע שמספיק לדון במקרה שבו $p < q$. נבחר ל G חבורת סילו־q Q. נסמן $N = N_G(Q)$. לפי המשפט השני של סילו, $(G : Q) \equiv 1 \mod q$. הואיל ו $|G| = pq$, מתקיֵם $|Q| = q$ ו $(G : N)$ הנו p או 1. המקרה השני אינו אפשרי כי אז $p \equiv 1 \mod q$, בסתירה ל $p < q$. במקרה הראשון, $G = N$, $Q \triangleleft G$, $Q \cong \mathbb{Z}/q\mathbb{Z}$ ו $G/Q \cong \mathbb{Z}/p\mathbb{Z}$. לכן, G פתירה. ∎

לחבורות סילו־p יש חשיבות גדולה בנתוח המבנה של חבורות סופיות. כדי לעשות אותן למכשיר עוד יותר יעיל נתאר את הקשר בין חבורות סילו־p של חבורה לבין חבורות סילו־p של חבורות חלקיות וחבורות מנה:

משפטון י.ט: *תהי N חבורה חלקית נורמלית של חבורה סופית G ותהי P חבורת סילו־p של G. אזי:*

(א) *$N \cap P$ היא חבורת סילו־p של N.*

(ב) *PN/N היא חבורת סילו־p של G/N.*

(ג) $N_G(P)N/N = N_{G/N}(PN/N)$.

הוכחת (א): קודם כל נשים לב ש $P \cap N$ היא חבורה חלקית של N שסדרה חזקה של p. ממשפט האיזומורפיזם השני נובע ש $(PN : P) = (N : P \cap N)$ זר ל p. לכן, $P \cap N$ הוא חבורת סילו־p של N.

הוכחת (ב): נסמן את המנה של חבורות מודולו N בגג. לפי משפט האיזומורפיזם השלישי, $(\bar{G} : \bar{P}) = (G : P)$ זר ל p. לכן, $\bar{P}$ הוא חבורת סילו־p של $\bar{G}$.

הוכחת (ג): מספיק להוכיח ש $\overline{N_G(P)} \le N_{\bar{G}}(\bar{P})$. לשם כך נתבונן באבר $g \in G$ כך ש $\bar{g} \in N_{\bar{G}}(\bar{P})$. כלומר, $\bar{P}^{\bar{g}} = \bar{P}$, או $P^g N = PN$. מכאן ש P^g הוא חבורת סילו־p של PN. לפי המשפט השני של סילו, קַיָם $n \in N$ כך ש $P^g = P^n$. לכן, $gn^{-1} \in N_G(P)$. מכאן ש $g \in N_G(P)n \le N_G(P)N$ ולכן, $\bar{g} \in \overline{N_G(P)}$. ∎

בעזרת שקולים דומים לאלו שהופיעו בהוכחת תוצאה י.ח (אם כי הרבה יותר מֻרכבים) אפשר להוכיח את המשפט הבא:

משפט י.י: *יהיו p, q, r מספרים ראשוניים. אזי:*

(א) *כל חבורה מסדר $p^n q$ פתירה.*

(ב) *כל חבורה מסדר $p^2 q^2$ פתירה.*

(ג) *אם $p > q > r$, אזי כל חבורה מסדר pqr פתירה.*

אפשר להשתמש במשפט י.י ושקולים נוספים כדי להוכיח:

משפט י.יא:

(א) *כל חבורה שסדרה קטן מ 60 פתירה.*

(ב) *החבורה הפשוטה היחידה (עד כדי איזומורפיזם) מסדר 60 היא A_5.*

יא. חבורות־p

מחוץ לחבורות החלופיות, חבורות־p הן החבורות המֻכרות ביותר. בסעיף הקודם הוכחנו כמה תכונות של חבורות אלו. בסעיף זה נוסיף כמה תוצאות על אלו שהשגנו בסעיף הקודם.

למה יא.א: *חבורה סופית G היא חבורת־p אם ורק אם הסדר של כל אבר בה הנו חזקה של p.*

הוכחה: הלמה נובע ממשפט לגרנז' וממשפט קושי. ∎

למה יא.ב:

(א) *חבורה חלקית של חבורת־p היא חבורת־p.*

(ב) *חבורת מנה של חבורת־p היא חבורת־p.*

(ג) *תהי N תת חבורה נורמלית של חבורה סופית G. נניח ש N וש G/N הן חבורות־p. אזי, G היא חבורת־p.*

בסעיף י הוכחנו שהמרכז של חבורת־p לא טריביאלית אינו טריביאלי. המשפט הבא יכליל תוצאה זו.

למה יא.ד: *תהי G חבורת p סופית ותהי U תת חבורה נאותה של G. אזי $U < N_G(U)$.*

הוכחה: לפי למה ה.א נתן להציג את G כאחוד זר $G = \dot\bigcup_{i=1}^r Ug_iU$, באשר $g_1, \ldots, g_r$ הם אברים של G ו $g_1 = e$. בפרט, $g_i \notin U$ עבור $i = 2, \ldots, r$. יתר על כן, לפי למה ה.ב,

$$|G| = \sum_{i=1}^r \frac{|U| \cdot |U|}{|U^{g_i} \cap U|}. \qquad (1)$$

לפי ההנחה $|G| = p^n$ ו $|U| = p^m$ באשר $m < n$. לכן, לפי (1),

$$p^{n-m} = 1 + \sum_{i=1}^r \frac{|U|}{|U^{g_i} \cap U|}. \qquad (2)$$

אלו היה $U^{g_i} \neq U$ לכל $2 \leq i \leq r$, היינו מקבלים שהמספרים $\frac{|U|}{|U^{g_i} \cap U|}$ הם חזקות שונות מ 1 של p, בסתירה ל (2). לכן קיָם $2 \leq j \leq r$ כך ש $U^{g_j} = U$. כלומר, $g_j \in N_G(U) \smallsetminus U$, כמבֻקש. ∎

חבורה חלקית H של חבורה G מכֻנה **מרבית**, אם $H < G$ ואם אין קיֶמת שום תת חבורה $H < K < G$.

למה יא.ה: *תהי G חבורת־p.*

(א) *אזי כל תת חבורה מרבית H של G הנה נורמלית ובעלת האנדקס p.*

(ב) *לכל תת חבורה נאותה U קיֶמת סדרה נורמלית $U = N_0 \lhd N_1 \lhd \cdots \lhd N_r = G$ כך ש $N_i/N_{i-1} \cong \mathbb{Z}/p\mathbb{Z}$.*

(ג) *קיֶמת ל G סדרה נורמלית עולה שכל גורמיה מעגליים מסדר p. בפרט, G פתירה.*

הוכחה: הטענות (א) ו (ב) נובעות מטענה (ב). כדי להוכיח את (ב) נסמן $|G| = p^n$ ו $|U| = p^m$. אזי $m < n$. לפי למה יא.ד החבורה $N_G(U)$ מקיפה ממש את U. לפי משפט קושי, קים ל $N_G(U)/N$ תת חבורה M_1 מסדר

p. נסמן ב N_1 את תת החבורה של N המקיפה את U כך ש $N_1/U = M_1$. אזי $U \triangleleft N_1$ ו N_1/U היא חבורה מעגלית מסדר p. הנחת אנדוקציה על האנדקס נותנת סדרה נורמלית $N_1 \triangleleft N_2 \triangleleft \cdots \triangleleft N_r = G$ שכל גורמיה מעגליים מסדר p. ∎

דֻגמה יא.ו: חבורת הָאַרְבָּעוֹן וחבורת הַשְּׁנִיּוֹן. נראה שיש בדיוק שתי חבורות לא אבליות מסדר 8 ונתאר את המבנה שלהן.

תהי G חבורה לא אבלית מסדר 8. בפרט הסדר של שום אבר של G אינו 8. לכן קיָם ל G אבר a מסדר 4 (אחרת היה $g^2 = 1$ לכל $g \in G$ ו G היְתה אבלית). בפרט $\langle a \rangle \triangleleft G$. נבחר $b \in G \smallsetminus \langle a \rangle$. אזי $G = \langle a, b \rangle$ ו $b^2 \in \langle a \rangle$. ולכן, $G = \langle a \rangle \cup \langle a \rangle b = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$. הואיל ו $G \triangleleft \langle a \rangle$, a^b יוצר את $\langle a \rangle$, לכן, $a^b = a$ או $a^b = a^3$. המקרה הראשון לא יתכן כי G אינה אבלית. לכן, $a^b = a^3$.

כמו כן, b^2 הנו חזקה של a. לא יתכן ש $b^2 = a$ או $b^2 = a^3$ כי בכל אחד מהמקרים היה $\mathrm{ord}(b) = 8$ ו $G = \langle b \rangle$. לכן, $b^2 = a^2$ או $b^2 = 1$.

מקרה א: $b^2 = a^2$. במקרה זה $G = \langle a, b \mid a^4 = b^4,\ a^b = a^{-1} \rangle$, החבורה G מסֻמנת ב Q_8 ונקראת **חבורת הארבעון** (quaternion group). נסמן $i = a$, $j = b$, $k = ab$ ו $i^2 = -1$. אזי $ij = k$, $jk = i$, $ki = j$, $i^2 = j^2 = k^2 = -1$, ו $(-1)^2 = 1$. ו $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$. תרשים החבורות החלקיות של Q_8 נראה כך:

$$\begin{tikzcd}[column sep=small]
 & Q_8 \arrow[dl, no head] \arrow[d, no head] \arrow[dr, no head] & \\
\langle i \rangle \arrow[dr, no head] & \langle j \rangle \arrow[d, no head] & \langle k \rangle \arrow[dl, no head] \\
 & \langle -1 \rangle \arrow[d, no head] & \\
 & 1 &
\end{tikzcd}$$

המרכז של Q_8 הנו החבורה $\langle -1 \rangle$ וכל תת חבורה של Q_8 נורמלית למרות ש Q_8 אינה אבלית.

מקרה ב: $b^2 = 1$. במקרה זה מסֻמנת החבורה G ב D_8 ונקראת **חבורת השניון** (dihedral group). הצגה שלה בעזרת יוצרים ויחסים: $D_8 = \langle a, b \mid a^4 = b^2 = 1,\ a^b = a^{-1} \rangle$. הצגה חלקית של שריג החבורות

החלקיות של D_8:

$$\begin{tikzcd}[arrows=dash]
\langle a \rangle \arrow[r] \arrow[d] & D_8 \arrow[d] \\
\langle a^2 \rangle \arrow[r] \arrow[d] & \langle a^2, b \rangle \arrow[d] \\
1 \arrow[r] & \langle b \rangle
\end{tikzcd}$$

האנדקסים בין שתי חבורות סמוכות בתרשים זה הם 2. החבורה $\langle b \rangle$ מסדר 2 אינה נורמלית ב D_8. המרכז של D_8 הנו $\langle a^2 \rangle$. ∎

יב. מַכְפֵּלוֹת יְשָׁרוֹת

אחת מהדרכים הפשוטות ביותר ליצר חבורה חדשה מחבורות נתונות היא לבנות את המכפלה הישרה שלהן.

תהיינה $G_1, \ldots, G_n$ חבורות. נהפך את המכפלה הקרטזית שלהן

$$G = \prod_{i=1}^{n} G_i = \{(x_1, \ldots, x_n) \mid x_i \in G_i,\ i = 1, \ldots, n\}$$

לחבורה על ידי שנגדיר כפל לפי מרכיבים:

$$(x_1, \ldots, x_n) \cdot (x'_1, \ldots, x'_n) = (x_1x'_1, \ldots, x_nx'_n)$$

אבר היחידה ב G הוא $(e_1, \ldots, e_n)$, באשר e_i הנו אבר היחידה בחבורה G_i. G תקרא **המכפלה הישרה** (direct product) של החבורות $G_1, \ldots, G_n$. את כל אחת מהחבורות G_i נתן לשכן באפן טבעי ב G על ידי ההגדרה

$$x_i \mapsto (e_1, \ldots, e_{i-1}, x_i, e_{i+1}, \ldots, e_n), \qquad x_i \in G_i$$

נסמן את התמונה של G_i תחת העתקה זו ב G_i^*. קל לודֵא את הטענות הבאות:

$(1a)$ $G = G_1^* \cdots G_n^*$.

$(1b)$ $G_i^* \lhd G$ לכל $1 \le i \le n$.

$(1c)$ $G_i^* \cap (G_1^* \cdots G_{i-1}^* G_{i+1}^* \cdots G_n^*) = E$ לכל $1 \le i \le n$.

$(1d)$ $xy = yx$ לכל $x \in G_i^*$ ו $y \in G_j^*$ אם $i \ne j$.

$(1e)$ אם $y_1 \cdots y_n = x_1 \cdots x_n$ ואם $x_i, y_i \in G_i^*$, אזי $x_i = y_i$ לכל i.

למה יב.א: *תהיינה $G_1, \ldots, G_n$ חבורות חלקיות של חבורה G. התנאים הבאים שקולים זה לזה:*

(א) *קיָם איזומורפיזם $\alpha\colon G \to \prod_{i=1}^{n} G_i$ המעביר את G_i על G_i^*.*

(ב) *(ב.א)* $G = G_1 \cdots G_n$;

(ב.ב) אם $i \ne j$*, אזי* $xy = yx$ *לכל* $x \in G_i$ *ו* $y \in G_j$;

(ב.ג) אם $x_1 \cdots x_n = y_1 \cdots y_n$ *ואם* $x_i, y_i \in G$ *לכל* i*, אזי* $x_i = y_i$ *לכל* i.

(ג) *(ג.א)* $G = G_1 \cdots G_n$;

(ג.ב) $G \lhd G_i$ *לכל* i;

(ג.ג) $G_i \cap (G_1 \cdots G_{i-1} G_{i+1} \cdots G_n) = E$.

אם התנאים של המשפט מתקיְמים, אומרים ש G היא **המכפלה הישרה של** $G_1, \ldots, G_n$. לפעמים, כאשר רוצים להבדיל בין שני סוגי המכפלות הישרות שהוגדרו כאן, קוראים לראשונה **מכפלה ישרה חיצונית** ולשניה **מכפלה ישרה פנימית.** בדרך כלל אין עושים את ההבדלה הזו.

אם החבורה G היא חלופית ופעֻלתה נכתב כחבור, קוראים למכפלה הישרה, **סכום ישר** וכותבים אותה כ $\bigoplus_{i=1}^n G_i$.

דֻגמה יב.ב: (א) נכפיל את החבורה המעגלית $\{1,-1\}$ בעצמה:

$$\{1,-1\}\times\{1,-1\}=\{(1,1),(1,-1),(-1,-1),(-1,-1)\}.$$

בחבורה זו ארבעה אברים. הסדר של כל אבר השונה מהיחידה הוא 2. בפרט, חבורה זו אינה מעגלית.

(ב) נסמן את החבורה המעגלית מסדר m ב C_n. אם m זר ל n $C_m\times C_n\cong C_{mn}$. אם a יוצר את C_m ו b יוצר את C_n, אזי (a,b) יוצר את $C_m\times C_n$.

(ג) יהי a יוצר של C_{mn}, באשר m ו n זרים זה לזה. אזי $\mathrm{ord}(a^m)=n$ ו $\mathrm{ord}(a^n)=m$ ו $C_{mn}=\langle a^m\rangle\times\langle a^n\rangle$.

(ד) יהי p מספר ראשוני. אזי C_{p^n} אינה נתנת לפרוק לא טריביאלי למכפלה ישרה של שתי חבורות. זוהי חבורה **אי פריקה**. ואכן, אם c יוצר של C_{p^n}, ו $m\le n$, אזי תת החבורה היחידה של C_{p^k} מסדר p^m היא $\langle c^{p^{n-m}}\rangle$. לכן, בהנתן שתי תת חבורות של C_{p^n} מוכלת תמיד אחת מהן באחרת.

(ה) החבורה $\mathbb{Z}$ אינה פריקה. ואכן, החתוך של כל שתי תת חבורות של $\mathbb{Z}$ אינו טריביאלי. ∎

למה יב.ג: *אם $G_1,\ldots,G_n$ הן חבורות סופיות, אזי* $|\prod_{i=1}^n G_i|=\prod_{i=1}^n |G_i|$.

למה יב.ד: *אם $H_i\lhd G_i$ עבור $i=1,\ldots,n$, אזי* $\prod_{i=1}^n G_i/\prod_{i=1}^n H_i\cong\prod_{i=1}^n G_i/H_i$.

למה יב.ה: *תהיינה G ו H חבורות. ההטלה $G\times H\to H$ המֻגדרת על ידי $(g,h)\mapsto h$ היא אפימורפיזם שגרעינו G. אפימורפיזם זה משרה אפוא איזומורפיזם $(G\times H)/G\cong H$.*

למה יב.ו: *תהיינה $G_1,\ldots,G_n$ חבורות חלקיות נורמליות של חבורה סופית G. נניח ש $\gcd(|G_i|,|G_j|)=1$ לכל i ו j השונים זה מזה ו $|G|=\prod_{i=1}^n |G_i|$. אזי:*

(א) $G=\prod_{i=1}^n G_i$.

(ב) $\mathrm{Aut}(G)\cong\prod_{i=1}^n \mathrm{Aut}(G_i)$.

הוכחת (א): טענה א נובעת מלמה יב.א ולמה יב.ג.

הוכחת (ב): יהי $\alpha\in\mathrm{Aut}(G)$. אזי $|\alpha(G_i)|=|G_i|$ ולכן, מהנחת הזרות נובע ש $\pi_i(\alpha(G_i))\le G_i$ (באשר π_i הוא ההטלה כל הקואורדינטה ה i־ית). משויון העָצְמות נובע ש $\alpha(G_i)=G_i$. ההעתקה $\alpha\mapsto(\alpha|_{G_1},\ldots,\alpha|_{G_n})$ היא האיזומורפיזם המבֻקש. ∎

למה יב.ז: *אם $G=\prod_{i=1}^n G_i$, אזי* $Z(G)=\prod_{i=1}^n Z(G_i)$.

יג. חֲבוּרוֹת חִלּוּפִיּוֹת

כאשר דנים בחבורות חלופיות נֹח להחליף את הכתיב הכפלי בכתיב חבורי ולסמן את פעֻלת החבורה ב $+$. אבר היחידה וכמוהו גם החבורה הטריביאלית יסֻמנו ב 0 ויִקראו **אבר האפס** ו**חבורת האפס** בהתאמה.

חבורה חלופית A תקרא **חבורת פִּתּוּל** אם הסדר של כל אחד מאבריה סופי. נאמר ש A **חַסְרַת פִּתּוּל** אם הסדר של כל אחד מאבריה השונים מאפס הוא אינסוף. נסמן ב A_{tor} את קבוצת כל אברי A בעלי סדר סופי. A_{tor} היא חבורת פתול ו A/A_{tor} היא חבורה חסרת פתול. לכל מספר טבעי n נסמן $A_n = \{a \in A \mid na = 0\}$ ולכל מספר ראשוני p נסמן $A_{p^\infty} = \bigcup_{i=1}^\infty A_{p^i}$.

את מושג אי התלות הלינארית של וקטורים במרחב וקטורי מעל שדה אפשר להעתיק לחבורות אבליות: נאמר שקבוצת אברים $a_1, \dots, a_k$ של A **אינה תלויה לינארית** אם $n_1a_1 + \cdots + n_ka_k \neq 0$ לכל k־יה $(n_1, \dots, n_k)$ שונה מאפס של מספרים שלמים. נאמר שהאבר b של A **תלוי לינארית** ב $a_1, \dots, a_k$ אם קיָם מספר שלם m שונה מאפס וקיָמים מספרים שלמים $n_1, \dots, n_k$ כך ש $mb = n_1a_1 + \cdots + n_ka_k$. שים לב לכך שכל אבר מסדר סופי של A תלוי לינארית בכל קבוצה אברים של A.

נאמר ששתי קבוצות $a_1, \dots, a_k$ ו $b_1, \dots, b_l$ **שקולות לינארית** אם כל אחד מהאברים בקבוצה האחת תלוי לינארית בקבוצה האחרת. קל לראות שיַחס השקילות הלינארית הנו יחס שקילות.

למה יג.א (משפט ההחלפה של שטייניץ): *תהיינה $a_1, \dots, a_k$ ו $b_1, \dots, b_l$ שתי קבוצות אברים של חבורה חלופית A. נניח שהקבוצה הראשונה אינה תלויה לינארית וכל אחד מהאברים בה תלוי לינארית בקבוצה השניה. אזי $k \le l$ ואפשר להחליף k אברים של הקבוצה השניה באברי הקבוצה הראשונה כך שהקבוצה המתקבלת תהיה שקולה לשניה.*

הוכחה: אנדוקציה על k נותנת ש $k-1 \le l$ ושאפשר להחליף $k-1$ מה b_j־ים ב $a_1, \dots, a_{k-1}$ כך שהקבוצה המתקבלת לאחר ההחלפה שקולה לינארית לקבוצה המקורית. על ידי מספור מחֻדש של ה b_j־ים נתן להניח שהקבוצה $a_1, \dots, a_{k-1}, b_k, \dots, b_l$ שקולה לינארית לקבוצה $b_1, \dots, b_l$. לפי ההנחה קיָמים $m_1, \dots, m_k, n_k, \dots, n_l$ שלמים כך ש $m_k \neq 0$ ו $m_ka_k = m_1a_1 + \cdots + m_{k-1}a_{k-1} + n_kb_k + \cdots + n_lb_l$. לא יתכן ש $l = k-1$ או ש $k \le l$ ו $n_k = \cdots = n_l = 0$, כי $a_1, \dots, a_k$ אינם תלויים לינארית. לכן $k \le l$. כמו כן, נוכל להניח ש $n_k \neq 0$. אזי $a_1, \dots, a_k, n_{k+1}, \dots, n_l$ שקולה לינארית ל $a_1, \dots, a_{k-1}, b_k, \dots, b_l$ ולכן ל $b_1, \dots, b_l$.

∎

מסקנה יג.ב: *אם שתי קבוצות לא תלויות לינארית של חבורה אבלית A שקולות לינארית, אזי יש להן אותו מספר אברים.*

הַדַּרְגָּה (rank) של חבורה אבלית A היא המספר של האברים בקבוצה המֵרַבִּית ב A שאינה תלויה לינארית. ממסקנה יג.ב נובע שמספר זה אינו תלוי בקבוצה המרבית אלא בחבורה. מההגדרה נובע שאם $A_0 \le A$, אזי $\mathrm{rank}(A_0) \le \mathrm{rank}(A)$. כמו כן נובע ממשפט ההחלפה של שטייניץ שאם A נוצרת על ידי n אברים, אזי $\mathrm{rank}(A) \le n$.

יד. חֲבוּרוֹת חִלּוּפִיּוֹת נוֹצָרוֹת סוֹפִית

בסעיף זה נחקר את המבנה של חבורות אבליות נוצרות סופית. נוכיח שכל חבורה כזו נתנת להצגה כסכום ישר של חבורות־p מעגליות נוצרות סופית ומספר עֻתקים של $\mathbb{Z}$ והצגה זו יחידה, עד כדי איזומורפיזם.

למה יד.א: *אם חבורה אבלית A נוצרת סופית, אזי דרגתה סופית.*

הוכחה: יהיו $b_1, \ldots, b_n$ יוצרים של A. כל אבר $a \in A$ הוא צרוף לינארי של $b_1, \ldots, b_n$ במקדמים שלמים. לכן, אם $a_1, \ldots, a_r$ אינם תלויים לינארית, נובע ממשפט ההחלפה של שטייניץ ש $r \leq n$. לכן, $\mathrm{rank}(A) \leq n$. ∎

חבורה חלופית נוצרת סופית A מכֻנה **חָפְשִׁית** אם היא סכום ישר של עתקים של $\mathbb{Z}$: $U_n = \bigoplus_{i=1}^n Z_i$. אם z_i הוא יוצר של Z_i, אזי $z_1, \ldots, z_n$ אינם תלויים לינארית ויוצרים את U_n. מהוכחת למה יד.א נובע ש $n = \mathrm{rank}(U_n)$. הקבוצה $z_1, \ldots, z_n$ נקראת **בָּסִיס** של U_n. כל $a \in U_n$ נתן להצגה באפן יחיד כצרוף לינארי של $z_1, \ldots, z_n$ עם מקדמים שלמים. בפרט, U_n חסרת פתול.

U_n הנה החבורה החלופית החפשית היחידה (עד כדי איזומורפיזם) מדרגה n.

כל בסיס אחר של U_n מתקבל מ $z_1, \ldots, z_n$ בעזרת מטריצה הפיכה ב $M_n(\mathbb{Z})$ (לחלופין, מטריצה ב $M_n(\mathbb{Z})$ שהדטרמיננטה שלה שוה ל ± 1). להפך, אם $z_i' = \sum_{j=1}^n \alpha_{ij} z_j$ ו (α_{ij}) היא מטריצה הפיכה ב $M_n(\mathbb{Z})$, אזי $z_1', \ldots, z_n'$ הוא בסיס של U_n. בפרט, אם $z_1' = z_1 + \alpha_2 z_2 + \cdots + \alpha_n z_n$ ו $\alpha_i \in \mathbb{Z}$, אזי $z_1', z_2, \ldots, z_n$ הוא בסיס של U_n.

אם B היא חבורה חלופית אזי כל העתקה α של הבסיס $\{z_1, \ldots, z_n\}$ של U_n לתוך חבורה חלופית B נתנת להרחבה באפן יחיד להומומורפיזם של U_n לתוך B. בפרט אם B נוצר על ידי n אברים, נוכל להעתיק את הבסיס על קבוצת יוצרים של B ולקבל אפימורפיזם $\alpha\colon U_n \to B$. ממשפט האיזומורפיזם הראשון נובע ש $U_n/\mathrm{Ker}(\alpha) \cong B$.

אם $z_1, \ldots, z_n$ הוא בסיס של U_n ו $y_1, \ldots, y_m$ הוא בסיס של U_m, אזי $y_1, \ldots, y_m, z_1, \ldots, z_n$ הנו בסיס של $U_m \oplus U_n$ ו $U_m \oplus U_n \cong U_{m+n}$.

משפט יד.ב (משפט החבורות החלקיות של U_n): *תהי V חבורה חלקית של U_n. אזי V חלופית חפשית ו $k = \mathrm{rank}(V) \leq n$. יתר על כן, קיָם בסיס $u_1, \ldots, u_n$ ל U_n, בסיס $v_1, \ldots, v_k$ ל V ומספרים טבעיים $\varepsilon_1, \ldots, \varepsilon_k$ כך ש $v_i = \varepsilon_i u_i$ ו $\varepsilon_i | \varepsilon_{i+1}$ עבור כל i.*

הוכחה באנדוקציה על n: אם $n = 1$, אזי $U_n \cong \mathbb{Z}$. במקרה זה מתלכד המשפט עם למה ג.ה.

נניח אפוא ש $n \geq 2$ ושהמשפט נכון עבור $n-1$. המשפט ברור כאשר $V = 0$. נניח אפוא ש $V \neq 0$ ונחלק את שארית ההוכחה לכמה חלקים:

חלק א: *בחירת* ε_1 *ו* u_1. נבחר $0 \neq v_1 \in V$, בסיס $u'_1, \dots, u'_n$ ל U_n ומספרים שלמים $\varepsilon_1, \alpha_2, \dots, \alpha_n$ כך ש $\varepsilon_1 > 0$,

$$v_1 = \varepsilon_1 u'_1 + \alpha_2 u'_2 + \cdots \alpha_n u'_n \tag{1}$$

ו ε_1 הוא המספר הטבעי הקטן ביותר המופיע בהצגות מהטפוס (1) (לוקחים בחשבון את כל הבסיסים האפשריים וכל האברים של V). נחלק את ה α_i־ים ב ε_1 עם שארית

$$\alpha_i = \varepsilon_1 q_i + r_i \qquad 0 \le r_i < \varepsilon_1, \quad i = 2, \dots, n.$$

נגדיר $u_1 = u'_1 + q_2 u'_2 + \cdots + q_n u'_n$. אזי $u_1, u'_2, \dots, u'_n$ הוא בסיס חדש של U_n ואת v_1 נתן להציג בעזרתו בצורה $v_1 = \varepsilon_1 u_1 + r_2 u'_2 + \cdots + r_n u'_n$. מהמזעריות של ε_1 נובע ש $r_2 = \cdots = r_n = 0$. לכן, $v_1 = \varepsilon_1 u_1$.

חלק ב: *פרוק ישר של* V. נסמן עתה $V' = V \cap \langle u'_2, \dots, u'_n \rangle$. אזי $V' \cap \langle v_1 \rangle = 0$. נוכיח ש $V = \langle v_1 \rangle + V'$. יהי

$$v = \beta_1 u_1 + \beta_2 u'_2 + \cdots + \beta_n u'_n$$

אבר של V עם $\beta_i \in \mathbb{Z}$. נרשם $\beta_1 = \varepsilon_1 q + r$ באשר $0 \le r < \varepsilon_1$. אזי V מכיל את האבר $v' = v - qv_1 = ru_1 + \beta_2 u'_2 + \cdots + \beta_n u'_n$. אלו היה $r \neq 0$, היינו מקבלים סתירה למזעריות של ε_1. לכן, $r = 0$. מכאן נובע ש $v' \in V'$ ו $v = qv_1 + v'$. בסכום הוכחנו ש $V = \langle v_1 \rangle \oplus V'$.

חלק ג: *שמוש בהנחת האנדוקציה.* ההוכחה מסתיֶמת אם $V' = 0$. אחרת מוכלת V' בחבורה החפשית $U' = \langle u'_2, \dots, u'_n \rangle$ מדרגה $n-1$. לפי הנחת האנדוקציה V' חפשית. יתר על כן, $k - 1 \le n - 1$, קיָם בסיס $u_2, \dots, u_n$ של V', קיָם בסיס $v_2, \dots, v_k$ של V' וקיָמים מספרים שלמים $\varepsilon_2, \dots, \varepsilon_n$ כך ש $v_i = \varepsilon_i u_i$ ו $\varepsilon_i | \varepsilon_{i+1}$ עבור $i = 2, \dots, n-1$.

חלק ד: *סיום ההוכחה.* אנו מקבלים ש $u_1, u_2, \dots, u_n$ הוא בסיס ל U_n, V היא חבורה חפשית מדרגה k שאינה עולה על n ו $v_1, \dots, v_2, \dots, v_n$ הוא בסיס של V. כדי לסים את הוכחת המשפט מספיק שנוכיח ש $\varepsilon_1 | \varepsilon_2$. יהי אפוא $\varepsilon_2 = \varepsilon_1 q' + r'$ באשר $0 \le r' < \varepsilon_1$. נחליף את הבסיס $u_1, u_2, \dots, u_n$ של U_n לבסיס $u_1^*, u_2, \dots, u_n$ באשר $u_1^* = u_1 - q' u_2$ ונרשם $v_2 - v_1 = (-\varepsilon_1) u_1^* + r' u_2$. מהמזעריות של ε_1 נובע שוב ש $r' = 0$. לכן $\varepsilon_1 | \varepsilon_2$, כמבֻקש. ∎

משפט יד.ג (המשפט היסודי של החבורות החלופיות הנוצרות סופית): *כל חבורה חלופית נוצרת סופית היא סכום ישר של חבורות מעגליות.*

הוכחה: תהי A חבורה חלופית הנוצרת על ידי n אברים $a_1, \dots, a_n$. אזי קיֶמת תת חבורה V של U_n כך ש $A \cong U_n / V$. לפי משפט החבורות החלקיות, V היא חבורה חפשית. נבחר ל U_n ו V בסיסים כנאמר במשפט הנ"ל.

אזי

$$U_n/V \cong \langle u_1\rangle/\langle \varepsilon_1 u_1\rangle \oplus \cdots \oplus \langle u_k\rangle/\langle \varepsilon_k u_k\rangle \oplus \langle u_{k+1}\rangle \oplus \cdots \oplus \langle u_n\rangle$$

עבור $1 \le i \le k$ המחֻבר $\langle u_i\rangle/\langle \varepsilon_i u_i\rangle$ הוא חבורה מעגלית מסדר ε_i, $n-k$ המחֻברים האחרונים הם חבורות מעגליות אינסופיות. ∎

הערה יד.ד: האברים $u_{k+1}, \dots, u_n$ אינם תלויים לינארית וכל אבר של U_n/V תלוי לינארית בהם. לכן $\mathrm{rank}(A) = n-k$.

ואכן, נסמן $\bar{u}_i = u_i + V$ עבור $i = 1, \dots, k$. כל $v \in U_n/V$ נתן להצגה בצורה $v = \sum_{i=1}^{k} \alpha_i \bar{u}_i + \sum_{i=k+1}^{n} \alpha_i u_i$ באשר $\alpha_i \in \mathbb{Z}$. אזי $\varepsilon_n v = \sum_{i=k+1}^{n} \varepsilon_n \alpha_i u_i$. ∎

כל חבורה מעגלית סופית נוכל לפרק לסכום ישר של חבורות מעגליות שסדרן הוא חזקה של מספר ראשוני.

משפט יד.ה: *כל חבורה חלופית נוצרת סופית A נתן להציג בצורה*

$$A \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_t^{\alpha_t}\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$$

חבורות אלו אינן נתנות לפרוק נוסף. כמוהן גם $\mathbb{Z}$ אינה נתנת לפרוק. נוכל אפוא לחזק את המשפט היסודי ולנסחו באפן הבא:

משפט יד.ה: *כל חבורה חלופית נוצרת סופית A נתן להציג בצורה*

$$A \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_t^{\alpha_t}\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$$

באשר *$p_1, \dots, p_t$ הם מספרים ראשוניים (לאו דוקא שונים) ומספר המחֻברים $\mathbb{Z}$ שוה לדרגת A.*

מטרתנו היא להראות שהפרוק של A יחיד עד כדי סדר המחֻברים. במלים אחרות, ברצוננו להוכיח שהמספרים $p_1^{\alpha_1}, \dots, p_r^{\alpha_r}$ מהוים שמורה של A. יחד עם זאת נרצה להראות מה הקשר בין השמורות של A לשמורות של תת חבורה של A. ההוכחה של יחידות הפרוק שנביא כאן תעבר דרך הוכחת משפט החבורה החלקית. לפני שננסח משפט זה נראה שאכן יש בו טעם על ידי הוכחת הלמה הבאה:

למה יד.ו: *אם A היא חבורה חלופית נוצרת סופית ואם $B \le A$, אזי גם B נוצרת סופית. אם A נוצרת על ידי n אברים, גם B נוצרת על ידי n אברים.*

הוכחה: A איזומורפית למנה U_n/V. B, בתור תת חבורה, איזומורפית ל U'/V באשר $U' \le U_n$. ממשפט החבורות החלקיות של U_n נובע ש U' נוצרת על ידי n אברים. לכן U'/V נוצרת אף היא על ידי n אברים. ∎

משפט יד.ז (משפט החבורה החלקית לחבורות חלופיות נוצרות סופית): *נניח ש בפרוק של חבורה חלופית A לסכום ישר של חבורות מעגליות אי פריקות מופיעים $r \geq 0$ מחֻברים מעגליים אינסופיים. יהי p מספר ראשוני. נניח גם שבפרוק הנ"ל מופיעים k מחֻברים שסדרן חזקה של p (k תלוי ב p) והסדרים של מחֻברים אלו הם $p^{\alpha_1}, p^{\alpha_2}, \dots, p^{\alpha_k}$ באשר $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_k$.*

תהי B תת חבורה של A. נניח שבפרוק כלשהוא של B לסכום ישר של חבורות מעגליות אי פריקות מופיעים $s \geq 0$ מחֻברים מעגליים אינסופיים ו l מחֻברים מעגליים שסדריהם $p^{\beta_1}, p^{\beta_2}, \dots, p^{\beta_l}$, באשר $\beta_1 \geq \beta_2 \geq \cdot \geq \beta_l$.

אזי $s \leq r$, $l \leq k$ ו $\beta_i \leq \alpha_i$ לכל $1 \leq i \leq l$.

הוכחה: קודם כל נשים לב לכך ש $s = \operatorname{rank}(B) \leq \operatorname{rank}(A) \leq r$. שנית נזכֹר ש $B_{p^\infty} = A \cap A_{p^\infty} \leq A_{p^\infty}$ ו k, $\alpha_1, \dots, \alpha_k$, l, $\beta_1, \dots, \beta_l$ תלויים אך ורק ב A_{p^∞} ו B_{p^∞}. נוכל אפוא להניח, בלי הגבלת הכלליות, ש $A = A_{p^\infty}$ ו $B = B_{p^\infty}$.

את תת החבורה של A המֻרכבת מכל האברים המתאפסים על ידי p סימנו ב A_p. חבורה זו היא סכום של k חבורות מעגליות מסדר p. בפרט $|A_p| = p^k$. ואכן, אם $A = \langle a_1 \rangle \oplus \cdots \oplus \langle a_k \rangle$ ו $\operatorname{ord}(a_j) = p^{\alpha_j}$ באשר $\alpha_j \geq 1$, אזי $A_p = \langle p^{\alpha_1 - 1} a_1 \rangle \oplus \cdots \oplus \langle p^{\alpha_k - 1} a_k \rangle$. בדומה B_p היא סכום ישר של l חבורות מעגליות מסדר p ו $|B_p| = p^l$. הואיל ו $B_p \leq A_p$, אנו מקבלים ש

$$l \leq k. \tag{1}$$

נניח עתה בשלילה ש $\beta_j > \alpha_j$, $\beta_1 \leq \alpha_1, \dots, \beta_{j-1} \leq \alpha_{j-1}$. אזי $\alpha_j < \alpha_{j-1}$. נסמן $C = p^{\alpha_j} A$. אזי, $C = \langle p^{\alpha_j} a_1 \rangle \oplus \cdots \oplus \langle p^{\alpha_j} a_{j-1} \rangle$. יהי $D = p^{\alpha_j} B$. אזי $D \leq C$ ו D מתפרק לפחות לסכום של j מחֻברים מעגליים שסדרם חזקת־p (כי $\beta_j > \alpha_j$) ואלו C מתפרק רק לסכום ישר של j מחֻברים כאלו. אם נפעיל את (1) לגבי החבורות C ו D נקבל ש $j \leq j - 1$, סתירה. ∎

אם נקח במשפט החבורה החלקית $B = A$ נקבל את משפט היחידות:

משפט יד.ו (משפט יחידות הפרוק של חבורות חלופיות נוצרות סופית): *תהי A חבורה חלופית נוצרת סופית. אזי נתן להציג את A בצורה יחידה כסכום ישר*

$$A \cong \mathbb{Z} \oplus \cdots \oplus \mathbb{Z} \oplus \bigoplus_p (\mathbb{Z}/p^{\alpha_{1,p}}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{\alpha_{k,p}}\mathbb{Z})$$

באשר מספר המחֻברים $\mathbb{Z}$ שוה לדרגה של A, p עובר על כל המספרים הראשוניים, $k = k(p)$ הוא מספר שלם אי שלילי השוה לאפס עבור כמעט כל p ו $\alpha_{1,p} \geq \cdots \geq \alpha_{k,p}$.

טו. שדות סופיים

בסעיף זה נביא את המשפטים היסודיים של השדות הסופיים.

משפטון טו.א: *כל תת חבורה סופית A של החבורה הכפלית של שדה K הנה מעגלית.*

הוכחה: בתור חבורה חלופית סופית, A היא מכפלה ישרה של חבורות סילו־p שלה. אם נוכיח שכל אחת מהחבורות האלו מעגלית, ינבע שגם A מעגלית. לכן אפשר להניח ש A חבורת־p סופית. יהי x אבר של A בעל סדר מרבי, p^m. אזי $1, x, \dots, x^{p^m-1}$ הם p^m שרשים שונים ב K של הפולינום $X^{p^m}-1$. באפן כללי, לפולינום ממעלה n עם מקדמים ב K יש לכל היותר n שרשים ב K. בפרט, במקרה שלנו, $1, x, \dots, x^{p^m-1}$ הם כל השרשים של הפולינום $X^{p^m}-1$ ב K. אם a הנו אבר כל A, אזי $\mathrm{ord}(a) = p^k$ באשר $k \le m$. לכן, $a^{p^m} = (a^{p^k})^{p^{m-k}} = 1$. מהנאמר לעיל נובע ש $a \in \{1, x, \dots, x^{p^m-1}\}$. לכן A חבורה מעגלית ו x יוצר שלה. ∎

תוצאה טו.ב: *אם F הוא שדה סופי, אזי $F^\times$ הנה חבורה מעגלית.*

למה טו.ג: *יהי F שדה סופי.*

(א) *קים מספר ראשוני יחיד p כך ש $\mathbb{F}_p \subseteq F$.*

(ב) $|F| = p^n$*, עבור איזה שהוא מספר טבעי n.*

(ג) $F^\times \cong C_{p^n-1}$.

הוכחה: רואים את F כמרחב וקטורי נוצר סופית מעל $\mathbb{F}_p$ ומסמנים $n = \dim(F)$. ∎

ללא הוכחה נביא את התוצאה הבסיסית הבאה מתורת השדות:

משפט טו.ד: *יהי K שדה ו $f(X)$ פולינום ממעלה חיובית עם מקדמים ב K. אזי קים שדה N המקיף את K בעל התכונות הבאות:*

(א) $f(X)$ *מתפרק לגורמים לינאריים מעל N.*

(ב) *אם N' הוא שדה הרחבה נוסף של K אשר מעליו $f(X)$ מתפרק לגורמים לינאריים, אזי קיָם שכון־ K של N לתוך N'.*

השדה N נקבע על ידי התכונות הנ"ל באפן יחיד עד כדי איזומורפיזם־ K ונקרא **שדה הפצול** *של $f(X)$ מעל K. יתר על כן, L מהוה מרחב וקטורי ממימד סופי מעל K.*

למה טו.ה: *אם F הוא שדה בעל אפיון p ו q הנו חזקה של p, אזי $(x+y)^q = x^q + y^q$ לכל $x, y \in F$.*

משפט טו.ו: *לכל p ראשוני ולכל n טבעי קיָם שדה יחיד עד כדי איזומורפיזם מסדר p^n. נסמנו ב $\mathbb{F}_{p^n}$.*

הוכחה: עבור $n = 1$, $\mathbb{F}_p = \mathbb{Z}/n\mathbb{Z}$. באפן כללי, יהי F שדה הפצול של הפולינום $f(X) = X^{p^n} - X$ מעל $\mathbb{F}_p$. הואיל ו $f'(X) = -1$, $\gcd(f(X), f'(X)) = 1$ ולכן יש ל $f(X)$ p^n שרשים שונים ב F. אסף השרשים

האלו סגור תחת חבור, כפל וחלוק ולכן מהוה תת שדה של F. מהיחידות של שדה הפצול נובע ש F הוא אכן אסף השרשים הנ"ל. מכאן נובעת היחידות. ∎

מהלמה נובע גם שכל אחת מההעתקות $\varphi_i\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ המֻגדרת על ידי $\varphi_i(x) = x^{p^i}$, $i = 0, 1, \ldots, n-1$, היא אוטומורפיזם של $\mathbb{F}_{p^n}$ מעל $\mathbb{F}_p$. אסף האוטומורפיזם מהוֶה חבורה, $\Phi = \{\varphi_0, \varphi_1, \ldots, \varphi_{n-1}\}$, ביחס לפעֻלת ההרכבה.

משפט טו.ז: *Φ היא חבורת כל האוטומורפיזם של $\mathbb{F}_{p^n}$ מעל $\mathbb{F}_p$. במלים אחרות, Φ הנה* **חבורת גלואה** $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ *של $\mathbb{F}_{p^n}$ מעל $\mathbb{F}_p$.*

הוכחה: יהי x יוצר של החבורה המעגלית $\mathbb{F}_{p^n}^\times$. הואיל ו $[\mathbb{F}_{p^n} : \mathbb{F}_p] = \dim \mathbb{F}_{p^n} = n$, קיָם פולינום מתֻקן $f \in \mathbb{F}_p[X]$ ממעלה n כך ש $f(x) = 0$. לכן $f(x^{p^i}) = \varphi_i(f(x)) = 0$. לכן, $x, x^p, x^{p^2}, \ldots, x^{p^n}$ הם בדיוק כל השרשים של $f(X)$. אם σ הנו אוטומורפיזם של $\mathbb{F}_{p^n}$, אזי σx הוא שרש של $f(X)$ ולכן קיָם i יחיד כך ש $\sigma(x) = \varphi_i(x)$. מכאן ש $\sigma(x^k) = \varphi_i(x^k)$ לכל k טבעי ולכן $\sigma = \varphi_i$. ∎

תוצאה טו.ח: *$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}))$ היא חבורה מעגלית מסדר n הנוצרת על ידי* **אוטומורפיזם פרובניוס** *φ_1 המֻגדר על ידי* $\varphi_1(x) = x^p$.

טז. אָפִיָנִים של חבורות חלופיות סופיות

המשפטים היסודיים של תורת החבורות החלופיות הנוצרות סופית מוצאים שִׁמוש נוסף בתורת האפינים של חבורות חלופיות סופיות. תורה זו מצדה מהוָה נדבך מהותי בהוכחת משפט דיריכלה על קיום אינסוף מספרים ראשוניים בסדרות חשבוניות מצֻמצמות.

בסעיף זה נשתמש בכתיב הכפלי עבור חבורות חלופיות. **אָפִין** (קמץ קטן) של חבורה חלופית סופית A הנו הומומורפיזם $\chi\colon A \to \mathbb{C}^\times$. בפרט, אם $n = |A|$ ו $a \in A$, אזי $\chi(a)^n = \chi(a^n) = \chi(1) = 1$. במלים אחרות, $\chi(a)$ הנו שֹרש יחידה מסדר המחלק את n. הואיל ויש רק n שֹרשים כאלו, קבוצת האפינים של A סופית. נסמן אותה ב $\mathrm{Hom}(A, \mathbb{C}^\times)$ או בְיֶתר קִצור ב $\hat{A}$. נהפֹך את $\hat{A}$ לחבורה חלופית על ידי שנגדיר כפל בין שני אפינים χ_1 ו χ_2 בעזרת הנֻסחה הבאה:

$$(\chi_1\chi_2)(a) = \chi_1(a)\chi_2(a).$$

אבר היחידה ב $\hat{A}$ הנו האפין ε המעתיק כל אבר של A ל 1. ההפוך נתן על ידי הנסחה $\chi^{-1}(a) = \chi(a)^{-1}$. התוצאות העקריות שנוכיח על האפינים הן נֻסחאות הנִצבות והאיזומורפיזם $A \cong \hat{A}$.

למה טז.א: *תהי A חבורה חלופית סופית ו $\chi \in \hat{A}$. אזי:*

$$\sum_{a \in A} \chi(a) = \begin{cases} |A| & \chi = \varepsilon \text{ אם} \\ 0 & \chi \neq \varepsilon \text{ אם} \end{cases}$$

הוכחה: נניח ש $\chi \neq \varepsilon$. אזי קיָם $b \in A$ כך ש $\varepsilon(b) \neq 1$. כאשר a עובר על כל אברי A, עובר ab על כל אברי A. לכן,

$$\sum_{a \in A} \chi(a) = \sum_{a \in A} \chi(ab) = \sum_{a \in A} \chi(a) \cdot \chi(b)$$

הואיל ו $\chi(b) \neq 1$, יכול השויון להתקיֵם רק אם $\sum_{a \in A} \chi(a) = 0$. ∎

נרחיב עת את ההתאמה $A \rightsquigarrow \hat{A}$ לפונקטור של קטגורית החבורות החלופיות סופיות לתוך עצמה:

לכל הומומורפיזם $\alpha\colon A \to B$ של חבורות חלופיות סופיות נגדיר הומומורפיזם $\hat{\alpha}\colon \hat{B} \to \hat{A}$ על ידי $\hat{\alpha}(\chi) = \chi \circ \alpha$. נשים לב לכך שכוון החִצים התהפך. בהתאם לכך, אם $\beta\colon B \to C$ הוא הומומורפיזם נוסף בין חבורות חלופיות סופיות, אזי $\widehat{\beta \circ \alpha} = \hat{\alpha} \circ \hat{\beta}$. אם α הנו העתקת הזהות של A, אזי $\hat{\alpha}$ הנו העתקת הזהות של $\hat{A}$. כללים אלו אומרים שההעתקה $A \rightsquigarrow \hat{A}$ הִנה **פונקטור קונטרה־וריאנטי**. נקרא לו **פונקטור הכובע**.

למה טז.ב: *פונקטור הכובע* **מְדֻיק משמאל***. במלים אחרות, אם*

$$1 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 1 \tag{1}$$

היא סדרה מדֻיקת קצרה של חבורות אבליות סופיות, אזי הסדרה

$$1 \longrightarrow \hat{C} \xrightarrow{\hat{\beta}} \hat{B} \xrightarrow{\hat{\alpha}} \hat{A} \tag{2}$$

מדֻיקת.

הוכחה: להוכחה שני חלקים:

חלק א: $\hat{\beta}$ *חד חד ערכית.* אם $\hat{\beta}(\chi) = \varepsilon_B$ עבור איזה שהוא $\chi \in \hat{C}$, אזי $\chi(\beta(b)) = 1$ לכל $b \in B$. הואיל ו β על, נובע מכאן ש $\chi(c) = 1$ לכל $c \in C$. לכן, $\chi = \varepsilon_C$.

חלק א: *דיוק ב* $\hat{B}$. ראשית, לכל $\chi \in \hat{C}$ ו $a \in A$ מתקיֵם $(\hat{\alpha} \circ \hat{\beta})(\chi)(a) = (\chi \circ \beta \circ \alpha)(a) = \chi(1) = 1$. שנית, נניח ש $\alpha(\chi) = \varepsilon_A$ עבור איזה שהוא $\chi \in \hat{B}$. אזי $\chi(\alpha(a)) = 1$ לכל $a \in A$. הואיל והסדרה המקורית מדֻיקת ב B, מתקיֵם $\chi(b) = 1$ לכל $b \in \mathrm{Ker}(\beta)$. לפי משפט האיזומורפיזם הראשון, קיָם הומומורפיזם $\psi\colon C \to \mathbb{C}^\times$ כך ש $\chi = \psi \circ \beta$. במלים אחרות, $\chi = \hat{\beta}(\psi)$. ∎

נוכיח בהמשך שפנקטור הכובע מדֻיק גם מימין. לצרך זה נראה שפקטור זה שומר על מכפלות ישרות:

למה טז.ג: *קיָם איזומורפיזם טבעי* $\hat{A} \times \hat{B} \cong \widehat{A \times B}$.

הוכחה: נתאים לכל אפין $\chi\colon A \times B \to \mathbb{C}^\times$ את זוג האפינים (χ_A, χ_B) של A ו B בהתאמה. אלו מֻגדרים על ידי הנֻסחאות $\chi_A(a) = \chi(a, 1)$ ו $\chi_B(b) = \chi(1, b)$. מנֻסחאות אלו עולה ש $\chi(a, b) = \chi_A(a)\chi_B(b)$. לכן, ההתאמה $\chi \mapsto (\chi_A, \chi_B)$ הנה איזומורפיזם של $\widehat{A \times B}$ על $\hat{A} \times \hat{B}$. ∎

משפטון טז.ד: *לכל חבורה סופית* A *קיָם איזומורפיזם (לא טבעי)* $A \cong \hat{A}$.

הוכחה: נפרק את A למכפלה ישרה של חבורות מעגליות $A = \prod_{i=1}^m A_i$ (משפט יד.ג). לפי למה טז.ג, $\hat{A} \cong \prod_{i=1}^m \hat{A}_i$. לכן נוכל להניח, בלי הגבלת הכלליות, ש A מעגלית מסדר n עם יוצר a.

יהי $\zeta_n = e^{2pi/n}$ שרש יחידה קדום מסדר n. לכל מספר טבעי k נגדיר $\chi_k \in \hat{A}$ על ידי $\chi_k(a) = \zeta_n^k$. ההעתקה $k \mapsto \chi_k$ הנה איזומורפיזם של $\mathbb{Z}/n\mathbb{Z}$ על $\hat{A}$. לכן $A \cong \hat{A}$. ∎

תוצאה טז.ה: *פקטור הכובע* **מדֻיק**. *במלים אחרות, אם* (1) *היא סדרה מדֻיקת קצרה של חבורות חלופיות סופיות, אזי גם הסדרה הבאה מדֻיקת:*

$$1 \longrightarrow \hat{C} \xrightarrow{\hat{\beta}} \hat{B} \xrightarrow{\hat{\alpha}} \hat{A} \longrightarrow 1 \tag{3}$$

הוכחה: על פי למה טז.ב מספיק להוכיח ש $\hat{\alpha}$ על. ואכן, $\mathrm{Im}(\hat{\alpha})$ היא תת חבורה של $\hat{A}$. לפי למה טז.ב, $\mathrm{Im}(\hat{\alpha}) \cong \hat{B}/\hat{\beta}(\hat{C})$. כמו כן, $\hat{\alpha}(\hat{C}) \cong \hat{C}$. לכן, לפי משפטון טז.ד,

$$|\mathrm{Im}(\hat{\alpha})| = |\hat{B}|/|\hat{\beta}(\hat{C})| = |\hat{B}|/|\hat{C}| = |B|/|C| = |A| = |\hat{A}|.$$

לכן, $\mathrm{Im}(\hat{\alpha}) = \hat{A}$. ∎

למה טז.ו: *תהי A חבורה חלופית סופית ו a אבר של A השונה מ 1. אזי קים $\chi \in \hat{A}$ כך ש $\chi(a) \neq 1$.*

הוכחה: כמו בהוכחת למה טז.ד נפרק את A למכפלה ישרה $A = \prod_{j=1}^{m} A_j$ של חבורות מעגליות. יהי $n_j = |A_j|$ ויהי a_j יוצר של A_j. אם $a \neq 1$, אזי $a = \prod_{j=1}^{m} a_j^{k_j}$ באשר $0 \leq k_j < n_j$ לכל j ואחד מהמעריכים שונה מ 0. בלי הגבלת הכלליות נניח ש $k_1 \neq 0$. נגדיר $\chi \in \hat{A}$ על ידי $\chi(a_1) = \zeta_{n_1}$ ו $\chi(a_j) = 1$ לכל $j \geq 2$. אזי $\chi(a) = \zeta_{n_1}^{k_1} \neq 1$. ∎

תוצאה טז.ז: *תהי A חבורה חלופית סופית ויהי $a \in A$. אזי*

$$\sum_{\chi \in \hat{A}} \chi(a) = \begin{cases} |A| & a = 1 \text{ אם} \\ 0 & a \neq 1 \text{ אם} \end{cases}$$

הוכחה: נניח ש $a \neq 1$. נבחר לפי למה טז.ו אפין $\psi \in \hat{A}$ כך ש $\psi(a) \neq 1$. כאשר χ עובר על כל אברי $\hat{A}$ עובר $\chi\psi$ על כל אברי $\hat{A}$. לכן,

$$\sum_{\chi \in \hat{A}} \chi(a) = \sum_{\chi \in \hat{A}} (\psi\chi)(a) = \psi(a) \sum_{\chi \in \hat{A}} \chi(a) .$$

לכן, $\sum_{\chi \in \hat{A}} \chi(a) \neq 1$. ∎

תהי A חבורה חלופית סופית. לכל $a \in A$ נגדיר $\psi_a \in \hat{\hat{A}}$ על ידי $\psi_a(\chi) = \chi(a)$. ההעתקה $a \mapsto \psi_a$ הנה הומומורפיזם טבעי של A לתוך $\hat{\hat{A}}$. נסמנו ב Ψ.

תוצאה טז.ח: *ההומומורפזם Ψ הנו איזומורפיזם.*

הוכחה: מתוצאה טז.ז נובע ש Ψ חד חד ערכי. ממשפטון טז.ד נובע ש $|\hat{\hat{A}}| = |\hat{A}| = |A|$. לכן, Ψ גם על. ∎

יז. פרוק הצגות למרכיבים אי פריקים

תורת ההַצגות ממשת חבורות סופיות כחבורות של מטריצות ומַקישה מתכונותיהן של המטריצות על תכונותיהן של החבורות. בסעיף זה נגדיר את המושגים הראשונים של תורת ההצגות ונוכיח שכל הצגה של חבורה סופית מתפרקת לסכום ישר של הצגות אי פריקות.

יהי V מרחב וקטורים ממוד סופי n מעל שדה המספרים המרֻכבים $\mathbb{C}$. נסמן ב $\mathrm{GL}(V)$ (או גם ב $\mathrm{Aut}(V)$) את אסף כל ההעתקות הלינאריות ההפיכות של V על עצמו. זוהי חבורה (אינסופית) האיזומורפית לחבורה $\mathrm{GL}_n(\mathbb{C})$ של כל המטריצות ההפיכות מסדר $n \times n$ מעל $\mathbb{C}$. האיזומורפיזם תלוי בבחירת הבסיס של V: אם $\mathbf{v}_1, \ldots, \mathbf{v}_n$ הוא בסיס של V, אזי ההעתקה T תעבר למטריצה (a_{ij}) שאבריה המֻגדדים על ידי הנֻסחה

$$Tv_j = \sum_{i=1}^{n} a_{ij} v_i. \tag{1}$$

תהי G חבורה סופית. **הצגה** של G לתוך V הנה הומומורפיזם $\rho\colon G \to \mathrm{GL}(V)$. בפרט מתקַיְמים התנאים הבאים:

$$\rho(gh) = \rho(g)\rho(h)$$

ו

$$\rho(1) = 1 \qquad \rho(g^{-1}) = \rho(g)^{-1} \tag{2}$$

לכל $g, h \in G$. במקרה זה נאמר ש V הוא **מרחב הצגה** של G (או לפעמים גם **הצגה** של G) ו $n = \dim(V)$ היא **מעלת ההצגה**. אם נקבע בסיס $\mathbf{v}_1, \ldots, \mathbf{v}_n$ ל V כפי שעשינו לעיל, תתאים לכל $g \in G$ מטריצה $(r_{ij}(g))$ ב $\mathrm{GL}_n(\mathbb{C})$ לפי הנֻסחה

$$\rho(g)\mathbf{v}_j = \sum_{i=1}^{n} r_{ij}(g)\mathbf{v}_i.$$

תכונת הכפליות (2) של ρ והנֻסחה הרגילה של כפל מטריצות גוררות את הקשר הבא עבור המספרים $r_{ij}(g)$:

$$r_{ik}(gh) = \sum_{j=1}^{n} r_{ij}(g) r_{jk}(h) \tag{3}$$

לכל $g, h \in G$ ולכל $1 \le i, j \le n$.

אומרים ששתי הצגות ρ, ρ' של G עם מרחבי הצגה V ו V' בהתאמה הנן **איזומורפיות** אם קיָם איזומורפיזם $\alpha\colon V \to V'$ כך ש

$$\alpha \circ \rho(g) = \rho'(g) \circ \alpha$$

לכל $g \in G$. אם $V = V'$ אזי, תנאי (4) שקול לקיום מטריצה $A \in \mathrm{GL}_n(\mathbb{C})$ כך $(r'_{ij}(g)) = A(r_{kl}(g))A^{-1}$.

דֻגמאות יז.א: (א) הצגה **ממעלה** 1 של חבורה G הנה הומומורפיזם $\rho\colon G\to\mathbb{C}^{\times}$. אם m הנו הסדר של G, אזי $\rho(g)^m=\rho(g^m)=\rho(1)=1$, כלומר $\rho(g)$ הנו שרש יחידה מסדר m. בפרט $|\rho(g)|=1$ לכל $g\in G$.

במקרה הפרטי ש $\rho(g)=1$ לכל $g\in G$ נאמר ש ρ הנו **הצגת היחידה**.

(ב) יהי $n=|G|$. נבחר בסיס $\mathbf{e}_h$ למרחב וקטורי V מעל $\mathbb{C}$ המצֻיָּן על ידי אברי G. לכל $g\in G$ תהי $\rho(g)\colon V\to V$ ההעתקה הלינארית הנקבעת על ידי הנֻסחה $\rho(g)(\mathbf{e}_h)=\mathbf{e}_{gh}$. באפן כזה מקבלים אנו הצגה של G מממעלה n הנקראת **ההצגה הרגולרית** של G. הואיל ו $\rho(g)\mathbf{e}_1=\mathbf{e}_g$, ההזזות של $\mathbf{e}_1$ תחת האברים $\rho(g)$ מהוות בסיס של V.

ההצגה הרגולרית של G ממלאת תפקיד מרכזי בתאור כל ההצגות של G. ביתר דיוק, כל הצגה של G הנה "חלקית" (במובן שיתברר מאוחר יותר) להצגה הרגולרית.

(ג) באפן כללי יותר, כל פְּעֻלה (משמאל) של G על קבוצה סופית X מגדירה הצגה ρ של G: אם נבחר בסיס $\mathbf{e}_x$ למרחב וקטורי V מעל $\mathbb{C}$ המצֻיָּן על ידי אברי X, יֻגדר $\rho(g)$ על ידי הנֻסחה הבאה: $\rho(g)e_{\mathbf{x}}=e_{g\mathbf{x}}$. זוהי **הצגת התמורות** של G בפָּעֳלו על X. ∎

נתבונן שוב בהצגה $\rho\colon G\to\mathrm{GL}(V)$ של חבורה סופית G. יהי W תת מרחב של V הנשמר תחת כל ההעתקות $\rho(g)$. הצמצום של העתקות אלו ל W מגדיר הצגה חדשה $\rho_W\colon G\to\mathrm{GL}(W)$ של G:

$$\rho_W(g)=\rho(g)|_W$$

לכל $g\in G$. נאמר ש $\rho|_W$ (לחלופין W) היא **הצגה חלקית** (או גם **תת הצגה**) של ρ (לחלופין V).

לדֻגמה יהי V ההצגה הרגולרית של G (דֻגמה (ב)), נתבונן בתת המרחב מממד 1 של V הנפרש על ידי הוקטור $\mathbf{v}=\sum_{h\in G}\mathbf{e}_h$. אזי $\rho(g)\mathbf{v}=\mathbf{v}$ לכל $g\in G$. לכן, W הוא תת הצגה של V ו ρ_W הנו הצגת היחידה של G.

נניח עתה ש W ו W' הן שני מרחבי הצגה חלקיים של V ביחס לחבורה סופית G כך ש $V=W\oplus W'$. במקרה זה נאמר ש ρ הנו **הסכום הישר** של ρ_W ו $\rho_{W'}$ ונכתב $\rho=\rho_W\oplus\rho_{W'}$. להפך, יהיו $\rho_1\colon G\to V_1$ ו $\rho_2\colon G\to V_2$ שתי הצגות של G. נבחר בסיסים $\mathbf{v}_{1,1},\dots,\mathbf{v}_{1,n_1}$ ו $\mathbf{v}_{2,1},\dots,\mathbf{v}_{2,n_2}$ ל V_1 ו V_2 בהתאמה. אזי $\mathbf{v}_{1,1},\dots,\mathbf{v}_{1,n_1},\mathbf{v}_{2,1},\dots,\mathbf{v}_{2,n_2}$ הנו בסיס של $V=V_1\oplus V_2$ ו $\rho\colon G\to\mathrm{GL}(V)$ המֻגדרת על ידי התנאי $\rho_{V_i}=\rho_i$, $i=1,2$ הנה סכום ישר של ההצגות ρ_1 ו ρ_2. יתר על כן, אם $R_i(g)$ היא המטריצה המיַצגת את ρ_i, אזי $R(g)=\left(\begin{smallmatrix}R_1(g)&0\\0&R_2(g)\end{smallmatrix}\right)$ היא המטריצה המיַצגת את ρ.

משפט יז.ב (Maschke): *תהי $\rho\colon G\to\mathrm{GL}(V)$ הצגה של חבורה סופית G ויהי W תת מרחב של V הנשמר על ידי G. אזי קַיָּם ל W משלים ישר W' הנשמר על ידי G.*

הוכחה: נבחר משלים ישר W_0 של W ב V שאינו נשמר בהכרח על ידי G. אזי $V=W_0\oplus W$. נסמן ב $\pi_0\colon V\to W$ את ההטלה של V על W. במלים אחרות, $\pi_0\colon V\to V$ הנו העתקה לינארית המקיֶּמת

לכל $w\in W$ $\pi_0(w)=w$ ו $\pi_0(V)=W$. נגדיר העתקה לינארית $\pi\colon V\to V$ שאפשר לראות אותה כ"מְמֻצע" של π_0 תחת G:

$$.\pi=\frac{1}{|G|}\sum_{h\in G}\rho(h)\pi_0\rho(h^{-1})$$

העתקה זו שומרת על W. ואכן, לכל $w\in W$ מתקיֵם

$$.\pi(w)=\frac{1}{|G|}\sum_{h\in G}\rho(h)\pi_0(\rho(h^{-1})w)=\frac{1}{|G|}\sum_{h\in G}\rho(h)\rho(h^{-1})w=\frac{1}{|G|}\sum_{h\in G}w=w$$

שנית, מתקיֵם $\pi(V)\subseteq W$. ואכן, אם $v\in V$, אזי $\pi_0(\rho(h^{-1}v))\in W$ ולכן גם $\rho(h)(\pi_0\rho(h^{-1})v)\in W$. מכאן ש $\pi(v)=\frac{1}{|G|}\sum_{h\in G}\rho(h)\pi_0\rho(h^{-1})v\in W$. לכן, π הנו הטלה ו $V=W\oplus W'$ באשר $W'=\{v\in V\mid \pi(v)=0\}$.

כדי לסיֵם את ההוכחה נותר לנו להוכיח ש G שומרת את W'. ואכן,

$$\begin{aligned}\rho(g)\pi\rho(g^{-1})&=\frac{1}{|G|}\sum_{h\in G}\rho(g)\rho(h)\pi_0\rho(h^{-1})\rho(g^{-1})\\&=\frac{1}{|G|}\sum_{h\in G}\rho(gh)\pi_0\rho((gh)^{-1})=\frac{1}{|G|}\sum_{k\in G}\rho(k)\pi_0\rho(k^{-1})=\pi\end{aligned}$$

לכן, $\pi\rho(g)=\rho(g)\pi$. אם $v\in W'$, אזי $\pi v=0$. לכן $\pi(\rho(g)v)=\rho(g)(\pi v)=0$ ומכאן ש $\pi v\in W'$, כמבֻקש. ∎

הצגה ρ של חבורה סופית G תכֻנה **אי פריקה** אם אי אפשר להציג אותה כסכום ישר של הצגות ממעלות נמוכות יותר.

מסקנה יז.ג: *כל הצגה ρ של חבורה סופית G נתן לפרק לסכום ישר של מספר סופי של הצגות אי פריקות.*

יח. אָפִיָנים של הצגות

תהי $\rho\colon G \to \mathrm{GL}(V)$ הצגה ממעלה n של חבורה סופית. נבחר בסיס $\mathbf{v}_1, \ldots, \mathbf{v}_n$ של V ולכל $g \in G$ נסמן

$$\chi(g) = \mathrm{trace}(R(g))$$

באשר $R(g)$ היא המטריצה המיַצגת את $\rho(g)$ ביחס ל $\mathbf{v}_1, \ldots, \mathbf{v}_n$. בחירה של בסיס אחר ל V תעביר את $R(g)$ למטריצה צמודה ולא תשנה את העקבה. לכן, $\chi(g)$ אינו תלוי בבחירת הבסיס. מכאן ש $\chi\colon G \to \mathbb{C}$ היא פונקציה התלויה רק ב ρ. פונקציה זו נקראת **האָפִין** של ρ.

העקבה של מטריצה היא שמורה (ביחס ליחס ההצמדה) הרחוקה מאד מלאפין את המטריצה: מטריצות בעלות עקבות זהות אינן בהכרח צמודות. מפתיע הדבר שהאפין של הצגה קובע אותה עד כדי איזומורפיזם. טענה זו נובעת מלמה של שוּר ומנֻסחאות הנצבות שנוכיח בסעיף זה.

למה יח.א: *יהי χ האפין של הצגה ρ ממעלה n.*

(א) $\chi(1) = n$.

(ב) $\chi(g^{-1}) = \overline{\chi(g)}$, *באשר הגג מסמן הצמדה מרֻכבת.*

(ג) $\chi(hgh^{-1}) = \chi(g)$ *לכל* $g, h \in G$.

הוכחה: נסמן כמוקדם ב $R(g)$ את המטריצה המיַצגת את g ביחס לבסיס קבוע $\mathbf{v}_1, \ldots, \mathbf{v}_n$ של מרחב ההצגה V של ρ. אזי $\rho(1)$ היא מטריצה היחידה מסדר $n \times n$ והעקבה שלה שוה ל n. בזאת הוכחנו את (א).

יהי g אבר של G. נשנה את הבסיס כך ש $R(g)$ תהיה מטריצה משֻׁלשית. יהיו $\lambda_1, \ldots, \lambda_n$ אֵברי האלכסון של $R(g)$. אלו הם הערכים העצמיים של $R(g)$ (כל אחד נלקח מספר פעמים כרִבויו). הואיל ו $R(g)^{|G|} = 1$ ולכן $\lambda_i^{|G|} = 1$ לכל i. מכאן ש $|\lambda_i| = 1$ הם שָׁרשי יחידה ו $\lambda_i^{-1} = \bar{\lambda}_i$. מצד שני, $R(g^{-1}) = R(g)^{-1}$ ו $\lambda_1^{-1}, \ldots, \lambda_n^{-n}$ הם אברי האלכסון של $R(g^{-1})$. לכן, $\chi(g^{-1}) = \sum_{i=1}^n \lambda_i^{-1} = \sum_{i=1}^n \bar{\lambda}_i = \overline{\chi(g)}$, כפי שנדרש ב (ב).

טענה (ג) נובעת מהשתמרות העקבה תחת הצמדה:

$$\chi(hgh^{-1}) = \mathrm{trace}(R(h)R(g)R(h)^{-1}) = \mathrm{trace}(R(g)) = \chi(g). \quad \blacksquare$$

פונקציה $\alpha\colon G \to \mathbb{C}$ המקיֶמת את תנאי (ג) של למה יח.א כלומר $\alpha(hgh^{-1}) = \alpha(g)$ לכל $g, h \in G$ נקראת **פונקציה מרכזית**. בהמשך מוכיחים שכל פונקציה מרכזית הנה צרוף לינארי של אָפינים עם מקדמים מרֻכבים.

למה יח.ב: *יהיו $\rho_i\colon G \to \mathrm{GL}(V_i)$ הצגות של G עם אפינים χ_i, $i = 1, 2$. אזי האפין של $\rho_1 \oplus \rho_2$ הנו $\chi_1 + \chi_2$.*

הוכחה: הטענה נובעת מכך שהעקבה של מטריצת גושים היא הסכום של העקבות של הגושים במטריצה. $\blacksquare$

תרגיל יח.ג: *תהי G חבורה הפועלת על קבוצה סופית X. נסמן ב ρ את הצגת התמורות המתאימה וב χ את האפין של ρ. הוכח שלכל $g \in G$ שוה $\chi(g)$ למספר האברים x המֻשבתים על ידי x.*

משפט המפתח להבנת האפינים שיך לשור (Schur):

משפטון יח.ד (שור): *תהיינה $\rho\colon G \to \mathrm{GL}(V)$ ו $\rho'\colon G \to \mathrm{GL}(V')$ הצגות אי פריקות של חבורה סופית G. תהי $T\colon V \to V'$ העתקה לינארית המקֻימת $T \circ \rho(g) = \rho'(g) \circ T$ לכל $g \in G$ (**תנאי התְאימות**).*

(א) *נניח שההצגות ρ ו ρ' אינן איזומורפיות. אזי $T = 0$.*

(ב) *נניח ש $V = V'$ ו $\rho = \rho'$. אזי קיָם $\lambda \in \mathbb{C}$ כך ש $\rho(g)\mathbf{v} = \lambda\mathbf{v}$ לכל $g \in G$ ו $\mathbf{v} \in V$.*

הוכחת א: נניח בשלילה ש $T \neq 0$, כלומר ש $\mathrm{Ker}(T) \neq V$. מהנחת התְאימות נובע ש $\mathrm{Ker}(T)$ נשמר על ידי $\rho(G)$. הואיל ו ρ אי פריקה, $\mathrm{Ker}(T) = 0$. במלים אחרות, T חד חד ערכי. שוב, מהנחת התאימות, נובע ש $T(V)$ נשמר על ידי $\rho'(G)$. הואיל ו ρ' אי פריקה, $T(V) = 0$ או $T(V) = V'$. האפשרות הראשונה סותרת את הנחת השלילה ואלו האפשרות השניה סותרת את ההנחה ש $V \ncong V'$. מסתירה זו נובע ש $T = 0$.

הוכחת ב: יהי λ ערך עצמי של T. אזי קיָם $\mathbf{v} \in V$, $\mathbf{v} \neq 0$ כך ש $T\mathbf{v} = \lambda\mathbf{v}$. לכן ההעתקה הלינארית $T' = T - \lambda$ של V לתוך V מקֻימת $\mathrm{Ker}(T') \neq 0$. מההנחה $T \circ \rho = \rho \circ T$ נובע ש $\mathrm{Ker}(T')$ נשמר על ידי G. הואיל ו ρ אי פריקה, נובע ש $T' = 0$. במלים אחרות, T הנה כפל בסקלר λ. ∎

תוצאה יח.ה: *תהיינה $\rho\colon G \to \mathrm{GL}(V)$ ו $\rho'\colon G \to \mathrm{GL}(V')$ הצגות אי פריקות של חבורה סופית G. תהי $T\colon V \to V'$ העתקה לינארית. נבנה את הממֻצע של T:*

$$T_0 = \frac{1}{|G|} \sum_{h \in G} \rho'(h)^{-1} T \rho(h)$$

(א) *אם ρ ו ρ' אינן איזומורפיות, אזי $T_0 = 0$.*

(ב) *אם $V = V'$, $n = \dim(V)$ ו $\rho = \rho'$, אזי $T_v\mathbf{v} = \frac{\mathrm{trace}(T)}{n}\mathbf{v}$ לכל $\mathbf{v} \in V$.*

הוכחה: נוכיח תחילה ש T_0 מקֻימת את תנאי התאימות ביחס ל ρ ו ρ', כלומר $T_0\rho(g) = \rho'(g)T_0$ לכל $g \in G$. ואכן,

$$\begin{aligned}
\rho'(g)^{-1} T_0 \rho(g) &= \frac{1}{|G|} \sum_{h \in G} \rho'(g)^{-1}\rho'(h)^{-1} T \rho(h)\rho(g) \\
&= \frac{1}{|G|} \sum_{h \in G} \rho'((hg)^{-1}) T \rho(hg) \\
&= \frac{1}{|G|} \sum_{k \in G} \rho'(k)^{-1} T \rho(k) = T_0
\end{aligned}$$

כנדרש. אם ρ אינו איזומורפי ל ρ', אזי $T_0 = 0$ (משפטון יח.ד(א)). נניח אפוא ש $V = V'$ וש $\rho = \rho'$. אזי, לפי משפטון יח.ד(ב), קיָם $\lambda \in \mathbb{C}$ כך ש $T_0\mathbf{v} = \lambda\mathbf{v}$ לכל $\mathbf{v} \in V$.

כדי לחשב את λ נוכיח ש $\mathrm{trace}(T) = \mathrm{trace}(T_0)$. ואכן,

$$\mathrm{trace}(T_0) = \frac{1}{|G|}\sum_{h\in G}\mathrm{trace}(\rho(h)^{-1}T\rho(h)) = \frac{1}{|G|}\sum_{h\in G}\mathrm{trace}(T) = \mathrm{trace}(T).$$

את העקבה של T_0 בתור העתקה סקלרית קל לחשב: $\mathrm{trace}(T_0) = n\lambda$. לכן, $T_0\mathbf{v} = \frac{\mathrm{trace}(T)}{n}\mathbf{v}$ לכל $\mathbf{v} \in V$.

∎

נתרגם עתה את תוצאה יח.ה לשפת המטריצות. לצרך זה נבחר בסיס $\mathbf{v}_1, \ldots, \mathbf{v}_n$ עבור V ובסיס $\mathbf{v}'_1, \ldots, \mathbf{v}'_{n'}$ עבור V'. נראה את $\rho(g)$ ואת $\rho'(g)$ כמטריצות לפי הבסיסים הנ"ל:

$$\rho(g) = (r_{ij}(g))_{1\le i,j\le n} \qquad \rho'(g) = (r'_{kl}(g))_{1\le k,l\le n'}$$

גם את ההעתקות הלינאריות T ו T_0 נציג בעזרת מטריצות לפי הבסיסים הנ"ל: $T = (t_{li})$ ו $T_0 = (t_{0,kj})$. הגדרת T_0 מקבלת במונחים אלו את הצורה הבאה:

$$t_{0,kj} = \frac{1}{|G|}\sum_{g\in G}\sum_{l,i} r'_{k,l}(h^{-1})t_{li}r_{ij}(g) = \frac{1}{|G|}\sum_{l,i}\Big(\sum_{g\in G} r'_{kl}(g^{-1})r_{ij}(g)\Big)t_{li} \tag{1}$$

תוצאה יח.ו: *תהיינה* $\rho\colon G \to \mathrm{GL}(V)$ *ו* $\rho'\colon G \to \mathrm{GL}(V')$ *הצגות אי פריקות לא איזומורפיות. נסמן* $n = \dim(V)$ *ו* $n' = \dim(V')$*. אזי*

$$\frac{1}{|G|}\sum_{g\in G} r'_{kl}(g^{-1})r_{ij}(g) = 0$$

עבור כל $1 \le i,j \le n$ *ו* $1 \le k,l \le n'$.

הוכחה: נראה את אגף ימין של (1) כתבנית לינארית במשתנים t_{li}. אם נתן ערכים למשתנים אלו נקבל העתקה לינארית $T\colon V \to V'$. הממֻצע שלה T_0 שוה ל 0, לפי תוצאה יח.ה(א). לכן, $t_{0,kl} = 0$ לכל k, l. במלים אחרות, התבנית הלינארית היא תבנית האפס. זה אומר שהמקדמים שלה שוים לאפס, כנאמר בתוצאה. ∎

תוצאה יח.ז: *תהי* $\rho\colon G \to \mathrm{GL}(V)$ *הצגה אי פריקה ויהי* $n = \dim(V)$*. אזי,*

$$\frac{1}{|G|}\sum_{g\in G} r_{kl}(g^{-1})r_{ij}(g) = \begin{cases} \frac{1}{n} & i = j \text{ ו } k = l \\ 0 & \text{אחרת} \end{cases}$$

הוכחה: *שוב, כמו בהוכחה של תוצאה יח.ו, נראה את אגף ימין של (1) כתבנית במשתנים t_{li}. אם נתן ערכים למשתנים אלו נקבל העתקה לינארית $T\colon V \to V$. הממֻצע שלה T_0 הנו כפל ב $\frac{1}{n}\mathrm{trace}(T)$ (תוצאה יח.ה(ב)). לכן (1) מקבל את הצורה*

$$\frac{1}{n}\mathrm{trace}(T)\delta_{kj} = \frac{1}{|G|}\sum_{l,i}\big(\sum_{g\in G} r_{kl}(g^{-1})r_{ij}(g)\big)t_{li}. \tag{2}$$

באשר δ_{kj} הנו פוקצית דלתא של קרונקר. אזי $\delta_{kj}=0$ ולכן כל המקדמים של אגף ימין של (2) שוים לאפס, כנִטען. במקרה שבו $k=j$ מקבלת (2) את הצורה

$$\frac{1}{n}\sum_{i=1}^{n} t_{ii} = \frac{1}{|G|}\sum_{l,i}\big(\sum_{g\in G} r_{jl}(g^{-1}r_{ij}(g)\big)t_{li} \tag{3}$$

השואת המקדמים של שני האגפים של (3) נותנת את שארית הנסחה בתוצאה אשר אותה אנו מבקשים להוכיח. ∎

עבור שתי פונקציות $\varphi, \psi\colon G \to \mathbb{C}$ נגדיר

$$\langle \varphi, \psi\rangle = \frac{1}{|G|}\sum_{g\in G}\varphi(g^{-1})\psi(g).$$

כאשר g עובר על כל אברי G, עובר גם g^{-1} על כל אברי G. לכן, $\langle\varphi,\psi\rangle = \langle\psi,\varphi\rangle$. במלים אחרות, התבנית $\langle\varphi,\psi\rangle$ סימטרית. מלבד זאת נובע מההגדרה שתבנית זו לינארית בכל אחד ממשתניה. את התוצאות יח.ו ו יח.ז נתן לנסח מחדש בעזרת התבנית שהגדרנו באפן הבא:

תוצאה יח.ח: *תהיינה ρ ו ρ' הצגות אי פריקות של חבורה סופית G ממעלות n ו n' בהתאמה. יהיו (r_{ij}) ו (r'_{kl}) המטריצות המתאימות להצגות אלו ביחס לבסיסים קבועים של מרחבי ההצגה.*

(א) *אם ρ אינה איזומורפית ל ρ', אזי $\langle r'_{kl}, r_{ij}\rangle = 0$ לכל i,j,k,l.*

(ב) *מתקיֵם $\langle r_{kl}, r_{ij}\rangle = \frac{1}{n}\delta_{kl}\delta_{ij}$.*

מתוצאה יח.ח יכולים אנו עתה להסיק את **נֻסחאות הנִצבות** של האפינים:

משפט יח.ט: *יהיו χ ו χ' אפינים אי פריקים של הצגות ρ ו ρ' ממעלות n ו n' בהתאמה של חבורה סופית $|G|$.*

(א) *אם ρ ו ρ' אינם איזומורפיים, אזי $\langle\chi,\chi'\rangle = 0$.*

(ב) *מִתקיֵם, $\langle\chi,\chi\rangle = 1$.*

הוכחה: תהיינה (r_{ij}) ו (r'_{kl}) המטריצות המיַצגות את ρ ו ρ' בהתאמה ביחס לבסיסים קבועים של מרחבי ההצגה. אזי $\chi = \sum_{i=1}^{n} r_{ii}$ ו $\chi' = \sum_{k=1}^{n'} r'_{kk}$. לכן, לפי תוצאה יח.ח, $\langle\chi',\chi\rangle = \sum_{k=1}^{n'}\sum_{i=1}^{n}\langle r'_{kk}, r_{ii}\rangle = 0$. מאידך, $\langle\chi,\chi\rangle = \sum_{i,j=1}^{n}\langle r_{ii}, r_{jj}\rangle = \sum_{i=1}^{n}\frac{1}{n} = 1$. ∎

נאמר שאפין χ של הצגה ρ הנו **אי פריק** אם ההצגה ρ אי פריקה. ממשפט יח.ט עולה **שהאורך** של אפין אי פריק שוה ל 1 ואלו אפינים אי פריקים **נצבים זה לזה**. בהמשך נראה שאסף האפינים האי פריקים של G מהוה בסיס נצבות מתֻקן (othonormal basis) למרחב הפונקציות המרכזיות של G.

משפט יח.י: *יהי V מרחב הצגה של חבורה סופית G בעל אפין χ ויהי $V=\bigoplus_{i=1}^m W_i$ הפרוק של V לסכום ישר של מרחבי הצגה אי פריקים. יהי W מרחב הצגה אי פריק של G עם אפין ψ. אזי מספר ה i־ים שעבורם $W_i \cong W$ שוה ל $\langle\psi,\chi\rangle$.*

הוכחה: יהי χ_i האפין של מרחב ההצגה W_i. לפי למה יח.ב, $\chi=\sum_{i=1}^m \chi_i$. נסמן ב I את קבוצת כל ה i־ים שעבורם $W_i \cong W$. לפי משפט יח.ט, $\langle\chi,\psi\rangle=\sum_{i=1}^m\langle\chi_i,\psi\rangle=\sum_{i=1}^m 1=|I|$ כנִטען. ∎

תוצאה יח.יא: *בסימונים של משפט יח.י, מספר ה W_i־ים האיזומורפיים ל W אינו תלוי בפרוק של V למרחבים אי פריקים שהתבוננו בו לעיל. מספר זה נקרא* **מספר הפעמים ש W מופיע ב V**.

הוכחה: המספר $\langle\chi,\psi\rangle$ אינו תלוי בפרוק. ∎

תוצאה יח.יב: *שתי הצגות ρ ו ρ' של חבורה סופית בעלי אותו אפין איזומורפיות זה לזה.*

הוכחה: לפי תוצאה יח.יא, מספר הפעמים שכל הצגה אי פריקה מופיע ב ρ וב ρ' שוה זה לזה. לכן ρ ו ρ' איזומורפיים זה לזה. ∎

התוצאה האחרונה מעמידה את למוד ההצגות על חקר האפינים המתאימים להם: יהיו $\chi_1,\ldots,\chi_s$ כל האפינים האי פריקים של G ו $W_1,\ldots,W_s$ מרחבי ההצגה המתאימים. כל מרחב הצגה V של G נתן לפרוק באפן יחיד כסכום ישר

$$V=\oplus_{i=1}^s m_iW_i$$

באשר m_i הם מספרים שלמים אי שליליים. האפין χ של W שוה ל $\sum_{i=1}^s m_i\chi_i$ ו $m_i=\langle\chi,\chi_i\rangle$. נֻסחאות הנִצבות בין האפינים גוררים ש

$$.\langle\chi,\chi\rangle=\sum_{i=1}^s m_i^2$$

מנֻסחה זו נובע הבֹחן הבא לאי פריקות של אפין:

משפט יח.יב: *יהי χ אפין של מרחב הצגה V. אזי $\langle\chi,\chi\rangle$ הנו מספר חיובי אי שלילי. יתר על כן, $\langle\chi,\chi\rangle=1$ אם רק אם χ אי פריק.*

הוכחה: ואכן, $s=1$ ו $m_1=1$ אם ורק אם $\sum_{i=1}^s m_i^2=1$. ∎

דוגמה יח.יג: תהי ρ הצגה עם אפין χ. מספר הפעמים שהצגת היחידה מופיעה ב ρ שווה ל $\langle \chi, 1\rangle = \frac{1}{|G|}\sum_{g\in G}\chi(g)$. ∎

תרגיל יח.יד: יהיו G חבורה סופית הפועלת משמאל על קבוצה סופית X, ρ הצגת התמורות המתאימה ו χ האפין של ρ.

(א) הוכח שמספר מסלולי־G של X שווה ל $\langle \chi, 1\rangle$, כלומר למספר הפעמים שבהם מופיע שהצגת היחידה מופיעה ב χ (רמז: הוכח שמספר זה שווה ל 1 אם הפעֻלה של G על X רגולרית.) בפרט, אם הפעֻלה של G על X יוצאת, $\rho = 1 \oplus \theta$, באשר θ הנה הצגה שאינה מכילה את הצגת היחידה. אם נסמן ב ψ את האפין של θ נקבל ש $\chi = 1 + \psi$ ו $\langle \psi, 1\rangle = 0$.

(ב) נגדיר פעֻלה של G על $X \times X$ על ידי הנֻסחה $g(x,y) = (gx, gy)$. הוכח שהאפין של הצגת התמורות המתאימה שווה ל χ^2. רמז: נצֵל את תרגיל יח.ג.

(ג) נניח שהפעֻלה של G על X **יוצאת פעמִים**, כלומר לכל x, y, x', y' המקיְמים $x \neq y$ ו $x' \neq y'$ קיָם $g \in G$ כך ש $gx = x'$ ו $gy = y'$. הוכח שהטענות הבאות שקולות זו לזו:

(ג.א) G יוצאת פעמִים.

(ג.ב) לפעֻלה של G על $X \times X$ יש שני מסלולים: האלכסון ומשלימוֹ.

(ג.ג) $\langle \chi^2, 1\rangle = 2$.

(ג.ד) ההצגה θ המֻגדרת ב (א) אי פריקה. ∎

נְיַשֵּׂם את הנֻסחאות דלעיל להצגה הרגולרית של חבורה:

משפטון יח.טו: *האפין r_G של ההצגה הרגולרית של חבורה סופית G מקיָם* $r_G(1) = |G|$ *ו* $r_G(g) = 0$ *לכל* $g \neq 0$.

הוכחה: נזכֹּר שלמרחב ההצגה V של ההצגה הרגולרית יש בסיס $\mathbf{v_h}$, באשר h עובר על אברי G ו $\rho(g)(\mathbf{v}_h) = \mathbf{v}_{gh}$. מכאן עולה ש r_G נִתן על ידי הנֻסחאות המופיעות במשפט. ∎

תוצאה יח.טז: *מספר הפעמים שהצגה אי פריקה ρ מופיעה בהצגה הרגולרית של חבורה סופית G שווה למעלתה.*

הוכחה: יהי χ האפין של ρ. לפי דֻגמה יח.יג שווה מספר הפעמים ש ρ מופיעה בהצגה הרגולרית של G ל $\langle r_G, \chi\rangle$. לפי משפטון יח.טו, $\langle r_G, \chi\rangle = \frac{1}{|G|}\sum_{g\in G} r_G(g^{-1})\chi(g) = \frac{1}{|G|}|G|\chi(1) = \deg(\rho)$. ∎

תוצאה יח.יז: *יהיו $W_1, \ldots, W_s$ מרחבי ההצגה האי פריקים של חבורה סופית G. אזי:*

(א) $\sum_{i=1}^{s}\dim(W_i)^2 = |G|$.

(ב) *אם* $g \neq 1$, *אזי* $\sum_{i=1}^{s}\deg(W_i)\chi_i(g) = 0$.

הוכחה: ראינו ש $r_G = \sum_{i=1}^{s}\dim(W_i)\chi_i$, כלומר $r_G(g) = \sum_{i=1}^{s}\dim(W_i)\chi_i(g)$ לכל $g \in G$. כידוע $\chi_i(g) = \dim(W_i)$. מאידך, $r_G(1) = |G|$ (משפט יח.טו). לכן, המקרה $g = 1$ נותן,

$\sum_{i=1}^{s} \dim(W_i)^2 = |G|$. אם $g \neq 1$, אזי $r_G(g) = 0$. לכן, $\sum_{i=1}^{g} \dim(W_i)\chi_i(g) = 0$, כפי שנטען. ∎

התוצאה האחרונה מקילה על מציאה כל ההצגות האי פריקות של חבורה סופית G: נניח ש $W_1, \ldots, W_s$ הן מרחבי הצגות לא איזומורפיות של G. אם $\sum_{i=1}^{s} \dim(W_i)^2 = |G|$, אזי לפי תוצאה יח.יז(א), אלו הן כל מרחבי ההצגות האי פריקות של G.