מבנים אלגבריים 1

מבוסס על הרצאות פרופ' ענר שלו
בקורס "מבנים אלגבריים 1" (80445)
האוניברסיטה העברית, סמסטר א' 2014
להערות: $nachi.avraham@gmail.com$
נחי

תודה לכל מי ששלח תיקונים, ובמיוחד לנעמה בויאר, ענבל יפה, דוד רייטבלט, רעות שאכו ואוריאל עצמון.
תודה גם לתום חן שנעזרתי בסיכום המומלץ שלו לאותו קורס.

תוכן עניינים

I תורת החבורות 5

1 חבורה 5

1.1 חבורה אבלית 6

1.2 תכונות של חבורות 6

1.3 חזקות בחבורות 8

1.4 סדר של חבורה או איבר 8

1.4.1 $o(x) \mid |G|$ 9

1.4.2 המשפט הקטן של פרמה 9

2 תתי־חבורות 10

3 מחלקות בחבורה (cosets) 11

3.1 אינדקס של תת־חבורה 12

3.2 משפט לגראנז' 12

4 חבורות נוצרות וציקליות 13

5 הצמדה 14

6 חבורות נורמליות 15

6.1 חבורות פשוטות 16

6.2 חבורות מנה 17

7 הומומורפיזם של חבורות 17

7.1 גרעין ותמונה של הומומורפיזם 18

8 משפטי האיזומורפיזמים של חבורות 20

8.1 משפט האיזומורפיזמים ה-I 20

8.2 ההטלה הקנונית $G \to G/N$ 22

8.3 משפט האיזומורפיזמים ה-II 22

8.4 משפט האיזומורפיזמים ה-III 23

8.5 משפט ההתאמה (איפיון תתי־חבורות של חבורות מנה) 24

9 אוטומורפיזמים של חבורה 25

9.1 אוטומורפיזמים פנימים 25

9.2 מרכז של חבורה 26

9.3 מכפלות ישרות 27

9.3.1 משפט השאריות הסיני 28

10 פעולה של חבורה על קבוצה 28

10.0.2 פעולה נאמנה (Faithful) 29

10.1 משפט קיילי 30

10.2 מסלולים ומייצבים 31

10.2.1 תכונות של מייצב 31

10.2.2 תכונות של מסלול 32

10.2.3 משפט מסלול־מייצב 33

10.3 פעולות טרנזיטיביות 34

10.4 ליבה (core) 34

10.4.1 שקילות פעולות 37

10.5 נקודות שבת 38

10.5.1 הלמה של ברנסייד 38

10.6 מחלקות צמידות ורכזים 39

10.6.1 משוואת המחלקות 40
10.7 משמר של תת־חבורה 41
11 משפט קושי 41
12 חבורות p 43
12.1 תורת סילו 44
12.1.1 משפט סילו ה-I 44
12.1.2 משפט סילו ה-II 46
12.1.3 משפט סילו ה-III 47
12.1.4 נורמליות ויחידות בחבורות p־סילו 48
12.1.5 משפט סילו ה-IV 48
12.1.6 משפט סילו ה-V 49
12.1.7 דוגמאות לחבורות p־סילו ושימוש בתורת סילו 50
12.2 תתי־חבורות של חבורות p 51
12.3 תתי־חבורות מקסימליות 52
13 סדרות נורמליות וסדרות הרכב 53
13.1 סדרות נורמליות 53
13.2 סדרות הרכב 53
13.3 קיום של סדרות הרכב (לחבורות סופיות) 54
13.4 יחידות של סדרות הרכב (עד־כדי סדר ואיזומורפיזם) 54
13.4.1 למת הפרפר של זסנהאוס 55
13.4.2 משפט העידון של שרייר 55
13.4.3 משפט ז'ורדן־הולדר 56
13.5 סדרות הרכב בחבורות שלמים 57
13.6 סדרות הרכב בחבורות תמורות 58
14 חבורות פתירות 59
15 קומוטטורים 62
15.1 תת־חבורה אופיינית 64
15.2 סדרה נגזרת 65
16 סקירה של כמה נושאים מתקדמים 66
16.1 משפט המבנה לחבורות אבליות נוצרות סופית 66
16.2 חבורות פשוטות סופיות 67
16.3 משפט הסדר האי־זוגי 67
16.4 השערת אורה (Ore) 67

II תורת החוגים 68

17 חוגים 68
18 אידאלים 70
18.1 פעולות על אידאלים 71
18.2 אידאל נוצר 71
18.3 חבורת האיברים ההפיכים 72
19 הומומורפיזמים של חוגים 72
20 חוגי מנה 73
20.1 ההטלה הקנונית $R \to {}^{R}/_{I}$ 75
21 משפטי האיזומורפיזמים של חוגים 75
21.1 משפט האיזומורפיזמים ה-I 75

21.2 משפט האיזומורפיזמים ה-II 76
21.3 משפט האיזומורפיזמים ה-III 76
22 משפט ההתאמה לחוגים 76
23 אידאל מקסימלי 77
23.1 קיום אידאל מקסימלי (הלמה של צורן) 77
24 תחום שלמות 78
24.1 יחס החלוקה 79
24.2 אי־פריקות וראשוניות 80
25 תחום ראשי 81
26 חוגים נתריים 83
26.1 פירוק איבר לא הפיך בתחום ראשי 83
27 החוג $\mathbb{F}[x]$ 85
27.1 שורש של פולינום 85
27.2 שדה הרחבה 86
27.3 שדה פיצול 88

חלק I
תורת החבורות

חבורה היא מושג שמכליל יחסי סימטריה שונים. למשל אוסף כל הסיבובים והשיקופים של משולש, ששומרים על סימטריה, מהווה חבורה.

1 חבורה

הגדרה: חבורה היא קבוצה G עם פעולה בינארית $\cdot : G\times G\to G$, המקיימת את התנאים הבאים:

1. **סגירות:** לכל $x,y\in G$ מתקיים $x\cdot y\in G$.[1]
2. **אסוציאטיביות:** לכל $x,y,z\in G$ מתקיים $(x\cdot y)\cdot z=x\cdot(y\cdot z)$.
3. **קיום איבר יחידה:** קיים $e\in G$ כך שלכל $x\in G$ מתקיים $x\cdot e=e\cdot x=x$.
4. **קיום הופכי:** לכל $x\in G$ קים איבר שיסומן $x^{-1}\in G$ המקיים $x^{-1}\cdot x=x\cdot x^{-1}=e$.

דוגמאות:

1. **החבורה הטריוויאלית:** חבורה בת איבר אחד שהינו איבר היחידה $\{e\}$.
2. **חבורות של שדות:**

(א) **חבורה כפלית:** לשדה $\mathbb{F}$ נסמן $\mathbb{F}^*=\mathbb{F}\backslash\{0\}$. החבורה הכפלית שלו היא $(\mathbb{F}^*,\cdot,1)$ ביחס לפעולת הכפל המוגדרת בשדה.

נשים לב כי $(\mathbb{F},\cdot,1)$ איננה חבורה שכן אין הופכי ל-0.

- דוגמאות אינסוף ממדיות לחבורות מסוג זה: $\mathbb{C}^*,\mathbb{R}^*,\mathbb{Q}^*$.
- דוגמאות סוף־ממדיות לחבורות מסוג זה: עבור p ראשוני, $\mathbb{Z}_p^*=\{1,...,p-1\}$ עם פעולת כפל מודולו p, היא חבורה בגודל $p-1$.
  ניתן להגדיר גם חבורה על חלק מהקבוצה $\mathbb{Z}_n$ עבור n שאיננו ראשוני, בכך שנגדיר:

$$\mathbb{Z}_n^*=\{1\le k\le n|\gcd(k,n)=1\}$$

ונקבל כי $(\mathbb{Z}_n^*,\cdot,1)$ היא חבורה ביחס לפעולת כפל מודולו n.

(א) **חבורה חיבורית:** לשדה $\mathbb{F}$, החבורה החיבורית שלו היא $(\mathbb{F},+,0)$, והיא חבורה ביחס לפעולת החיבור המוגדרת בשדה. (ההופכי של פעולה זו הוא הנגדי).
במקרה זה, $(\mathbb{Z}_n,+,0)$ היא חבורה חיבורית לכל n טבעי ולא רק עבור ראשוניים כמו במקרה הכפלי.

[1] נשים לב שתנאי זה גם נובע מהגדרת הפעולה $\cdot : G\times G\to G$.

1.1 חבורה אבלית

הגדרה: חבורה G נקראת **קומוטטיבית** או **אבלית** אם לכל $x,y\in G$ מתקיים $x\cdot y=y\cdot x$.

כל החבורות שהזכרנו עד כה היו אבליות.

דוגמאות לחבורות שאינן אבליות:

1. **החבורה הלינארית הכללית** (GL_n): בהנתן שדה $\mathbb{F}$, נגדיר את אוסף המטריצות ההפיכות מגודל $n\times n$ מעל השדה:[2]

$$GL_n\left(\mathbb{F}\right)=\left\{A\in M_n\left(\mathbb{F}\right)\mid\det\left(A\right)\neq 0\right\}$$

האוסף הנ"ל הוא חבורה כאשר פעולת החבורה תהיה פעולת כפל מטריצות ואיבר היחידה הוא $I_{n\times n}$.

2. נסמן ב-S_n את אוסף התמורות על המספרים $\{1,...,n\}$. זוהי חבורה ביחס לפעולת הרכבת פונקציות, ואיבר היחידה הוא תמורת הזהות.

גודל החבורה הוא $n!$, ובפרט לכל $3\leq n$ זוהי חבורה לא־אבלית.

3. נסמן ב-A_n את אוסף התמורות הזוגיות על המספרים $\{1,...,n\}$.[3] הסגירות של החבורה נובעת מכך שסימן של תמורה הוא כפלי:

$$\operatorname{sgn}\left(\sigma\tau\right)=\operatorname{sgn}\left(\sigma\right)\cdot\operatorname{sgn}\left(\sigma\right)$$

איבר היחידה הוא תמורת הזהות והאיבר ההופכי הוא התמורה ההופכית σ^{-1}.
גודל החבורה הוא $\frac{n!}{2}$.

4. **החבורה הלינארית המיוחדת** (SL_n):

$$SL_n\left(\mathbb{F}\right)=\left\{A\in M_n\left(\mathbb{F}\right)\mid\det\left(A\right)=1\right\}\subset GL_n\left(\mathbb{F}\right)$$

איבר היחידה כאן הוא עדיין $I_{n\times n}$ וסגירות נובעת מכפליות של הדטרמיננטה:

$$\det\left(AB\right)=\det\left(A\right)\det\left(B\right)$$

לכן אם $\det\left(A\right)=\det\left(B\right)=1$ נקבל כי $\det\left(AB\right)=1$.

1.2 תכונות של חבורות

תהא $(G,\cdot,e)$ חבורה, אזי:

1. איבר היחידה הוא יחיד.
2. ההופכי של כל איבר מוגדר ביחידות.
3. לכל $x\in G$ מתקיים $\left(x^{-1}\right)^{-1}=x$.

---

[2] אוסף המטריצות מגודל $n\times n$ מעל שדה $\mathbb{F}$ מסומן $M_n\left(\mathbb{F}\right)$.

[3] - "חילוף" הוא תמורה מהצורה (xy). כלומר תמורה שמחליפה מיקום של שני איברים.
- כל תמורה ניתנת להצגה כמספר סופי של חילופים.
- "תמורה זוגית" היא תמורה שניתן להצגה כמספר זוגי של חילופים, אחרת זו "תמורה אי־זוגית". כל תמורה היא זוגית או אי־זוגית.

4. לכל $x,y\in G$ מתקיים $(xy)^{-1}=y^{-1}x^{-1}$.

הוכחה:

1. נניח כי a,e הם איברי יחידה בחבורה, מכך נקבל כי $e=a\cdot e=a$.
2. יהי $x\in G$ ונניח כי a,x^{-1} הופכיים שלו. נקבל כי:

$$a=e\cdot a=\left(x^{-1}x\right)\cdot a=x^{-1}\cdot(xa)=x^{-1}\cdot e=x^{-1}$$

3. נשים לב כי x הוא הופכי ל-x^{-1} לפי ההגדרה, ולכן $x=\left(x^{-1}\right)^{-1}$, ומיחידות ההופכי נובע כי x הוא ההופכי של x^{-1}.
4. נוכיח כי זה ההופכי:

$$(xy)\left(y^{-1}x^{-1}\right)=x\left(y\cdot y^{-1}\right)x^{-1}=x\cdot e\cdot x^{-1}=x\cdot x^{-1}=e$$

חישוב דומה ייתן את אותה תוצאה עבור $\left(y^{-1}x^{-1}\right)(xy)$. ■

טענה: תהי G חבורה כך שלכל $x\in G$ מתקיים $x^2=e$, אזי G אבלית.

הוכחה: מהנתון $x^2=e$ לכל $x\in G$ נובע כי $x=x^{-1}$ לכל $x\in G$.

יהיו $g,h\in G$. מתקיים כי:

$$(gh)^2=e\iff(gh)(gh)=e\iff(gh)(hg)^{-1}=e\iff gh=hg$$

והשוויון השמאלי נובע מהנתון. ■

טענה: תהי G חבורה ונקבע $g\in G$ כלשהו. אזי ההעתקה $f:G\to G$ המוגדרת על ידי $f(x)=g\cdot x$ (כפל משמאל) היא חח"ע ועל (תמורה).

גם ההעתקה המקבילה של כפל מימין באיבר קבוע $f(x)=x\cdot g$ היא תמורה, וההוכחה כמעט זהה.

הוכחה:

נראה כי f חח"ע: יהיו $x,y\in G$, נחשב:

$$\begin{gathered}f(x)=f(y)\\ \Downarrow\\ gx=gy\\ \Downarrow\\ g^{-1}gx=g^{-1}gy\\ \Downarrow\\ x=y\end{gathered}$$

נראה כי f היא על: יהי $h\in G$, נמצא $x\in G$ שעבורו $f(x)=h$. נבחר $x=g^{-1}h$ ונקבל:

$$f\left(g^{-1}h\right)=g\cdot\left(g^{-1}h\right)=\left(gg^{-1}\right)h=he=h$$

■

מסקנה: בלוח הכפל של כל חבורה כל שורה וכל עמודה הן פרמוטציות של איברי החבורה. לחילופין, לוח הכפל של כל חבורה (סופית) מהווה ריבוע קסם.

ההפך לא נכון. יש הרבה יותר ריבועי קסם מאשר חבורות סופיות.

1.3 חזקות בחבורות

הגדרה: עבור כל $n > 0$, פעולת החזקה בחבורה עבור n טבעי מוגדרת $x^n = \underbrace{x \cdot x \cdot ... \cdot x}_{n\,\text{times}}$.

כמו־כן נגדיר $x^0 = e$ וכן $x^{-n} = \left(x^{-1}\right)^n$.

תכונות: תהי G חבורה ויהי $x \in G$, אזי לכל $n, m \in \mathbb{Z}$ מתקיים:

1. $x^{-n} = \left(x^{-1}\right)^n = \left(x^n\right)^{-1}$
2. $x^n x^m = x^{n+m}$
3. $\left(x^n\right)^m = x^{n \cdot m}$

(ההוכחה מושארת כתרגיל).

1.4 סדר של חבורה או איבר

הגדרה: תהי G חבורה, נאמר כי הגודל של G שמסומן $|G|$ הוא **הסדר של החבורה**.

אם G היא סופית יש לה סדר טבעי, ואם G אינסופית נסמן $|G| = \infty$.

הגדרה: תהי G חבורה ויהי $x \in G$, נגדיר את הסדר (order) של x להיות $0 < m$ הטבעי המינימלי שעבורו $x^m = e$. במקרה ולא קיים m כזה נאמר שהסדר של x אינסופי.

נהוג לסמן את הסדר של איבר ע"י $|x|$ או $o\left(x\right)$.

דוגמאות:

1. בכל חבורה מתקיים $o\left(e\right) = 1$ וזהו האיבר היחיד מסדר 1.
2. בחבורה $\mathbb{R}^*$ סדרי איברים אפשריים הם $1, 2, \infty$ בלבד.
   לדוגמה $o\left(2\right) = \infty$, שכן לא קיימת חזקה טבעית של 2 שעבורה $2^m = 1$.
3. בחבורה $\mathbb{C}^*$ קיימים איברים מסדר m לכל m טבעי (אלו הם שורשי היחידה המתאימים).
4. בחבורה הכפלית $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$ כל האיברים הם מסדר 1 או 2.

טענה: תהי G חבורה סופית, אזי לכל $x \in G$ יש סדר סופי.

הוכחה: נבחר $x \in G$ ונתבונן באוסף כל חזקותיו $P\left(x\right) = \{x^n | n \in \mathbb{N}\}$. מסגירות החבורה ידוע כי כל האיברים הללו שייכים ל-G ולכן $P\left(x\right) \subseteq G$ ומכך בהכרח קיימות חזרות. בפרט קיימים $k < n$ טבעיים שעבורם $x^n = x^k$ ולכן $x^{n-k} = e$, ומכאן שהסדר של x^{n-k} הוא לכל היותר $n - k$. ■

טענה: תהי G חבורה ויהי $x \in G$ כך ש-$o\left(x\right) = n$, אזי $x^m = e$ אמ"ם $n | m$.

תזכורת: לכל n, m טבעיים יש r, q שלמים יחידים, כך ש-$m = nq + r$, כאשר $0 \leq r < n$. (ניתן להוכיח באינדוקציה).

הוכחה: (כיוון ראשון)

נניח כי $n|m$, צ"ל כי $x^m = e$. מהנתון נובע שקיים k שלם שעבורו $m = nk$, ומכאן:

$$x^m = \left(x^{nk}\right) = \left(x^n\right)^k = e^k = e$$

(כיוון שני)

נניח כי $x^m = e$, צ"ל כי $n|m$. נחלק את m ב-n עם שארית $m = nq + r$ כאשר $0 \leq r < n$. מכך נקבל:

$$e = x^m = \left(x^{nq+r}\right) = x^{nq}x^r = \left(x^n\right)^q x^r = e^q x^r = x^r$$

אם $0 < r$ נקבל סתירה למינימליות של n, ולכן $r = 0$ ולכן $m|n$. ■

תכונות: תהי G חבורה, אזי:

1. $o\left(x\right) = o\left(x^{-1}\right)$ לכל $x \in G$.
2. $o\left(x\right) = o\left(g^{-1}xg\right)$ לכל $x, g \in G$.
3. בפרט מתקיים $o\left(gh\right) = o\left(hg\right)$ (גם אם החבורה לא אבלית).

1.4.1 $o\left(x\right) \mid |G|$

תהי G חבורה אבלית סופית, אזי לכל $x \in G$ מתקיים $x^{|G|} = e$.[4]

מסקנה: בתנאים אלה נסיק כי $|x| \mid |G|$ לכל $x \in G$.

הוכחה: נניח כי $|G| = n$, $G = \{x_1, ..., x_n\}$. בהינתן $x \in G$ כלשהו נתבונן באיברים $xx_1, ..., xx_n$, ונשים לב כי זו תמורה על איברי החבורה. כלומר קיימת $\pi \in S_n$ כך ש-$xx_i = x_{\pi(i)}$, $1 \leq i \leq n$.

מכך שהחבורה אבלית נסיק כי:

$$x^n x_1 x_2 ... x_n = \left(xx_1\right)\left(xx_2\right)...\left(xx_n\right) = x_{\pi(1)}x_{\pi(2)}...x_{\pi(n)} = x_1 x_2 ... x_n$$

מכאן ש-$x^n = e$. ■

מסקנה: לכל $x \in \mathbb{Z}_p^*$ מתקיים $x^{p-1} = 1$, עבור p ראשוני. זאת מכך ש-$\mathbb{Z}_p^* = \{1, ..., p-1\}$ ולכן $\left|\mathbb{Z}_p^*\right| = p - 1$.

1.4.2 המשפט הקטן של פרמה

יהיו x שלם ו-p ראשוני, אזי $x^p \equiv x \bmod p$.[5]

הוכחה: אם $p|x$ אז $0 \equiv 0 \bmod p$. נניח כי $p \nmid x$. נסמן $x = qp + r$ כאשר $0 \leq r < p$. מההנחה $p \nmid x$ נובע כי $0 < r < p$ ממש, ולכן $r \in \mathbb{Z}_p^*$.

---

[4] בהמשך נוכיח זאת לכל חבורה סופית.

[5] משמעות הסימון $a = b \bmod p$ היא כי $p|a-b$. כלומר ל-a, b אותה שארית בחלוקה ב-p.

מהמשפט הקודם נובע כי $r^{p-1}=1$ ב-$\mathbb{Z}_p^*$, כלומר $r^{p-1}=1 \mod p$ ב-$\mathbb{Z}$. נחשב:

$$\begin{gathered} x=qp+r \\ \Downarrow \\ x\equiv r \mod p \\ \Downarrow \\ x^{p-1}\equiv r^{p-1} \mod p = 1 \mod p \\ \Downarrow \\ x^p \equiv x \mod p \end{gathered}$$

■

2 תתי־חבורות

הגדרה: תהי G חבורה, תת־קבוצה $\emptyset \neq H \subseteq G$ נקראת תת־חבורה של G, אם H עצמה מהווה חבורה ביחס לפעולה המוגדרת ב-G.

כלומר אם לכל $x,y\in H$ מתקיים $x\cdot y \in H$ וכן לכל $x\in H$ מתקיים $x^{-1}\in H$.[6]
נהוג לסמן תת־חבורה $H\leq G$.

הגדרה־שקולה: תהי G חבורה, תת־קבוצה $\emptyset \neq H \subseteq G$ נקראת תת־חבורה של G אם לכל $x,y\in H$ מתקיים $xy^{-1}\in H$.

הוכחה: (כיוון ראשון)

נניח את ההגדרה הראשונה, ונקבל כי מסגירות מתקיים לכל $x,y\in H$ כי $xy^{-1}\in H$ וכן כי $H\neq\emptyset$.

(כיוון שני)

נתון כי $H\neq \emptyset$ ולכן קיים $x\in H$. מהתנאי בהגדרה השנייה נובע כי $e=xx^{-1}\in H$.

נראה סגירות להופכי: עבור $x\in H$ מתקיים גם $e\in H$ ולכן $ex^{-1}=x^{-1}\in H$.

נראה סגירות תחת הכפל: עבור $x,y\in H$ נקבל כי $ey^{-1}=y^{-1}\in H$ ולכן $xy=x\left(y^{-1}\right)^{-1}\in H$. ■

טענה: תהי G חבורה אבלית. אם $|G|=p$ עבור p ראשוני, אזי תתי החבורות היחידות שלה הן $G,\{e\}$.[7]

הוכחה: תהי $H\leq G$. אם $H=\{e\}$ סיימנו, לכן נניח $H\neq\{e\}$, כלומר יש $e\neq x\in H$.

נזכור שהראינו כי $|x|\,\big|\,|G|=p$ וידוע כי $|x|>1$ (כי $x\neq e$) ומכאן כי $|x|=p$.

מכאן נובע כי כל האיברים $e,x,x^2,...,x^{p-1}$ שונים, כי אם $x^i=x^j$ אז $x^{i-j}=e$ בסתירה לכך ש-$|x|=p$.

אם כך קיבלנו p איברים שונים זה מזה שמוכלים ב-H, ולכן בהכרח $H=G$. ■

טענה: תהי G חבורה ויהיו $K,H\leq G$, אזי $K\cap H\leq G$.

הטענה נכונה לחיתוך של כל כמות תתי־חבורות.

---

[6] מההנחה כי H אינה ריקה נובע כי יש $x\in H$, מקיום ההופכי והסגירות נסיק כי $e=xx^{-1}\in H$.
[7] בהמשך נוכיח זאת לכל חבורה.

3 מחלקות בחבורה (cosets)

הגדרה: תהי G חבורה ותהי $H \leq G$. נקבע $g \in G$ ונגדיר מחלקה שמאלית וימנית של H (בהתאמה):

$$gH = \{gh | h \in H\} \quad Hg = \{hg | h \in H\}$$

הערה: לכל $h \in H$, מסגירות לכפל נובע שמתקיים $hH = Hh = H$.

הערה: מכך שכפל באיבר מהחבורה מגדיר תמורה על איברי החבורה, נסיק שעבור G חבורה ו-$H_1, H_2 \leq G$, כך ש-$H_1 \subseteq H_2$, לכל $g \in G$ מתקיים $gH_1 \subseteq gH_2$. ובאופן זהה גם עבור מחלקות ימניות.

טענה: תהי $H \leq G$, אזי $g_1H = g_2H \iff g_2^{-1}g_1 \in H$.

הוכחה: (כיוון ראשון)

אם $g_1H = g_2H$ אז בפרט $g_1 = g_1 \cdot e \in g_2H$ ולכן קיים $h \in H$ כך ש-$g_1 = g_2h$, ומכאן כי $g_2^{-1}g_1 = h \in H$.

(כיוון שני)

אם $g_2^{-1}g_1 \in H$ אז $g_2^{-1}g_1H = H$ ולכן קיים $h \in H$ כך ש-$g_2^{-1}g_1 = h$, כלומר $g_1 = g_2^{-1}h$ ומכאן כי $g_1H = (g_2h)H = g_2H$. ■

טענה: תהי $H \leq G$, אזי כל זוג מחלקות שמאליות (או ימניות) הן זרות או שוות.

הוכחה: נראה כי אם $g_1H \cap g_2H \neq \emptyset$ אז $g_1H = g_2H$.

מההנחה שהחיתוך אינו ריק נובע שיש $h_1, h_2 \in H$, לא בהכרח שונים, כך שמתקיים $g_1h_1 = g_2h_2$.

יהי $g_1h \in gH$ כלשהו, נסיק כי:

$$g_1h = g_1eh = g_1h_1h_1^{-1}h = (g_1h_1)\left(h_1^{-1}h\right) =$$

$$= (g_2h_2)\left(h_1^{-1}h\right) = g_2\left(h_2h_1^{-1}h\right) \in g_2H$$

ולכן מתקיים כי $g_1H \subseteq g_2H$. באופן סימטרי נוכל להסיק גם את ההכלה ההפוכה, ונקבל $g_1H = g_2H$. ■

משפט: תהי $H \leq G$, אזי קיימת קבוצת אינדקסים I (סופית או לא) כך שמתקיים:

$$G = \biguplus_{i \in I} g_iH, \; g_i \neq g_j$$

[הסימון $\biguplus$ מתייחס לאיחוד זר.]

כלומר, איחוד כל המחלקות השמאליות (או הימניות) הזרות מהווה חלוקה של החבורה.

הוכחה: ברור כי מתקיים $G=\bigcup\limits_{g\in G} gH$, מכיוון שכל $g\in G$ מקיים $g\in gH$.

האיחוד שהגדרנו אולי אינו זר, ולכן ניקח את כל המחלקות השונות זו מזו ונסמנן ב-g_iH, $i\in I$ (כלומר נמחק את כל החזרות), ונקבל כי $g_iH\neq g_jH$ לכל $i\neq j$.

מטענה קודמת נובע כי $g_iH\cap g_jH=\emptyset$ ולכן קיבלנו כי האיחוד לא ישתנה, ומתקיים:

$$G=\bigcup_{g\in G} gH=\bigcup_{i\in I} g_iH$$

■

3.1 אינדקס של תת־חבורה

הגדרה: תהי $H\leq G$, נגדיר את האינדקס של H ב-G להיות מספר המחלקות השמאליות השונות של H ב-G. נסמן זאת $[G:H]$.

טענה: האינדקס של תת־חבורה מוגדר היטב ללא תלות במחלקות ימניות או שמאליות. כלומר מספר המחלקות הימניות שווה למספר המחלקות השמאליות.

הוכחה: תהי $H\leq G$. נגדיר העתקה בין אוסף המחלקות הימניות לבין אוסף המחלקות השמאליות על־ידי $gH\mapsto (gH)^{-1}=Hg^{-1}$.

נוכיח שהיא חח"ע: נניח כי $g_1H=g_2H$, ראינו שזה תנאי שקול לכך שמתקיים $g_2^{-1}g_1\in H$. מהיות H תת־חבורה נקבל כי $g_1^{-1}g_2=\left(g_2^{-1}g_1\right)^{-1}\in H$. מהפעלת התנאי השקול הנ"ל למחלקות ימניות, נקבל שזה אומר כי $Hg_2^{-1}=Hg_1^{-1}$.

נוכיח שהיא על: כל מחלקה ימנית Hg מתקבלת מהמחלקה השמאלית $g^{-1}H$.

מכך שזו העתקה חח"ע ועל נובע כי מספר המחלקות השמאליות והימניות שווה.■

3.2 משפט לגראנז'

משפט: תהי $H\leq G$, סופית או לא, אזי $|G|=[G:H]\cdot|H|$.

הוכחה: ראינו כי $G=\biguplus\limits_{i\in I} g_iH$ כאיחוד זר ולכן ברור כי $[G:H]=|I|$, כי שניהם מייצגים את מספר המחלקות השונות. נסיק מכך:

$$|G|=\sum_{i\in I}|g_iH|=\sum_{i\in I}|H|=|I|\cdot|H|=[G:H]\cdot|H|$$

השוויון השני נובע מכך שגודל של מחלקה לא משתנה כתוצאה מכפל בקבוע של כל איבריה. ■

מסקנה: אם G סופית אז $[G:H]=\frac{|G|}{|H|}$.

משפט לגראנז': תהי G חבורה סופית ותהי $H\leq G$, אזי $|H|\,\big|\,|G|$.

הוכחה: נובע מהמשפט האחרון.

מסקנה 1: אם G סופית, אז לכל $x \in G$ מתקיים $|x|\,\big|\,|G|$.

מכך גם נובע שמתקיים $x^{|G|} = e$, לפי טענה קודמת שאם $|x|\,\big|\,n$ אז $x^n = e$.

הוכחה: נסמן ב-$\langle x \rangle$ את תת החבורה הנוצרת על־ידי x. קל לראות שזו זו תת־חבורה.

ממשפט לגראנז' נובע כי $|\langle x \rangle|\,\big|\,|G|$, וקל לראות שמתקיים $|x| = |\langle x \rangle|$, כי $\langle x \rangle = \{e, x, x^2, ..., x^{|x|-1}\}$, ולכן נסיק כי $|x|\,\big|\,|G|$. ■

מסקנה 2: לחבורה G מסדר p ראשוני יש רק שתי תת־חבורות - G, $\{e\}$.

מסקנה 3: כל חבורה G מסדר p ראשוני היא ציקלית (כלומר נוצרת על־ידי איבר $x \in G$), ולכן גם אבלית.

הוכחה: ניקח $e \neq g \in G$ ונתבונן בתת החבורה שהוא יוצר, ונשים לב שהיא בהכרח לא טריוויאלית. גודל תת־חבורה זו חייב לחלק את $p = |G|$ ולכן $p = |\langle g \rangle|$, כלומר $\langle g \rangle = G$. ■

מסקנה 4: יש רק "חבורה אחת" מכל סדר p ראשוני. כלומר עד כדי איזומורפיזם. (נראה בהמשך).

4 חבורות נוצרות וציקליות

הגדרה: תהי G חבורה ויהי $x \in G$, נגדיר את החבורה הנוצרת על ידי x להיות $\langle x \rangle = \{x^k | k \in \mathbb{Z}\}$. כלומר אוסף כל החזקות של x ב-G. קל לראות שזו תת־חבורה.

הגדרה: תהי G חבורה ותהי $X \subseteq G$ תת־קבוצה. נגדיר את תת־החבורה של G הנוצרת על ידי X להיות $\langle X \rangle = \bigcap_{\substack{H \leq G \\ X \subseteq H}} H$.

הערות:

1. אם $X = \{x_1, ..., x_n\}$ נסמן $\langle X \rangle = \langle x_1, ..., x_n \rangle$.
2. מאחר וחיתוך של תת־חבורות הוא תת־חבורה נקבל כי $\langle X \rangle$ היא תת־חבורה של G.
3. אם H תת־חבורה של G שמכילה את X, אז $\langle X \rangle \subseteq H$. מכך ניתן לראות כי $\langle X \rangle$ היא תת־החבורה המינימלית ב-G (ביחס להכלה) שמכילה את X ולכן היא מוגדרת ביחידות.
4. אם $\langle X \rangle = G$ נאמר ש-X יוצרת את G או ש-X מהווה קבוצת יוצרים של G.
5. אם $\langle X \rangle = G$ אבל לכל $Y \subset X$ ממש מתקיים $\langle Y \rangle \neq G$, נאמר ש-X היא קבוצת יוצרים מינימלית של G (ביחס להכלה).

אפיון־שקול: תהי G חבורה ותת־קבוצה $X \subseteq G$, החבורה הנוצרת $\langle X \rangle$ היא אוסף כל המכפלות הסופיות של איברי X (ה"מילים"):

$$\langle X \rangle = \{x_1^{\varepsilon_1} \cdot ... \cdot x_n^{\varepsilon_n} | 0 \leq n \in \mathbb{N},\, x_i \in X,\, \varepsilon_i \in \{\pm 1\}\} \equiv S$$

כאשר מכפלה באורך 0 מוגדרת להיות e ולכן בפרט $\langle\emptyset\rangle = \{e\}$.

ההגדרה הקודמת שנתנו הייתה הגדרה "מלמעלה" ומאידך זוהי הגדרה על ידי בנייה "מלמטה".

הוכחה: ראשית נראה כי S היא תת־חבורה של G:

סגירות: כל איבר של S הוא מכפלה סופית של איברי X והופכיהם, לכן מכפלה של שני איברים כאלו היא עדיין מכפלה סופית של איברי X והופכיהם.

קיום יחידה: $e \in S$ שכן הגדרנו מכפלה ריקה להיות e.

סגירות להופכי: בהנתן $x_1^{\varepsilon_1}...x_n^{\varepsilon_n} \in S$ קל לראות כי:

$$(x_1^{\varepsilon_1}...x_n^{\varepsilon_n})^{-1} = x_n^{-\varepsilon_n}...x_1^{-\varepsilon_1} \in S$$

באופן מיידי ניתן לראות כי $X \subseteq S$ שכן לכל $x \in X$ מתקיים $x = x^1 \in S$ (מכפלה באורך 1). לכן $\langle X\rangle \subseteq S$.

כעת נראה את ההכלה ההפוכה: בהנתן $x_1^{\varepsilon_1}...x_n^{\varepsilon_n} \in S$ נשים לב כי לכל $1 \le i \le n$ מתקיים $x_i \in \langle X\rangle$.

ידוע כי $\langle X\rangle$ תת־חבורה ולכן לכל $\varepsilon_i \in \{\pm 1\}$ מתקיים $x_i^{\varepsilon_i} \in \langle X\rangle$, וכן $x_1^{\varepsilon_1}...x_n^{\varepsilon_n} \in \langle X\rangle$.

מכך ניתן לראות כי אכן מתקיים שיוויון $S = \langle X\rangle$, כנדרש.

הגדרה: חבורה G נקראת ציקלית, אם היא נוצרת על ידי איבר אחד $x \in G$. כלומר קיים $x \in G$ כך ש-$G = \langle x\rangle$.

טענה: כל חבורה ציקלית היא אבלית.

הוכחה: לכל $g, h \in \langle x\rangle$ קיימים $m, n \in \mathbb{Z}$ כך ש-$g = x^m$ ו-$h = x^n$, ומכך:

$$gh = x^m x^n = x^{m+n} = x^{n+m} = x^n x^m = hg$$

■

5 הצמדה

הגדרה: תהי G חבורה, עבור $x, g \in G$ ההצמדה של x על ידי g מוגדרת ומסומנת $x^g =: g^{-1}xg$.

הגדרה: תהי G חבורה ויהי $x \in G$, מחלקת הצמידות של x ב-G מוגדרת ומסומנת:

$$x^G =: \left\{g^{-1}xg | g \in G\right\} = \left\{gxg^{-1} | g \in G\right\}$$

הערה: יחס הצמידות הוא יחס שקילות. כלומר מקיים רפלקסיביות (x צמוד ל-x על־ידי e), סימטריות (אם x צמוד ל-y אז y צמוד ל-x) וטרנזיטיביות (אם x צמוד ל-y ו-y צמוד ל-z, אז x צמוד ל-z).

הערה: $G=x_1^G \uplus ... \uplus x_n^G$ כאיחוד זר.[8]

תכונות:

1. $|x^g|=|x|$

2. $(xy)^g=x^g y^g$, כי:

$$g^{-1}xyg=g^{-1}xgg^{-1}yg=x^g y^g$$

3. $(x^n)^g=(x^g)^n$, כי:

$$gx^ng^{-1}=gxx...xg^{-1}=gxgg^{-1}xgg^{-1}...gg^{-1}xg^{-1}=\left(gxg^{-1}\right)^n$$

4. הפונקציה $x\mapsto x^g$ היא חח"ע ועל $G\to G$.

חח"ע:

$$x^g=y^g\Longrightarrow gxg^{-1}=gyg^{-1}\Longrightarrow x=y$$

על: כל $x\in G$ מתקבל על־ידי הצמדה של $g^{-1}xg$ ב-g.

6 חבורות נורמליות

תהא G חבורה ותהי $N\le G$. נאמר כי N היא תת־חבורה נורמלית ב-G ונסמן $N\lhd G$, אם לכל $g\in G$ מתקיים $gNg^{-1}\subseteq N$.

תנאים שקולים לנורמליות

תהא $N\le G$. התנאים הבאים שקולים:

1. $N\lhd G$
2. לכל $g\in G$ מתקיים $gNg^{-1}=N$.
3. לכל $g\in G$ מתקיים $gN=Ng$.
4. N היא איחוד מחלקות צמידות ב-G.

הוכחה: $(2\Leftarrow 1)$

[8] כל זוג מחלקות צמידות הם זהות או זרות, וכל x שייך למחלקת צמידות כלשהי. ניקח רק מחלקות צמידות שונות ונקבל את המבוקש.

נתון כי $N \lhd G$, כלומר $gNg^{-1} \subseteq N$. נרצה להראות את ההכלה ההפוכה:

$$gNg^{-1} \subseteq N$$
$$\Downarrow$$
$$g^{-1}N\left(g^{-1}\right)^{-1} \subseteq N$$
$$\Downarrow$$
$$gg^{-1}N\left(g^{-1}\right)^{-1}g^{-1} \subseteq gNg^{-1}$$
$$\Downarrow$$
$$N \subseteq gNg^{-1}$$

($2 \Leftarrow 1$**)** טריוויאלי.

($3 \Leftarrow 2$)

$$gNg^{-1} = N$$
$$\Downarrow$$
$$gN = Ng$$

($2 \Leftarrow 3$)

$$gN = Ng$$
$$\Downarrow$$
$$gNg^{-1} = N$$

($4 \Leftarrow 1$) אם $gNg^{-1} \subseteq N$ אז כל $n \in N$ מקיים $n = gmg^{-1}$ ל-$m \in N$. כלומר כל איברי N הם צמודים של איבר כלשהו.

($1 \Leftarrow 4$) מהנתון ש-N איחוד של מחלקות צמידות נובע כי $N = \bigcup_{n \in N} n^G$, כלומר כל $gng^{-1} \in N$ ולכן $gNg^{-1} \subseteq N$. ■

טענה: תהי $H \leq G$ תת־חבורה כך ש-$[G:H] = 2$, אזי $H \lhd G$.

הוכחה: מכך ש-$[G:H] = 2$ נובע שיש רק שתי מחלקות שמאליות. כלומר $G = H \biguplus gH$ עבור $g \in G \backslash H$ כלשהו. מכך שהאיחוד זר נובע $gH = G \backslash H$.

מספר המחלקות הימניות שווה למספר המחלקות השמאליות, ולכן נקבל מאותו נימוק שמתקיים $G = H \biguplus Hg$, וכנ"ל $Hg = G \backslash H$.

משני השוויונים נסיק כי $gH = Hg$, וקיבלנו את אחד התנאים השקולים לנורמליות.
■

6.1 חבורות פשוטות

החבורות הפשוטות הסופיות נחשבות ל"אטומים" בעולם החבורות. בסוף המאה ה-20 הוכח "משפט המיון לחבורות פשוטות סופיות", שמיין את כל סוגי החבורות הפשוטות הסופיות.

הגדרה: חבורה $G \neq \{e\}$ נקראת **פשוטה**, אם תת החבורות הנורמליות היחידות שלה הן $G, \{e\}$.

טענה: כל חבורה מסדר ראשוני היא פשוטה.

הוכחה: הראינו שלכל חבורה מסדר ראשוני אין תת־חבורות לא טריוויאליות, ובפרט אין לה תת־חבורות נורמליות לא טריוויאליות. ■

6.2 חבורות מנה

הגדרה: נניח כי $N \lhd G$, נגדיר את הקבוצה $G/N = \{gN | g \in G\}$.[9]

נגדיר כפל על הקבוצה הזו $aN \cdot bN = \{xy | x \in aN,\, y \in bN\}$.

טענה: $aNbN = abN$

הוכחה:

$$aNbN = a\left(Nb\right)N = a\left(bN\right)N = abN$$

כאשר השוויון השני נובע מנורמליות N ב-G. (ניתן להגדיר כך מראש את פעולת הכפל). ■

טענה: הקבוצה G/N היא חבורה ביחס לכפל שהגדרנו.

הוכחה: איבר היחידה הוא $eN = N$, כי $\left(gN\right)N = Ng\left(N\right) = gN$.

נחשב אסוציאטיביות:

$$aN\left(bNcN\right) = aN\left(bcN\right) = a\left(bc\right)N = \left(ab\right)cN = \left(abN\right)cN = \left(aNbN\right)cN$$

קיום הופכי: $\left(gN\right)^{-1} = g^{-1}N$, שכן:

$$\left(gN\right)\left(g^{-1}N\right) = \left(gg^{-1}\right)N = N$$

דוגמאות:

1. $G/G = \{G\} \cong \{e\}$ כי G משמשת פה כתת החבורה הנורמלית, והראינו שאיבר היחידה בחבורת המנה הוא תת החבורה הנורמלית.
2. $G/\{e\} = \{g \cdot \{e\} | g \in G\} \cong G$

טענה: בחבורה G סופית מתקיים $|G/N| = \frac{|G|}{|N|}$.

הוכחה: ראינו כי $\frac{|G|}{|N|} = [G:N]$. כמו־כן $|G/N|$ הוא גודל אוסף המחלקות השמאליות השונות, שזה בדיוק האינדקס של N ב-G. ■

7 הומומורפיזם של חבורות

הגדרה: יהיו G, H חבורות. העתקה מהצורה $f : G \to H$ נקראת **הומומורפיזם** אם לכל $x, y \in G$ מתקיים:

$$f\left(x \cdot y\right) = f\left(x\right) \cdot f\left(y\right)$$

נשים לב כי הכפל על x, y הוא הפעולה המוגדרת ב-G, והכפל על $f\left(x\right), f\left(y\right)$ הוא הפעולה המוגדרת ב-H.

[9] קל לראות שמתקיים $|G/N| = [G:N]$.

- הומומורפיזם **חח"ע** נקרא **מונומורפיזם**
- הומומורפיזם **על** נקרא **אפימורפיזם**
- הומומורפיזם **חח"ע ועל** נקרא **איזומורפיזם**

אם קיים איזומורפיזם $f : G \to H$, מסמנים $G \cong H$.

טענה: תהי $f : G \to H$ הומומורפיזם, אזי:

1. $f(e_G) = e_H$
2. $f\left(x^{-1}\right) = f^{-1}(x)$
3. $f\left(x^k\right) = f^k(x)$ לכל k שלם.

הוכחה:

1. נחשב:

$$f(e_G) = f(e_G e_G) = f(e_G) f(e_G)$$

$$\Downarrow$$

$$f(e_G) = e_H$$

2. נחשב:

$$f(x) f\left(x^{-1}\right) = f\left(xx^{-1}\right) = f(e) = e$$

$$f\left(x^{-1}\right) f(x) = f\left(x^{-1}x\right) = f(e) = e$$

3. מהכפליות נובע באינדוקציה שמתקיים:

$$f(x_1 x_2 ... x_n) = f(x_1) f(x_2) ... f(x_n)$$

עבור $x_1 = x_2 = ... = x_n$ נקבל את השוויון הנדרש עבור $0 < n$.
בשילוב טענה 2 נקבל את הטענה עבור $n < 0$. ■

7.1 גרעין ותמונה של הומומורפיזם

הגדרה: יהי $f : G \to H$ הומומורפיזם. מגדירים:

$$\ker(f) = \{x \in G | f(x) = e_H\} \subseteq G$$

$$\text{image}(f) = \{f(x) \in H | x \in G\} \subseteq H$$

טענה:

1. $\ker(f)$ הוא תת־חבורה נורמלית של G.
2. $\text{image}(f)$ הוא תת־חבורה (לאו דווקא נורמלית) של H.

הוכחה:

1. איבר יחידה: $f(e)=e$ ולכן $e\in\ker(f)$.
סגירות לכפל:

$$\begin{gathered}x,y\in\ker(f)\\ \Downarrow\\ f(x)=f(y)=e\\ \Downarrow\\ f(xy)=f(x)f(y)=e\\ \Downarrow\\ xy\in\ker(f)\end{gathered}$$

סגירות להופכי:

$$\begin{gathered}x\in\ker(f)\\ \Downarrow\\ f(x)=e\\ \Downarrow\\ f\left(x^{-1}\right)=f^{-1}(x)=e^{-1}=e\\ \Downarrow\\ x^{-1}\in\ker(f)\end{gathered}$$

נראה שזו תת־חבורה נורמלית. כלומר יש להראות כי אם $x\in\ker(f)$, אז לכל $g\in G$ מתקיים $gxg^{-1}\in\ker(f)$. נחשב:

$$f\left(gxg^{-1}\right)=f(g)f(x)f\left(g^{-1}\right)=f(g)f\left(g^{-1}\right)=f\left(gg^{-1}\right)=e$$

2. איבר יחידה: $e=f(e)$ ולכן $e\in\text{image}(f)$.
סגירות לכפל:

$$\begin{gathered}x,y\in\text{image}(f)\\ \Downarrow\\ \exists_{t_1,t_2\in G}\, x=f(t_1),\ y=f(t_2)\\ \Downarrow\\ xy=f(t_1)f(t_2)=f(t_1t_2)\\ \Downarrow\\ xy\in\text{image}(f)\end{gathered}$$

סגירות להופכי:

$$\begin{gathered}f(x)\in\text{image}(f)\\ \Downarrow\\ f\left(x^{-1}\right)\in\text{image}(f)\\ \Downarrow\\ f^{-1}(x)\in\text{image}(f)\end{gathered}$$

נראה דוגמה לתת־חבורה $\mathrm{image}\left(f\right)$ שאינה נורמלית. ניקח את ההומומורפיזם $f:S_{2}\to S_{3}$ המוגדר להיות:

$$f\left(x\right)=\begin{cases} e & x=e\\ \left(12\right) & x=\left(12\right)\end{cases}$$

נשים לב כי $\ker\left(f\right)=\left\{ e\right\} ,\mathrm{image}\left(f\right)=\left\{ e,\left(12\right)\right\}$, אבל S_{2} אינה נורמלית ב-S_{3}. ■

טענה: הומומורפיזם f הוא חח"ע אמ"מ $\ker\left(f\right)=\left\{ e\right\}$.

הוכחה: (כיוון ראשון)

אם $x\in\ker\left(f\right)$ אז $f\left(x\right)=e$. אבל ידוע כי $f\left(e\right)=e$ ולכן $f\left(x\right)=f\left(e\right)$. מכך ש-$f$ חח"ע נובע $x=e$.

(כיוון שני)

נניח כי $\ker\left(f\right)=\left\{ e\right\}$. נניח כי $f\left(x\right)=f\left(y\right)$, ונחשב:

$$\begin{gathered}f\left(x\right)=f\left(y\right)\\ \Downarrow\\ f\left(x\right)f^{-1}\left(y\right)=e\\ \Downarrow\\ f\left(xy^{-1}\right)=e\\ \Downarrow\\ xy^{-1}=e\\ \Downarrow\\ x=y\end{gathered}$$

■

טענה: יהי $f:G_{1}\to G_{2}$ הומומורפיזם ותהי $H\leq G_{2}$, אזי המקור של H, כלומר הקבוצה $A=:\left\{ g\in G_{1}|\exists_{h\in H}f\left(g\right)=h\right\} \subseteq G_{1}$, היא תת־חבורה של G_{1}.

הוכחה: מתקיים כי $e\in H$ וכן $f\left(e\right)=e$ ולכן $e\in A$.

סגירות לכפל מתקיימת כי לכל $g_{1},g_{2}\in A$ קיימים $f\left(g_{1}\right),f\left(g_{2}\right)\in H$, ולכן מתקיים:

$$f\left(g_{1}g_{2}\right)=f\left(g_{1}\right)f\left(g_{2}\right)\in H$$

ומכאן כי $g_{1}g_{2}\in A$.

סגירות להופכי מתקיימת כי לכל $g\in A$ קיים $f\left(g\right)\in H$. אבל H תת־חבורה ולכן $f^{-1}\left(g\right)\in H$ ומכאן כי $f\left(g^{-1}\right)\in H$, כלומר $g^{-1}\in A$. ■

8 משפטי האיזומורפיזמים של חבורות

8.1 משפט האיזומורפיזמים ה-I

יהי $f:G\to H$ הומומורפיזם של חבורות, אזי $\mathrm{image}\left(f\right)\cong{}^{G}/_{\ker\left(f\right)}$.

הוכחה: יהי $f : G \to H$ הומומורפיזם. נסמן $K = \ker(f) \lhd G$.

1. נגדיר פונקציה מהצורה $\Psi : {}^{G}\!/_{K} \to \text{image}(f)$ להיות $\Psi(xK) = f(x)$, ונוכיח כי היא איזומורפיזם.
ראשית נראה כי Ψ מוגדרת היטב (כלומר אינה תלויה בנציגים): כלומר יש להוכיח כי אם $xK = yK$ אז $\Psi(xK) = \Psi(yK)$, כלומר $f(x) = f(y)$.
נשים לב שמצד אחד מתקיים:

$$\begin{gathered} xK = yK \\ \Downarrow \\ x^{-1}y \in K \\ \Downarrow \\ f\left(x^{-1}y\right) = e \\ \Downarrow \\ f(x) = f(y) \end{gathered}$$

כאשר הגרירה האחרונה נובעת מתכונות ההומומורפיזם.

2. נוכיח כי Ψ הומומורפיזם:

$$\Psi(xKyK) = \Psi(xyK) = f(xy) = f(x)\,f(y) = \Psi(xK)\,\Psi(yK)$$

3. נוכיח כי Ψ חח"ע:

$$\begin{gathered} \Psi(xK) = \Psi(yK) \\ \Downarrow \\ f(x) = f(y) \\ \Downarrow \\ f\left(x^{-1}y\right) = e \\ \Downarrow \\ x^{-1}y \in K \\ \Downarrow \\ x^{-1}yK = K \\ \Downarrow \\ xK = yK \end{gathered}$$

4. נוכיח כי Ψ על: צ"ל שלכל $y \in \text{image}(f)$ קיים $x \in G$ כך ש-$y = \Psi(xK)$.
אבל כל איבר ב-$\text{image}(f)$ הוא מהצורה $f(x)$, ולכן $xK \mapsto f(x)$ וקיים x כנדרש.

5. נסיק כי Ψ הומומורפיזם חח"ע ועל בין ${}^{G}\!/_{K}$ לבין $\text{image}(f)$, ולכן ${}^{G}\!/_{K} \cong \text{image}(f)$. ■

דוגמאות:

1. ההעתקה $\text{sgn} : S_n \to \{\pm 1\}$ היא הומומורפיזם בגלל כפליות הסימן.
כמו־כן מתקיים $\ker(\text{sgn}) = A_n$, $\text{image}(\text{sgn}) = \{\pm 1\} \cong \mathbb{Z}_2$, ולכן נסיק ${}^{S_n}\!/_{A_n} \cong \mathbb{Z}_2$.
מכך גם נובע כי $[S_n : A_n] = 2$ ולכן $A_n \lhd S_n$.

2. ההעתקה $\det : GL_n(\mathbb{F}) \to \mathbb{F}^*$ היא הומומורפיזם בגלל כפליות הדטרמיננטה. כמו־כן מתקיים $\text{image}(\det) = \mathbb{F}^*$, $\ker(\det) = SL_n(\mathbb{F})$, ולכן נסיק $GL_n/SL_n \cong \mathbb{F}^*$.

8.2 ההטלה הקנונית $G \to G/N$

הגדרה: תהי G חבורה ותהי $N \lhd G$. נגדיר העתקה מהצורה $\pi : G \to G/N$ באופן הבא:

$$\pi(g) = gN = Ng \in G/N$$

טענה: π היא הומומורפיזם של חבורות, והיא העתקה על.

הוכחה: נראה כי זה הומומורפיזם:

$$\pi(gh) = ghN = gNhN = \pi(g)\pi(h)$$

נראה כי זו העתקה על: לכל $gN \in G/N$ מתקיים כי $gN = \pi(g)$. ■

8.3 משפט האיזומורפיזמים ה-II

טענה: תהי G חבורה ויהיו תתי החבורות $H \le G$, $K \lhd G$, אזי מתקיים:

1. $H \cap K \lhd H$
2. $HK \le G$
3. $K \lhd HK$

הוכחה:

1. $H \cap K$ הוא חיתוך של תת־חבורות ולכן הוא תת־חבורה. נראה כי $H \cap K \lhd H$:

$$h(H \cap K)h^{-1} = \left(hHh^{-1}\right) \cap \left(hKh^{-1}\right) = H \cap K$$

כאשר השוויון הראשון נובע מכך ש-$hHh^{-1} = H$ והשני נובע מכך ש-$h \in H$ ומכך ש-K נורמלית ב-G.

2. **למה:** יהיו $H, K \le G$, אזי $HK = \{hk | h \in H, k \in K\} \subseteq G$ היא תת־חבורה של G אמ"מ $HK = KH$. (ההוכחה מושארת כתרגיל)

אם כך מספיק להראות כי $HK = KH$:

$$HK = \bigcup_{h \in H} hK = \bigcup_{h \in H} Kh = KH$$

כאשר השוויון השני נובע מנורמליות K ב-G.

3. נראה כי $K \lhd HK$. ראשית ברור כי $K \le HK$. נורמליות מתקיימת כי אם $g \in HK$ אז גם $g \in G$, ומנורמליות K ב-G נובע כי $gKg^{-1} = K$.

משפט האיזומורפיזם השני: תהי G חבורה ויהיו תתי־חבורות $H \leq G$, $K \lhd G$, אזי מתקיים $H/_{H\cap K} \cong {}^{HK}/_{K}$.

הוכחה: נתבונן בהטלה הקנונית הכללית $\pi : G \to G/N$ המוגדרת $\pi(g) = gN$.

נצמצם את π ל-H, כך ש-$\pi|_H : H \to G/K$ עם אותה ההגדרה - $\pi(h) = hK$.
מכיוון ש-π היא הומומורפיזם, גם הצמצום שלה ל-H נשאר הומומורפיזם.

נחשב את $\ker(\pi|_H), \text{image}(\pi|_H)$ כדי להשתמש במשפט האיזומורפיזם הראשון:

$$\ker(\pi|_H) = \left\{ h \in H | \pi(h) = \underbrace{e_{G/K}}_{=K} \right\} = \{h \in H | hK = K\} = \{h \in H | h \in K\} = H \cap K$$

$$\text{image}(\pi|_H) = \{\pi(h) | h \in H\} = \{hK | h \in H\} = \{hkK | h \in H, k \in K\} = {}^{HK}/_{K}$$

כעת לפי משפט האיזומורפיזם הראשון נקבל $H/_{H\cap K} \cong {}^{HK}/_{K}$. ■

8.4 משפט האיזומורפיזמים ה-III

תהי G חבורה ויהיו $H, K \lhd G$ כך ש-$K \subseteq H$, אזי ${}^{G/K}/_{H/K} \cong G/H$.

הערה: נשים לב שמתקיים $H/K \lhd G/K$ ולכן הביטוי במשפט מוגדר. את ההוכחה לכך נסיק במהלך הוכחת המשפט.

הוכחה: נתבונן בהעתקה $f : G/K \to G/H$ המוגדרת $f(gK) = gH$.

ראשית נראה שההעתקה מוגדרת היטב (לא תלויה בנציגים):

$$\begin{gathered} g_1K = g_2K \\ \Downarrow \\ g_1^{-1}g_2 \in K \subseteq H \\ \Downarrow \\ g_1H = g_2H \\ \Downarrow \\ f(g_1K) = f(g_2K) \end{gathered}$$

נראה כי f הומומורפיזם:

$$f(g_1Kg_2K) = f(g_1g_2K) = g_1g_2H = g_1Hg_2H = f(g_1K)\, f(g_2K)$$

נחשב את $\ker(f), \text{image}(f)$ כדי להשתמש במשפט האיזומורפיזם הראשון:

$$\ker(f) = \left\{gK | f(gK) = e_{G/H}\right\} = \{gK | gH = H\} = \{gK | g \in H\} = H/K$$

מכאן ש-$H/K \lhd G/K$, כי כל גרעין של הומומורפיזם הוא תת־חבורה נורמלית.

$$\text{image}(f) = G/H$$

כעת לפי משפט האיזומורפיזם הראשון נקבל ${}^{G/K}/_{H/K} \cong G/H$. ■

טענה: כל תת־חבורה נורמלית של G היא גרעין של הומומורפיזם מ-G לחבורה כלשהי.

הוכחה: תהי $N \lhd G$ ונתבונן בהטלה $\pi : G \to {}^{G}/_{N}$ המוגדרת להיות: $\pi\left(g\right) = gN$.
ראינו שזה הומומורפיזם, וכן מתקיים:

$$\ker \pi = \left\{g \in G | \pi\left(g\right) = e_{G/N}\right\} = \left\{g \in G | gN = N\right\} = \left\{g \in G | g \in N\right\} = N$$

■

8.5 משפט ההתאמה (איפיון תתי־חבורות של חבורות מנה)

משפט: תהי $N \lhd G$. קיימת התאמה חח"ע ועל בין קבוצת תתי החבורות $\left\{\overline{H} | \overline{H} \leq {}^{G}/_{N}\right\}$ לבין קבוצת תתי החבורות $\left\{H | N \lhd H \leq G\right\}$.

הערה: המשפט לא מגדיר הומומורפיזם של חבורות, כי קבוצות אלה אינן בהכרח חבורות.

הוכחה: התאמה זו ניתנת על־ידי ההטלה הקנונית $\pi : G \mapsto {}^{G}/_{N}$. כלומר ההתאמה מהצורה $\left\{H | N \lhd H \leq G\right\} \to \left\{\overline{H} | \overline{H} \leq {}^{G}/_{N}\right\}$ ניתנת על־ידי ${}^{H}/_{N} \leq {}^{G}/_{N}$ $H \mapsto$.

- נראה שזו התאמה על: תהי $\overline{H} \leq {}^{G}/_{N}$, נגדיר $H = \pi^{-1}\left(\overline{H}\right)$. הראינו שהמקור תחת הומומורפיזם של כל תת־חבורה הוא תת־חבורה, ולכן H שהגדרנו היא תת־חבורה. לכן H היא המקור של $\overline{H}$, כלומר ההתאמה היא על.
- נראה שזו התאמה חח"ע: יהיו $H_1, H_2 \leq G$ שמכילות את N ומקיימות $\pi\left(H_1\right) = \pi\left(H_2\right)$, כלומר ${}^{H_1}/_{N} = {}^{H_2}/_{N}$.

יהי $h_1 \in H_1$. מההנחה נובע שקיים $h_2 \in H_2$ כך שמתקיים $h_1 N = h_2 N$, ולכן יש $n \in N$ המקיים $h_1 = h_2 n$ (כי $e \in N$). אבל $N \subseteq H_2$ ולכן $h_1 \in H_2$ ומכאן כי $H_1 \subseteq H_2$.

באופן סימטרי נובע כי $H_2 \subseteq H_1$, ולכן $H_1 = H_2$, כלומר π חח"ע. ■

טענה: ההתאמות הללו שומרות על הכלות ועל נורמליות. כלומר:

$$N \subseteq H_1 \subseteq H_2 \iff {}^{H_1}/_{N} \subseteq {}^{H_2}/_{N}$$

$$N \lhd H \lhd G \iff {}^{H}/_{N} \lhd {}^{G}/_{N}$$

הוכחה: שמירת ההכלה ברורה. נראה שהנורמליות גם משתמרת.

בכיוון ראשון: נניח כי $H \lhd G$. משמע לכל $g \in G$ ולכל $h \in H$ מתקיים $ghg^{-1} \in H$, לכן לכל $hN \in {}^{H}/_{N}$ ולכל $gN \in {}^{G}/_{N}$ מתקיים:

$$\left(gN\right) hN \left(gN\right)^{-1} = ghg^{-1}N \in {}^{H}/_{N}$$

וזו ההגדרה של ${}^{H}/_{N} \lhd {}^{G}/_{N}$.

בכיוון שני: נניח כי ${}^{H}/_{N} \lhd {}^{G}/_{N}$. אז לכל $g \in G$ ולכל $h \in H$ מתקיים:

$$ghg^{-1}N = \left(gN\right) hN \left(gN\right)^{-1} \in {}^{H}/_{N}$$

ולכן $ghg^{-1} \in H$, וזו ההגדרה של $H \lhd G$. ■

9 אוטומורפיזמים של חבורה

הגדרה: **אוטומורפיזם** של חבורה G הוא איזומורפיזם מהצורה $f:G\to G$.

דוגמאות:

1. בחבורה $(\mathbb{Z},+,0)$ האוטומורפיזמים היחידים הם $\pm$ הזהות.
2. לכל חבורה אבלית G, ההעתקה $f(g)=g^{-1}$ היא אוטומורפיזם.

הגדרה: נגדיר את $Aut(G)$ להיות אוסף כל האוטומורפיזמים של G, ונגדיר פעולה $f_1\cdot f_2=f_1\circ f_2$. כלומר כפל של אוטומורפיזמים הוא ההרכבה שלהם.

טענה: תחת פעולת ההרכבה, $Aut(G)$ היא חבורה.

הוכחה: סגירות תחת פעולת ההרכבה: הרכבה של העתקות חח"ע ועל היא העתקה חח"ע ועל, ומכיוון שהתחום והטווח הם G, נקבל כי ההרכבה גם היא ב-$Aut(G)$.

איבר היחידה הוא האוטומורפיזם Id.

אסוציאטיביות נובעת מאסוציאטיביות של הרכבת פונקציות.

סגירות להופכי נובעת מכך שהאוטומורפיזמים הם העתקות חח"ע ועל. ■

9.1 אוטומורפיזמים פנימים

הגדרה: נקבע $g\in G$ ונגדיר העתקה $\psi_g:G\to G$ להיות הצמדה ב-g. כלומר לכל $x\in G$ מגדירים $\psi_g(x)=gxg^{-1}$. להעתקות מהצורה הזו קוראים **אוטומורפיזם פנימי**.

טענה: $\psi_g\in Aut(G)$.

הוכחה: ראינו כי ψ_g היא חח"ע ועל. נותר להוכיח כפליות:

$$\psi_g(xy)=g(xy)g^{-1}=g\left(x\left(g^{-1}g\right)y\right)g^{-1}=g\left(\left(xg^{-1}\right)(gy)\right)g^{-1}=$$

$$=\left(gxg^{-1}\right)\left(gyg^{-1}\right)=\psi_g(x)\psi_g(y)$$

מכאן ש-ψ_g איזומורפיזם, ומהגדרתו נובע כי הוא גם אוטומורפיזם. ■

הערה: נשים לב כי G חבורה אבלית אמ"מ $\psi_g=Id$ לכל $g\in G$.

הגדרה: $Inn(G)$ הוא כל האוטומורפיזמים הפנימיים של G.

טענה: $Inn(G)\lhd Aut(G)$

הוכחה: ראשית נראה כי $Inn(G)$ תת־חבורה של $Aut(G)$.,

איבר היחידה קיים כי ברור שמתקיים $Id\in Inn(G)$, מכיוון ש-$\psi_e=Id$.

נראה סגירות להרכבה. יש להראות כי $\psi_g\circ\psi_h\in Inn(G)$ לכל $g,h\in G$. לשם כך מספיק להוכיח כי $\psi_g\circ\psi_h=\psi_{gh}$. נחשב עבור כל $x\in G$:

$$(\psi_g\circ\psi_h)(x)=\psi_g(\psi_h(x))=\psi_g\left(hxh^{-1}\right)=g\left(hxh^{-1}\right)g^{-1}=$$

$$=(gh)x\left(h^{-1}g^{-1}\right)=(gh)x(gh)^{-1}=\psi_{gh}(x)$$

נראה קיום הופכי. יש להראות כי $(\psi_g)^{-1} \in Inn(G)$ לכל $g \in G$. לשם כך מספיק להוכיח כי $(\psi_g)^{-1} = \psi_{g^{-1}}$. נחשב עבור כל $x \in G$:

$$\left(\psi_g \circ \psi_{g^{-1}}\right)(x) = \psi_g\left(\psi_{g^{-1}}(x)\right) = \psi_g\left(g^{-1}x\left(g^{-1}\right)^{-1}\right) =$$

$$= \psi_g\left(g^{-1}xg\right) = g\left(g^{-1}xg\right)g^{-1} = x$$

ומחישוב דומה נקבל $\psi_{g^{-1}} \circ \psi_g = Id$.

מכאן שמתקיים $Inn(G) \leq Aut(G)$. נותר להראות כי $Inn(G) \lhd Aut(G)$.

יהיו $\psi_g \in Inn(G)$ ו-$\varphi \in Aut(G)$. כדי להראות נורמליות מספיק להראות שמתקיים:

$$\varphi \circ \psi_g \circ \varphi^{-1} = \psi_{\varphi(g)} \in Inn(G)$$

נחשב עבור כל $x \in G$:

$$\left(\varphi \circ \psi_g \circ \varphi^{-1}\right)(x) = \varphi\left(\psi_g\left(\varphi^{-1}(x)\right)\right) = \varphi\left(g\varphi^{-1}(x)g^{-1}\right) =$$

$$= \varphi(g)\varphi\left(\varphi^{-1}(x)\right)\varphi\left(g^{-1}\right) = \varphi(g)x\varphi\left(g^{-1}\right) = \varphi(g)x\varphi^{-1}(g) = \psi_{\varphi(g)}(x)$$

■

הגדרה: $Out(G) = {}^{Aut(G)}/_{Inn(G)}$

9.2 מרכז של חבורה

הגדרה: המרכז של חבורה G מוגדר ומסומן:

$$Z(G) = \{g \in G | \forall_{x \in G}\, gx = xg\}$$

הערות:

1. G אבלית $\Leftrightarrow Z(G) = G$
2. $Z(GL_n(\mathbb{F}))$ הוא כל המטריצות הסקלאריות, כלומר המטריצות שהן מכפלה של מטריצת היחידה בסקלר.
3. $Z(S_n) = \{Id\}$ לכל $3 \leq n$. (ההוכחה מושארת כתרגיל. יש להראות שכל תמורה שאינה הזהות, אינה במרכז).

טענה: $Z(G) \lhd G$

הוכחה: ראשית נראה כי $Z(G) \leq G$.

ברור כי $e \in Z(G)$.

נראה סגירות לכפל. יהיו $g, h \in Z(G)$. לכל $x \in G$ מתקיים:

$$x(gh) = (xg)h = (gx)h = g(xh) = g(hx) = (gh)x$$

נראה קיום הופכי. נניח כי $g \in Z(G)$, אז מתקיים לכל x:

$$g^{-1}x = \left(x^{-1}g\right)^{-1} = \left(gx^{-1}\right)^{-1} = xg^{-1}$$

מכאן שמתקיים $Z(G) \leq G$.

נותר להראות כי $Z(G) \lhd G$. אבל נשים לב שלכל $g \in Z(G)$ מתקיים כי $xgx^{-1} = g$ לכל $x \in G$, ולכן $xZ(G)z^{-1} = Z(G)$, כלומר $Z(G) \lhd G$.■

טענה: $G/Z(G) \cong Inn(G)$

הוכחה: נשתמש במשפט האיזומורפיזמים הראשון.

נגדיר העתקה $f : G \to Inn(G)$ להיות $f(g) = \psi_g$ (נזכור כי $\psi_g(x) = gxg^{-1}$).

הראינו כי $\psi_{gh} = \psi_g\psi_h$, ולכן מתקיים $f(gh) = f(g)f(h)$, כלומר f הומומורפיזם של חבורות.

נחשב את $\ker(f), \text{image}(f)$ כדי להשתמש במשפט האיזומורפיזם הראשון:

$$\ker(f) = \left\{g \in G | f(g) = e_{Inn(G)} = Id\right\} = \{g \in G | \psi_g = Id\} = Z(G)$$

כאשר השוויון האחרון נובע מכך שאוסף ה-$g \in G$ המקיימים $\psi_g(x) = gxg^{-1} = x$ הוא בדיוק אוסף ה-$g \in G$ המקיימים $gx = xg$.

כמו־כן ברור שמתקיים $\text{image}(f) = Inn(G)$. מכאן נקבל לפי משפט האיזומורפיזמים הראשון $G/Z(G) \cong Inn(G)$. ■

דוגמאות:

1. $GL_n(\mathbb{F})/Z(GL_n(\mathbb{F})) \cong Inn(GL_n(\mathbb{F}))$, כאשר $Z(GL_n(\mathbb{F}))$ הוא אוסף המטריצות הסקלאריות.

   מסמנים $PGL_n(\mathbb{F}) =: GL_n(\mathbb{F})/Z(GL_n(\mathbb{F}))$.

2. $SL_2(\mathbb{F})/Z(SL_2(\mathbb{F})) \cong Inn(SL_2(\mathbb{F}))$, ונשים לב כי $Z(SL_2(\mathbb{F})) = \left\{\pm\begin{pmatrix} 1 & \\ & 1 \end{pmatrix}\right\}$.

   מסמנים $PSL_2(\mathbb{F}) =: SL_2(\mathbb{F})/\left\{\pm\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right\}$.

9.3 מכפלות ישרות

הגדרה: יהיו H, G חבורות. מגדירים ומסמנים את **המכפלה הישרה** שלהן:

$$G \times H =: \{(g,h) | g \in G, h \in H\}$$

מגדירים על קבוצה זו כפל באמצעות כפל של הנציגים המתאימים:

$$(g,h)(g',h') = (g \cdot g', h \cdot h')$$

קל לראות שתחת פעולה זו, $G \times H$ היא חבורה.

הכללה: יהיו $G_1, ..., G_n$ חבורות. מגדירים ומסמנים את **המכפלה הישרה** של כולן:

$$G_1 \times ... \times G_n =: \{g_1 \cdot ... \cdot g_n | g_i \in G_i,\ i = 1, ..., n\}$$

הערה: ניתן גם להגדיר גם מכפלה ישרה על מספר כלשהו של חבורות, לאו דווקא סופי.

9.3.1 משפט השאריות הסיני

יהיו $m_1, ..., m_n$ מספרים טבעיים זרים בזוגות. כלומר לכל $i \neq j$ מתקיים $\gcd(m_i, m_j) = 1$. ויהיו $a_1, ..., a_n$ שלמים כלשהם.
נתבונן במערכת השקילויות הבאה:

$$\begin{cases} x \equiv a_1 \mod (m_1) \\ \vdots \\ x = a_n \mod (m_n) \end{cases}$$

אזי קיים פתרון למערכת, ופתרון זה הוא יחיד מודולו $m_1 \cdot ... \cdot m_n$.

מסקנה: אם $m_1, ..., m_n$ טבעיים זרים בזוגות, אזי:

$$\mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_n} \cong \mathbb{Z}_{m_1 \cdot ... \cdot m_n}$$

הוכחה: (של המסקנה) יהי $(a_1, ..., a_n) \in (\mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_n})$. נתאים לו איבר ב-$\mathbb{Z}_{m_1 \cdot ... \cdot m_n}$, שייבחר כפתרון היחיד של מערכת השקילויות:

$$\begin{aligned} x &\equiv a_1 \mod (m_1) \\ &\vdots \\ x &= a_n \mod (m_n) \end{aligned}$$

קיבלנו התאמה מהצורה $(a_1, ..., a_n) \mapsto x \in \mathbb{Z}_{m_1 \cdot ... \cdot m_n}$.

ניתן להראות שזו התאמה שמייצרת איזומורפיזם. ■

נוסחה:

$$|G_1 \times ... \times G_n| = |G_1| \cdot ... \cdot |G_n|$$

10 פעולה של חבורה על קבוצה

הגדרה: תהי G חבורה ותהי X קבוצה. **פעולה של G על X** היא העתקה מהצורה $G \times X \to X$, המסומנת $(gx) \mapsto g.x$, שמקיימת שני תנאים:

1. $e.x = x$
2. $(gh).x = g.(h.x)$ לכל $x \in X$

הערה: נשים לב שבתנאי 2, הפעולות שב-$(gh).x$ הן פעולת הכפל בחבורה ופעולת החבורה על הקבוצה. לעומת זאת הפעולות שב-$g.(h.x)$ שתי הפעולות הן של החבורה על הקבוצה.

טענה: כל פעולה של חבורה על קבוצה מגדירה תמורה של איברי הקבוצה.

הוכחה: בהינתן פעולה $g.x$ של חבורה G על קבוצה X, נראה שלכל $g\in G$ ההעתקה $x\mapsto g.x$ היא חח"ע ועל.

חח"ע: אם $g.x=g.y$ אזי מהתכונות של הפעולה נובע:

$$y=e.y=g^{-1}g.y=g^{-1}.\left(g.x\right)=g^{-1}.\left(g.y\right)=g^{-1}g.x=e.x=x$$

על: כל $x\in X$ מתקבל על־ידי $g^{-1}.x\mapsto g.\left(g^{-1}.x\right)=gg^{-1}.x=x$. ■

הגדרה: לכל קבוצה X מסמנים $Sym\left(X\right)=\left\{f:X\rightarrow X|f\text{ is bijection}\right\}$. נשים לב שזו חבורה ביחס לפעולת ההרכבה.

טענה: תהי G חבורה ו-X קבוצה. אזי כל פעולה של G על X מגדירה הומומורפיזם מהצורה $G\rightarrow Sym\left(X\right)$, וכל הומומורפיזם כנ"ל מגדיר פעולה של G על X.

הוכחה: תהי G חבורה ו-X קבוצה. נוכיח את שני הכיוונים.

1. נניח כי נתונה פעולה של G על X שנסמן $g.x$. נראה כי ההעתקה $\varphi\left(g\right)$ המוגדרת בהינתן $g\in G$ לכל $x\in X$ להיות $\varphi\left(g\right)\left(x\right)=g.x$, היא העתקה מהצורה $\varphi:G\rightarrow Sym\left(X\right)$ והיא הומומורפיזם.
   (א) מהטענה שהוכחנו לעיל נובע שאכן $\varphi\left(g\right)\in Sym\left(X\right)$.
   (ב) נראה כי $\varphi\left(g\right)$ הומומורפיזם. לכל $x\in X$ מתקיים:

$$\varphi\left(gh\right)\left(x\right)=\left(gh\right).\left(x\right)=g.\left(hx\right)=\varphi\left(g\right)\left(hx\right)=$$

$$=\varphi\left(g\right)\left(\varphi\left(h\right)\left(x\right)\right)=\left(\varphi\left(g\right)\circ\varphi\left(h\right)\right)\left(x\right)$$

2. נניח כי נתון הומומורפיזם $\varphi:G\rightarrow Sym\left(X\right)$. נראה כי הפעולה $G\times X\rightarrow X$ המוגדרת להיות $g.x=\varphi\left(g\right)\left(x\right)$ היא פעולה של G על X. נראה ששתי האקסיומות מתקיימות:

$$e.x=\varphi\left(e\right)\left(x\right)=Id\left(x\right)=x$$

$$\left(gh\right).x=\varphi\left(gh\right)\left(x\right)=\left(\varphi\left(g\right)\circ\varphi\left(h\right)\right)\left(x\right)=$$

$$=\varphi\left(g\right)\left(\varphi\left(h\right)\left(x\right)\right)=g.\left(\varphi\left(h\right)\left(x\right)\right)=g.\left(h.x\right)$$

■

10.0.2 פעולה נאמנה (Faithful)

הגדרה: פעולה של חבורה על קבוצה תיקרא **נאמנה** אם ההומומורפיזם $\varphi:G\rightarrow Sym\left(X\right)$ המתאים לה הוא חח"ע.

הגדרה שקולה: פעולה של חבורה על קבוצה תיקרא **נאמנה** אמ"מ מתקיים כי לכל $e\neq g\in G$ קיים $x\in X$ כך ש-$g.x\neq x$. כלומר כל $g\neq e$ צריך לשנות לפחות איבר אחד בקבוצה.

הוכחת השקילות: נניח כי φ הומומורפיזם חח"ע ול-$g \in G$ כלשהו מתקיים $g.x = x$ לכל $x \in X$. מכאן שמתקיים $\varphi(g)(x) = x$ ומכיוון ש-φ הומומורפיזם חח"ע נובע כי $g = e$.

נניח שמתקיימת ההגדרה השקולה. כדי להראות חח"ע מספיק להראות כי הגרעין של φ טריוויאלי. אם $\varphi(g) = e_{Sym(X)} = Id$ אז $\varphi(g)(x) = x$ לכל x ולכן $g = e$, כלומר הגרעין טריוויאלי. ■

דוגמה: נניח כי G פועלת על G באמצעות הצמדה. כלומר $g.x = gxg^{-1}$ עבור $x, g \in G$.

זו לא בהכרח פעולה נאמנה, כי אם g אבלית מתקיים $gxg^{-1} = x$ עבור כל g, ולכן הגרעין לא טריוויאלי.

ניתן לראות כי בדוגמה זו הפעולה נאמנה אמ"מ $Z(G) = \{e\}$.

מסקנה: אם הפעולה של G על X נאמנה, אז $\varphi : G \to Sym(X)$ היא מונומורפיזם (הומומורפיזם חח"ע, כי הגרעין טריוויאלי) ולכן אפשר לייצר איזומורפיזם מהצורה $\varphi : G \to \text{image}(\varphi)$.

10.1 משפט קיילי

כל חבורה G ניתנת לשיכון ב-$Sym(G)$, ואם G מסדר סופי אז היא ניתנת לשיכון ב-$S_{|G|}$. כלומר כל G איזומורפית לתת־חבורה של $Sym(G)$, ואם זוהי חבורה מסדר סופי אז G איזומורפית לתת־חבורה של $S_{|G|}$.

הוכחה 1: נגדיר $X = G$ ונגדיר פעולה של G על עצמה כפעולה של חבורה על קבוצה, באמצעות פעולת הכפל בחבורה.

זוהי פעולה נאמנה ולכן G איזומורפית לתת־חבורה של $Sym(G)$ כפי שראינו כמסקנה לעיל.

כך גם במקרה בו $|G| = n$ סופי מתקיים כי:

$$Sym\{(g_1, ..., g_n)\} \cong Sym(\{1, ..., n\}) = S_n$$

■

הוכחה 2: (מפורשת יותר) לכל $g \in G$ נגדיר העתקה $\tau_g : G \to G$ להיות $\tau_g(x) = gx$. זו העתקה חח"ע ועל, ולכן לכל $g \in G$ מתקיים כי $\tau_g \in Sym(G)$.

נגדיר שיכון $\varphi : G \to Sym(G)$ על־ידי $\varphi(g) = \tau_g$. ראינו כי זה הומומורפיזם. נראה כי זה חח"ע:

$$g \in \ker(\varphi)$$
$$\Updownarrow$$
$$\varphi(g) = Id$$
$$\Updownarrow$$
$$\tau_g = Id$$
$$\Updownarrow$$
$$\forall_{x \in G}\, gx = x$$
$$\Updownarrow$$
$$g = e$$

מכאן ש-$\ker(\varphi) = e$, לכן היא חח"ע והיא מהווה שיכון של G ב-$Sym(G)$.

ככלל, תמונה של הומומורפיזם היא תת־חבורה, ולכן G איזומורפית לתת החבורה שמוגדרת על־ידי התמונה של φ. ■

הערה: אם $|G| = n$ אז $Sym(G) \cong S_n$. נזכור שמתקיים $|S_n| = n!$, ולכן G משוכנת ב-S_n כתת־חבורה בגודל n.

מכאן כי $G \cong S_n$ אמ"מ $n = n!$ כלומר $n = 2$.

10.2 מסלולים ומייצבים

הגדרה: תהי G חבורה שפועלת על קבוצה X ויהי $x \in X$.

המסלול של x מוגדר להיות:

$$O(x) =: \{g.x \in X | g \in G\}$$

הגדרה: תהי G חבורה שפועלת על קבוצה X ויהי $x \in X$.

המייצב של x מוגדר להיות:

$$G_x =: Stab(x) =: \{g \in G | g.x = x\}$$

10.2.1 תכונות של מייצב

טענה: מייצב של איבר הוא תת־חבורה.

הוכחה: $e \in G_x$ מכיוון שלכל $x \in X$ מתקיים $e.x = x$.

עבור כל $g, h \in G_x$ מתקיים $g.x = h.x = x$, ולכן עבור המכפלה מתקיים:

$$(gh).x = g.(h.x) = g.x = x$$

עבור כל $g \in G_x$ מתקיים $g.x = x$, ולכן עבור ההופכי מתקיים:

$$g^{-1}.x = g^{-1}.(g.x) = \left(g^{-1}g\right).x = e.x = x$$

טענה: תהי G חבורה שפועלת על קבוצה X, אזי לכל $h \in G$ מתקיים:

$$G_{h.x} = hG_xh^{-1}$$

כלומר תתי החבורות $G_{h.x}, G_x$ צמודות ב-G.

הוכחה: נוכיח הכלה בשני הכיוונים.

יהי $y \in hG_xh^{-1}$. כלומר $y = hgh^{-1}$ עבור g המקיים $g.x = x$. נחשב:

$$\left(hgh^{-1}\right).(h.x) = \left(hgh^{-1}h\right).x = (hg).x = h.(g.x) = h.x$$

ולכן $y\in G_{h.x}$ ונסיק כי $hG_xh^{-1}\subseteq G_{h.x}$.
יהי $y\in G_{h.x}$. כלומר מתקיים $y.\left(h.x\right)=h.x$. נסיק כי:

$$\left(h^{-1}yh\right).x=h^{-1}.\left(\left(yh\right).x\right)=h^{-1}.\left(y.\left(h.x\right)\right)=h^{-1}.\left(h.x\right)=x$$

לכן קיבלנו כי $h^{-1}yh\in G_x$ ומכאן כי $y\in hG_xh^{-1}$ ונסיק כי $G_{h.x}\subseteq hG_xh^{-1}$.
נסיק כי $G_{h.x}=hG_xh^{-1}$. ■

מסקנות: אם G חבורה שפועלת על קבוצה X, לכל $x\in X$ מתקיים:

1. אם $y\in O\left(x\right)$ אז G_x,G_y תתי־חבורות צמודות.
2. אם $y\in O\left(x\right)$ אז $G_x\cong G_y$, ולכן מתקיים $\left|G_x\right|=\left|G_y\right|$.
3. אם $y\in O\left(x\right)$ וגם $G_x\lhd G$, אז $G_x=G_y$.

הוכחה:

1. מכך ש-$y\in O\left(x\right)$ נובע שיש $h\in G$ כך ש-$y=h.x$. נסיק לפי הטענה הקודמת:

$$G_y=G_{h.x}=hG_xh^{-1}$$

2. בהינתן $h\in G$, נגדיר העתקה מהצורה $\psi_h:G\to G$ להיות ההצמדה:

$$\psi_h\left(g\right)=hgh^{-1}$$

.

זהו אוטומורפיזם פנימי ל-G ולכן בפרט גם לתת־חבורות של G. מכאן שמתקיים:

$$G_x\cong\psi_h\left(G_x\right)=hG_xh^{-1}=G_{h.x}=G_y$$

3. מנורמליות נובע שמתקיים:

$$G_y=G_{h.x}=hG_xh^{-1}=G_x$$

הערה: אם $y\notin O\left(x\right)$ לא ידוע דבר על הקשר בין G_x לבין G_y.

10.2.2 תכונות של מסלול

טענה: תהי G חבורה שפועלת על קבוצה X באמצעות $g.x$, אזי לכל $x,y\in X$ מתקיים כי $O\left(x\right)=O\left(y\right)$ או $O\left(x\right)\cap O\left(y\right)=\emptyset$.

הוכחה: נניח כי $O(x)\cap O(y)\neq\emptyset$ ונראה כי $O(x)=O(y)$.

יהי $z\in O(x)\cap O(y)$. בפרט $z\in O(x),O(y)$ ולכן קיימים $g,h\in G$ כך ש-$z=g.x=h.y$. מכאן שמתקיים $x=\left(g^{-1}h\right).y$ ולכן $x\in O(y)$.

ככלל, נקודה ב-$O(x)$ היא מהצורה $u.x$ עבור $u\in G$ כלשהו, ולכן נסיק כי:

$$u.x=u.\left(g^{-1}h\right).y=\left(ug^{-1}h\right).y\in O(y)$$

ומכאן ש-$O(x)\subseteq O(y)$.

באופן דומה נקבל את ההכלה ההפוכה, ולכן נקבל $O(x)=O(y)$. ■

טענה: תהי G חבורה שפועלת על קבוצה X באמצעות $g.x$, אזי $X=\biguplus_{i\in I}O(x_i)$, כאשר $\biguplus$ מסמן איחוד זר.

הוכחה: ניתן לראות כי השתייכות למסלול היא יחס שקילות על X. מכאן שמחלקות השקילות של יחס זה מהוות חלוקה של X.

באופן מפורש, נבחר נציגים $x_i\in X$, $i\in I$, כך ש-$O(x_i)\neq O(x_j)$ לכל $i\neq j$. מטענה קודמת נובע כי $O(x_i)\cap O(x_j)=\emptyset$. כמו־כן ידוע כי עבור כל $x\in X$ מתקיים $x\in O(x)$.

מכאן שקיבלנו איחוד זר שמכסה את הקבוצה, ולכן זו חלוקה. ■

10.2.3 משפט מסלול־מייצב

משפט: תהי G חבורה שפועלת על קבוצה X. לכל $x\in X$ מתקיים $|O(x)|=[G:G_x]$. כלומר גודל המסלול הוא האינדקס של המייצב ב-G.

הערה: בחבורות סופיות, לפי משפט לגראנז' מתקיים $[G:G_x]=\frac{|G|}{|G_x|}$, ולכן נסיק כי במקרה זה:

$$|O(x)|\cdot|G_x|=|G|$$

כלומר הגודל של כל מסלול מחלק את גודל החבורה.

הוכחה: G/G_x הוא אוסף המחלקות השמאליות של G_x ב-G. מסמנים $[G:G_x]=|G/G_x|$. נראה כי הגודל שווה באמצעות הגדרה של העתקה חח"ע ועל ביניהם.

נגדיר העתקה מהצורה $\varphi:G/G_x\to O(x)$ להיות $\varphi(gG_x)=g.x$.

ההעתקה φ מוגדרת היטב, כי אם $g_1G_x=g_2G_x$, אז $G_x=g_1^{-1}g_2G_x$ ולכן $g_1^{-1}g_2\in G_x$. נסיק מכך:

$$\varphi(g_1G_x)=g_1.x=g_1.\left(g_1^{-1}g_2.x\right)=g_2.x=\varphi(g_2G_x)$$

נראה כי φ חח"ע:

$$\varphi(g_1G_x)=\varphi(g_2G_x)$$
$$\Downarrow$$
$$g_1.x=g_2.x$$
$$\Downarrow$$
$$\left(g_1^{-1}g_2\right).x=x$$
$$\Downarrow$$
$$g_1^{-1}g_2\in G_x$$
$$\Downarrow$$
$$g_1^{-1}g_2G_x=G_x$$
$$\Downarrow$$
$$g_1G_x=g_2G_x$$

נראה כי φ על: בהינתן $g.x\in O(x)$ מוגדרת המחלקה השמאלית $gG_x\in {}^{G}/_{G_x}$, ולכן היא מתקבלת על־ידי $\varphi(gG_x)=g.x$.

אם־כך קיימת העתקה חח"ע ועל $O(x)\to {}^{G}/_{G_x}$, ולכן $|O(x)|=|{}^{G}/_{G_x}|$. ■

10.3 פעולות טרנזיטיביות

הגדרה: תהי G חבורה שפועלת על X. נאמר שהפעולה **טרנזיטיבית** אם יש מסלול יחיד. כלומר, לכל $x,y\in X$ קיים $g\in G$ כך ש-$g.x=y$.

דוגמאות:

1. פעולת ההצמדה $g.x=gxg^{-1}$ עבור $G=X$ אינה טרנזיטיבית עבור כל $G\neq\{e\}$, כי עבור כל $h\in Z(G)$ מתקיים $O(h)=\{h\}$ (ובפרט $O(e)=\{e\}$).
2. הפעולה הטבעית של החבורה S_n על הקבוצה $\{1,2,...,n\}$ טרנזיטיבית, כי עבור כל $x,y\in\{1,2,...,n\}$ יש $\sigma\in S_n$ כך ש-$\sigma.x=\sigma(x)=y$.

הגדרה: **חבורת תמורות** היא תת־חבורה של S_n, שפועלת על הקבוצה $\{1,2,...,n\}$.

הגדרה: חבורת תמורות G נקראת **טרנזיטיבית** אם היא טרנזיטיבית על $\{1,2,...,n\}$. כלומר אם המסלול שלה ב-$\{1,2,...,n\}$ הוא יחיד. כלומר אם לכל $i,j\in\{1,2,...,n\}$ יש $g\in G$ כך ש-$g.i=j$.

הערה: חבורה G פועלת טרנזיטיבית על קבוצה X אמ"מ עבור ההומומורפיזם $\varphi:G\to Sym(X)$ הנובע מהפעולה מתקיים כי $\varphi(G)=Im(\varphi)$ היא תת־חבורה טרנזיטיבית של $Sym(X)$.

10.4 ליבה (core)

נניח כי G חבורה ו-$H\leq G$ תת־חבורה. ניתן ל-G לפעול על הקבוצה $X={}^{G}/_{H}=\{gH|g\in G\}$ (לא דרשנו ש-H תהיה נורמלית ולכן X אינה בהכרח חבורה) על־ידי להיות $a.gH=agH$ עבור כל $a\in G$.

קל לראות שזו פעולה של חבורה על קבוצה, כמו־כן זו פעולה טרנזיטיבית כי עבור כל $xH,yH\in X$ מתקיים כי $\left(yx^{-1}\right).xH=yx^{-1}xH=yH$.

נשים לב שהמייצב של H ביחס לפעולה זו הוא:

$$G_H = \{a \in G | a.H = aH = H\} = \{a \in G | a \in H\} = H$$

טענה: $G_{gH} = gHg^{-1}$

הוכחה: ראינו שבאופן כללי מתקיים $G_{h.x} = hG_xh^{-1}$, ולכן במקרה זה $G_{gH} = G_{g.H} =$ $gG_Hg^{-1} = gHg^{-1}$. ■

טענה: אם φ הוא ההומומורפיזם המתאים לפעולה של G על הקבוצה G/H, אזי מתקיים $\ker(\varphi) = \bigcap_{g\in G} gHg^{-1}$.

למה: תהי G הפועלת על X, ויהי ההומומורפיזם $\varphi : G \to Sym(X)$ הנובע מהפעולה. אזי $\ker(\varphi) = \bigcap_{x\in X} G_x$.

הוכחה:

$$g \in \ker(\varphi)$$
$$\Updownarrow$$
$$\varphi(g) = Id$$
$$\Updownarrow$$
$$\varphi(g)(x) = x \, \forall_{x\in X}$$
$$\Updownarrow$$
$$g.x = x \, \forall_{x\in X}$$
$$\Updownarrow$$
$$g \in G_x \, \forall_{x\in X}$$
$$\Updownarrow$$
$$g \in \bigcap_{x\in X} G_x$$

הוכחה: מהלמה ומטענה קודמת נובע כי עבור $\varphi : G \to Sym(G/H)$ מתקיים:

$$\ker(\varphi) = \bigcap_{x\in X} G_x = \bigcap_{g\in G} G_{gH} = \bigcap_{g\in G} gHg^{-1}$$

■

הגדרה: נניח כי G חבורה ו-$H \leq G$ תת־חבורה, ומגדירים פעולה של G על G/H באמצעות $a.gH = agH$ לכל $a \in G$.

כפי שראינו גרעין פעולה זו הוא $\bigcap_{g\in G} gHg^{-1}$, ונהוג לקרוא לו **הליבה** (core) של H ב-G. מסמנים:

$$H_G =: \bigcap_{g\in G} gHg^{-1}$$

תכונות:

1. $H_G \lhd G$. כי ראינו ש-H_G גרעין של הומומורפיזם, וכל גרעין כזה הוא תת־חבורה נורמלית.
2. $H_G \subseteq H$. כי בחיתוך שמגדיר את H_G מופיע האיבר $eHe^{-1} = H$, ולכן כל איבר בחיתוך מוכל בפרט ב-H.
3. אם $G \rhd N \subseteq H$ אז $N \subseteq H_G$. כי מנורמליות מתקיים $N = gNg^{-1} \subseteq gHg^{-1}$ לכל $g \in G$, ולכן $N \subseteq \bigcap_{g\in G} gHg^{-1} = H_G$.
4. מסעיף 3 נובע כי H_G היא התת־חבורה הנורמלית המקסימלית של G המוכלת ב-H.

דוגמה: ניקח את $G = S_n$ וכן $H = S_{n-1} \cong \{\sigma \in S_n | \sigma(n) = n\}$.

נשים לב כי $S_{n-1} = G_n$ (המייצב של n). נוכיח כי הליבה של S_{n-1} ב-S_n היא $\{e\}$.

יהי $\varphi : G \to \underbrace{Sym(\{1,2,...,n\})}_{=S_n}$. נראה שזו פעולה נאמנה ולכן $\ker(\varphi) = \{e\}$,

ולפי למה קודמת נסיק שמתקיים $H_G = \bigcap_{x\in\{1,2,...,n\}} G_x = \ker(\varphi) = \{e\}$.

ראינו כי המייצב של n הוא S_{n-1}, ומטרנזיטיביות הפעולה נסיק כי כל מייצב אחר G_i, $1 \le i < n$ הוא צמוד של H. (כי מייצבי נקודות באותו מסלול הם צמודים, ובפעולה טרנזיטיבית יש מסלול יחיד).

כל צמודי H הם מייצבי נקודות כלשהן, לפי הנוסחה $G_{hx} = hG_xh^{-1}$, ולכן אם ניקח $x = n$ נקבל:

$$G_{hn} = hG_nh^{-1} = hS_{n-1}h^{-1}$$

מכאן שקבוצת צמודי $H = S_{n-1}$ היא קבוצת מייצבי הנקודות ב-$G = S_n$, מכאן שחיתוך קבוצת צמודי H הוא בדיוק הליבה של H ב-G, שכפי שראינו שווה ל-$\ker(\varphi) = \{e\}$.

טענה: (הכללה של הדוגמה האחרונה) נניח כי G פועלת טרנזיטיבית על X ויהי $x \in X$. אזי:

1. קבוצת המייצבים $\{gG_xg^{-1} | g \in G\}$ היא קבוצת הצמודים $\{G_y | y \in X\}$.
2. אם $\varphi : G \to Sym(X)$ הומומורפיזם הנובע מהפעולה, אז:

$$\ker(\varphi) = \bigcap_{y\in X} G_y = \bigcap_{g\in G} gHg^{-1} = H_G$$

הוכחה:

1. יהיו $y \in X$, $g \in G$ כך ש-$y = g.x$ (מטרנזיטיביות פעולת G על X נובע שקיים g כנ"ל). נקבל:

$$G_y = G_{g.x} = gG_xg^{-1}$$

מכאן שכל מייצב הוא צמוד. מצד שני נקבל שכל צמוד gG_xg^{-1} הוא המייצב של $g.x$. לכן נקבל את השוויון.

2. נובע מטענה קודמת. ■

10.4.1 שקילות פעולות

הגדרה: תהי G חבורה הפועלת על קבוצות X, Y.

נאמר שפעולת G על X **שקולה** לפעולת G על Y, אם קיימת העתקה חח"ע ועל $f : X \to Y$ המקיימת $f(g.x) = g.f(x)$ לכל $g \in G$ ולכל $x \in X$.[10]

משפט: כל פעולה טרנזיטיבית של G על X, שקולה לפעולה של G על G/G_x, לכל $x \in X$.

הוכחה: יהי $x \in X$. נסמן $Y = G/G_x = \{gG_x | g \in G\}$ ונגדיר העתקה $f : Y \to X$ להיות $f(gG_x) = g.x$.

ראינו כי f מוגדרת היטב וכי היא חח"ע ועל (הראינו שיש התאמה חח"ע $G/G_x \to O(x)$).

במקרה שלנו $O(x) = X$ מטרנזיטיביות, ולכן f חח"ע וגם על.

נראה כי f משמרת את הפעולה. צ"ל כי $f(g.y) = g.f(y)$ עבור כל $aG_x = y \in G/G_x$:

$$f(g.aG_x) = f(gaG_x) = (ga).x = g(a.x) = g.f(aG_x)$$

מכאן כי הפעולה של G על X שקולה לפעולה של G על G/G_x. ■

טענה: נניח כי G חבורה ו-$H \leq G$ כך שמתקיים $|G:H| = n < \infty$, אזי $|G:H_G| \,|\, n!$.

ובפרט קיימת תת־חבורה $N \lhd G$ כך ש-$|G:N| \,|\, n!$ (כי ניתן לבחור את $N = H_G$).

הוכחה: נתבונן בפעולת G על G/H ובהומומורפיזם $\varphi : G \to Sym(G/H)$ המתקבל ממנה.

ידוע כי $|G/H| = |G:H| = n$ ולכן $Sym(G/H) \cong S_n$. מכאן שנוכל להתבונן בה"כ בהומומורפיזם $\varphi : G \to S_n$.

ממשפט האיזומורפיזם הראשון נובע שלכל הומומורפיזם מתקיים $G/\ker(\varphi) \cong Im(\varphi)$, ולכן בפרט במקרה הנוכחי מתקיים:

$$G/H_G \cong Im(\varphi) \leq S_n$$

ממשפט לגראנז' נובע כי $|Im(\varphi)| \,|\, |S_n| = n!$ ולכן $|G/H_G| = |G:H_G| \,|\, n!$. ■

מסקנות:

1. אם G חבורה סופית כך ש-$|G| \nmid n!$, וכן $H \leq G$ תת־חבורה מאינדקס $1 < n$, אזי G אינה פשוטה.

[10] נשים לב שבצד שמאל זו הפעולה על X ובצד ימין זו הפעולה על Y.

2. אם G חבורה סופית כך ש-$|G| > n!$ ויש לה תת־חבורה $H \leq G$ מאינדקס $n > 1$, אזי G אינה פשוטה.

הוכחות:

1. ראינו כי $|G : H_G|\,|n!$ ולפי הנתון $|G| \nmid n!$, לכן בהכרח $H_G \neq \{e\}$, שכן אחרת היינו מקבלים $|G : H_G| = |G|$ בסתירה לנתונים. לכן הליבה שהיא תת־חבורה נורמלית, אינה טריוויאלית.

   כמו־כן נשים לב גם שמתקיים $H_G \neq G$ כי לפי הנתון $|G : H| > 1$ ולכן $H_G \subseteq H < G$ ממש. מכאן שיש תת־חבורה נורמלית שאינה טריוויאלית ואינה G כולה, ולכן G אינה פשוטה.

2. בגלל ש-$|G| > n!$ אז $|G| \nmid n!$, ומהמסקנה הקודמת נובע כי G לא פשוטה.

10.5 נקודות שבת

הגדרה: בהינתן פעולה של חבורה G על קבוצה X, לכל $g \in G$ נגדיר:

$$\text{fix}\,(g) = |\{x \in X | g.x = x\}|$$

10.5.1 הלמה של ברנסייד

תהי G חבורה סופית שפועלת על קבוצה סופית X, ונניח שמספר המסלולים הוא k. אזי מתקיים:

$$\frac{1}{|G|}\sum_{g\in G}\text{fix}\,(g) = k$$

הוכחה: נגדיר את הקבוצה:

$$A = \{(g,x)\,|g \in G,\, x \in X,\, g.x = x\} \subseteq G \times X$$

נחשב את הגודל של A בשתי צורות שונות, לפי איברי G ולפי איברי X.

$$|A| = \sum_{g\in G}|\{x \in X|g.x = x\}| = \sum_{g\in G}\text{fix}\,(g)$$

נניח כי יש k מסלולים שונים שנסמן $X_1, ..., X_k$. הראינו שמתקיים $X = X_1 \uplus ... \uplus X_k$ כאיחוד זר.

$$|A| = \sum_{x\in X}|\{g \in G|g.x = x\}| = \sum_{x\in X}|G_x| = \sum_{i=1}^{k}\left(\sum_{x\in X_i}|G_x|\right)$$

משפט מסלול־מייצב קובע כי $|X_i| = |G : G_x| = \frac{|G|}{|G_x|}$ ולכן $|G_x| = \frac{|G|}{|X_i|}$. מכאן נובע:

$$\sum_{x\in X_i}|G_x| = \sum_{x\in X_i}\frac{|G|}{|X_i|} = |G|\sum_{x\in X_i}\frac{1}{|X_i|} = |G|\,\frac{1}{|X_i|}\,|X_i| = |G|$$

נסיק אם־כך מהשוויון האחרון:

$$|A|=\sum_{i=1}^{k}\left(\sum_{x\in X_i}|G_x|\right)=\sum_{i=1}^{k}|G|=k\,|G|$$

משתי הצורות הללו יחד נקבל כי:

$$k\,|G|=\sum_{g\in G}\mathrm{fix}\,(g)$$

נחלק ב-$|G|$ ונקבל את הלמה. ■

מסקנות:

1. אם G פועלת טרנזיטיבית על X אז יש לה מסלול אחד בלבד, ולכן $\frac{1}{|G|}\sum_{g\in G}\mathrm{fix}\,(g)=1$.

   בפרט למשל ראינו כי S_n פועלת טרנזיטיבית על $X=\{1,...,n\}$ ולכן $\frac{1}{n!}\sum_{\sigma\in S_n}\mathrm{fix}\,(\sigma)=1$.

   כמו־כן עבור $n\le 3$ מתקיים כי A_n פועלת טרנזיטיבית על $X=\{1,...,n\}$ ולכן $\frac{1}{\left(\frac{n!}{2}\right)}\sum_{\sigma\in A_n}\mathrm{fix}\,(g)=1$.

2. נראה שלכל $n\le 3$, קיים איבר ללא נקודת שבת בתת־חבורת התמורות הזוגיות A_n.

   נשים לב כי $(1...n)=(12)(23)...(n-1,n)$ הוא איבר ללא נקודת שבת ב-S_n. אם n אי־זוגי אז $(1...n)\in A_n$ וסיימנו, ואם n זוגי נבחר את התמורה $\left(1...\frac{n}{2}\right)\left(\frac{n}{2}...n\right)$.

טענה: תהי G חבורה סופית הפועלת טרנזיטיבית על קבוצה סופית X, כך ש-$|X|>1$, אזי קיימת $g\in G$ ללא נקודת שבת.

הוכחה: נניח שלכל $g\in G$ יש נקודת שבת, ולכן לכל $g\in G$ מתקיים $1\le \mathrm{fix}\,(g)$.

עבור $e\in G$ מתקיים כי $\mathrm{fix}\,(e)=|X|>1$ ולכן נקבל מהלמה של ברנסייד כי $\frac{1}{|G|}\sum_{g\in G}\mathrm{fix}\,(g)>1$, בסתירה לכך ש-$G$ טרנזיטיבית על X. ■

10.6 מחלקות צמידות ורכזים

תזכורת: תהי G חבורה ויהי $x\in G$, מחלקת הצמידות של x מוגדרת להיות:

$$x^G=\left\{gxg^{-1}|g\in G\right\}$$

נשים לב ש-x^G הוא המסלול של $x\in G$ בפעולת G על עצמה באמצעות הצמדה.

הגדרה: נניח כי G פועלת על עצמה באמצעות הצמדה. נגדיר את **הרכז** של $x\in G$ ב-G להיות המייצב של x ביחס לפעולת הצמדה:

$$G_x=\left\{g\in G|gxg^{-1}=x\right\}=\{g\in G|gx=xg\}=:C_G\,(x)$$

הערות:

1. $C_G(x)$ הוא תת־חבורה לכל $x \in G$, כי הראינו שכל מייצב נקודה הוא תת־חבורה.
2. $Z(G) = \bigcap_{x \in G} C_G(x)$.

טענה: $\left|x^G\right| = |G : C_G(x)|$ לכל $x \in G$.

הוכחה: משפט מסלול־מייצב קובע כי באופן כללי $|O(x)| = |G : G_x|$.

במקרה הנוכחי מתקיים $O(x) = x^G$, $G_x = C_G(x)$, ולכן נציב ונקבל את הטענה.

■

מסקנה: $\left|x^G\right| \mid |G|$ לכל $x \in G$.

הוכחה: באופן כללי גדלי מסלולים מחלקים את גודל החבורה. ■

10.6.1 משוואת המחלקות

תהי G חבורה סופית. נניח כי $x_1^G, ..., x_k^G$ הן k מחלקות הצמידות השונות שגודלן גדול מ-1, כלומר $\left|\left\{gx_ig^{-1} | g \in G\right\}\right| = \left|x_i^G\right|$, אזי:

$$|G| = |Z(G)| + \sum_{i=1}^{k} \left|x_i^G\right| = |Z(G)| + \sum_{i=1}^{k} |G : C_G(x_i)|$$

(השוויון השני נובע מטענה קודמת $\left|x^G\right| = |G : C_G(x)|$).

הוכחה: נשים לב כי מכיוון ש-G מתחלקת לאיחוד זר של מחלקות צמידות, אז $|G|$ שווה לסכום הגדלים שלהן.

נסמן ב-$z_1, ..., z_l$ את איברי $Z(G)$. נשים לב שמתקיים $\left|x^G\right| = 1$ אמ"מ $x \in Z(G)$, ולכן מחלקות הצמידות בגודל 1 הן איברי המרכז: $\{z_1\}, ..., \{z_l\}$.

מכאן נקבל כי $|G|$ היא סכום איברי המרכז עם שאר מחלקות הצמידות בגודל גדול מ-1:

$$|G| = \sum_{j=1}^{l} |\{z_j\}| + \sum_{i=1}^{k} \left|x_i^G\right|$$

■

דוגמה: נניח כי $G = S_3$ כך ש-$Z(G) = \{e\}$. נחשב את גדלי המסלולים:

$$(12)^G = \{(12), (13), (23)\} \Rightarrow \left|(12)^G\right| = 3$$

$$(123)^G = \{(123), (132)\} \Rightarrow \left|(123)^G\right| = 2$$

לכן נקבל ממשוואת המחלקות:

$$6 = 3! = |S_3| = |Z(S_3)| + \left|(12)^G\right| + (123)^G = 1 + 3 + 2 = 6$$

10.7 משמר של תת־חבורה

תהי G חבורה ונגדיר $X = \{H | H \leq G\}$. נגדיר פעולה של G על X באמצעות הצמדה:

$$(g, H) \mapsto H^g = gHg^{-1} \leq G$$

את המייצב של תת־חבורה H ביחס לפעולה זו מגדירים להיות **המשמר** של H ב-G. כלומר, מתקיים כי המשמר הוא:

$$N_G(H) = \{g \in G | (g, H) = H\} = \left\{g \in G | gHg^{-1} = H\right\}$$

תכונות המשמר:

1. $N_G(H) \leq G$
2. $H \lhd N_G(H)$ (ומכלל כך $H \subseteq N_G(H)$)
3. $|G : N_G(H)| = |\{H^g | g \in G\}|$

הוכחה:

1. הוכחנו באופן כללי שהמייצב של איבר בקבוצה שפועלת עליה חבורה, הוא תת־חבורה.
2. מהגדרת המשמר נובע כי $g \in N_G(H)$ אמ"מ $H^g = H$. בפרט מתקיים $H^h = H$ לכל $h \in H$, ולכן $H \subseteq N_G(H)$.

   הנורמליות של H נובעת מהגדרת המשמר, שכן לכל $g \in N_G(H)$ מתקיים $gHg^{-1} = H$.
3. משפט מסלול־מייצב קובע באופן כללי כי $|O(x)| = |G : G_x|$, ולכן:

$$|\{H^g | g \in G\}| = |O(H)| = |G : G_H| = |G : N_G(H)|$$

■

הערות:

1. המשמר $N_G(H)$ הוא התת־חבורה המקסימלית ב-G ביחס לתכונה $H \lhd N_G(H)$.
2. $H \lhd G$ אמ"מ $G = N_G(H)$
3. מספר צמודי H ב-G סופית מחלק את $|G|$, כי מספר זה הוא גודל המסלול של H, וככלל גודל מסלול מחלק את גודל החבורה.

11 משפט קושי

תהי G חבורה סופית ויהי p ראשוני המחלק את $|G|$, אזי יש ב-G איבר מסדר p.

הערה: סדר של איבר מחלק את גודל החבורה, ולכן בהכרח הטענה נכונה רק ל-$p | |G|$.

הוכחה: תהי G חבורה סופית ויהי p ראשוני המחלק את $|G|$.

1. נגדיר את הקבוצה:

$$X=\{(g_1,g_2,...,g_p)\,|g_i\in G,\ g_1\cdot g_2\cdot...\cdot g_p=e\}\subseteq\underbrace{G\times G\times...\times G}_{p\,\text{times}}$$

- נשים לב שלאחר שקובעים $p-1$ איברים, האיבר ה-p נקבע ביחידות כדי לקיים את התנאי $g_1\cdot g_2\cdot...\cdot g_p=e$. מכאן שמספר האפשרויות להרכיב איברים ב-X הוא $|G|^{p-1}$, כלומר $|X|=|G|^{p-1}$.
- נשים לב גם שאיברי X סגורים להזזה ציקלית. כלומר אם $(g_1,g_2,...,g_p)\in X$ אז גם $(g_2,...,g_p,g_1)\in X$, שכן באמצעות הצמדה ב-g_1^{-1} נקבל $g_2\cdot...\cdot g_p\cdot g_1=e$.

  לכן נקבל באופן אינדוקטיבי שלכל k מתקיים כי אם $(g_1,g_2,...,g_p)\in X$ אז גם $(g_{k+1},g_{k+2},...,g_p,g_1,...,g_k)\in X$.

2. נגדיר פעולה של החבורה $\mathbb{Z}_p$ על הקבוצה X להיות:

$$(q,(g_1,...,g_p))\mapsto(g_{q+1},...,g_p,g_1,...,g_q)\in X$$

עבור $q\in\mathbb{Z}_p$. קל לוודא שזו פעולה של חבורה על קבוצה.

- כמו בכל פעולה של חבורה על קבוצה, גודל כל מסלול מחלק את גודל החבורה $|\mathbb{Z}_p|=p$, ומכך ש-p ראשוני נסיק כי גדלי המסלולים האפשריים הם $1,p$.
- נניח שיש n מסלולים בגודל 1 ו-m מסלולים בגודל p. ידוע כי הקבוצה היא איחוד זר של המסלולים של איברים בה, ולכן מתקיים $|X|=n\cdot 1+m\cdot p$.

  מכיוון ש-$p\,||G|$ וכן $|X|=|G|^{p-1}$, נסיק מכך ש-$n=|X|-mp$ שמתקיים $p|n$. כלומר מספר המסלולים בגודל 1 מתחלק ב-p.

3. נשים לב שלאיבר $(g_1,g_2,...,g_p)\in X$ יש מסלול בגודל 1 אמ"מ $(g_1,g_2,...,g_p)=(g_2,...,g_p,g_1)$, וזה אמ"מ $(g_2,...,g_p,g_1)=(g_3,...,g_1,g_2)$, וכן הלאה.

   כלומר מסלול בגודל 1 הוא רק לאיברים מהצורה $(g,g,...,g)\in G$, כלומר איברים המקיימים $\underbrace{g\cdot g\cdot...\cdot g}_{p\,\text{times}}=g^p=e$.

   מכך ש-p ראשוני נובע שאם $g^p=e$ ל-$g\in G$ כלשהו, אז אין $1<k<p$ שמקיים $g^k=e$, שכן בהכרח $p\nmid k$. לכן נקבל:

$$n=|\{g\in G|g^p=e\}|=|\{e\}\cup\{g\in G|\,|g|=p\}|=1+|\{g\in G|\,|g|=p\}|$$

מכאן שמספר האיברים מסדר p ב-G הוא $n-1$.

מכך ש-$p|n$ נובע $n-1\equiv-1 \mod p$. ברור כי $0\not\equiv-1 \mod p$ ולכן בהכרח $n-1\neq 0$. כלומר מספר האיברים מסדר p הוא טבעי ששונה מ-0, משמע קיים איבר מסדר p. ■

דוגמאות: נשים לב שהוכחת המשפט לא מספקת דרך למצוא את האיבר שסדרו p.

איבר מסדר p ב-S_n הוא תמורה מהצורה $(1...p)$.

אם $n=2p$ אפשר לבחור גם $(1...p)\,(p+1...2p)$.

איבר מסדר p ב-$GL_2\left(\mathbb{Z}_p\right)$ הוא מטריצה מהצורה $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$, כי מתקיים:

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^p = \begin{pmatrix} 1 & xp \\ 0 & 1 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod p$$

12 חבורות p

הגדרה: חבורה G נקראת **חבורת** p עבור p ראשוני כלשהו, אם הסדר של כל איבר ב-G הוא חזקה כלשהי של p. כלומר $\forall_{g\in G}\,\exists_{m\in\mathbb{N}}\,|g|=p^m$

m אינו יחיד בהכרח ובחירתו יכולה להיות תלויה ב-g.

טענה: G חבורה סופית היא חבורת p אמ"מ $|G|=p^n$ עבור n כלשהו.

הוכחה: (כיוון ראשון)

אם $|G|=p^n$, מטענה שהוכחנו נובע שהסדר של כל איבר ב-G מחלק את גודל החבורה. מכיוון ש-p ראשוני האיברים היחידים שמחלקים את p^n הן חזקות נמוכות יותר של p, ולכן הסדר של כל איבר הוא חזקה של p (הקטנה מ-n).

(כיוון שני)

נניח כי G חבורת p סופית. נניח בשלילה כי $|G|\neq p^n$ לכל n. ניתן לפרק את הגודל של G לגורמים ראשוניים, ולכן קיים ראשוני q, $q\neq p$, כך ש-$q||G|$.

ממשפט קושי נובע שקיים $g\in G$ שמקיים $o\left(g\right)=q$, למרות ש-q אינו חזקה של p, וזאת בסתירה להיות G חבורת p. ■

משפט: תהי $G\neq\{e\}$ חבורת p סופית, אזי $Z\left(G\right)\neq\{e\}$. כלומר לחבורת p סופית לא טריוויאלית, יש איבר שונה מ-e שמתחלף עם כל השאר.

הוכחה: נתבונן במשוואת המחלקות:

$$|G|=|Z\left(G\right)|+\sum_{i=1}^{k}\left|x_i^G\right|$$

כאשר x_i^G היא מחלקת צמידות בגודל גדול מ-1.

מכך ש-G חבורת p סופית ושגודלי מחלקות צמידות מחלקים את גודל החבורה נובע כי $\left|x_i^G\right|\,\big|\,|G|=p^n$. לכן נסיק כי $\left|x_i^G\right|=p^{n_i}$, עבור $0<n_i<n$ ומכאן ש-$p|\left|x_i^G\right|$ לכל i.

נעביר אגפים במשוואת המחלקות ונקבל כי $|Z\left(G\right)|=|G|-\sum_{i=1}^{k}\left|x_i^G\right|$. כלומר גודל המרכז הוא סכום של ביטויים המחלקים את p, ולכן הוא מחלק את p. מכאן ש-$|Z\left(G\right)|>1$, כלומר יש איבר לא טריוויאלי במרכז. ■

מסקנה: אם G חבורת p סופית,[11] אזי G פשוטה אמ"מ $G\cong\mathbb{Z}_p$.

[11] קיימות חבורות p שאינן סופיות, למשל מכפלות ישרות אינסופיות של $\mathbb{Z}_p$.

הוכחה: בכיוון אחד, ראינו כבר כי $\mathbb{Z}_p$ פשוטה, ולכן אם $G \cong \mathbb{Z}_p$ אז גם G פשוטה.

בכיוון שני, נניח כי G חבורת p סופית פשוטה. מההנחה כי היא פשוטה משמע $|G| > 1$, ומהמשפט שהוכחנו נובע כי $|Z(G)| > 1$.

ככלל, מרכז של חבורה הוא תת־חבורה נורמלית, ולכן האפשרות היחידה שבה יש תת־חבורה נורמלית בחבורה פשוטה היא $Z(G) = G$, כלומר G חבורה אבלית.

ברור כי $p||G|$ ולכן ממשפט קושי קיים $g \in G$ כך ש-$|g| = p$. נשים לב שלתת החבורה הנוצרת על־ידו מתקיים $p = |\langle g\rangle| \leq |G| = p^n$.

מכיוון ש-G אבלית החבורה הנוצרת של g היא נורמלית, ומכך ש-G פשוטה נובע כי $|G| = |\langle g\rangle|$. כלומר $|G| = p$, ומכאן כי היא איזומורפית ל-$\mathbb{Z}_p$. ■

למה: תהי G חבורה כך ש-$G/Z(G)$ חבורת מנה ציקלית, אזי G אבלית (ולכן $G = Z(G)$ ומכאן כי $G/Z(G) = \{e\}$).

ההוכחה מושארת כתרגיל.

מסקנה: כל חבורה מסדר p^2 היא אבלית.

הוכחה: אם $|G| = p^2$, ממשפט קודם נובע $Z(G) \neq \{e\}$ ולכן $|Z(G)|$ הוא p או p^2, ומכאן נסיק כי $|G/Z(G)|$ הוא 1 או p.

אם $|G/Z(G)| = 1$ אז $G = Z(G)$ ולכן G אבלית. אם $|G/Z(G)| = p$ אז היא בהכרח ציקלית (כל חבורה מגודל ראשוני היא ציקלית).

לכן חבורת המנה מסדר ראשוני והיא ציקלית, ומהלמה האחרונה נובע כי G אבלית, כלומר $Z(G) = G$. ■

12.1 תורת סילו

12.1.1 משפט סילו ה-I

תהי G חבורה סופית ויהי p ראשוני. נניח כי p^n היא חזקת p המקסימלית המחלקת את $|G|$, אזי קיימת תת־חבורה $P \leq G$ מגודל p^n (לא בהכרח יחידה).
לחבורה P הנ"ל קוראים **חבורת p־סילו**. לעתים מסמנים:

$$Syl_p(G) = \left\{P \leq G \middle| |P| = p^n,\, p^n \middle| |G|,\, p^{n+1} \nmid |G|\right\}$$

כלומר זהו אוסף החבורות p־סילו של חבורה G.

הערות:

1. אם $n = 0$ נקבל כי $p \nmid |G|$ ולכן נבחר $P = \{e\}$.
2. אם $|G| = p^n$ נוכל לבחור $P = G$.
3. בהמשך נוכיח שלכל $p^k||G|$ קיימת תת־חבורה בגודל p^k.
תוצאה זו תכליל את משפט קושי, שעוסק במקרה $n = 1$.[12]

תזכורת: המקדם הבינומי מוגדר: $\binom{k}{l} = \frac{k!}{l!(k-l)!} = \frac{k(k-1)\dots(k-l+1)}{l(l-1)\dots 2\cdot 1}$

[12] לפי משפט קושי אם $p||G|$ אז יש $x \in G$ כך ש-$|x| = p$, ולכן קיימת תת־חבורה $p = |\langle x\rangle|$.

למה: לכל p ראשוני ולכל m טבעי המקיימים $p\nmid m$, לכל n טבעי מתקיים $p\nmid\binom{p^n\cdot m}{p^n}$.

הוכחה: לפי הגדרת הבינום מתקיים:

$$\binom{n}{k}=\frac{n!}{k!\left(n-k\right)!}=\frac{n\left(n-1\right)...1}{k\left(k-1\right)...1\cdot\left(n-k\right)\left(n-k-1\right)...1}=\frac{n\left(n-1\right)...\left(n-k+1\right)}{k\left(k-1\right)...1}$$

ולכן מתקיים:

$$\binom{p^n\cdot m}{p^n}=\frac{p^nm\left(p^nm-1\right)...\left(p^nm-p^n+1\right)}{p^n\left(p^n-1\right)...2\cdot 1}=\frac{p^nm}{p^n}\cdot\frac{\left(p^nm-1\right)}{\left(p^n-1\right)}\cdot...\cdot\frac{\left(p^nm-p^n+1\right)}{1}$$

נתבונן באיבר כללי במכפלה הנ"ל $\frac{p^nm-i}{p^n-i}$. נוכיח כי לכל k אם $p^k|p^nm-i$ (המונה) אז $p^k|p^n-i$ (המכנה), לכל $0\leq i\leq p^n-1$.

במקרה $i=0$ מתקיים כי אם $p^k|p^nm$ אז $p^k|p^n$ כי הנחנו $p\nmid m$.

במקרה $1\leq i\leq p^n-1$ מתקיים מצד אחד כי $p^n\nmid i$ אבל $p^n|p^nm$ ולכן בהכרח $p^n\nmid p^nm-i$. מצד שני אם בכל זאת $p^k|p^nm-i$ אז בהכרח $k<n$. לכן $p^k|p^n$.

ניתן לכתוב $i=p^nm-\left(p^nm-i\right)$ ולכן בהכרח גם $p^k|i$, ומכאן $p^k|p^n-i$, כי הוא מחלק כל אחד מהם לחוד.

מכאן שבאיבר הכללי $\frac{p^nm-i}{p^n-i}$ כל חזקת p במונה מצטמצמת על־ידי איבר מתאים במכנה, כי אם חזקת p מחלקת את המונה היא תחלק גם את המכנה, ולכן הביטוי כולו לא יתחלק ב-p. ■

הוכחת משפט סילו הראשון

1. נתון כי p^n היא חזקה מקסימלית של p שמחלקת את $|G|$, ולכן נוכל לסמן $|G|=p^n\cdot m$ כאשר $p\nmid m$.

   נגדיר את הקבוצה $X=\{B\subseteq G||B|=p^n\}$, ונגדיר פעולה של G על X להעתיק $g.B=gB$[13].

   נשים לב שמבחירת B נובע שמתקיים $|gB|=|B|=p^n$ (ההעתקה שהגדרנו היא חח"ע ולכן הגודל לא משתנה).

   נשים לב כי $|X|=\binom{p^nm}{p^n}$, שכן זהו מספר האפשרויות לבחור תת־קבוצות של p^n איברים מתוך p^nm איברים, ולכן נסיק מהלמה כי $p\nmid|X|$.

2. ככלל, בפעולה של חבורה על קבוצה, הקבוצה היא איחוד זר של כלל המסלולים בה. לכן $|X|$ שהגדרנו הוא סכום גדלי המסלולים בפעולה שהגדרנו. מכך נסיק שבהכרח קיים מסלול Y שלא מתחלק ב-p, כי אחרת בהכרח $p||X|$.

   תהי $B\in Y$. ממשפט מסלול־מייצב הקובע שגודל מסלול של איבר הוא אינדקס המייצב, נסיק שמתקיים $|Y|=|O\left(B\right)|=|G:G_B|$.

3. נשים לב כי המייצב שהגדרנו עבור B הנ"ל הוא $G_B=\{g\in G|gB=B\}$. נוכיח כי G_B היא תת־חבורה של G והיא בגודל p^n. כלומר $P=G_B$ היא חבורת p־סילו.

   (א) G_B הוא מייצב של איבר ביחס לפעולה של חבורה על קבוצה, ולכן הוא תת־חבורה.

[13] נשים לב כי $gB\subseteq G$ אך לא בהכרח תת־חבורה שלה.

(ב) נראה כי הוא חבורת p־סילו:

מבחירת המסלול Y נובע כי $\frac{|G|}{|G_B|}=|G:G_B|=|O(B)|=|Y|\nmid p$.

אם כך מצד אחד מתקיים $p^n||G|$ ומצד שני $p\nmid\frac{|G|}{|G_B|}$ ולכן בהכרח כי $p^n||G_B|$ (כדי שהשבר יצטמצם), ומכאן כי $p^n\leq|G_B|$.

נוכיח את אי השוויון ההפוך. נקבע $b\in B$. מתקיים לכל $g\in G_B$ כי $gb\in gB=B$. מכאן ש-$G_BB\subseteq B$, ולכן נסיק כי:

$$p^n=|B|\geq|G_Bb|=|G_B|$$

כאשר אי השוויון נובע מכך ש-$G_BB\subseteq B$, והשוויון השני נובע מכך שההעתקה $x\mapsto xb$ היא חח"ע.

משני אי השוויונים נסיק כי $|G_B|=p^n$, ולכן $G_B\leq G$ חבורת p־סילו. ■

הערה: אם $P\leq G$ חבורת p־סילו, אז גם $P^g=gPg^{-1}$ לכל $g\in G$ היא חבורת p־סילו, כי $|P^g|=|P|=p^n$. מכאן שאם P לא נורמלית ב-G יש יותר מחבורת p־סילו אחת.

נוכיח בהמשך כי עד־כדי הצמדה, חבורת p־סילו היא יחידה.

12.1.2 משפט סילו ה-II

נסמן ב-$Syl_p(G)$ את אוסף חבורות ה-p־סילו של G. מתקיים $|Syl_p(G)|\equiv 1 \mod p$.

למה 1: יהיו $P,Q\leq G$ חבורות p, כך שמתקיים כי $Q\nsubseteq P$, וכן Q משמרת את P,[14] אזי:

1. PQ היא חבורת p ב-G.
2. $P\subsetneqq PQ$

הוכחה:

1. נתון שלכל $x\in Q$ מתקיים $xPx^{-1}=P$ או באופן שקול $xP=Px$. מכאן נובע $QP=PQ$ ולכן נסיק כי $PQ\leq G$.[15] הוכחנו (בתרגול) שבמקרה זה מתקיים $|PQ|=\frac{|P||Q|}{|P\cap Q|}$.

   נתון כי $|P|=p^k,\ |Q|=p^l$ כי הן חבורות p, ולכן $|PQ|=\frac{p^kp^l}{|P\cap Q|}|p^{k+l}$.

   מתכונות המספרים הראשוניים נובע שקיים m טבעי כך שמתקיים $|PQ|=p^m$ (כי רק חזקות של ראשוני מחלקות חזקה של ראשוני), משמע PQ חבורת p.
2. נשים לב שמתקיים $P=Pe\subseteq PQ$ וכן $Q=eQ\subseteq PQ$.

   לו $PQ=P$ אז $Q\subseteq PQ \Leftarrow Q\subseteq P$, בסתירה להנחה $Q\nsubseteq P$. לכן בהכרח $P\subsetneqq PQ$. ■

למה 2: יהי $T\neq\emptyset$ אוסף חבורות p־סילו של G שסגור להצמדה,[16] אזי $|T|\equiv 1 \mod p$.

---

[14] כלומר $P^x=xPx^{-1}=P$ לכל $x\in Q$. ובאופן שסימנו זאת לעיל: $Q\subseteq N_G(P)$ (המשמר).

[15] מכפלה של תת־חבורות היא תת־חבורה אמ"מ הן מתחלפות בכפל.

[16] כלומר לכל $x\in G$ ולכל $P\in T$ מתקיים $P^x=xPx^{-1}\in T$.

הוכחה:

1. תהי $Q \in T$, כלומר $Q \leq G$ חבורת p־סילו. נגדיר פעולה של החבורה Q על הקבוצה T באמצעות הצמדה (T סגורה להצמדה לפי הגדרתה).

   נחלק את T למסלולים ביחס לפעולת Q עליה. נשים לב כי $\{Q\}$ מסלול בגודל 1, כי הפעולה מוגדרת ביחס ל-Q, ולכל $y \in Q$ מתקיים $Q^y = Q$.

2. נוכיח כי $\{Q\}$ הוא המסלול היחיד בגודל 1: נניח בשלילה כי $\{P\}$ מסלול בגודל 1, כך ש-$Q \neq P$, ושתיהן חבורות p־סילו. כלומר מתקיים $P^x = P$ לכל $x \in Q$.

   מתקיים $Q \not\subseteq P$, כי $|Q| = |P|$ וגם $P \neq Q$, וכן גם מתקיים כי $xPx^{-1} = P$ לכל $x \in Q$ מההנחה שזה מסלול בגודל 1, ומכאן שמתקיימים תנאי למה 1. לכן $G \geq PQ \supsetneqq P$, כך ש-PQ חבורת p.

   נניח כי $p^n || G|$ היא החזקה המקסימלית ביחס לתכונה זו. משמע מתקיים $|P| = p^n$ (כי זו חבורת p־סילו), ומכך ש-$PQ \supsetneqq P$ נסיק $|PQ| = p^N$ עבור $n < N$.

   ממשפט לגראנז' נובע כי $p^N || G|$, בסתירה לכך ש-p^n היא החזקה המקסימלית המקיימת $p^n || G|$. לכן $\{Q\}$ הוא המסלול היחיד מגודל 1.

3. ממשפט מסלול־מייצב נובע שגדלי המסלולים בפעולה של חבורה על קבוצה מחלקים את גודל החבורה. בפרט במקרה שלנו מתקיים כי $|Q| = p^n$, ולכן גדלי המסלולים הם חזקות p.

4. אם כך מצאנו שגדלי כל המסלולים הם חזקות של p וגם גדולים מ-1 (לבד מ-$\{Q\}$).

   נזכור שגודל הקבוצה הוא סך גדלי המסלולים, ולכן $|T|$ מורכב מסכום של חזקות p ועוד 1, מכאן ש-$|T| \equiv 1 \mod p$. ■

הוכחת משפט סילו השני

ממשפט סילו הראשון נובע כי $Syl_p(G) \neq \emptyset$, וכן $Syl_p(G)$ סגורה להצמדה, כי אם $P \in Syl_p(G)$ כך ש-$|P| = p^n$, אז לכל $x \in G$ מתקיים $|P^x| = p^n$ ולכן $P^x \in Syl_p(G)$.
לכן מתקיימים תנאי למה 2 שקובעת כי $|Syl_p(G)| \equiv 1 \mod p$. ■

12.1.3 משפט סילו ה-III

כל זוג של חבורות p־סילו של חבורה סופית G, הן צמודות.

הוכחה: נניח בשלילה שקיימות זוג חבורות p־סילו שאינן צמודות. מכאן שבפעולת החבורה G על הקבוצה $Syl_p(G)$ באמצעות הצמדה קיימים לפחות שני מסלולים $T_1 \neq T_2$, $T_1, T_2 \subseteq Syl_p(G)$.

שני המסלולים T_1, T_2 עומדים בתנאי למה 2, שכן הם לא ריקים והם סגורים להצמדה כי הם מסלולים בפעולת הצמדה, ולכן מתקיים $T_1, T_2 \equiv 1 \mod p$.

נתבונן באיחוד $T_1 \cup T_2$. קבוצה זו אינה ריקה וסגורה להצמדה ולכן גם היא עומדת בתנאי למה 2, כך שמתקיים $|T_1 \cup T_2| \equiv 1 \mod p$.

מצד שני, כל המסלולים זרים ולכן $|T_1 \cup T_2|$ הוא איחוד זר, ומכאן שמתקיים:

$$|T_1 \cup T_2| = |T_1| + |T_2| = 2 \mod p \neq 1 \mod p$$

וזו סתירה. ■

מסקנה: $|Syl_p(G)|\,|\,|G|$

הוכחה: $Syl_p(G)$ הוא מסלול של פעולה, ובאופן כללי גודל של מסלול מחלק את גודל החבורה הפועלת. ■

12.1.4 נורמליות ויחידות בחבורות p־סילו

טענה: תהי G חבורה ו־P חבורת p־סילו שלה. אזי P היא חבורת p־סילו יחידה אמ"מ $P \lhd G$.

הוכחה: (כיוון ראשון)

אם P היא חבורת p־סילו היחידה של G, אז לכל $x \in G$ מתקיים כי $\left|xPx^{-1}\right| = |P|$ ולכן גם xPx^{-1} היא חבורת P־סילו. מהיחידות נובע כי $xPx^{-1} = P$, כלומר $P \lhd G$.

(כיוון שני)

נניח כי $P \lhd G$ חבורת p־סילו ותהי $Q \le G$ חבורת p־סילו כלשהי.

ממשפט סילו השלישי נובע כי כל חבורת p־סילו Q היא מהצורה $Q = P^x$ עבור $x \in G$ כלשהו, ולכן מהנתון כי $P \lhd G$ נובע כי $Q = P^x = P$. ■

12.1.5 משפט סילו ה־IV

תהי G חבורה סופית ויהי p ראשוני. לכל $p^k\,|\,|G|$ (לא בהכרח $p^k \parallel |G|$) קיימת $Q \le G$ כך ש־$|Q| = p^k$.

הערה: זו הכללה של משפט סילו הראשון, ובפרט גם הכללה של משפט קושי. ההוכחה תהיה דומה להוכחת משפט סילו הראשון.

הוכחה:

1. נתון כי p^n היא חזקה מקסימלית של p שמחלקת את $|G|$, ולכן נוכל לסמן $|G| = p^n \cdot m$ כאשר $p \nmid m$.
2. בהינתן k נגדיר את הקבוצה $X = \left\{B \subseteq G \,\middle|\, |B| = p^k\right\}$. קל לראות כי $|X| = \binom{|G|}{p^k} = \binom{p^n \cdot m}{p^k}$.

   נוכיח כי $p^{n-k} \parallel |X|$:

$$|X| = \binom{p^n m}{p^k} = \frac{p^n m}{p^k} \cdot \frac{p^n m - 1}{p^k - 1} \cdot \ldots \cdot \frac{p^n m - i}{p^k - i} \cdot \ldots \cdot \frac{p^n m - p^k + 1}{1} =$$

$$= p^{n-k} \cdot m \cdot \underbrace{\frac{p^n m - 1}{p^k - 1} \cdot \ldots \cdot \frac{p^n m - i}{p^k - i} \cdot \ldots \cdot \frac{p^n m - p^k + 1}{1}}_{=:A}$$

   מהלמה שלפני הוכחת משפט סילו הראשון נסיק כי $p \nmid A$. נצרף את ההנחה כי $p \nmid m$, ונסמן $|X| = p^{n-k} \cdot t$ כאשר $p \nmid t$. מביטוי זה ניכר בבירור כי $p^{n-k} \parallel |X|$.

3. נגדיר פעולה של G על X להעתיק $g.B=gB$.[17]

מאחר ו-$|X|$ היא סכום גודלי המסלולים, נסיק שבהכרח קיים מסלול שאינו מתחלק ב-p^{n-k+1}. שכן לו כל המסלולים היו מתחלקים ב-p^{n-k+1} היה מתקיים גם $p^{n-k+1}||X|$.

נניח כי $O(B)$ הוא המסלול שלא מתחלק ב-p^{n-k+1} עבור $B\in X$ כלשהי, ונוכיח כי המייצב G_B הוא חבורה בגודל p^k.

4. נניח כי $|G_B|=p^i\cdot l$ עבור $p\nmid l$. נוכיח כי $p^k=p^i\cdot l$.

(א) ראשית נרצה להראות כי $p^k|p^i\cdot l$, כלומר ש-$k\leq i$.
ממשפט מסלול־מייצב נובע כי:

$$p^{n-k+1}\nmid|O(B)|=\frac{|G|}{|G_B|}=\frac{p^n\cdot m}{p^i\cdot l}=p^{n-i}\cdot\frac{m}{l}$$

נשים לב כי אם $i<k$ אז $n-k+1\leq n-i$ ולכן מכך ש-$p^{n-i}||O(B)|$ נסיק כי גם $p^{n-k+1}||O(B)|$, וזו סתירה. לכן $k\leq i$ ומכאן $p^k\leq p^i\cdot l$.

(ב) כעת נוכיח את אי השוויון ההפוך $p^i\cdot l\leq p^k$.
נקבע $b\in B$ עבור התת־קבוצה B הנ"ל. לכל $g\in G_B$ מתקיים כי $gb\in gB=B$ ולכן $G_Bb\subset B$ ומכאן כי $|G_B|=|G_Bb|\leq|B|=p^k$.

משני אי השוויונים נסיק כי $p^k=p^i\cdot l=|G_B|$, ולכן G_B תת־חבורה בגודל p^k. ■

12.1.6 משפט סילו ה-V

תהי G חבורה סופית ותהי $Q\leq G$ חבורת p. אזי קיימת חבורת p־סילו P כך ש-$Q\subseteq P$.
כלומר כל חבורת p אפשר להרחיב לחבורת p־סילו.

הוכחה:

1. ניתן ל-Q לפעול על הקבוצה $Syl_p(G)$ באמצעות הצמדה. נניח בשלילה שלא קיימת חבורת p־סילו P כך ש-$Q\subseteq P$.

2. נראה שלא קיים מסלול בגודל 1 בפעולת Q על $Syl_p(G)$. אם נניח כי $\{P\}$ מסלול בגודל 1 אז בהכרח $xPx^{-1}=P$ לכל $x\in Q$, משמע Q משמרת את P, ובמקביל מההנחה בשלילה נובע כי $Q\nsubseteq P$. הוכחנו שבתנאים אלה מתקיים כי כי $P\subsetneqq PQ\leq G$, כלומר PQ חבורת p גדולה מ-P, בסתירה למקסימליות של P כחבורת p־סילו.[18] מכאן שאין מסלולים בגודל 1 בפעולת Q על $Syl_p(G)$.

3. ידוע כי Q חבורת p אז נסמן $|Q|=p^k$. גודל של כל מסלול בפעולת Q על $Syl_p(G)$ מחלק את $|Q|=p^k$, ולכן גודל של כל מסלול מתחלק ב-p, שכן הוא גדול מ-1.

ככלל גודל של קבוצה הוא סכום גודלי המסלולים, ולכן נסיק כי $p||Syl_p(G)|$ כלומר $|Syl_p(G)|\equiv 0 \mod p$, בסתירה למשפט סילו השני שקובע $|Syl_p(G)|\equiv 1 \mod p$. ■

[17] נשים לב כי $gB\subseteq G$ אך לא בהכרח תת־חבורה שלה.

[18] הוכחנו את הטענה הכללית הבאה: אם G חבורה סופית ו-P,Q חבורות p וכן Q משמרת את P וכן $Q\nsubseteq P$, אזי $PQ\leq G$ היא חבורת p המכילה ממש את P.

12.1.7 דוגמאות לחבורות p־סילו ושימוש בתורת סילו

1. נתבונן בחבורה S_p ל-p ראשוני. החבורה $\langle(1...p)\rangle$ היא חבורת p־סילו כי $p \parallel p!$, וקל לראות כי גודל החבורה הנוצרת מהאיבר הנ"ל הוא p. למעשה כל מחזור באורך p איברים שונים ייצור חבורת p־סילו.

נזכור כי תמורות הן צמודות אמ"מ יש להן אותו מבנה מחזורים, ומכאן כי כל המעגלים הנ"ל צמודים זה לזה, כלומר כל חבורות p־סילו של S_p צמודות, בהתאם למשפט סילו השלישי.

נתבונן ב-S_{2p-1}. מתקיים:

$$|S_{2p-1}| = (2p-1)! = 1 \cdot 2 \cdot ... \cdot p \cdot (p+1) \cdot ... \cdot (2p-1)$$

ולכן $p \parallel (2p-1)!$, ומכאן כי גם במקרה זה חבורות p־סילו הן המחזורים שהגדרנו לעיל.

נתבונן ב-S_{2p} עבור $p \neq 2$. מתקיים:

$$|S_{2p}| = (2p)! = 1 \cdot 2 \cdot ... \cdot p \cdot ... \cdot 2p$$

מכאן כי $p^2 \parallel (2p)!$ ולכן חבורת p־סילו היא מגודל p^2. חבורה בגודל כזה מתקבלת למשל על־ידי:

$$\langle (1...p), (p+1...2p) \rangle$$

2. נתבונן בחבורה $GL_2(\mathbb{F}_p)$ ל-p ראשוני. מתקיים כי:

$$|GL_2(\mathbb{F}_p)| = (p^2-1)(p^2-p) = p(p^2-1)(p-1)$$

ומכאן כי חבורת p־סילו של $GL_2(\mathbb{F}_p)$ היא מגודל p. חבורה בגודל כזה מתקבלת למשל על־ידי:

$$\left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} | x \in \mathbb{F}_p \right\}$$

באופן כללי, עבור החבורה $GL_n(\mathbb{F}_p)$ ל-p ראשוני, מתקיים כי $p^{\binom{n}{2}} \parallel |GL_n(\mathbb{F}_p)|$ ולכן חבורת p־סילו לדוגמה תהיה מהצורה:

$$\left\langle \begin{pmatrix} 1 & * & \dots & * \\ & 1 & \dots & * \\ & & \ddots & \vdots \\ & & & 1 \end{pmatrix} \right\rangle$$

3. נניח כי $|G| = 35 = 5 \cdot 7$.

ממשפט סילו השני נובע כי $|Syl_5(G)| \equiv 1 \mod 5$ ולכן $|Syl_5(G)| \in \{1, 6, 11, 16\}$. הסקנו לעיל כי $|Syl_p(G)| \mid |G|$ ולכן בהכרח $|Syl_5(G)| = 1$.

באותו אופן נקבל כי $|Syl_7(G)| \equiv 1 \mod 7$ ולכן $|Syl_7(G)| \in \{1,8,15\}$ ומכך ש-$|Syl_p(G)|\,|\,|G|$ נסיק שבהכרח $|Syl_7(G)| = 1$.

נניח P_5 חבורת 5־סילו וכי P_7 חבורת 7־סילו. ראינו כי הן יחידות ולכן שתיהן נורמליות.

מתקיים כי גודלן הוא 5 ו-7 בהתאמה, ובהכרח $P_5 \cap P_7 = \{e\}$, שכן גודל חבורת החיתוך חייב לחלק גם את 5 וגם את 7.

נקבל לפי משפט האיזומורפיזם השני כי:

$$|P_5P_7| = \frac{|P_5|\,|P_7|}{|P_5 \cap P_7|} = \frac{5\cdot 7}{1} = 35$$

ולכן $P_5P_7 = G$ והוכחנו כי בתנאים אלה (תת־חבורות נורמליות, בעלות חיתוך טריוויאלי שכפל של שתיהן הוא כל החבורה) מתקיים $G = P_5 \times P_7 \cong \mathbb{Z}_5 \times \mathbb{Z}_7$.

כלומר יש חבורה אחת בלבד מגודל 35, עד־כדי איזומורפיזם.

4. נניח כי $|G| = 36 = 2^2 \cdot 3^2$. נוכיח כי G לא פשוטה.

ממשפט סילו הראשון נובע שיש חבורת 3־סילו שנסמן P_3, וממשפט סילו השני נובע כי $|Syl_3(G)| \equiv 1 \mod 3$ ולכן $|Syl_3(G)| \in \{1,4,7,10,13,16\}$. כדי שגודל זה יחלק גם את 36 בהכרח $|Syl_3(G)| \in \{1,4\}$.

נשים לב כי $\left|{}^{G}/_{P_3}\right| = \frac{36}{9} = 4$. ניתן ל-$G$ לפעול על קבוצת ארבעת המחלקות הללו. נתבונן בהומומורפיזם שמוגדר על־ידי פעולה זו מהצורה $\varphi : G \to Sym\left({}^{G}/_{P_3}\right) \cong S_4$. ידוע כי $\ker(\varphi) \lhd G$, ולכן כדי לראות ש-G אינה פשוטה די להראות כי $\ker(\varphi)$ אינה טריוויאלית.

נניח בשלילה כי $\ker(\varphi) = \{e\}$, משמע φ הומומורפיזם חח"ע. אולם זה לא ייתכן כי התחום של φ הוא קבוצה מגודל 36 והטווח שלו קבוצה מגודל 4, ולכן הוא תת־חבורה נורמלית שאינה טריוויאלית. כמו־כן $\ker(\varphi) \neq G$ כי $\ker(\varphi) \subseteq P_3$, ולכן G אינה פשוטה.

12.2 תתי־חבורות של חבורות p

משפט: תהי G חבורת p סופית ותהי $H \lneqq G$ תת־חבורה, אזי $H \lneqq N_G(H)$.[19]

הוכחה: נסמן $X = \left\{H^g = gHg^{-1} | g \in G\right\}$ וניתן ל-G לפעול טרנזיטיבית על X באמצעות הצמדה.

נשים לב כי X הוא מסלול (יחיד) ביחס לפעולה הזו ולכן $|X|\,|\,|G|$. מכיוון ש-$|G| = p^n$ (כי היא חבורת p) נסיק כי $|X| = p^k$ עבור $0 \le k \le n$.

אם $k = 0$ אז ל-H יש צמוד יחיד ולכן זה בהכרח היא עצמה, כלומר $gHg^{-1} = H$ לכל $g \in G$ ומכאן כי $H \lhd G$ כולה ולכן $H \lneqq G = N_G(H)$.

נוכיח למקרה $0 < k$. מכך ש-$|X| = p^k$ נובע כי $p\,|\,|X|$. ניתן ל-H לפעול על X על־ידי הצמדה.

H היא תת־חבורה של חבורת p ולכן $|H| = p^l$, ומכאן כי גודלי המסלולים בפעולה הנ"ל מחלקים את p^l.

[19] תזכורת: $N_G(H) = \left\{g \in G | gHg^{-1} = H\right\}$

נשים לב כי $\{H\}$ היא מסלול בגודל 1, כי $hHh^{-1}=H$ לכל $h\in H$. אם זה המסלול היחיד בגודל 1, נובע כי $|X|$ הוא סכום גודלי המסלולים שרק אחד מהם בגודל 1 וכל השאר מתחלקים ב-p ולכן $|X|\equiv 1 \mod p$, בסתירה לכך ש-$p||X|$.

לכן קיים מסלול נוסף בגודל 1 שנסמן $\{K\}$, $H\neq K$. כלומר יש $g\in G$ כך ש-$K=gHg^{-1}$, וכן לכל $h\in H$ מתקיים $hKh^{-1}=K$. לכן מתקיים:

$$\forall_{h\in H}\, h\left(gHg^{-1}\right)h^{-1}=gHg^{-1}$$
$$\Downarrow$$
$$\forall_{h\in H}\, g^{-1}hgHg^{-1}h^{-1}g=H$$

$$\forall_{h\in H}\, g^{-1}hg\in N_G\left(H\right)$$

מההנחה בשלילה $N_G\left(H\right)=H$ נובע כי $g^{-1}hg\in H$ לכל $h\in H$, ומכאן כי $gHg^{-1}\subset H$.

מכיוון שאלו חבורות שוות־גודל בהכרח מתקיים גם $K=gHg^{-1}=H$, בסתירה להנחה $K\neq H$. ■

12.3 תתי־חבורות מקסימליות

הגדרה: תהי G חבורה. $H\leq G$ תיקרא **תת־חבורה מקסימלית** אם מתקיים $H\neq G$, וכן לא קיימת תת־חבורה $K\leq G$ כך ש-$H<K<G$ ממש.

הערות:

1. ייתכן שקיימות כמה חבורות מקסימליות.
2. אם $G\neq\{e\}$ חבורה סופית, אז יש לה תת־חבורה מקסימלית.[20]
3. תת־חבורה ממש מסדר מקסימלי היא מקסימלית, אבל ההיפך לא נכון. כלומר יש תתי־חבורות מקסימליות מגדלים שונים, שאחת גדולה מהאחרת.

   למשל $\mathbb{Z}_{15}\cong\mathbb{Z}_3\times\mathbb{Z}_5$, ולכן $\mathbb{Z}_3,\mathbb{Z}_5$ שתיהן מקסימליות, בעוד שידוע כי אחת גדולה מהאחרת. במפורש: $\{0,3,6,9,12\}$, $\{0,5,10\}$ שתיהן תתי־חבורות מקסימליות ב-$\mathbb{Z}_{15}$.

משפט: תהי G חבורת p סופית. אזי כל תת־חבורה מקסימלית של G היא חבורה נורמלית מאינדקס p. כלומר, אם $H<G$ ת"ח מקסימלית אז $H\lhd G$ וכן $|G:H|=p$.

נשים לב כי בפרט אם $G=p^n$, אז יש H מקסימלית המקיימת $|H|=p^{n-1}$.

הוכחה:

תהי $H<G$ מקסימלית. מהמשפט הקודם נובע כי $H\lneqq N_G\left(H\right)\leq G$. ממקסימליות H נובע כי $N_G\left(H\right)=G$ ומכאן כי $H\lhd G$ (זו המשמעות של העובדה שהמשמר הוא כל החבורה).

נוכיח כי $\frac{|G|}{|H|}=|G:H|=p$ ונשתמש במשפט ההתאמה.[21]

[20] ניתן לבנות אותה באופן הבא: אם $G_0=\{e\}$ מקסימלית סיימנו, ואם לא אז קיימת תת־חבורה G_1, $G_0<G_1<G$ כלשהי. אם היא מקסימלית סיימנו, ואם לא נמשיך את התהליך. תהליך זה יסתיים לאחר מספר סופי של שלבים כי G סופית.

[21] המשפט קובע שיש התאמה חח"ע ועל קבוצת תתי החבורות $\left\{\overline{H}|\overline{H}\leq G/N\right\}$ לבין קבוצת תתי החבורות $\{H|N\subseteq H\leq G\}$, המתקבלת באמצעות ההעתקה $K\mapsto K/H$, וכי התאמה זו משמרת נורמליות.

למה: עבור $G \triangleleft H$ וגם $H \lneqq G$, אז H מקסימלית אמ"מ אין ל-G/H תתי־חבורות מלבד G/H ו-$\{e\} \cong H/H$.

הוכחה: ממשפט ההתאמה נובע כי כל תתי החבורות של G/H הן מהצורה K/H עבור $H \leq K \leq G$.

לכן מהנתון ש-H נורמלית ומקסימלית נובע כי לא קיימת $G \lneqq K \lneqq H$ ולכן לא קיימת תת־חבורה ממש שאינה טריוויאלית מהצורה $K/H \leq G/H$. ■

מכאן של-G/H אין כלל תתי־חבורות ולכן בפרט היא פשוטה, וידוע כי היא חבורת p שכן $\frac{p^n}{p^k} = \frac{|G|}{|H|} = |G/H|$ ל-$k < n$.

הוכחנו שכל חבורת p פשוטה היא איזומורפית ל-$\mathbb{Z}_p$ ולכן $G/H \cong \mathbb{Z}_p$, כלומר מתקיים $|G : H| = |G/H| = p$. ■

13 סדרות נורמליות וסדרות הרכב

13.1 סדרות נורמליות

הגדרה: תהי G חבורה. **סדרה נורמלית** ב-G היא אוסף של תתי־חבורות $\{G_i\}$ מהצורה:

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright ... \triangleright G_n = \{e\}$$

מקובל לקרוא ל-n אורך הסדרה.

הערות:

1. ייתכנו חזרות. כלומר ייתכן שקיים i כך ש-$G_i = G_{i+1}$.
2. נזכור שנורמליות היא לא תכונה טרנזיטיבית. כלומר גם אם $G \triangleleft K \triangleleft H$ לא בהכרח $G \triangleleft H$.

הגדרה: בהינתן סדרה נורמלית, נאמר ש**הגורמים** שלה הן חבורות המנה G_i/G_{i+1} עבור $0 \leq i \leq n-1$.

הגדרה: נאמר שסדרה נורמלית $\{H_j\}$ ב-G היא **עידון** של סדרה נורמלית $\{G_i\}$ ב-G, אם $\{H_j\}$ מתקבלת מ-$\{G_i\}$ על־ידי תוספת של תתי־חבורות לסדרה.

13.2 סדרות הרכב

הגדרה: סדרה נורמלית $\{G_i\}$ ב-G נקראת **סדרת הרכב**, אם כל הגורמים שלה G_i/G_{i+1} הם פשוטים.

הערה: אם סדרה נורמלית היא סדרת הרכב אז $G_i \neq G_{i+1}$ לכל $0 \leq i \leq n-1$, אחרת המנה תהיה $\{e\}$ שאינה נחשבת חבורה פשוטה.

טענה: סדרה נורמלית $\{G_i\}$ ב-G היא סדרת הרכב אמ"מ גם אין בה חזרות וגם לא ניתן לעדן אותה ללא הוספת חזרות.

כלומר $\{G_i\}$ סדרת הרכב אמ"מ גם אין בה חזרות וגם לא ניתן למצוא $G_i \triangleright N \triangleright G_{i+1}$ כך שההכלות הן באופן חזק.

הוכחה: משפט ההתאמה קובע שעבור $G \triangleright N$ קיימת התאמה חח"ע ועל בין $\{\overline{H} | \overline{H} \leq G/N\}$ לבין $\{H | N \subseteq H \leq G\}$, והתאמה זו משמרת נורמליות.

כלומר במקרה שלנו לכל i, קיימת התאמה חח"ע ועל בין תתי החבורות מהצורה $G_i \triangleright N \triangleright G_{i+1}$ לבין תתי החבורות מהצורה $\{e\} \cong G_{i+1}/G_{i+1} \triangleleft N/G_{i+1} \triangleleft G_i/G_{i+1}$.

מכאן שמתקיים:

הסדרה הנורמלית $\{G_i\}$ סדרת הרכב, כלומר G_i/G_{i+1} פשוטה לכל i $\iff$ לכל i אין ת"ח נורמלית חדשה $G_i/G_{i+1} \triangleright N/G_{i+1} \triangleright G_{i+1}/G_{i+1}$ $\iff$ אין ת"ח נורמלית חדשה $G_i \triangleright N \triangleright G_{i+1}$. ■

דוגמה: נניח כי $|G| = p^n$. הוכחנו לעיל שיש לה תת־חבורה מקסימלית $G \triangleright H$ מאינדקס p, כלומר מתקיים $G/H \cong \mathbb{Z}_p$.

נבנה ל-G סדרת הרכב באופן הבא: נגדיר $G_0 = G$. לכל i נגדיר את G_{i+1} להיות תת החבורה המקסימלית הנורמלית של G_i. זה תהליך סופי כי G סופית וכן הגורמים איזומורפיים ל-$\mathbb{Z}_p$ ולפיכך פשוטים, ונקבל סדרת הרכב.

13.3 קיום של סדרות הרכב (לחבורות סופיות)

משפט: לכל חבורה סופית יש סדרת הרכב.

הוכחה: תהי G סופית. אם $G = \{e\}$ יש לה סדרת הרכב טריוויאלית. לכן נניח $G \neq \{e\}$, ונבנה סדרת הרכב באופן הבא: נגדיר $G_0 = G$, ונבחר את G_1 להיות התת־חבורה (ממש) הנורמלית המקסימלית ב-G (מקסימלית ביחס להכלה). מסופיות G קיימת תת־חבורה כזאת.

לכל i, נבחר את G_{i+1} להיות התת־חבורה (ממש) הנורמלית המקסימלית ב-G_i. מסופיות G נובע שהתהליך ייעצר לאחר מספר סופי של שלבים. ■

טענה: כל סדרה נורמלית ללא חזרות של חבורה סופית, ניתנת לעידון לסדרת הרכב.

הוכחה: מתחילים להוסיף את תת החבורות הנורמליות שחסרות בסדרת הנורמלית עד שלא ניתן להמשיך יותר. התהליך ייעצר כי החבורה סופית, והעידון שיתקבל הוא סדרת הרכב כי אין חזרות לפי הנתון ולפי הבנייה, וכן לא ניתן לעדן אותה יותר כי הוספנו את כל תתי החבורות האפשריות. (לפי איפיון שקול לסדרת הרכב). ■

13.4 יחידות של סדרות הרכב (עד־כדי סדר ואיזומורפיזם)

שקילות של סדרות הרכב: יהיו $\{A_i\}_{i=1}^{n}, \{B_j\}_{j=1}^{m}$ סדרות הרכב של חבורה G. נאמר שסדרות אלו **שקולות** אם גורמיהן זהים עד־כדי שינוי סדר ועד־כדי איזומורפיזם.

כלומר $B_j/B_{j+1} \cong A_i/A_{i+1}$ לכל i עבור j כלשהו. בפרט הסדרות באותו אורך, כלומר $n = m$.

בפרק זה נוכיח שלכל חבורה, סופית או לא, כל סדרות ההרכב שלה שקולות.

13.4.1 למת הפרפר של זסנהאוס

תהי G חבורה, ונניח כי כי $A \lhd A^* \leq G$ וכן $B \lhd B^* \leq G$. אזי:

$$A\left(A^*\cap B\right)\lhd A\left(A^*\cap B^*\right)$$

$$B\left(A\cap B^*\right)\lhd B\left(A^*\cap B^*\right)$$

וכן גם מתקיים:

$$A(A^*\cap B^*)/A(A^*\cap B)\cong B(A^*\cap B^*)/B(A\cap B^*)$$

הוכחת הלמה תילמד בתרגול.

13.4.2 משפט העידון של שרייר

לכל שתי סדרות נורמליות של חבורה G (לאו דווקא סופית) יש עידונים שקולים.

הוכחה:

1. נניח כי $\{A_i\}_{i=0}^n,\{B_j\}_{j=0}^m$ סדרות נורמליות של G. נרצה ליצור עידון לכל אחת מהן, ולהראות ששני העידונים המתקבלים שקולים.

- ניצור עידון ל-$\{A_i\}_{i=0}^n$. לשם כך נגדיר $A_{ij}=A_{i+1}\left(A_i\cap B_j\right)$ כאשר $0\leq i\leq n-1,\, 0\leq j\leq m-1$.
ראשית נשים לב שמלמת הפרפר נובע שלכל i מתקיים $A_{ij}\rhd A_{i,j+1}$.
עוד נשים לב שמתקיים:

$$A_{i0}=A_{i+1}\left(A_i\cap B_0\right)=A_{i+1}\left(A_i\cap G\right)=A_{i+1}A_i=A_i$$

$$A_{im}=A_{i+1}\left(A_i\cap B_m\right)=A_{i+1}\left(A_i\cap\{e\}\right)=A_{i+1}$$

כעת נבצע את העידון: לכל $0\leq i\leq n-1$ נוסיף בתווך של $A_i\rhd A_{i+1}$ את התת־חבורות:

$$A_i=A_{i0}\rhd A_{i1}\rhd\ldots\rhd A_{im}=A_{i+1}$$

- ניצור עידון ל-$\{B_j\}_{j=0}^m$ (בדיוק באותו אופן). לשם כך נגדיר באופן סימטרי $B_{ji}=B_{j+1}\left(B_j\cap A_i\right)$.
מאותן סיבות, גם כאן מתקיים $B_{i0}=B_i$ וכן $B_{jn}=B_{j+1}$, וגם $B_{ji}\rhd B_{j,i+1}$.
באותו אופן נבצע את העידון: לכל $0\leq j\leq m-1$ נוסיף בתווך של $B_j\rhd B_{j+1}$ את התת־חבורות:

$$B_j=B_{j0}\rhd B_{j1}\rhd\ldots\rhd B_{jn}=B_{j+1}$$

את העידון נבצע באופן מילוני. כלומר קודם לפי i (כלומר לפי $\{A_i\}_{i=0}^{n}$) ואז לפי j (כלומר לפי $\{B_j\}_{j=0}^{m}$).

2. נראה ששני העידונים שהתקבלו שקולים.
נשים לב שגורם כללי בסדרה המעודנת לפי i יהיה מהצורה:

$$A_{ij}/A_{i,j+1} = A_{i+1}(A_i \cap B_j)/A_{i+1}(A_i \cap B_{j+1})$$

ונשים לב שגורם כללי בסדרה המעודנת לפי j הוא מהצורה:

$$B_{ji}/B_{j,i+1} = B_{j+1}(B_j \cap A_i)/B_{j+1}(B_j \cap A_{i+1})$$

מלמת הפרפר נובע כי:

$$A_{ij}/A_{i,j+1} \cong B_{ji}/B_{j,i+1}$$

לכן כל הגורמים של הסדרות המעודנות איזומורפיים, ומכאן שעד־כדי סדר העידונים שקולים. ■

13.4.3 משפט ז'ורדן־הולדר

כל סדרות ההרכב של חבורה, סופית או לא, הן שקולות.

הוכחה: יהיו $\{G_i\}_{i=0}^{n}, \{H_j\}_{j=0}^{m}$ סדרות הרכב של חבורה G. ממשפט העידון של שרייר נובע שלזוג הסדרות הללו קיימים עידונים שקולים, שנסמן $\{G_i'\}_{i=0}^{N}, \{H_j'\}_{j=0}^{N}$ בהתאמה (העידונים באותו אורך כי הם שקולים).

נתון כי אלו סדרות הרכב, ולכן כל עידון יכול להוסיף חזרות בלבד. כל חזרה מוסיפה את הגורם $\{e\}$ בלבד, מספר כלשהו של פעמים. מכאן כי:

$$\{G_i'\}_{i=0}^{N} = \{G_i\}_{i=0}^{n} + l_1 \cdot \{e\} \qquad \{H_j'\}_{j=0}^{N} = \{H_j\}_{j=0}^{m} + l_2 \cdot \{e\}$$

מכאן שהגורמים של $\{G_i'\}_{i=0}^{N}$ הם בדיוק הגורמים של $\{G_i\}_{i=0}^{n}$ בתוספת $\{e\}$, וכן גם הגורמים של $\{H_j'\}_{j=0}^{N}$ הם בדיוק הגורמים של $\{H_j\}_{j=0}^{m}$ בתוספת $\{e\}$.

משקילות הסדרות המעודנות נובע שגורמיהן איזומורפיים ולכן $l_1 = l_2$, ומהזהות בין גורמי סדרות ההרכב לגורמי העידונים שלהן נובע שגורמי סדרות ההרכב איזומורפיים, כלומר סדרות ההרכב שקולות. ■

מסקנה: (המשפט היסודי של האריתמטיקה) הפירוק של כל מספר שלם לגורמים ראשוניים הוא יחיד.

הוכחה: יהי $k \in \mathbb{Z}$ ונניח כי יש לו שני פירוקים לראשוניים: $k = p_1 \cdot p_2 \cdot \ldots \cdot p_n = q_1 \cdot q_2 \cdot \ldots \cdot q_m$ (ייתכנו חזרות).

כל אחד מהפירוקים יוצר סדרת הרכב של החבורה $\mathbb{Z}_k$, בהתאמה באופן הבא:

$$\mathbb{Z}_k \rhd \langle p_1 \rangle \rhd \langle p_1 p_2 \rangle \rhd \ldots \rhd \langle p_1 \cdot p_2 \cdot \ldots \cdot p_{n-1} \rangle \rhd \langle 0 \rangle$$

$$\mathbb{Z}_k \rhd \langle q_1 \rangle \rhd \langle q_1 q_2 \rangle \rhd \ldots \rhd \langle q_1 \cdot q_2 \cdot \ldots \cdot q_{m-1} \rangle \rhd \langle 0 \rangle$$

כאשר גורמי ההרכבים הם $\mathbb{Z}_{p_1}, \ldots, \mathbb{Z}_{p_{n-1}}$ ו-$\mathbb{Z}_{q_1}, \ldots, \mathbb{Z}_{q_{m-1}}$ בהתאמה.

ממשפט ז'ורדן הולדר נובע כי שתי סדרות ההרכב הללו שקולות, כלומר כל גורם $\mathbb{Z}_{p_i}$ איזומורפי ל-$\mathbb{Z}_{q_j}$ כלשהו. מכאן בהכרח כל p_i שווה ל-q_j כלשהו. כלומר כל הראשוניים המופיעים בפירוק אחד מופיעים בדיוק גם בשני (עד־כדי שינוי סדר). ■

13.5 סדרות הרכב בחבורות שלמים

לחבורה $\mathbb{Z}_k$ כללית נבנה סדרת הרכב באמצעות הפירוק של k לגורמים ראשוניים. כלומר אם $k = p_1 \cdot p_2 \cdot \ldots \cdot p_n$ (ייתכנו חזרות) אז סדרת הרכב תתקבל על־ידי:

$$\mathbb{Z}_k \rhd \langle p_1 \rangle \rhd \langle p_1 \cdot p_2 \rangle \rhd \ldots \rhd \langle p_1 \cdot p_2 \cdot \ldots \cdot p_{n-1} \rangle \rhd \langle p_1 \cdot p_2 \cdot \ldots \cdot p_{n-1} \cdot p_n \rangle = \langle 0 \rangle$$

כאשר הגורמים יהיו:

$$\mathbb{Z}_k/\langle p_1 \rangle \cong \mathbb{Z}_{p_1}$$

$$\langle p_1 \rangle/\langle p_1 \cdot p_2 \rangle \cong \mathbb{Z}_{p_2}$$

$$\langle p_1 \cdot p_2 \rangle/\langle p_1 \cdot p_2 \cdot p_3 \rangle \cong \mathbb{Z}_{p_3}$$

$$\vdots$$

$$\langle p_1 \cdot p_2 \cdot \ldots \cdot p_{n-1} \rangle/\langle 0 \rangle \cong \mathbb{Z}_{p_n}$$

נשים לב שסדר הפירוק של n לראשוניים לא משנה ולכן כל פירוק ייתן את אותה סדרת הרכב, עד־כדי שינוי סדר ואיזומורפיזם.

דוגמה: נבנה שתי סדרות הרכב לחבורה $\mathbb{Z}_{30}$.

נגדיר סדרת הרכב אחת להיות $\mathbb{Z}_{30} \rhd \langle 2 \rangle \rhd \langle 6 \rangle \rhd \langle 0 \rangle$. נראה שזו אכן סדרת הרכב:

$$\mathbb{Z}_{30}/\langle 2 \rangle \cong \mathbb{Z}_2$$

$$\langle 2 \rangle/\langle 6 \rangle \cong \mathbb{Z}_3$$

$$\langle 6 \rangle/\langle 0 \rangle \cong \mathbb{Z}_5$$

נגדיר סדרת הרכב נוספת להיות $\mathbb{Z}_{30} \rhd \langle 3 \rangle \rhd \langle 15 \rangle \rhd \langle 0 \rangle$. נראה שזו אכן סדרת הרכב:

$$\mathbb{Z}_{30}/\langle 3 \rangle \cong \mathbb{Z}_3$$

$$\langle 3 \rangle/\langle 15 \rangle \cong \mathbb{Z}_5$$

$$\langle 15 \rangle/\langle 0 \rangle \cong \mathbb{Z}_2$$

נשים לב שקיבלנו את אותם הגורמים בשינוי סדר ועד־כדי איזומורפיזם, בהתאם למשפט ז'ורדן־הולדר.

משפט: לחבורה $\mathbb{Z}$ אין סדרת הרכב.

הוכחת המשפט: (הוכחה ראשונה) לצורך ההוכחה נראה שתי טענות־עזר.

למה 1: תהי $\{G_i\}_{i=0}^n$ סדרה נורמלית ב-G, אזי $|G| = \prod_{i=0}^n |G_i/G_{i+1}|$.

הוכחה:

$$\prod_{i=0}^{n}\left|{}^{G_i}/_{G_{i+1}}\right| = \left|{}^{G}/_{G_1}\right|\cdot\left|{}^{G_1}/_{G_2}\right|\cdot\ldots\cdot\left|{}^{G_{n-1}}/_{\{e\}}\right| =$$

$$= \frac{|G|}{|G_1|}\cdot\frac{|G_1|}{|G_2|}\cdot\ldots\cdot\frac{|G_{n-2}|}{|G_{n-1}|}\cdot\frac{|G_{n-1}|}{1} = |G|$$

הוכחת המקרה האינסופי מושארת כתרגיל (מספיק להראות שקיימת חבורת מנה ${}^{G_i}/_{G_{i+1}}$ אינסופית). ■

למה 2: כל חבורה אבלית ופשוטה איזומורפית ל-$\mathbb{Z}_p$ עבור p ראשוני כלשהו.

הוכחה: נניח כי G חבורה אבלית פשוטה. ניקח $e \neq x \in G$ ונתבונן בתת החבורה שהוא יוצר $\langle x\rangle$.

G אבלית ולכן $\langle x\rangle \lhd G$, ומכך ש-G פשוטה נובע כי $G = \langle x\rangle$. כלומר G ציקלית.

נניח בשלילה כי G אינסופית. אזי $G \cong \mathbb{Z}$ באמצעות $k \mapsto x^k$ (קל לוודא שזה איזומורפיזם), בסתירה לכך ש-G פשוטה, כי למשל חבורת הזוגיים נורמלית ב-$\mathbb{Z}$ ולכן החבורה $\left\{x^{2m}|m \in \mathbb{N}\right\}$ תהיה נורמלית ב-G.

לכן G בהכרח חבורה ציקלית סופית כך ש-$G = \langle x\rangle$, ומכאן כי אם $|G| = k$ אז $G \cong \mathbb{Z}_k$ ל-k שלם כלשהו.

נשים לב שבהכרח k ראשוני, כי אם $p|k$ נבחר תת־חבורה $\langle x^p\rangle$ חלקית ממש ל-G. היא נורמלית כי החבורה כולה ציקלית ולכן אבלית, בסתירה לפשטות G.

מכאן שבהכרח $k = p$ ראשוני, ולכן $G \cong \mathbb{Z}_p$. ■

כעת נוכיח את המשפט: נניח בשלילה כי $\{G_i\}_{i=0}^{n}$ סדרת הרכב של $\mathbb{Z}$. לכל i, מכך ש-$G_i \leq \mathbb{Z}$ נובע כי G_i אבלית, ולכן גם חבורת המנה ${}^{G_i}/_{G_{i+1}}$ אבלית. כמו־כן, מההנחה ש-$\{G_i\}_{i=0}^{n}$ סדרת הרכב נובע שהגורמים פשוטים.

אם כך מהלמה השנייה נובע כי ${}^{G_i}/_{G_{i+1}} \cong \mathbb{Z}_{p_i}$ לכל i עבור p_i ראשוני כלשהו, ולכן מהלמה הראשונה נובע כי $|\mathbb{Z}| = \prod_{i=0}^{n}\left|{}^{G_i}/_{G_{i+1}}\right| = p_1\cdot\ldots\cdot p_n < \infty$, וזו סתירה. ■

הוכחת המשפט: (הוכחה שנייה) לצורך ההוכחה נראה טענת־עזר.

למה: כל תת־חבורה של $\mathbb{Z}$ שאינה טריוויאלית, איזומורפית ל-$\mathbb{Z}$.

הוכחה: נשים לב כי $n\mathbb{Z} \cong \mathbb{Z}$ לכל n שלם, למשל באמצעות האיזומורפיזם $i \mapsto ni$. המשך ההוכחה מושאר כתרגיל. ■

כעת נוכיח את המשפט: נניח בשלילה כי $\mathbb{Z} = G_0 \rhd G_1 \rhd \ldots \rhd G_{n-1} \rhd G_n = \{0\}$ סדרת הרכב ב-$\mathbb{Z}$.

בסדרת הרכב אין חזרות, ולכן מתקיים $\{0\} \neq G_{n-1} < \mathbb{Z}$. מהלמה נובע כי $G_{n-1} \cong \mathbb{Z}$ ולכן ${}^{G_{n-1}}/_{\{0\}} \cong {}^{\mathbb{Z}}/_{\{0\}} \cong \mathbb{Z}$, בסתירה לכך שהגורמים פשוטים. ■

13.6 סדרות הרכב בחבורות תמורות

- לחבורות S_1, S_2 יש סדרות הרכב טריוויאליות.
- לחבורה S_3 יש סדרת הרכב $S_3 \rhd A_3 \rhd \{e\}$ וגורמי ההרכב הם $\mathbb{Z}_2, \mathbb{Z}_3$.

- לחבורה S_4 יש סדרת הרכב $S_4 \rhd A_4 \rhd \mathbb{Z}_2\times\mathbb{Z}_2 \rhd \{e\}$ וגורמי ההרכב הם $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_2\times\mathbb{Z}_2$.

  נשים לב כי $\mathbb{Z}_2\times\mathbb{Z}_2$ איזומורפית לחבורת קליין $\{e, (12)(34), (13)(24), (14)(23)\} \leq S_4$.

- לחבורה S_n עבור $n \geq 5$ יש סדרת הרכב $S_n \rhd A_n \rhd \{e\}$ וגורמי ההרכב הם $\mathbb{Z}_2, A_n$.

  הדבר נובע מכך ש-A_n פשוטה עבור כל $n \geq 5$.

14 חבורות פתירות

הגדרה: סדרה נורמלית נקראת **סדרה פתירה** אם כל הגורמים שלה אבליים.

כלומר סדרה נורמלית $\{G_i\}_{i=0}^n$ המקיימת ${}^{G_i}/_{G_{i+1}}$ אבלית לכל i.

הגדרה: חבורה G נקראת **פתירה** אם יש לה סדרה פתירה.

הערה היסטורית: חבורות פתירות קשורות לפתרון משוואות פולינומיאליות מעל שדה.

קיימות נוסחאות לפתרון משוואות פולינומיאליות ממעלות $1,2,3,4$, אבל עבור $n \geq 5$ לא קיימת נוסחה כללית לפיתרון. עם זאת, עבור חלק מהמשוואות הפולינומיאליות קיימת נוסחה לפתרון כללי גם עבור $n \geq 5$. גלואה הצליח להתאים לכל משוואה פולינומיאלית חבורה, והראה שקיום נוסחה לפתרון שקול לפתירות של החבורה המתאימה.

כפי שמיד נראה, העובדה ש-S_n פתירה עבור $4 \geq n$ ואינה פתירה עבור $n \geq 5$, קשורה לכך שלמשוואות פולינומיאליות ממעלה ≤ 4 קיימת נוסחה לפתרון ולמשוואות כנ"ל ממעלה ≥ 5 לא קיימת נוסחה לפתרון.

דוגמאות יסודיות:

1. כל חבורה G אבלית היא פתירה.

   נימוק: $G \rhd \{e\}$ היא סדרה נורמלית שגורם ההרכב שלה הוא $G \cong {}^{G}/_{\{e\}}$ ולכן הוא אבלי.

2. S_n עבור $n \leq 4$ פתירה.

   נימוק: כפי שראינו לעיל כל גורמי ההרכב של סדרת ההרכב שלה איזומורפיים ל-$\mathbb{Z}_k$ כלשהי.

3. כל חבורה G פשוטה ולא אבלית אינה פתירה.

   נימוק: בכל סדרה נורמלית של G יש מקום שבו $G \rhd \{e\}$ מפשטות G, ולכן יש לה גורם הרכב $G \cong {}^{G}/_{\{e\}}$ שאינו אבלי.

4. A_n, S_n עבור $n \geq 5$ אינן פתירות.

   נימוק: לכל $n \geq 5$ החבורה A_n פשוטה ולא אבלית, ולכן אינה פתירה לפי המקרה הקודם.

   לכל $n \geq 5$ סדרת הרכב של החבורה S_n היא מהצורה $S_n \rhd A_n \rhd \{e\}$, ולכן יש לה גורם הרכב $A_n \cong {}^{A_n}/_{\{e\}}$ שאינו אבלי.

5. כל חבורת p סופית היא פתירה.[22]

נימוק: קל לבנות לה סדרת הרכב כך שכל גורמי ההרכב יהיו איזומורפיים ל-$\mathbb{Z}_p$, ולכן הם כולם יהיו אבליים.

טענה: כל חבורה פשוטה פתירה היא בהכרח $\mathbb{Z}_p$ ל-p ראשוני כלשהו.

הוכחה: הוכחנו שחבורה פשוטה לא אבלית אינה פתירה, ולכן אם חבורה פתירה היא אבלית. הוכחנו לעיל גם שכל חבורה פשוטה ואבלית היא $\mathbb{Z}_p$. ■

משפט: חבורה סופית היא פתירה אמ"מ כל גורמי ההרכב שלה הם $\mathbb{Z}_{p_i}$, עבור p_i ראשוניים.

הוכחה: (כיוון ראשון) נניח כי כל גורמי ההרכב של G הם $\mathbb{Z}_{p_1},...,\mathbb{Z}_{p_n}$ (ייתכנו חזרות), אז הם אבליים ולכן זו סדרה פתירה.

(כיוון שני) תהי G סופית ופתירה, ונניח כי $G=G_0\rhd G_1\rhd...\rhd G_n=\{e\}$ סדרה פתירה. נניח ללא הגבלת הכלליות שאין חזרות.

הוכחנו שבחבורה סופית כל סדרה נורמלית ללא חזרות ניתנת לעידון לסדרת הרכב, ולכן ניתן להניח ללא הגבלת הכלליות שזו אכן סדרת הרכב.

מההנחה שזו סדרה פתירה נובע כי G_i/G_{i+1} חבורה אבלית לכל i. תהי $A\rhd B$ חוליה כלשהי בסדרת ההרכב. נשים לב שמתקיים לפי משפט האיזומורפיזם השלישי כי $A/B\cong {}^{A/G_{i+1}}/_{B/G_{i+1}}$, ומכך שמתקיים כי $A/G_{i+1}\leq G_i/G_{i+1}$ וכך גם ל-B, נובע כי הן תת־חבורות של חבורות אבליות ולכן הן אבליות. חבורת מנה של חבורה אבלית היא אבלית, ולכן גם A/B אבלית.

אם כך A/B פשוטה ואבלית, וכפי שהוכחנו כל חבורה מטיפוס כזה היא $\mathbb{Z}_p$ ל-p ראשוני. ■

מסקנה: עידון של כל סדרה פתירה הוא סדרה פתירה.

טענה: תהי G חבורה פתירה, אזי:

1. כל תת־חבורה של G היא פתירה.
2. כל חבורת מנה של G היא פתירה.

הוכחה:

1. תהי $H\leq G$ ותהי $\{G_i\}_{i=0}^n$ סדרה פתירה של G. נוכיח כי $\{H\cap G_i\}_{i=0}^n$ היא סדרה פתירה של H.

   (א) ראשית קל לראות כי $H\cap G_{i+1}\lhd H\cap G_i$, שכן לכל $g\in H\cap G_i$ מתקיים:

$$(H\cap G_{i+1})^g=H^g\cap G_{i+1}^g=H\cap G_{i+1}$$

   כאשר השוויון השני נובע מכך ש-$g\in H$ וגם $g\in G_i\leq G_{i+1}$.
   לכן נקבל שהסדרה $\{H\cap G_i\}_{i=0}^n$ סדרה נורמלית של H (נשים לב שאכן $H\cap G_0=H\cap G=H$ וכן $H\cap G_n=H\cap\{e\}=\{e\}$).

[22] קיימות חבורות p שאינן סופיות. למשל מכפלות ישרות אינסופיות.

(ב) נותר להראות שזו סדרה פתירה. לצורך כך נוכיח שמתקיים:

$$H\cap G_i/H\cap G_{i+1} \cong (H\cap G_i)G_{i+1}/G_{i+1} \leq G_i/G_{i+1}$$

ומכך ש-G_i/G_{i+1} גורם הרכב אבלי, כי $\{G_i\}_{i=0}^n$ סדרה פתירה ל-G, ינבע כי $H\cap G_i/H\cap G_{i+1}$ גורם הרכב אבלי, ומזה נסיק כי $\{H\cap G_i\}_{i=0}^n$ סדרה פתירה של H.

תזכורת: משפט האיזומורפיזם השני קובע כי אם $N \lhd G$, $K \leq G$, אז $K/K\cap N \cong KN/N$.

נציב במשפט את החבורות $G_{i+1} \lhd G_i$, $H\cap G_i \leq G_i$ ונקבל:

$$H\cap G_i/(H\cap G_i)\cap G_{i+1} \cong (H\cap G_i)G_{i+1}/G_{i+1}$$

$$\Downarrow$$

$$H\cap G_i/(H\cap G_{i+1}) \cong (H\cap G_i)G_{i+1}/G_{i+1}$$

2. תהי $N \lhd G$. נשים לב כי $G \rhd N \rhd \{e\}$ סדרה נורמלית.

תהי $\{G_i\}_{i=0}^n$ סדרה פתירה של G. ממשפט העידון של שרייר נובע שלכל זוג סדרות נורמליות יש עידונים שקולים. לכן לסדרה הנורמלית $G \rhd N \rhd \{e\}$ קיים עידון שקול לעידון של $\{G_i\}_{i=0}^n$.

ידוע כי עידון של סדרה פתירה הוא סדרה פתירה, ולכן כל גורמי ההרכב של העידונים השקולים הללו הם אבליים, ולכן העידון של $G \rhd N \rhd \{e\}$ הוא סדרה פתירה.

נסמן את הסדרה הפתירה שמתקבלת מהעידון הנ"ל:

$$G = H_0 \rhd H_1 \rhd ... \rhd H_k = N \rhd N_1 \rhd ... \rhd N_l = \{e\}$$

ממשפט ההתאמה נובע שהסדרה הבאה היא סדרת הרכב של G/N:

$$G/N = H_0/N \rhd H_1/N \rhd ... \rhd H_k/N = N/N \cong \{e\}$$

וזו גם סדרה פתירה, כי לפי משפט האיזומורפיזם השלישי מתקיים:

$$H_i/N/H_{i+1}/N \cong H_i/H_{i+1}$$

וידוע כי H_i/H_{i+1} אבלית מפתירות הסדרה שהתקבלה מהעידון. ■

טענה: תהי G חבורה ותהי $N \lhd G$. אם $N, G/N$ חבורות פתירות אז גם G פתירה.

הוכחה: ניקח סדרה פתירה של N:

$$N = N_0 \rhd N_1 \rhd ... \rhd N_l = \{e\}$$

וניקח סדרה פתירה של G/N:

$$G/N = G_0/N \rhd G_1/N \rhd ... \rhd G_k/N = \{e\}$$

ממשפט ההתאמה נסיק כי $G = G_0 \rhd G_1 \rhd ... \rhd G_k = N$, ולכן נקבל כי הסדרה הבאה היא סדרת הרכב של G:

$$G = G_0 \rhd G_1 \rhd ... \rhd G_k = N = N_0 \rhd N_1 \rhd ... \rhd N_l = \{e\}$$

ידוע כי ${}^{N_i}\!/_{N_{i+1}}$ אבלית מפתירות N. נשים לב כי ממשפט האיזומורפיזם השלישי נובע כי:

$${}^{G_i/N}\!\Big/_{G_{i+1}/N} \cong {}^{G_i}\!/_{G_{i+1}}$$

ולכן גם ${}^{G_i}\!/_{G_{i+1}}$ אבלית מפתירות ${}^{G}\!/_{N}$. לכן זו סדרה פתירה ומכאן כי G פתירה. ■

הערה: הטענה האחרונה מספקת הוכחה נוספת לכך ש-$|G| = p^n$ פתירה, באינדוקציה על גודל החבורה.

אם $G = \{e\}$ הטענה טריוויאלית. נניח $|G| > 1$. ממשפט שהוכחנו נובע שבמקרה זה גם $|Z(G)| > 1$, ולכן $|{}^{G}\!/_{Z(G)}| = \frac{|G|}{|Z(G)|} < |G|$. החבורה ${}^{G}\!/_{Z(G)}$ היא חבורת p סופית, ולכן מהנחת האינדוקציה היא פתירה.

אם כך נקבל שמתקיימים תנאי המשפט האחרון עבור בחירת החבורה הנורמלית להיות $Z(G)$ נסיק כי G פתירה.

הערה: **משפט ברנסייד** מרחיב את הטענה האחרונה וקובע שכל חבורה מהצורה $|G| = p^n q^m$ ל-p, q ראשוניים היא פתירה.

ההוכחה למשפט משתמשת בהצגות של חבורות וזה נושא מתקדם יותר מהקורס הנוכחי.

הערה: עבור $|G| = p_1^{n_1} \cdot p_2^{n_2} \cdot p_3^{n_3}$ הטענה לא מתקיימת. כך למשל ראינו כי $|A_5| = 2^2 \cdot 3 \cdot 5$ אינה פתירה.

15 קומוטטורים

הגדרה: **קומוטטור** בחבורה G הוא איבר מהצורה $[x, y] =: x^{-1}y^{-1}xy$ עבור $x, y \in G$.

קל לראות כי $[x, y] = e \iff xy = yx$.

הגדרה: **חבורת הקומוטטור** היא החבורה הנוצרת על־ידי אוסף כל הקומוטטורים.

כלומר אם G חבורה, מסמנים את חבורת הקומוטטור $G' =: \langle \{[x, y] \,|x, y \in G\} \rangle$.

טענה: אוסף הקומוטטורים הוא קבוצה סגורה להופכי ולהצמדה אך אינה בהכרח סגורה לכפל. לכן היא לא בהכרח תת־חבורה.

הוכחה: נראה סגירות להופכי:

$$[x, y]^{-1} = \left(x^{-1}y^{-1}xy\right)^{-1} = y^{-1}x^{-1}yx = [y, x]$$

נראה סגירות להצמדה:

$$g\left[x,y\right]g^{-1}=g\left(x^{-1}y^{-1}xy\right)g^{-1}=\left(gx^{-1}g^{-1}\right)\left(gy^{-1}g^{-1}\right)\left(gxg^{-1}\right)\left(gyg^{-1}\right)=$$

$$=\left(gxg^{-1}\right)^{-1}\left(gyg^{-1}\right)^{-1}\left(gxg^{-1}\right)\left(gyg^{-1}\right)=\left[gxg^{-1},gyg^{-1}\right]$$

■

טענה: $G' \lhd G$

הוכחה: תהי X קבוצת הקומוטטורים ב-G, כך ש-$G' = \langle X \rangle$. ראינו שקבוצה זו סגורה להצמדה ולכן $X^g \subseteq X$ לכל $g \in G$.

כל איבר ב-G' הוא מהצורה $x_1 \cdot x_2 \cdot \ldots \cdot x_n$, $x_i \in X$, ולכן נקבל כי $(x_1 \cdot x_2 \cdot \ldots \cdot x_n)^g = x_1^g \cdot x_2^g \cdot \ldots \cdot x_n^g \in \langle X \rangle = G$ מהסגירות להצמדה, ולכן $G'^g \subseteq G'$ לכל $g \in G$, כלומר $G' \lhd G$. ■

טענה: G/G' אבלית.

הוכחה: תהי $\pi : G \to G/G'$ ההטלה הקנונית, כלומר $\pi(g) = gG'$ לכל $g \in G$.

מתקיים כי π הומומורפיזם על, ולכן כל איבר ב-G/G' הוא מהצורה $\pi(x)$ עבור $x \in G$ כלשהו. אם כך מספיק להראות שלכל $x, y \in G$ מתקיים $[\pi(x), \pi(y)] = e$ לכל $x, y \in G$, וזה אפיון שקול לאבליות.

נחשב:

$$\left[\pi\left(x\right),\pi\left(y\right)\right]=\pi^{-1}\left(x\right)\pi^{-1}\left(y\right)\pi\left(x\right)\pi\left(y\right)=$$

$$=\pi\left(x^{-1}\right)\pi\left(y^{-1}\right)\pi\left(x\right)\pi\left(y\right)=\pi\left(x^{-1}y^{-1}xy\right)=\pi\left(\left[x,y\right]\right)=$$

נשים לב כי $[x,y] \in G'$ ולכן $\pi([x,y]) = [x,y]\,G' = G'$, כלומר:

$$\left[\pi\left(x\right),\pi\left(y\right)\right]=\pi\left(\left[x,y\right]\right)=G'\cong\left\{e_{G/G'}\right\}$$

ומכאן האבליות. ■

טענה: G' היא התת־חבורה הנורמלית המינימלית ביחס לתכונה שחבורת המנה המתקבלת ממנה אבלית.

הוכחה: תהי $N \lhd G$ כך ש-G/N אבלית. צריך להראות כי $G' \subseteq N$. נשים לב שלשם כך די להראות כי $X \subseteq N$ (אוסף הקומוטטורים), שכן N תת־חבורה ולכן גם תת החבורה הנוצרת $\langle X \rangle = G'$ תוכל בה.

יהי $[x,y] \in X$. מאבליות G/N נובע כי $xNyN = yNxN$ ולכן לא קשה לראות כי $[x,y]\,N = [xN, yN] = N$, ומכאן בהכרח $[x,y] \in N$. ■

דוגמאות:

1. G אבלית $\iff$ $[x,y] = e$ לכל $x, y \in G$ $\iff$ $G' = \{e\}$.
2. אם G פשוטה ולא אבלית אז $G' = G$.

נימוק: ידוע $G' \lhd G$, ומפשטות G נובע $G' = \{e\}$, G. לא ייתכן $G' = \{e\}$ כי אז G הייתה אבלית, ולכן בהכרח $G' = G$.

15.1 תת־חבורה אופיינית

הגדרה: תת חבורה $N \leq G$ תיקרא **אופיינית**, אם לכל $\varphi \in Aut\left(G\right)$ מתקיים $\varphi\left(N\right) \subseteq N$.[23] במקרה כזה נסמן $N \operatorname{char} G$.

הגדרה שקולה: תת־חבורה $N \leq G$ היא אופיינית אמ"מ לכל $\varphi \in Aut\left(G\right)$ מתקיים $\varphi\left(N\right) = N$.

הוכחה: קל לראות שמספיק להוכיח שמתקיים $N \subseteq \varphi\left(N\right)$ לכל $\varphi \in Aut\left(G\right)$.

יהי $\varphi \in Aut\left(G\right)$. מתקיים כי גם $\varphi^{-1} \in Aut\left(G\right)$, ומאופייניות N נובע כי $\varphi^{-1}\left(N\right) \subseteq N$ ומכאן קל לראות כי $N \subseteq \varphi\left(N\right)$. ■

טענה: אם $N \operatorname{char} G$ אז $N \lhd G$.

הוכחה: נתון שלכל אוטומורפיזם מתקיים $\varphi\left(N\right) \subseteq N$. נבחר אוטומורפיזם $\varphi_g\left(x\right) = x^g$ (הצמדה) ונקבל $\varphi_g\left(N\right) = N^g \subseteq N$, וזו ההגדרה לנורמליות. ■

משפט: $G' \operatorname{char} G$

למה: נרחיב את ההגדרה לאופייניות לתת קבוצה כלשהי של G. כלומר $X \subseteq G$ תיקרא קבוצה אופיינית אם לכל $\varphi \in Aut\left(G\right)$ מתקיים $\varphi\left(X\right) \subseteq X$.

מתקיים כי אם X קבוצה אופיינית אז $\langle X\rangle$ תת־חבורה אופיינית.

הוכחה: איבר כללי של $\langle X\rangle$ הוא מהצורה $x_1^{\varepsilon_1}\cdot\ldots\cdot x_n^{\varepsilon_n}$ עבור $\varepsilon_i \in \{\pm 1\}$. לכן לכל $\varphi \in Aut\left(G\right)$ מתקיים:

$$\varphi\left(x_1^{\varepsilon_1}\cdot\ldots\cdot x_n^{\varepsilon_n}\right) = \varphi\left(x_1^{\varepsilon_1}\right)\cdot\ldots\cdot\varphi\left(x_n^{\varepsilon_n}\right)$$

אבל מאופייניות X נובע כי $\varphi\left(x_i\right) \in X$ לכל i, ולכן המכפלה של כולם שייכת ל-$\langle X\rangle$, כלומר $\langle X\rangle \operatorname{char} G$. ■

הוכחה: מהלמה נובע שמספיק להראות שאוסף הקומוטטורים X אופייני, ומכאן נסיק כי $G' = \langle X\rangle$ אופיינית.

יהי $[x,y] \in X$ ויהי $\varphi \in Aut\left(G\right)$. הראינו לעיל שמתקיים:

$$\varphi\left([x,y]\right) = \left[\varphi\left(x\right),\varphi\left(y\right)\right] \in X$$

ולכן X אופיינית, וזה משלים את ההוכחה. ■

דוגמאות:

1. כל תת־חבורה מהצורה $\left\langle\left\{x^2 | x \in G\right\}\right\rangle$ היא ת"ח אופיינית, וזאת כי $\left\{x^2 | x \in G\right\}$ קבוצה אופיינית:

$$\varphi\left(x^2\right) = \varphi^2\left(x\right) \in \left\{x^2 | x \in G\right\}$$

2. $Z\left(G\right)$ תת־חבורה אופיינית.

[23] תזכורת: $Aut\left(G\right)$ הוא אוסף האיזומורפיזמים מ-G על עצמה, שמכונים אוטומורפיזמים.

למה: אופייניות היא יחס טרנזיטיבי. כלומר אם $M \operatorname{char} N \operatorname{char} G$, אז $M \operatorname{char} G$.

הוכחה: יהי $\varphi \in Aut\left(G\right)$, נוכיח כי $\varphi\left(M\right) \subseteq M$. נתון כי $\varphi\left(N\right) \subseteq N$ מאופייניות N ב-G.

נשים לב כי $\varphi|_N \in Aut\left(N\right)$, שכן מתקיים $\varphi\left(N\right) = N$ (איפיון שקול לאופייניות) ולכן $\varphi|_N : N \to N$ היא חח"ע, והעתקה חח"ע בין קבוצות שוות גודל היא גם על.

לכן $\varphi|_N \in Aut\left(N\right)$ ומאופייניות M ב-N נובע כי $\varphi|_N\left(M\right) \subseteq M$, אבל קל לראות כי $\varphi|_N\left(M\right) = \varphi\left(M\right)$ ולכן $\varphi\left(M\right) \subseteq M$, כלומר $M \operatorname{char} G$. ■

15.2 סדרה נגזרת

הגדרה: תהי G חבורה. **הסדרה הנגזרת** של G היא הסדרה $\left\{G^{(i)}\right\}$, כאשר $G^{(0)} = G$, $G^{(1)} = G'$ וככלל $G^{(i+1)} = \left(G^{(i)}\right)'$.

הערה: נשים לב כי $G^{(i)}/G^{(i+1)} =: G^{(i)}/\left(G^{(i)}\right)'$ אבלית, כפי שהוכחנו לעיל באופן כללי על חבורת הקומוטטור.

טענה: $G^{(i)} \lhd G$ לכל i.

הוכחה: באינדוקציה על i, כשמשתמשים בטענה:

$$G^{(i+1)} = \left(G^{(i)}\right)' \operatorname{char} G^{(i)} \operatorname{char} G$$

ובטרנזיטיביות האופייניות. ■

משפט: G פתירה אמ"מ $G^{(n)} = \{e\}$ ל-n כלשהו. כלומר אם הסדרה הנגזרת מגיעה ל-$\{e\}$.

הוכחה: (כיוון ראשון) נניח כי הסדרה הנגזרת מגיעה ל-$\{e\}$, כלומר:

$$G = G^{(0)} \rhd G^{(1)} \rhd \ldots \rhd G^{(n)} = e$$

אזי זו סדרה נורמלית, ומכך ש-$G^{(i)}/G^{(i+1)}$ אבלית נובע כי זו סדרה פתירה.

(כיוון שני) נניח כי G פתירה, ותהי $\{G_i\}_{i=0}^{n}$ סדרה פתירה של G.

למה: $G^{(i)} \subseteq G_i$ לכל i.

הוכחה: באינדוקציה על i. אם $i = 0$ אז $G^{(0)} = G \subseteq G_0 = G$. נניח כי $G^{(i)} \subseteq G_i$, נסיק כי:

$$G^{(i+1)} = \left(G^{(i)}\right)' \subseteq \left(G_i\right)'$$

מפתירות G נובע כי G_i/G_{i+1} אבלית. ראינו שבאופן כללי אם G/N אבלית אז $G' \subseteq N$, ולכן נסיק שבמקרה זה מתקיים $G_i' \subseteq G_{i+1}$, כנדרש. ■

מהלמה נובע שבפרט עבור n מתקיים $G^{(n)} \subseteq G_n = \{e\}$, ולכן בהכרח $G^{(n)} = \{e\}$, כנדרש. ■

הגדרה: האורך הנגזר של חבורה פתירה, הוא ה-n הטבעי המינימלי המקיים $G^{(n)} = \{e\}$.
מסמנים מושג זה $dl\left(G\right)$. (derive length)

מושג זה תופס במובן כלשהו את "דרגת הפתירות" של חבורה. כלומר ל-n קטן הסדרה פתירה מהר.

דוגמאות:

1. $G = \{e\} \iff dl\left(G\right) = 0$
2. $G \iff G' = \{e\} \iff dl\left(G\right) \leq 1$ אבלית
3. דוגמה לחבורה פתירה מסובכת (כלומר dl שלה גדול): חבורת המטריצות המשולשיות עליונות מגודל $k \times k$, שהן הפיכות.

   תרגיל: (לא פשוט) להראות שחבורה זו פתירה, וכי האורך הנגזר שלה הוא בערך $\log_2\left(k\right)$.

   רמז: ניתן להיעזר בעובדה שבחבורת הקומוטטור שלה, האלכסון יהיה כולו 1-ים, ובחבורת הקומוטטור של חבורת הקומוטטור נקבל 0-ים באלכסון כלשהו.
4. **הגדרה:** אומרים כי G חבורה **מטא־אבלית** אם קיימת תת־חבורה $A \lhd G$ אבלית כך שגם G/A אבלית.

   - למשל חבורת התמורות S_3 מטא־אבלית כי A_3 אבלית וכן גם $S_3/A_3 \cong \mathbb{Z}_2$ ולכן אבלית.

   - למשל החבורה הדיהדרלית D_n מטא־אבלית כי תת־חבורת הסיבובים שבה אבלית (כי האינדקס שלה הוא 2), וכן גם חבורת המנה המתקבלת ממנה היא אבלית (מאותה סיבה).

   טענה: $dl\left(G\right) \leq 2 \iff G$ מטא־אבלית.

   הסבר: נניח כי $dl\left(G\right) = 2$, משמע יש סדרה פתירה $G \rhd G' \rhd \{e\}$, ולכן $A = G'$ וכן גם ראינו כי G/G' אבלית.

מסקנות:

1. לכל חבורה פתירה יש סדרה פתירה המורכבת כולה מתת־חבורות נורמליות. כלומר יש סדרה $\{G_i\}$ כך ש-$G_i \lhd G$ לכל i (ולא רק $G_i \lhd G_{i-1}$).

   הוכחה: הראינו שכל חבורת קומוטטורים $G^{(i)}$, לא משנה מאיזה סדר, נורמלית בחבורה כולה, ולכן הסדרה הנגזרת מקיימת את הנדרש.
2. אם $G \neq \{e\}$ פתירה, אז קיימת $\{e\} \neq A \lhd G$ אבלית.

   הוכחה: יהי $n = dl\left(G\right)$, כלומר $G^{(n)} = \{e\}$. מתקיים $G^{(n-1)} \neq \{e\}$ כי n מינימלי ביחס לתכונה זו. ניקח $A = G^{(n-1)}$ ונשים לב כי $A' = \left(G^{(n-1)}\right)' = G^{(n)} = \{e\}$, וכפי שראינו זה תנאי שקול לאבליות.

16 סקירה של כמה נושאים מתקדמים

16.1 משפט המבנה לחבורות אבליות נוצרות סופית

כל חבורה אבלית G נוצרת סופית, כלומר $G = \langle X \rangle$ עבור $X \subseteq G$ תת־קבוצה סופית, היא איזומורפית למכפלה ישרה של חבורות ציקליות. כלומר:

$$G \cong \mathbb{Z} \times \mathbb{Z} \times ... \times \mathbb{Z} \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times ... \times \mathbb{Z}_{n_l}$$

מסקנה: אם G חבורה אבלית סופית לא ייתכן שבמכפלה הישרה שלה מופיעה $\mathbb{Z}$, ולכן $G \cong \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_l}$.

הערה: אם G אבלית אך לא נוצרת סופית המשפט אינו בהכרח נכון. למשל $(\mathbb{Q}, +, 0)$ אינה נוצרת סופית (תרגיל לא קשה), והיא אכן לא מכפלה ישרה מהצורה הנ"ל.

16.2 חבורות פשוטות סופיות

כל החבורות הפשוטות הסופיות מתמיינות לשלושה סוגים:

- החבורות הפשוטות האבליות הן $\mathbb{Z}_p$.
- החבורות הפשוטות הלא־אבליות הן A_n ל-$5 \leq n$, וחבורות מטיפוס לי (סוגים שונים של חבורות מטריצות, למשל $PSL_n(\mathbb{Z}_p)$ המוגדרת להיות חבורת המנה של המטריצות עם דטרמיננטה 1 חלקי המרכז).
- 26 חבורות פשוטות ספוראדיות, כלומר שאינן נכללות באף משפחה אינסופית.

משפט המיון לחבורות פשוטות סופיות קובע שאלו כל סוגי החבורות הפשוטות הסופיות.

16.3 משפט הסדר האי־זוגי

כל חבורה סופית מסדר אי־זוגי היא פתירה.

מסקנה: כל חבורה סופית פשוטה שאינה אבלית היא מסדר זוגי, כי היא לא יכולה להיות פתירה.

לכן ממשפט קושי יש בה איבר מסדר 2, ואיבר כזה מכונה "אינבולוציה".

16.4 השערת אורה (Ore)

אם G חבורה פשוטה סופית, אז כל איבר בה הוא קומוטטור.
אמנם ידוע כי $G' = G$ במקרה זה, אולם זה רק אומר שכל $g \in G$ הוא מכפלת קומוטטורים.
ההשערה אומרת שכל איבר הוא קומוטטור בעצמו.
ההשערה הועלתה ב-1951 והוכחה ב-2008. (בין השאר על־ידי ענר שלו).

חלק II
תורת החוגים

17 חוגים

הקדמה: ניתן להגדיר חוג כשדה שאינו בהכרח קומוטטיבי ושאין בו בהכרח איבר הופכי לכל איבר. ההגדרות הבאות יתחילו "מלמטה".

הגדרה: **מונואיד** $(R,\cdot,1)$ הוא קבוצה R עם פעולה דו־מקומית (כלומר $R\times R\to R$) "כפל" המקיימת את התנאים:

1. **אסוציאטיביות:** לכל $x,y,z\in R$ מתקיים $(x\cdot y)\cdot z=x\cdot(y\cdot z)$
2. **קיום איבר יחידה:** קיים איבר $1\in R$ כך שלכל $x\in R$ מתקיים $1\cdot x=x\cdot 1=x$.

הערה: ניתן להגדיר מונואיד גם כחבורה שאינה מקיימת את התנאי של קיום איבר הופכי. כלומר, מונואיד שבו לכל איבר יש איבר הופכי, הוא חבורה.

הגדרה: **חוג** $(R,+,\cdot,0,1)$ הוא קבוצה R עם שתי פעולות דו־מקומיות (כלומר $R\times R\to R$) "כפל" ו"חיבור", ולפחות שני איברים $0,1$, כך שמתקיימים התנאים הבאים:

1. $(R,+,0)$ הוא **חבורה חיבורית אבלית**.
2. $(R,\cdot,1)$ הוא **מונואיד**.
3. **דיסטריבוטיביות:** לכל $x,y,z\in R$ מתקיים:

$$(x+y)\cdot z=x\cdot z+y\cdot z$$

$$x\cdot(y+z)=x\cdot y+x\cdot z$$

הערה: בכל חוג R מתקיים $x\cdot 0=0\cdot x=0$ לכל $x\in R$, כי $x\cdot 0=x\cdot(0+0)=x\cdot 0+x\cdot 0$.

הגדרה: חוג שבו הכפל קומוטטיבי נקרא **חוג קומוטטיבי**.

הגדרה: חוג R שבו לכל $0\neq x\in R$ קיים איבר הופכי ביחס לפעולת הכפל, נקרא **חוג חילוק**.

הגדרה: חוג חילוק קומוטטיבי נקרא **שדה**.

דוגמאות:

1. $(\mathbb{Z},+,\cdot,0,1)$ הוא חוג קומוטטיבי, אולם זה לא חוג חילוק כי למשל $2^{-1}\notin\mathbb{Z}$.
2. $(\mathbb{Z}_n,+,\cdot,0,1)$ הוא חוג קומוטטיבי, והוא שדה $\iff$ n ראשוני.
3. בהינתן שדה $\mathbb{F}$, נסמן את אוסף הפולינומים במשתנה אחד מעליו ב-$\mathbb{F}[x]$.
   $(\mathbb{F}[x],+,\cdot,0,1)$ הוא חוג קומוטטיבי, אולם הוא לא שדה כי למשל הפולינום x אינו הפיך בחוג.
   קבוצת פולינומים ב-n משתנים, המסומנת $\mathbb{F}[x_1,...,x_n]$, גם היא מהווה חוג ביחס לפעולות אלו.

4. בהינתן שדה $\mathbb{F}$, נסמן את אוסף המטריצות מגודל $n \times n$ מעליו ב-$M_n(\mathbb{F})$. $(M_n(\mathbb{F}), +, \cdot, 0, I)$ כאשר 0 מטריצת האפס ו-I מטריצת היחידה, הוא חוג לא־קומוטטיבי עבור כל $2 \leq n$. זה גם לא חוג חילוק כי לא דרשנו שהמטריצות יהיו הפיכות.

הקווטרניונים

נגדיר:

$$H =: \left\{a \cdot 1 + b \cdot i + c \cdot j + d \cdot k | a, b, c, d \in \mathbb{R}, \;\; i^2 = j^2 = k^2 = -1\right\}$$

מהתנאים המגדירים את החבורה נובע כי:

$$ij = k, \; jk = i, \; ki = j$$

$$ji = -k, \; kj = -i, \; ik = -j$$

ונובעת טבלת הכפל הבאה:

	$\mathbf{1}$	$-\mathbf{1}$	$\mathbf{i}$	$-\mathbf{i}$	$\mathbf{j}$	$-\mathbf{j}$	$\mathbf{k}$	$-\mathbf{k}$
$\mathbf{1}$	1	-1	i	$-i$	j	$-j$	k	$-k$
$-\mathbf{1}$	-1	1	$-i$	i	$-j$	j	$-k$	k
$\mathbf{i}$	i	$-i$	-1	1	k	$-k$	$-j$	j
$-\mathbf{i}$	$-i$	i	1	-1	$-k$	k	j	$-j$
$\mathbf{j}$	j	$-j$	$-k$	k	-1	1	i	$-i$
$-\mathbf{j}$	$-j$	j	k	$-k$	1	-1	$-i$	i
$\mathbf{k}$	k	$-k$	j	$-j$	$-i$	i	-1	1
$-\mathbf{k}$	$-k$	k	$-j$	j	i	$-i$	1	-1

זה למעשה מרחב ווקטורי ממימד 4 מעל $\mathbb{R}$, שהבסיס שלו הוא $\{1, i, j, k\}$.
החיבור מוגדר בחבורה זו רכיב־רכיב, והכפל מוגדר כמו בממשיים, כך שמתקיימת דיסטריבוטיביות.
קל לראות שזה חוג לא קומוטטיבי, אך זה חוג חילוק, כפי שהוכיח **המילטון**, שכן ההופכי של איבר כללי $x = a \cdot 1 + b \cdot i + c \cdot j + d \cdot k \neq 0$ הוא האיבר:

$$x^{-1} = \frac{a \cdot 1 - b \cdot i - c \cdot j - d \cdot k}{\sqrt{a^2 + b^2 + c^2 + d^2}}$$

וחישוב מייגע נותן שמתקיים $x \cdot x^{-1} = x^{-1} \cdot x = 1$.

הגדרה: יהי $(R, +, \cdot, 0, 1)$ חוג, אומרים כי תת־קבוצה $S \subseteq R$ היא **תת־חוג** אם מתקיים כי $0, 1 \in S$ וכן S סגורה לכפל, לחיבור ולנגדי.

דוגמאות:

1. $\mathbb{Z}$ הוא תת־חוג של $\mathbb{Q}$; $\mathbb{Q}$ הוא תת־חוג של $\mathbb{R}$; $\mathbb{R}$ הוא תת־חוג של $\mathbb{C}$.
2. $M_n(\mathbb{Z})$ הוא תת־חוג של $M_n(\mathbb{Q})$; $M_n(\mathbb{Q})$ הוא תת־חוג של $M_n(\mathbb{R})$; $M_n(\mathbb{R})$ הוא תת־חוג של $M_n(\mathbb{C})$.
3. $n\mathbb{Z}$ <u>אינו</u> תת־חוג של $\mathbb{Z}$ ל-$2 \leq n$, כי $1 \notin n\mathbb{Z}$.

18 אידאלים

הגדרה: יהי $(R,+,\cdot,0,1)$ חוג. אומרים כי I הוא **אידאל** ב-R ומסמנים $I\lhd R$, אם מתקיימים שני התנאים הבאים:

1. $(I,+,0)$ היא תת־חבורה של $(R,+,0)$
2. I סגור לכפל חיצוני מימין ומשמאל בתוך R. כלומר לכל $i\in I$ ולכל $r\in R$ מתקיים $r\cdot i, i\cdot r\in I$.

הערה: במקרה שיש סגירות לכפל מימין בלבד או משמאל בלבד, אומרים כי זה **אידאל ימני** או **אידאל שמאלי**, בהתאמה. מה שהגדרנו כ"אידאל" סתם הוא **אידאל דו־צדדי**.

טענה: אידאל שמכיל את 1 הוא החוג כולו.

הוכחה: יהי $I\lhd R$ אידאל ונניח $1\in I$. מסגירות האידאל לכפל חיצוני נובע כי $1\cdot r\in I$ לכל $r\in R$ ולכן $R\subseteq I$, ומכאן בהכרח $I=R$. ■

דוגמה: $n\mathbb{Z}\lhd\mathbb{Z}$, כי לכל n טבעי ולכל $a,b\in\mathbb{Z}$ מתקיים $a\left(nb\right)=n\left(ab\right)\in n\mathbb{Z}$.

ראינו כי תת החבורות היחידות של החבורה $\mathbb{Z}$ הם $n\mathbb{Z}$. מכך נובע שהאידאלים היחידים של החוג $\mathbb{Z}$ הם $n\mathbb{Z}$.

הגדרה: יהי R חוג קומוטטיבי ויהי $a\in R$. נגדיר את **האידאל הראשי** שנוצר על־ידי a להיות:

$$aR=:(a)=:\{ar|r\in R\}$$

דוגמה: קל לראות כי $\{0\}=0R=(0)$, $R=1R=(1)$.

הגדרה: חוג $R\neq\{0\}$ נקרא **חוג פשוט** אם יש לו שני אידאלים בלבד. כלומר האידאלים היחידים שלו הם R, $\{0\}$.

טענה: יהי R חוג קומוטטיבי, אזי R חוג פשוט אמ"מ R שדה.

הוכחה: (כיוון ראשון)

נניח כי R חוג פשוט ויהי $x\in R$ $x\neq 0$. מתקיים כי האידאל הראשי שנוצר על־ידי x אינו טריוויאלי ולכן מפשטות R נובע $R=(x)$ ובפרט $1\in(x)$, ולכן קיים $r\in R$ כך ש-$xr=1$.

נתון כי R חוג קומוטטיבי ולכן $r=x^{-1}$, משמע לכל איבר$\neq 0$ קיים הופכי, ולכן זה שדה.
(כיוון שני)

נניח כי R שדה ויהי $I\lhd R$. צריך להראות כי אם $I\neq\{0\}$ אז $I=R$. יהי $0\neq x\in I$, מכך ש-R שדה נובע כי $x^{-1}\in R$ ולכן $1\in I$, וכפי שהוכחנו לעיל מכך נובע $I=R$. ■

18.1 פעולות על אידאלים

הגדרה: יהי R חוג ויהיו האידאלים $I, J \lhd R$. **חיבור** שלהם מוגדר:

$$I + J = \{i + j | i \in I, j \in J\}$$

והכללה של החיבור למספר כלשהו של אידאלים $I_\alpha \lhd R$ עבור $\alpha \in A$ כאשר A סופית או אינסופית, היא:

$$\sum_{\alpha \in A} I_\alpha =: \left\{ \sum_{\alpha \in A} i_\alpha | i_\alpha \in I_\alpha \right\}$$

כאשר $i_\alpha = 0$ למעט מספר סופי של פעמים.

הגדרה: יהי R חוג ויהיו האידאלים $I, J \lhd R$. **כפל** שלהם מוגדר:

$$I \cdot J = \{i_1 j_1 + ... + i_k j_k | 0 \leq k, \ i_l \in I, \ j_l \in J\}$$

הערה: לו היינו מגדירים את הכפל $I \cdot J = \{i \cdot j | i \in I, j \in J\}$ לא הייתה מתקיימת בהכרח סגירות לחיבור ולכן זה לא היה בהכרח אידאל.

טענה:

- **חיתוך** (סופי או אינסופי) של אידאלים בחוג נתון הוא אידאל.
- **חיבור** (סופי או אינסופי) של אידאלים בחוג נתון הוא אידאל.
- **כפל** של אידאלים בחוג נתון הוא אידאל.

ההוכחה מושארת כתרגיל.

הערה: איחוד של אידאלים אינו בהכרח אידאל. למשל $2\mathbb{Z}, 5\mathbb{Z} \lhd \mathbb{Z}$, אבל $2\mathbb{Z} \cup 5\mathbb{Z}$ אינו אידאל של $\mathbb{Z}$.

18.2 אידאל נוצר

הגדרה: יהי R חוג ותהי $X \subseteq R$ תת־קבוצה כלשהי. נגדיר ונסמן את האידאל הנוצר על־ידי X להיות:

$$(X) = \bigcap_{X \subseteq I \lhd R} I$$

זה אידאל כי חיתוך של אידאלים הוא אידאל. קל לראות כי זה האידאל המינימלי ביחס להכלה שמכיל את X.

איפיון־שקול: יהי R חוג ותהי $X \subseteq R$ תת־קבוצה. נגדיר $(X) = \{\sum_{i=1}^{n} r_i x_i s_i | r_i, s_i \in R, \ x_i \in X, \ n \in \mathbb{N}\}$. כלומר אוסף כל הצירופים הלינאריים הסופיים של איברי X.

הוכחה: נוכיח את השקילות למקרה של חוג R קומוטטיבי ותת־קבוצה $X = \{x_1, ..., x_k\}$ סופית. ההכללה לא קשה.

קל לראות שאוסף הצירופים הלינאריים מוכל ב-$\bigcap_{X\subseteq I\lhd R} I$, כי כל אידאל שמכיל את X הוא סגור מהגדרתו ולכן מכיל כל צירוף לינארי.

ההכלה בכיוון השני נובעת מכך שאוסף הצירופים הלינאריים עצמו עומד בהגדרה של אידאל, וממינימליות $\bigcap_{X\subseteq I\lhd R} I$ נובעת ההכלה המבוקשת. ■

הערה: אידאל ראשי שהגדרנו לעיל עבור $x \in R$ הוא מקרה פרטי של אידאל נוצר עבור תת־קבוצה $X = \{x\}$.

18.3 חבורת האיברים ההפיכים

הגדרה: איבר $r \in R$ בחוג נקרא **הפיך** אם יש לו הופכי כפלי. כלומר קיים $s \in R$ כך שמתקיים $sr = rs = 1$.

הגדרה: בהינתן חוג R מסמנים ב-R^* את קבוצת האיברים ההפיכים.

טענה: $(R^*, \cdot, 1)$ היא חבורה.

הוכחה: סגירות לכפל נובעת מכך שאם $r, s \in R^*$ אז $r^{-1}, s^{-1} \in R^*$ ולכן:

$$(rs)(rs)^{-1} = rss^{-1}r^{-1} = 1$$

כלומר גם rs הפיך ולכן $rs \in R^*$. ■

דוגמאות:

1. לכל שדה $\mathbb{F}$ מתקיים $\mathbb{F}^* = \mathbb{F} \backslash \{0\}$.
2. $\mathbb{Z}^* = \{-1, 1\}$
3. $M_n^*(\mathbb{F}) = GL_n(\mathbb{F})$
4. $\mathbb{F}^*[x] \cong \mathbb{F}^*$. כלומר כל הפולינומים ממעלה 0, לא כולל 0 כפולינום, שכן רק פולינומים ממעלה 0 הם הפיכים.
5. $\mathbb{Z}_n^* = \{0 \le k \le n | \gcd(k, n) = 1\}$

טענה: יהי $I \lhd R$. אם I מכיל איבר הפיך אז $I = R$.

הוכחה: מהנתון נובע $I \cap R^* \neq \emptyset$. יהי $r \in I \cap R^*$, מתקיים כי $r^{-1} \in R$ ולכן $1 = r^{-1}r \in I$. הוכחנו לעיל שכל אידאל שמכיל את היחידה שווה לחוג כולו. ■

19 הומומורפיזמים של חוגים

הגדרה: יהיו R, S חוגים. פונקציה $f : R \to S$ נקראת **הומומורפיזם של חוגים** אם מתקיימים התנאים הבאים:

1. $f(x + y) = f(x) + f(y)$ לכל $x, y \in R$
2. $f(x \cdot y) = f(x) \cdot f(y)$ לכל $x, y \in R$

3. $f(1_R)=1_S$

- הומומורפיזם **חח"ע** נקרא **מונומורפיזם**
- הומומורפיזם **על** נקרא **אפימורפיזם**
- הומומורפיזם **חח"ע ועל** נקרא **איזומורפיזם**

אם קיים איזומורפיזם $f:R\to S$, מסמנים $R\cong S$.

הערה: התנאי הראשון מגדיר את f גם כהומומורפיזם של החבורות $(S,+_S,0_S)$, $(R,+_R,0_R)$.
מכאן כי $f(0_R)=0_S$ וכן $f(-x)=-f(x)$, כפי שראינו בהומומורפיזמים של חבורות.

הערה: נשים לב שהתנאי השלישי לא נובע מהקודמים, כי למשל $f(x)=0$ הוא הומומורפיזם לולי תנאי זה.

דוגמאות:

1. ההומומורפיזם היחיד $f:\mathbb{Z}\to\mathbb{Z}$ הוא הומורפיזם הזהות, כי בהכרח $f(1)=1$, ובאינדוקציה נובע כי $f(n)=n$ לכל n טבעי, וכן בהכרח $f(-x)=-f(x)$ ולכן $f(a)=a$ לכל a שלם.
2. $z\mapsto\overline{z}$ הוא הומומורפיזם מהצורה $f:\mathbb{C}\to\mathbb{C}$.

טענה: יהי $f:R\to S$ הומומורפיזם של חוגים, אזי:

1. $Im(f)=\{f(x)|x\in R\}$ היא תת־חוג של S.
2. $\ker(f)=\{x\in R|f(x)=0\}$ הוא אידאל של R.

הוכחה: הטענה הראשונה קלה. נראה את הטענה השנייה (לא כי היא קשה אלא כי היא חשובה).

ראשית נראה כי $\ker(f)$ תת־חבורה חיבורית:

- סגירות לחיבור נובעת מכך שלכל $x,y\in\ker(f)$ מתקיים כי $f(x+y)=f(x)+f(y)=0$ ולכן $x+y\in\ker(f)$.

- סגירות להופכי נובעת מכך שלכל $x\in\ker(f)$ מתקיים כי $f\left(x^{-1}\right)=f^{-1}(x)=0^{-1}=0$ ולכן $x^{-1}\in\ker(f)$.

- הראינו לעיל גם כי $f(0)=0$ ולכן $0\in\ker(f)$.

נותר להראות כי $\ker(f)$ סגור לכפל חיצוני כדי שהוא יהיה אידאל. יהי $x\in\ker(f)$ ויהי $r\in R$. מתקיים כי $f(rx)=f(r)f(x)=r\cdot 0=0$ ולכן $rx\in\ker(f)$. ■

20 חוגי מנה

הגדרה: בהינתן חוג R ואידאל $I\lhd R$, נגדיר $R/I=:\{x+I|x\in R\}$, כאשר $x+I=:\{x+i|i\in I\}$.

- נגדיר בקבוצה זו **חיבור** באמצעות חיבור על הנציגים:

$$(x+I)+(y+I)=(x+y)+I$$

ראינו כבר שחיבור זה מוגדר היטב על חבורות מנה, ולכן גם כאן הוא אכן הופך את R/I לחבורת מנה חיבורית.

- נגדיר בקבוצה זו **כפל** באמצעות כפל על הנציגים:

$$(x+I)\cdot(y+I)=x\cdot y+I$$

  - נוכיח שהכפל מוגדר היטב ואינו תלוי בנציגים. כלומר יש להוכיח שאם $x+I=x'+I$ וגם $y+I=y'+I$ אז $xy+I=x'y'+I$.
נשים לב כי:

$$x+I=x'+I \iff x-x'\in I$$

$$y+I=y'+I \iff y-y'\in I$$

[24]

נסמן $\alpha=x-x'$, $\beta=y-y'$, ונשים לב שתחת סימונים אלה $x'=x+\alpha$, $y'=y+\beta$. נחשב:

$$x'y'+I=(x+\alpha)(y+\beta)+I=$$

$$=xy+x\beta+\alpha y+\alpha\beta+I$$

נשים לב כי מהסגירות החיצונית של אידאל נובע כי $x\beta,\alpha y,\alpha\beta\in I$ ולכן נסיק:

$$x'y'+I=xy+I$$

- קל לבדוק שאכן $(R/I,+,\cdot,I,1+I)$ מהווה חוג, והוא מכונה "חוג מנה".

דוגמאות:

1. כפי שראינו מתקיים $n\mathbb{Z}\lhd\mathbb{Z}$, ולכן נקבל כי $\mathbb{Z}/n\mathbb{Z}=\{k+n\mathbb{Z}|k\in\mathbb{Z}\}\cong\mathbb{Z}_n$.
2. לכל חוג מתקיים $R/\{0\}\cong R$
3. תרגיל: $\mathbb{R}[x]/(x^2+1)\cong\mathbb{C}$, כאשר $\left(x^2+1\right)$ האידאל הראשי שנוצר מהפולינום x^2+1.

[24] באותו אופן שראינו לחבורות $N\lhd G$ כי $g_1N=g_2N \iff g_1g_2^{-1}\in N$

20.1 ההטלה הקנונית $R \to {}^{R}\!/_{I}$

הגדרה: נניח כי R חוג וכי $I \lhd R$ אידאל. נגדיר העתקה $\pi : R \to {}^{R}\!/_{I}$ להיות $\pi(x) = x+I$.

טענה: זה הומומורפיזם של חוגים שהוא על. מתקיים כי $Im(\pi) = {}^{R}\!/_{I}$, $\ker(\pi) = I$.

הוכחה: ברור כי $Im(\pi) = {}^{R}\!/_{I}$. העובדה $\ker(\pi) = I$ נובעת כי:

$$x \in \ker(\pi) \iff \pi(x) = 0 \iff x + I = I \iff x \in I$$

■

מסקנה: ראינו כבר שכל גרעין של הומומורפיזם הוא אידאל, הטענה האחרונה קובעת גם שכל אידאל הוא גרעין של הומומורפיזם.

21 משפטי האיזומורפיזמים של חוגים

21.1 משפט האיזומורפיזמים ה-I

אם $f : R \to S$ הומומורפיזם של חוגים, אזי $Im(f) \cong {}^{R}\!/_{\ker(f)}$.

הוכחה:

1. נסמן $I = \ker(f)$ (ראינו שזה אכן אידאל), ונגדיר העתקה $\varphi : {}^{R}\!/_{I} \to Im(f)$ להיות $\varphi(x+I) = f(x)$. נוכיח כי φ הוא איזומורפיזם.
2. נראה כי φ מוגדר היטב ללא תלות בנציגים.
כלומר יש להראות כי אם $x + I = y + I$ אז $f(x) = f(y)$, ואכן מתקיים:

$$\begin{gathered} x + I = y + I \\ \Updownarrow \\ x - y \in I = \ker(f) \\ \Downarrow \\ f(x-y) = 0 \\ \Downarrow \\ f(x) = f(y) \end{gathered}$$

3. נראה כי φ מקיים את שלושת התנאים להומומורפיזם.
(א) חיבוריות:

$$\varphi(x + I + y + I) = \varphi(x + y + I) = f(x+y) =$$

$$= f(x) + f(y) = \varphi(x+I) + \varphi(y+I)$$

(ב) כפליות:

$$\varphi((x+I)(y+I)) = \varphi(xy+I) = f(xy) =$$

$$f(x) f(y) = \varphi(x+I)\varphi(y+I)$$

(ג) $1\to 1$:

$$\varphi\left(1_{R/I}+I\right)=f\left(1_{R/I}\right)=1_S$$

4. נראה כי φ על: כל איבר ב-$Im\left(f\right)$ הוא מהצורה $f\left(x\right)$ ל-$x\in R$, ולכן $\varphi\left(x+I\right)$ ייתן את $f\left(x\right)$.
5. נראה כי φ חח"ע:

$$\begin{gathered}\varphi\left(x+I\right)=\varphi\left(y+I\right)\\ \Downarrow\\ f\left(x\right)=f\left(y\right)\\ \Downarrow\\ f\left(x-y\right)=0\\ \Downarrow\\ x-y\in\ker\left(f\right)=I\\ \Updownarrow\\ x+I=y+I\end{gathered}$$

■

21.2 משפט האיזומורפיזמים ה-II

נניח כי R חוג, $S\subseteq R$ תת־חוג וכי $I\lhd R$ אידאל. אזי:

1. $S+I$ תת־חוג של R.
2. $I\lhd S+I$
3. $S\cap I\lhd S$

ומתקיים האיזומורפיזם $S+I/I\cong S/I\cap S$.

- ההוכחה כמעט זהה להוכחה של המשפט המקביל לחבורות.

21.3 משפט האיזומורפיזמים ה-III

נניח כי R חוג, $I,J\lhd R$ אידאלים כך שמתקיים $J\subseteq I$, אזי $I/J\lhd R/J$ ומתקיים האיזומורפיזם $R/J/I/J\cong R/I$.

- ההוכחה כמעט זהה להוכחה של המשפט המקביל לחבורות.

22 משפט ההתאמה לחוגים

יהי R חוג ויהי $I\lhd R$ אידאל, אזי:

1. קיימת התאמה חח"ע ועל בין קבוצת תתי החוגים של R/I לבין קבוצת תתי החוגים $S\leq R$ המקיימים $I\subseteq S$.

   התאמה זו ניתנת על־ידי ההעתקה $S/I\mapsto S$.

2. קיימת התאמה חח"ע ועל בין קבוצת האידאלים של R/I לבין קבוצת האידאלים $J \lhd R$ המקיימים $I \subseteq J$.

התאמה זו ניתנת על־ידי ההעתקה $J/I \mapsto J$.

- ההוכחה כמעט זהה להוכחה של המשפט המקביל לחבורות.

23 אידאל מקסימלי

הגדרה: בהינתן חוג R ואידאל $I \lhd R$, אומרים כי I **אידאל מקסימלי** אם מתקיים $I \neq R$ וגם לכל אידאל $J \lhd R$, אם מתקיים $I \subseteq J$ אז $J = I$ או $J = R$.

טענה: $I \lhd R$ אידאל מקסימלי אמ"מ R/I חוג פשוט.

הוכחה: I מקסימלי $\iff$ האידאלים המכילים אותו הם רק I, R $\iff$ האידאלים ב-R/I הם רק $\{0\}$,R/I $\cong I/I$ $\iff$ R/I חוג פשוט.

כאשר השקילות האמצעית נובעת ממשפט ההתאמה לחוגים. ■

דוגמה: $p\mathbb{Z}$ ל-p ראשוני הוא אידאל מקסימלי בחוג $\mathbb{Z}$. זה נובע מכך שמתקיים $\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$ ולכן זה שדה, ושדה הוא תמיד חוג פשוט.

מסקנה: אם R חוג קומוטטיבי ו-$I \lhd R$ אידאל, אזי I אידאל מקסימלי אמ"מ R/I שדה.

הוכחה: הראינו כי I אידאל מקסימלי אמ"מ R/I פשוט. ראינו כי חוג קומוטטיבי הוא פשוט אמ"מ הוא שדה. ■

23.1 קיום אידאל מקסימלי (הלמה של צורן)

טענה: בכל חוג $R \neq \{0\}$ קיים אידאל מקסימלי, וכן כל אידאל $I \lhd R$ ממש ניתן להרחבה לאידאל מקסימלי, כלומר יש $I \subseteq J \lhd R$ כך ש-J אידאל מקסימלי.

הוכחה: נשתמש ב**למה של צורן**, שקובעת שבקבוצה סדורה חלקית, אם לכל שרשרת (דהיינו תת־קבוצה סדורה מלא) יש חסם מלעיל אז יש לה איבר מקסימלי.

נגדיר את הקבוצה $X = \{J \lhd R | I \subseteq J,\ J \neq R\}$. מתקיים כי $X \neq \emptyset$ כי $I \in X$. נסדר את X באמצעות יחס ההכלה, וזהו יחס סדר חלקי.

ראשית נראה שלכל שרשרת יש חסם מלעיל: תהי $\{J_\alpha\}_{\alpha \in A}$ שרשרת ב-X, נבחר את $\bigcup_{\alpha \in A} J_\alpha$ ונראה שזה חסם מלעיל.[25]

נשים לב שבדרך כלל איחוד של אידאלים אינו אידאל, אבל כאן מכיוון שמדובר בשרשרת ביחס להכלה, האיחוד של כולן הוא אידאל. קל לראות שלכל $\alpha \in A$ מתקיים $J_\alpha \subseteq \bigcup_{\alpha \in A} J_\alpha$, ולכן זה חסם מלעיל.

אם־כך לפי הלמה של צורן קיים ב-X איבר מקסימלי שנסמן J, שמהשתייכותו לקבוצה נובע כי הוא אידאל המקיים $I \subseteq J \neq R$.

לכן בכל חוג $R \neq \{0\}$ מכיוון שיש לו אידאל $\{0\}$ יש לו אידאל מקסימלי. ■

[25] נשים לב כי $\bigcup_{\alpha \in A} J_\alpha \neq R$, כי אחרת היה מתקיים כי $1 \in R = \bigcup_{\alpha \in A} J_\alpha$ ולכן יש α כך ש-$1 \in J_\alpha$, ובמקרה כזה הוכחנו כי $J_\alpha = R$, בסתירה להגדרת הקבוצה X.

מסקנה: לכל חוג $R \neq \{0\}$ קיים אפימורפיזם (הומומורפיזם על) מהצורה $\varphi : R \to S$, כאשר S חוג פשוט.

הוכחה: יהי $J \lhd R$ אידאל מקסימלי. נגדיר $S = {}^{R}\!/_{J}$ ולכן S חוג פשוט (כי כל חלוקה באידאל מקסימלי נותנת חוג מנה פשוט).

נגדיר הומומורפיזם $\varphi : R \to {}^{R}\!/_{J}$ באמצעות ההטלה הקנונית $x \mapsto x + J$. קל לראות שזו העתקה על. ■

מסקנה: לכל חוג קומוטטיבי $R \neq \{0\}$ קיים שדה $\mathbb{F}$ כך שיש אפימורפיזם $\varphi : R \to \mathbb{F}$.

הוכחה: באותו אופן שהוכחנו את המסקנה הקודמת, מקומוטטיביות R ינבע כי ${}^{R}\!/_{J}$ יהיה חוג פשוט וקומוטטיבי, ולכן שדה. ■

24 תחום שלמות

הגדרה: חוג קומוטטיבי R נקרא **תחום שלמות**, אם מתקיים כי אם $xy = 0$ אז $x = 0$ או $y = 0$.

דוגמאות:

1. כל שדה הוא תחום שלמות.
2. $\mathbb{Z}$ הוא תחום שלמות.
3. $\mathbb{Z}_n$ תחום שלמות $\iff$ n ראשוני.
4. כל תת־חוג של שדה הוא תחום שלמות.

משפט: חוג הוא תחום שלמות אמ"מ הוא ניתן לשיכון בתוך שדה, כלומר אמ"מ הוא איזומורפי לתת־חוג של שדה.

הוכחה: ברור כי אם חוג איזומורפי לתת־חוג של שדה הוא תחום שלמות.

נניח כי R תחום שלמות, נרחיב אותו לשדה ובכך נראה כי הוא משוכן בשדה. את הבנייה של השדה נעשה בדיוק באותו אופן בו נבנה שדה הרציונליים $\mathbb{Q}$ מתוך חוג השלמים $\mathbb{Z}$.

נגדיר קבוצה $X = \{(a,b)\,|a,b \in R,\ b \neq 0\}$ ונגדיר עליה יחס $\sim$ להיות $ab' = a'b \iff (a,b) \sim (a',b')$. קל לראות שזה יחס סדר (רפלקסיבי, סימטרי וטרנזיטיבי).

נגדיר מחלקות שקילות תחת היחס $\sim$ להיות $\frac{a}{b} = \{(a',b') \in X|\,(a',b') \sim (a,b)\}$.

נגדיר פעולת $+$ להיות $\frac{a}{b} + \frac{a'}{b'} = \frac{ab'+ba'}{bb'}$, ונגדיר פעולת $\cdot$ להיות $\frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}$, כאשר בגלל ש-$b, b' \neq 0$ אז גם $bb', b'b \neq 0$. יש להראות כי אין תלות בנציגים.

כעת נגדיר שדה $\mathbb{F} = \left\{\frac{a}{b}|a,b \in R,\ b \neq 0\right\}$, כאשר $0 = \frac{0}{1}$ האיבר האדיש לחיבור וכן $1 = \frac{1}{1}$ האיבר האדיש לכפל. נוכיח כי $\mathbb{F}$ שדה ושאכן R משתכן בו.

ראשית סגירות להופכי נובעת כי $\frac{b}{a} \in \mathbb{F} \Longleftarrow 0 = b \cdot 0 \neq a \cdot 1 \Longleftarrow \frac{0}{1} \neq \frac{a}{b} \in \mathbb{F}$, וברור כי $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$סגירות לנגדי גם ברורה, ושאר התנאים נובעים באופן דומה מהבנייה של $\mathbb{Q}$ מתוך $\mathbb{Z}$.

כעת נוכל לשכן את R בתוך $\mathbb{F}$ באמצעות $\varphi : R \to \mathbb{F}$ המוגדר להיות $\varphi(a) = \frac{a}{1}$. ■

נהוג לכנות את $\mathbb{F}$ שבנינו **שדה השברים של** R.

טענה: אם $xy = xz$ עבור $x, y, z \in R$ תחום שלמות, וכן $x \neq 0$, אזי $y = z$.

הוכחה: $xy - xz = 0 \Longleftarrow x(y - z) = 0 \Longleftarrow y - z = 0 \Longleftarrow y = z$. ■

24.1 יחס החלוקה

הגדרה: יהי R תחום שלמות ויהיו $0 \neq a, b \in R$. אומרים כי $a|b$ (a מחלק את b) אם קיים $c \in R$ כך שמתקיים $b = ac$.

הערה: נשים לב שזה לא יחס שקילות, כי למרות שמתקיימות רפלקסיביות וטרנזיטיביות, אנטי־סימטריה לא מתקיימת. למשל בתחום השלמות $\mathbb{Z}$ מתקיים $5 \mid -5$ וגם $-5|5$, אבל $5 \neq -5$.

הגדרה: יהיו $0 \neq a, b \in R$ עבור R תחום שלמות. אומרים כי a, b **חברים**, אם יש $u \in R$ הפיך (כלומר $u^{-1} \in R$) כך שמתקיים $b = au$.

הערה: קל לוודא שיחס החברות הוא יחס שקילות.

טענה: $a|b \iff (a) \supseteq (b)$ (סימון לאידאלים הנוצרים)

הוכחה: (כיוון ראשון)

אם $a|b$ אז $b = ac$, ולכן $(b) = (ac) = acR$. אבל ברור שמתקיים $acR \subseteq aR = (a)$.

(כיוון שני)

נניח כי $(b) \subseteq (a)$. ברור כי $b \in (b)$ ולכן $b \in (a)$ ומכאן כי יש c המקיים $b = ac$, כלומר $a|b$. ■

טענה: יהי R תחום שלמות ויהיו $0 \neq a, b \in R$, אזי התנאים הבאים שקולים:

1. $a \sim b$ (ביחס החברות)
2. $a|b$ וגם $b|a$
3. $(a) = (b)$

הוכחה: ($1 \Leftarrow 2$) אם $a \sim b$ אז יש u הפיך המקיים $b = au$ ולכן $a|b$.

($2 \Leftarrow 3$) מהטענה הקודמת נובע כי גם $(b) \subseteq (a)$ וגם $(a) \subseteq (b)$ ולכן $(a) = (b)$.

($3 \Leftarrow 1$) נניח כי $(a) = (b)$ ולכן בפרט $a \in (a) = (b)$ כלומר $a = bv$, ובאותו אופן גם $(a) = (b) \ni b$ כלומר $b = au$. נסיק מכך כי $a = bv = auv$. נצמצם ב-a כי $a \neq 0$ ונקבל $uv = 1$, כלומר u, v הפיכים ומכאן כי $a \sim b$ ביחס החברות. ■

דוגמאות:

1. בשדה כל $a, b \neq 0$ חברים, כי $b = a\left(a^{-1}b\right)$.
2. בחוג $\mathbb{Z}$ האיברים ההפיכים היחידים הם ± 1 ולכן $a \sim b \iff a = \pm b$.
3. בחוג $\mathbb{F}[x]$ ההפיכים הם הפולינומים הקבועים והשונים מ-0, ולכן $p(x) \sim q(x)$ אמ"מ קיים $0 \neq c \in \mathbb{F}$ המקיים $p(x) = cq(x)$ (ובפרט יש להם אותם שורשים).

24.2 אי־פריקות וראשוניות

הגדרה: יהי R תחום שלמות. $0 \neq a \in R$ נקרא **אי־פריק** אם a לא הפיך וגם לכל $x, y \in R$ אם $a = xy$ אז x הפיך או y הפיך.

דוגמה: בחוג $\mathbb{Z}$ האי־פריקים הם הראשוניים (בסימן חיובי או שלילי).

הערה: נניח כי $a = xy$ אי־פריק. אם x הפיך אז מההגדרה נובע $y \sim a$ (ביחס החברות) וכן אם y הפיך אז $x \sim a$. לכן אם a אי־פריק בהכרח $y \sim a$ או $x \sim a$.

הגדרה: יהי R תחום שלמות. $0 \neq a \in R$ נקרא **ראשוני** אם a לא הפיך וגם לכל $x, y \in R$ אם $a|xy$ אז $a|x$ או $a|y$.

טענה: אם a ראשוני אז a אי־פריק.

הוכחה: נניח כי $a = xy$ לא הפיך ראשוני. צריך להראות כי x הפיך או y הפיך. ברור ש-$a|a = xy$ ולכן מהנתון נובע $a|x$ או $a|y$.

אם $a|x$ כלומר $x = ab$ ולכן $a = xy = aby$, ומכיוון שמדובר בתחום שלמות נצמצם ונקבל $by = 1$ משמע y הפיך.

בדיוק באותו אופן נקבל כי אם $a|y$ אז x הפיך, ולכן y הפיך או x הפיך, כנדרש. ∎

הגדרה: נאמר כי a **מחלק ממש** של b, אם $a|b$ וגם a לא חבר של b. כלומר קיים c שאינו הפיך כך ש-$b = ac$.[26][27]

טענה: a אי־פריק אמ"מ כל מחלק ממש שלו הפיך.

הוכחה: (כיוון ראשון)

נניח כי a אי־פריק. לכן אם $x|a$ ממש, כלומר $a = xy$ ל-y לא הפיך, אז מהגדרת אי־פריקות נובע כי בהכרח x הפיך.

(כיוון שני)

נניח שכל מחלק ממש של a הפיך עבור a הפיך, ונניח כי $a = xy$, לכן x למשל הפיך ולכן a אי־פריק. ∎

טענה: $a \neq 0$ הוא ראשוני אמ"מ ${}^{R}/_{(a)}$ תחום שלמות.[28]

הוכחה: (כיוון ראשון)

יהי a ראשוני. נסמן $\overline{R} = {}^{R}/_{(a)}$ ונוכיח כי זה תחום שלמות. יהיו $\overline{x}, \overline{y}, \in \overline{R}$ המקיימים $\overline{x} \cdot \overline{y} = \overline{0}$, צריך להראות כי $\overline{x} = \overline{0}$ או $\overline{y} = \overline{0}$.[29]

נשים לב כי ההעתקה $x \mapsto \overline{x} = x + (a)$ היא ההטלה הקנונית שהיא הומומורפיזם, ולכן מתקיים $(x + (a))(y + (a)) = \overline{x} \cdot \overline{y} = \overline{x \cdot y} = \overline{0} = (a)$, משמע $xy \in (a)$ וראינו שזה תנאי שקול לכך ש-$a|xy$.

---

[26] לו c היה הפיך, אז $a \sim b$ ביחס החברות.

[27] לא ייתכן שיש u הפיך המקיים $b = au$, כי מכיוון שזה תחום שלמות ניתן לצמצם ולקבל $c = u$.

[28] זה לא נכון כאשר a אינו ראשוני. כך למשל $\mathbb{Z}$ תחום שלמות אבל ${}^{\mathbb{Z}}/_{(4)}$ אינו תחום שלמות.

[29] נשים לב שלפי הגדרת חוג המנה מתקיים כי $\overline{0} = 0 + (a) = (a)$.

מהנתון ש-a ראשוני נובע כי $a|x$ או $a|y$, כלומר $x\in(a)$ או $y\in(a)$, מכאן כי $\overline{0}=(a)=x+(a)=\overline{x}$ או $\overline{0}=(a)=y+(a)=\overline{y}$, כנדרש.

(כיוון שני)

נניח כי ${}^{R}/_{(a)}$ תחום שלמות ונוכיח כי a ראשוני, כלומר אם $a=xy$ אז $a|x$ או $a|y$.

נשים לב כי $xy=a$ ולכן $xy\in(a)$, כלומר $0=\overline{xy}=\overline{x}\,\overline{y}$, ומהנתון שחוג המנה תחום שלמות נובע כי $\overline{x}=\overline{0}$ או $\overline{y}=\overline{0}$, כלומר $x\in(a)$ או $y\in(a)$, וזה תנאי שקול לכך ש-$a|x$ או $a|y$. ■

טענה: a מחלק ממש של b אמ"מ $(a)\supsetneq(b)$.

הוכחה: (כיוון ראשון)

אם a מחלק ממש את b אז בפרט $a|b$ ולכן כפי שראינו $(b)\subseteq(a)$. נניח בשלילה $(a)=(b)$, כפי שראינו זה תנאי שקול לכך ש-$a\sim b$ ביחס החברות, וזאת בסתירה להנחה ש-a מחלק ממש את b.

(כיוון שני)

נניח כי $(a)\supsetneq(b)$. ראשית בפרט $(a)\supseteq(b)$ ולכן $a|b$. ראינו ש-$(a)=(b)$ הוא תנאי שקול ל-$a\sim b$ ביחס החברות, ולכן מכך ש-$(a)\neq(b)$ נובע כי a אינו חבר של b, כלומר a מחלק של b אבל אינו חבר שלו, ולכן a מחלק ממש של b. ■

דוגמה: נראה דוגמה לאיבר אי־פריק שאינו ראשוני. נגדיר את החוג הבא:

$$\mathbb{Z}\left[\sqrt{-5}\right]=:\left\{a+b\sqrt{-5}|a,b\in\mathbb{Z}\right\}$$

מתקיים כי $2\cdot 3=6=\left(1-\sqrt{-5}\right)\left(1+\sqrt{-5}\right)$, ומכאן כי $2|\left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right)$.

מצד אחד ניתן להראות כי $2\nmid\left(1+\sqrt{-5}\right)$ וכן $2\nmid\left(1-\sqrt{-5}\right)$, ולכן 2 אינו ראשוני. מצד שני 2 אינו פריק (תרגיל).

25 תחום ראשי

הגדרה: תחום שלמות R (שהוא בפרט חוג קומוטטיבי) נקרא **תחום ראשי**, אם כל אידאל בו הוא ראשי.

טענה: $\mathbb{Z}$ הוא תחום ראשי.

הוכחה ראשונה: ראינו שכל תת־חבורה של $\mathbb{Z}$ היא מהצורה $n\mathbb{Z}=(n)$, וכל אידאל הוא בפרט תת־חבורה ולכן כל אידאל הוא מהצורה (n).

הוכחה שנייה: יהי $I\lhd\mathbb{Z}$ אידאל. אם $I=\{0\}$ אז פשוט $I=(0)$. לכן נניח $I\neq\{0\}$, ולכן ללא הגבלת הכלליות קיים $0<n\in I$[30] ונבחר אותו כך שיהיה מינימלי ביחס לתכונה זו. נוכיח כי $I=(n)$.

ראשית מהיות I אידאל נובע שהוא סגור לכפל חיצוני ולכן אם $n\in I$ אז $(n)=n\mathbb{Z}\subseteq I$. נוכיח כי $I\subseteq n\mathbb{Z}$.

[30] אם במקרה תפסנו $n<0$, מהיות I אידאל נובע כי $-n\in I$ ונוכל לבחור אותו.

יהי $m\in I$. נחלק את m ב-n עם שארית ונקבל $m=nq+r$ עבור $0\leq r<n$. אם $r=0$ סיימנו, שכן $m=nq$ ולכן $m\in(n)$, לכן נניח בשלילה $0<r$.

מתקיים כי $r=m-nq\in I$, אבל נשים לב כי $r<n$, בסתירה למינימליות n. ■

טענה: עבור שדה $\mathbb{F}$, חוג הפולינומים במשתנה אחד $\mathbb{F}[x]$ הוא תחום ראשי.

הוכחה: למשפט החילוק עם שארית של שלמים קיים משפט מקביל לפולינומים, ביחס לדרגת הפולינום. כלומר לכל זוג פולינומים $f(x),g(x)$ קיים פולינום יחיד $q(x)$ כך שמתקיים $f(x)=g(x)q(x)+r(x)$, כאשר $r(x)$ פולינום המקיים $0\leq \deg(r(x))<\deg(q(x))$.

קל לראות שבהינתן אידאל $0\neq I\lhd\mathbb{F}[x]$ ניקח פולינום $0\neq f(x)\in I$ ממעלה מינימלית. קל לראות כי $(f(x))\subseteq I$, וההכלה ההפוכה נובעת בדיוק באותו אופן של ההוכחה הקודמת. ■

טענה: יהי R תחום ראשי ויהי $0\neq a\in R$, אזי התנאים הבאים שקולים:

1. a אי־פריק
2. (a) אידאל מקסימלי
3. $R/(a)$ שדה

הוכחה: ראינו שבאופן כללי אידאל $I\lhd R$ הוא מקסימלי אמ"מ R/I שדה. לכן מספיק להראות את השקילות $1\iff 2$.

$(1\Longleftarrow 2)$

נניח כי a אי־פריק, צ"ל כי (a) אידאל מקסימלי. יהי $(a)\subseteq J\lhd R$ אידאל. נניח $(a)\neq J$ ונוכיח שזה גורר $J=R$.

מהנתון ש-R תחום ראשי נובע ש-J אידאל ראשי. כלומר יש $b\in R$ המקיים $J=(b)$. מההנחה $(a)\subsetneqq(b)\lhd R$ נובע כי b מחלק ממש של a.

הוכחנו שאם a אי־פריק אז כל מחלק ממש שלו הפיך, ולכן b הפיך. מכאן כי $J\ni 1=bb^{-1}$ וכפי שראינו זה גורר $J=R$.

$(2\Longleftarrow 1)$

נניח כי (a) אידאל מקסימלי, צ"ל כי a אי־פריק. ראינו כי a אי־פריק אמ"מ כל מחלק ממש שלו הפיך, ולכן מספיק להוכיח שכל מחלק ממש של a הפיך.

נניח כי b מחלק ממש של a, מכאן כי $(a)\subsetneqq(b)$. ממקסימליות (a) נובע כי $(b)=R$ ולכן בפרט $1\in(b)$, כלומר יש $c\in(b)$ המקיים $bc=1$, כלומר b הפיך. ■

טענה: בתחום ראשי כל אי־פריק הוא ראשוני.

הוכחה: אם R תחום ראשי ו-$a\in R$ אי־פריק, הראינו שזה אומר כי $R/(a)$ שדה, ולכן בפרט $R/(a)$ תחום שלמות, והראינו לעיל שזה תנאי שקול לכך ש-a ראשוני. ■

מסקנה: הראינו כבר שכל ראשוני הוא אי־פריק. לכן נסיק כי בתחום ראשי איבר הוא פריק אמ"מ הוא ראשוני.

26 חוגים נתריים

הגדרה: אומרים שחוג R הוא **חוג נתרי** (על־שם המתמטיקאית אמי נתר), או שהוא מקיים את **תנאי השרשרת העולה**, אם לכל סדרה אינסופית של אידאלים מהצורה $I_1 \subsetneqq I_2 \subsetneqq ... \subsetneqq I_k \subsetneqq ...$ קיים n כך שלכל $n \leq m$ מתקיים $I_n = I_m$.

משפט: כל תחום ראשי הוא חוג נתרי. כלומר מקיים את תנאי השרשרת העולה.

הוכחה: תהי $\{I_n\}$ שרשרת אינסופית של אידאלים בתחום ראשי R.

נגדיר $J = \bigcup_n I_n$. עקרונית איחוד של אידאלים אינו בהכרח אידאל, אולם מכיוון שכאן מדובר בשרשרת זה אידאל.[31]

מהנתון ש-R תחום ראשי נובע כי J אידאל ראשי, ולכן $J = (c)$ ל-$c \in R$ כלשהו. בפרט $c \in J$ ולכן קיים m המקיים $c \in I_m$. מהיות I_m אידאל נובע כי $(c) \subseteq I_m \subseteq J = (c)$, ולכן בהכרח $I_m = (c) = J$, והחל מהמקום ה-m מתקיים תנאי השרשרת העולה, ולכן R חוג נתרי. ■

הערה: חוג הוא נתרי אמ"מ כל אידאל בו נוצר סופית. לא נוכיח משפט זה.

הגדרה: אומרים שתחום שלמות R מקיים את **תנאי שרשרת המחלקים**, אם <u>לא</u> קיימת שרשרת אינסופית של מחלקים ממש. כלומר שרשרת $(a_n)_{n\geq 1}$ כך שלכל n מתקיים כי a_{n+1} מחלק ממש של a_n.

טענה: כל חוג נתרי (ובפרט כל תחום ראשי) מקיים את תנאי שרשרת המחלקים.

הוכחה: לו הייתה שרשרת מחלקים אינסופית $\{a_n\}$ היינו מקבלים שלכל n מתקיים כי a_{n+1} מחלק ממש של a_n.

ראינו שזה תנאי שקול לכך שמתקיים $(a_n) \subsetneqq (a_{n+1})$, כלומר קיימת שרשרת אידאלים אינסופית שאינה מתייצבת, ולכן החוג לא מקיים את תנאי השרשרת העולה. ■

26.1 פירוק איבר לא הפיך בתחום ראשי

משפט: בכל תחום ראשי, כל איבר $a \neq 0$ שאינו הפיך ניתן להצגה כמכפלה של אי־פריקים, וההצגה יחידה עד כדי שינוי סדר וחברויות.

לצורך הוכחת המשפט נוכיח כמה טענות־עזר.

למה 1: יהי R חוג נתרי, אז כל $0 \neq a \in R$ לא הפיך מתחלק באיבר אי־פריק.

הוכחה: אם a אי־פריק בעצמו, סיימנו כי $a|a$, לכן נניח כי a פריק, כלומר יש לו מחלק ממש שאינו הפיך שנסמן a_1. אם a_1 אי־פריק בעצמו סיימנו, לכן נניח כי a_1 פריק, כלומר יש לו מחלק ממש שאינו הפיך שנסמן a_2... וכך נמשיך ונקבל שרשרת של מחלקים ממש $a_1|a_2|...|a_n|...$.

ראינו שכל חוג נתרי מקיים את תנאי שרשרת המחלקים, ולכן שרשרת זו תיעצר. ■

[31] הסגירות לכפל מידית שכן כל $a \in J$ שייך לאידאל I_n כלשהו, ומהיות I_n אידאל הוא סגור לכפל חיצוני ולכן $ar \in I_n \subseteq J$ לכל $r \in R$. הסגירות לחיבור נובעת מכך ש-$\{I_n\}$ שרשרת ביחס להכלה, ולכן לכל $a, b \in J$ קיים n מספיק גדול כך ש-$a, b \in I_n$, ולכן $a + b \in I_n \subseteq J$.

למה 2: יהי R תחום שלמות נתרי, ולפיכך מקיים את תנאי שרשרת המחלקים, אזי כל $R \ni a \neq 0$ הוא מכפלה של אי־פריקים.

הוכחה: מלמה 1 נובע שקיים אי־פריק $p_1 \in R$ המקיים $p_1|a$, ולכן $a = p_1a_1$ ל-$a_1 \in R$ כלשהו.

אם a_1 הפיך אז $a \sim p_1$ ביחס החברות, וכל חבר של אי־פריק הוא אי־פריק. לכן a אי־פריק השווה למכפלה של אי־פריקים באורך 1 (כלומר $a = a$).

לכן נניח כי a_1 לא הפיך, ולכן מלמה 1 נובע שיש לו מחלק אי־פריק $p_2 \in R$ כך שמתקיים $a_1 = p_2a_2$ ולכן $a = p_1p_2a_2$.

אם a_2 אי־פריק סיימנו, שכן הצגנו את a כמכפלה של אי־פריקים.

גם אם a_2 הפיך סיימנו, כי אז $a_1 \sim p_2$ ביחס החברות ולכן a_1 אי־פריק ומתקיים $a = p_1a_1$ כנדרש.

אחרת, כלומר אם a_2 אינו הפיך אז מלמה 1 הוא מתחלק באיבר אי־פריק p_3 ומתקיים $a_2 = p_3a_3$ ולכן שוב נקבל $a = p_1p_2p_3a_3$.

נמשיך באופן זה ונקבל כי a_{n+1} מחלק ממש של a_n, שכן $a_n = p_{n+1}a_{n+1}$ ולכן נקבל שרשרת של מחלקים ממש שמתנאי הלמה חייבת להיעצר. כלומר קיים n טבעי כך ש-a_n יהיה הפיך, אחרת יהיה לו מחלק ממש שימשיך את השרשרת.

לכן מתקיים $a = p_1p_2...p_na_n$ כאשר a_n הפיך. נשים לב שהאיבר p_na_n גם הוא אי־פריק כי $p_na_n \sim p_n$ ביחס החברות, ולכן a הוא מכפלה של אי־פריקים. ■

מסקנה: בתחום ראשי, כל איבר $a \neq 0$ לא הפיך ניתן להצגה כמכפלה של אי־פריקים.

הוכחה: כל תחום ראשי הוא תחום נתרי, כלומר מקיים את תנאי השרשרת העולה, ולכן מקיים גם את תנאי שרשרת המחלקים, ומלמה 2 נובעת הטענה. ■

למה 3: יהי R תחום שלמות בו כל איבר אי־פריק הוא ראשוני, אז כל שתי הצגות של איבר כמכפלת אי־פריקים הן שקולות עד־כדי שינוי סדר וחברויות.

הוכחה: צריך להראות שאם $p_1, ..., p_n$ אי־פריקים וגם $q_1, ..., q_m$ אי־פריקים, ומתקיים $p_1p_2...p_n = q_1q_2...q_m$, אז $n = m$, ולאחר שינוי סדר ואינדוקס מחודש $p_1 \sim q_1, p_2 \sim q_2, ..., p_n \sim q_n$.

נראה זאת באינדוקציה על n. עבור $n = 1$ אם מתקיים $p_1 = q_1q_2...q_m$ אז $p_1|p_1 = q_1q_2...q_m$ ולכן אם נסמן $x = q_1$, $y = q_2...q_m$ נקבל כי $p_1|xy$ כאשר x אי־פריק. לכן מתקיים כי x הפיך או y הפיך. אבל ידוע כי x לא הפיך (כי הוא אי־פריק) ולכן y הפיך, וזו סתירה כי זה אומר ש-$q_2, ..., q_m$ הפיכים. מכאן שמתקיים $m = 1$ ולכן $p_1 = q_1$.

נניח את הטענה ל-$n - 1 \geq 2$ כלשהו ונניח כי $p_1p_2...p_n = q_1q_2...q_m$. מתקיים כי $p_1|p_1p_2...p_n = q_1q_2...q_m$ ומכיוון ש-p_1 אי־פריק נובע כי הוא ראשוני ומכאן כי $p_1|q_j$ עבור $1 \leq j \leq n$, וללא הגבלת הכלליות לאחר שינוי סדר נקבל $p_1|q_1$.

מאחר ושניהם אי־פריקים נובע כי $p_1 \sim q_1$ ביחס החברות. מהנחת האינדוקציה נקבל שעד־כדי שינוי סדר מתקיים $p_2 \sim q_2, p_3 \sim q_3, ..., p_n \sim q_n$ וכן $n - 1 = m - 1$, ולכן בתוספת המסקנה $p_1 \sim q_1$ נקבל כי $n = m$ וכן $p_i \sim q_i$ לכל $1 \leq i \leq n$. ■

משפט: יהי R תחום ראשי בו כל אי־פריק הוא ראשוני, אז יש בו פריקות חד־ערכית.

הוכחה: בכל תחום ראשי יש פריקות חד־ערכית, כי כל תחום ראשי הוא נתרי וכל אי־פריק בתחום ראשי הוא ראשוני. ■

טענה: החוג $\mathbb{F}[x,y]$ הוא תחום שלמות שאינו תחום ראשי.

הוכחה: קל לראות שמדובר בתחום שלמות. נראה שהוא לא תחום ראשי, כלומר קיים בו אידאל שאינו ראשי. נראה שהאידאל הנוצר הבא אינו ראשי:

$$I=(x,y)=:\{f(x,y)\cdot x+g(x,y)\cdot y|f,g\in\mathbb{F}[x,y]\}$$

עבור $x\neq cy$ לכל $c\in\mathbb{F}$.

נניח בשלילה כי I אידאל ראשי. כלומר יש פולינום $h\in\mathbb{F}[x,y]$ כך שמתקיים $I=(h)$.

מתקיים כי h לא הפיך, אחרת $I=\mathbb{F}[x,y]$ וזה לא ייתכן כי יש פולינומים בשני משתנים שלא מתאפסים בערכים $(0,0)$.

מכיוון ש-$x,y\in I=(h)$ נובע כי $h|x$ וכן $h|y$. אבל מאחר ו-h לא הפיך וכן x,y אינם פריקים כפולינומים, נובע כי $h\sim x$ וכן $h\sim y$ ביחס החברות, וזה יחס שקילות ולכן מטרנזיטיביות $x\sim y$, כלומר $x=cy$, בסתירה לבחירה שלהם. ■

הערה: למרות שהחוג $\mathbb{F}[x,y]$ אינו תחום ראשי, מתקיימת בו פריקות חד־ערכית. כמו־כן הוא חוג נתרי.

27 החוג $\mathbb{F}[x]$

תזכורת: הראינו כי החוג $\mathbb{F}[x]$ הוא תחום ראשי.

כמו־כן ניתן לראות שלכל $p,q\in\mathbb{F}[x]$ מתקיים:

$$\deg(p\pm q)\leq\max\{\deg(p),\deg(q)\}$$

$$\deg(p\cdot q)=\deg(p)+\deg(q)$$

לכן מתקיים שכל הפולינומים באידאל הנוצר (p) הם לפחות ממעלה $\deg(p)$, וככלל, לכל אידאל הנוצר על־ידי כמה פולינומים, כל הפולינומים בו הם לפחות ממעלת הפולינום היוצר בעל המעלה המינימלית.

27.1 שורש של פולינום

משפט: לכל $f\in\mathbb{F}[x]$ ולכל $\alpha\in\mathbb{F}$:

1. קיים $g\in\mathbb{F}[x]$ כך ש-$f(x)=(x-\alpha)g(x)+f(\alpha)$
2. מתקיים $f(\alpha)=0 \iff (x-\alpha)|f$

הוכחה:

1. נחלק את f בפולינום $x-\alpha$ עם שארית, ונקבל $f(x)=(x-\alpha)g(x)+r(x)$ כאשר $\deg(r)<\deg(x-\alpha)$ ולכן $r(x)=\beta$ עבור $\beta\in\mathbb{F}$.
נשים לב שאם נציב α נקבל $f(\alpha)=r(\alpha)=\beta$, ולכן נסיק:

$$f(x)=(x-\alpha)g(x)+f(\alpha)$$

2. בכיוון ראשון, אם $f(\alpha)=0$ אז בחילוק של f ב-$(x-\alpha)$ עם שארית נקבל:

$$f(x)=(x-\alpha)g(x)+f(\alpha)=(x-\alpha)g(x)$$

ולכן $(x-\alpha)\,|\,f$.
בכיוון שני, אם $(x-\alpha)\,|\,f$ אז $f(x)=(x-\alpha)g(x)$ עבור $g\in\mathbb{F}[x]$, ולכן $f(\alpha)=0$. ■

27.2 שדה הרחבה

טענה: אם $p\in\mathbb{F}[x]$ פולינום אי־פריק, אז $\mathbb{F}[x]/(p)$ הוא שדה.

הוכחה: ידוע כי $\mathbb{F}[x]$ הוא תחום ראשי, ובכל תחום ראשי אי־פריקות של איבר שקולה להיות חוג המנה המתקבל מהאידאל הנוצר על־ידו שדה. ■

הגדרה: בהינתן שדה $\mathbb{F}$, **שדה הרחבה** שלו הוא שדה $\mathbb{E}$, כך ש-$\mathbb{F}\subseteq\mathbb{E}$ וכן הפעולות ב-$\mathbb{F}$ נשמרות תחת הפעולות החדשות ב-$\mathbb{E}$.

טענה: לכל $p\in\mathbb{F}[x]$ שאינו קבוע, קיים שדה הרחבה $\mathbb{E}$ של $\mathbb{F}$ שבו ל-p יש שורש.

הוכחה: יהי $p\in\mathbb{F}[x]$ שאינו קבוע. אם p פריק אז הוא לא הפיך ולכן יש לו פירוק למכפלה של פולינומים אי־פריקים כפי שהראינו. לכן מספיק להראות שהטענה נכונה לכל פולינום אי־פריק.

נניח כי p אי־פריק. נסמן $\mathbb{E}=\mathbb{F}[x]/(p)$, וכפי שראינו זה שדה. איבר כללי של חוג מנה כזה הוא $\overline{g}\in\mathbb{E}$ עבור $g\in\mathbb{F}[x]$, והוא מהצורה $\overline{g}=g+(p)$.

כעת נראה של-p יש שורש ב-$\mathbb{E}$. נסמן $p(x)=\sum_{i=1}^{n}a_ix^i$ ונשים לב שעבור $\overline{x}\in\mathbb{E}$ מתקיים:

$$p(\overline{x})=\sum_{i=1}^{n}a_i\overline{x}^i=\overline{\sum_{i=1}^{n}a_ix^i}=\overline{p(x)}=\overline{0}$$

כאשר השוויון השני נובע מכך שפעולה על מחלקה מבוצעת על הנציגים, והשוויון האחרון נובע מכך שמתקיים:

$$\overline{p(x)}=p(x)+(p(x))=(p(x))=\overline{0}$$

נשים לב כי $\left\{\overline{\lambda}\middle|\lambda\in\mathbb{F}\right\}\cong\mathbb{F}$, על־ידי המיפוי $\lambda\mapsto\overline{\lambda}$. מכאן שהאיבר המתאים $x\in\mathbb{F}$ הוא שורש של p.■

טענה: אם $p\in\mathbb{F}[x]$ פולינום אי־פריק ממעלה d, אז $\mathbb{F}[x]/(p)=:\mathbb{E}$ הוא מרחב וקטורי ממימד d מעל $\mathbb{F}$.

הוכחה:

1. ראשית $\mathbb{F}$ תת־שדה של $\mathbb{E}$, וזאת על־ידי האיזומורפיזם $x \mapsto \overline{x}$ לכל $x \in \mathbb{F}$, כאשר $\overline{x} = x + (p) \in \mathbb{E}$. כל שדה הוא מרחב וקטורי מעל תת־שדה שלו, ולכן $\mathbb{E}$ הוא מרחב וקטורי מעל $\mathbb{F}$.
2. כדי להראות ש-$\mathbb{E}$ הוא ממעד d, מספיק להראות שהוא איזומורפי למרחב וקטורי כלשהו שהוא ממעד d מעל $\mathbb{F}$.

(א) נראה שהקבוצה $Y =: \{f \in \mathbb{F}[x] \,|\, \deg(f) < d\}$ היא מרחב וקטורי כנ"ל.
ראשית נגדיר בקבוצה זו פעולות מודולו p. המשמעות של מודולו p נובעת מכך שניתן לחלק כל פולינום בפולינום p עם שארית, ולכן לכל $f, g \in Y$ מתקיים:

$$f(x) = pq_1 + r_1 \equiv r_2 \mod (p)$$

$$g(x) = pq_2 + r_2 \equiv r_2 \mod (p)$$

כאשר $\deg(r_i) < \deg(p) = d$, ולכן:

$$\deg(r_1 + r_2) \leq \max\{\deg(r_1), \deg(r_2)\} < d$$

ולכן $r_1 + r_2 \in Y$. מכאן שהחיבור מוגדר היטב על־ידי $f + g = r_1 + r_2$.
לצורך הגדרת הכפל, נחלק את הפולינום $f \cdot g$ בפולינום p עם שארית, ונקבל:

$$f \cdot g = pq_3 + r_3 \equiv r_3 \mod (p)$$

כאשר $\deg(r_3) < \deg(p) = d$, ולכן $r_3 \in Y$. מכאן שהכפל מוגדר היטב על־ידי $f \cdot g = r_3$.

(ב) נגדיר התאמה $\varphi : Y \to \mathbb{E}$ על־ידי $\varphi(r) = r + (p)$. נראה כי זה איזומורפיזם של שדות.

i. נראה שזה הומומורפיזם:

$$\varphi(r + s) = r + s + (p) = r + (p) + s + (p) = \varphi(r) + \varphi(s)$$

$$\varphi(r \cdot s) = r \cdot s + (p) = [r + (p)] \cdot [s + (p)] = \varphi(r) \cdot \varphi(s)$$

כאשר הפעולות בשדה $\mathbb{E}$ מוגדרות על הנציגים.

ii. נראה שזו התאמה חח"ע: יהיו $r_1 \neq r_2$ השייכים לאותה מחלקה ב-$\mathbb{E}$. לכן $r_1 - r_2 \neq 0$ וזהו פולינום ממעלה קטנה מ-d. נשים לב שכל איבר ב-(p) הוא מהצורה $g \cdot p$ ל-$g \in \mathbb{F}[x]$ ולכן מעלתו לפחות d, ומכאן כי $r_1 - r_2 \notin (p)$ ולכן:

$$\varphi(r_1) = r_1 + (p) \neq r_2 + (p) = \varphi(r_2)$$

כלומר המחלקות ב-$\mathbb{E}$ המתקבלות על־ידי φ שונות, ולכן זהו הומומורפיזם חח"ע.

iii. נראה שזו התאמה על: בכל מחלקה $g+(p)\in\mathbb{E}$ קיים נציג ממעלה קטנה מ-d, והוא זה שממופה אליה על־ידי φ.

3. אם כך $Y\cong\mathbb{E}$. לכן כפי שראינו $\mathbb{F}$ תת־שדה שלהם וניתן להתייחס אליהם כאל מרחב וקטורי מעל $\mathbb{F}$. קל לראות שהאוסף $\left\{1,x,x^2,...,x^{d-1}\right\}$ הוא בסיס של Y מעל $\mathbb{F}$, ולכן $\mathbb{E}$ הוא אכן מרחב וקטורי ממימד d. ■

הערה: בפרט גם האוסף המתאים $\left\{\overline{1},\overline{x},\overline{x^2},...,\overline{x^{d-1}}\right\}$ יהיה בסיס של $\mathbb{E}$.

מסקנה: לכל פולינום $f\in\mathbb{F}[x]$ שאינו קבוע קיים שורש בשדה הרחבה $\mathbb{F}\subseteq\mathbb{E}$ ממימד סופי.

27.3 שדה פיצול

הגדרה: יהי $f\in\mathbb{F}[x]$ פולינום ממעלה n, ויהי $\mathbb{E}$ שדה הרחבה של $\mathbb{F}$. נאמר כי f **מתפצל** מעל $\mathbb{E}$ או ש-$\mathbb{E}$ הוא **שדה פיצול** של f, אם מתקיים כי $f(x)=\lambda(x-\alpha_1)\cdot...\cdot(x-\alpha_n)$ עבור $\alpha_1,...,\alpha_n\in\mathbb{E}$, ובפרט $\alpha_1,...,\alpha_n$ הם בדיוק שורשי f.

משפט קרונקר: לכל $f\in\mathbb{F}[x]$ קיים שדה פיצול $\mathbb{F}\subseteq\mathbb{E}$ ממימד סופי.

הוכחה: באינדוקציה על מעלת f. למקרה $n=0$ מתקיים $f=\lambda$ ל-$\lambda\in\mathbb{F}$ ולכן נבחר $\mathbb{E}=\mathbb{F}$.

נניח את הטענה לכל פולינום ממעלה קטנה מ-$n=\deg(f)$. מטענה קודמת נובע שקיים שדה פיצול $\mathbb{F}\subseteq\mathbb{E}$ ממימד סופי שבו יש ל-f שורש שנסמן $\alpha\in\mathbb{E}$. מטענה קודמת נובע $(x-\alpha)|f$ ולכן קיים $g\in\mathbb{F}[x]$ כך ש-$f(x)=(x-\alpha)g(x)$.

מתקיים $\deg(g)=n-1$ ולכן מהנחת האינדוקציה נובע שקיים שדה פיצול $\mathbb{E}\subset\mathbb{E}'$ ממימד סופי וכן קיימים $\alpha_1,...,\alpha_{n-1}\in\mathbb{E}'$ כך שמתקיים:

$$g(x)=\lambda(x-\alpha_1)\cdot...\cdot(x-\alpha_{n-1})$$

ומכאן כי:

$$f(x)=(x-\alpha)\cdot g(x)=(x-\alpha)\cdot\lambda(x-\alpha_1)\cdot...\cdot(x-\alpha_{n-1})$$

כלומר $\mathbb{E}'$ שדה פיצול של f. ■