

מבנים אלגבריים - גרסה מקוצרת

עוזי וישנה

מבנים אלגבריים - גרסה מקוצרת

מהדורה 2.57 למתרגל

זוהי גרסת המחצית של חוברת הקורס "מבנים אלגבריים" למדעי המחשב, 89-214. היא מבוססת על הגרסה המלאה, וכוללת את הדברים החיוניים בלבד. מספרי הסעיפים ותת-הסעיפים נשארו כשהיו.

עוזי וישנה, 2.2012

תוכן עניינים

1	מבוא לתורת המספרים	1
5	חבורות למחצה ומונוידיים	2
6	חבורות ותת-חבורות	3
10	משפט לגרנז'	4
13	הומומורפיזמים ותת-חבורות נורמליות	5
16	סריג תת-החבורות	6
18	הצמדה ומחלקות הצמידות	7
20	אוטומורפיזמים	8
21	חבורות של תמורות	9
22	חבורות אבליות	10
25	מבוא לחוגים	11
31	מבוא לשדות סופיים	12

1 מבוא לתורת המספרים

מושגים: יחס החלוקה, מחלק משותף מקסימלי; חילוק עם שארית ואלגוריתם אוקלידס; איברים זרים; מספרי אי-פריק ומספר ראשוני. פירוק יחיד לגורמים. שקילות מודולו n . משפט השאריות הסיני.

1.0 המספרים השלמים

בפרק זה, **מערכת המספרים השלמים** היא המערכת הכוללת מלבד הקבוצה \mathbb{Z} של המספרים השלמים, גם את פעולות החיבור (+) והכפל (\cdot) ואת יחס הסדר ($<$ ו- \leq), עם התכונות

המוכרות מבית הספר היסודי: $a + (b + c) = (a + b) + c$, אם $a < b$ ו- $0 < c$ אז $ac < bc$, וכדומה.

את הערך המוחלט מגדירים לפי יחס הסדר: $|a| = a$ אם $a \geq 0$, ו- $|a| = -a$ אם $a < 0$. קבוצת המספרים הטבעיים $\mathbb{N} = \{a \in \mathbb{Z} : a \geq 0\}$ מקיימת את תכונת הסדר הטוב, שלפיה לכל קבוצה לא ריקה יש איבר מינימלי.

תרגיל 1.1 ()** הסק מתכונת הסדר הטוב את אקסיומת האינדוקציה: אם $A \subseteq \mathbb{N}$ היא קבוצה המקיימת את שתי ההנחות

$$\bullet 0 \in A$$

$$\bullet \text{ לכל } n \in \mathbb{N}, \text{ אם } n \in A \text{ אז } n + 1 \in A$$

$$\text{אז } A = \mathbb{N}$$

1.1 יחס החלוקה

מגדירים יחס בינארי על המספרים השלמים:

הגדרה 1.2 $a|b$ ("מחלק את b") אם קיים $c \in \mathbb{Z}$ כך ש- $b = ac$.

תרגיל 1.3 (*) הוכח שהיחס טרנזיטיבי ורפלקסיבי. יחס כזה נקרא **קדם-סדר**.

תרגיל 1.4 (*) אם $a|b$ ו- $b \neq 0$ אז $|a| \leq |b|$.

תרגיל 1.5 ()** מצא את האיברים המינימליים והמקסימליים ביחס לקדם-סדר שהגדרנו.

הגדרה 1.6 האיברים $a, b \in \mathbb{Z}$ הם **חברים** אם $a|b$ ו- $b|a$. במקרה כזה מסמנים $a \sim b$.

תרגיל 1.7 ()** הוכח שיחס החברות הוא יחס שקילות.

הגדרה 1.8 מחלקת החברות $[a]$ מחלקת את b אם $a|b$.

תרגיל 1.9 ()** הוכח שיחס החלוקה בין מחלקות מוגדר היטב. כלומר, אם $a \sim a'$ ו- $b \sim b'$, אז $a|b$ אם ורק אם $a'|b'$.

משפט 1.10 היחס 'מחלק' הוא יחס סדר חלש (כלומר, אנטיסימטרי, רפלקסיבי וטרנזיטיבי) על אוסף מחלקות החברות ב- \mathbb{Z} .

1.2 אוקלידיות

משפט 1.11 ('האוקלידיות של \mathbb{Z} ') לכל $n \in \mathbb{Z}$ ו- $d \neq 0$ קיימים q, r כך ש- $n = qd + r$ ו- $0 \leq r < |d|$.

אוקלידיות היא שם אחר לעוצמה כאפשר לחלק עם ארית.

1.3 המחלק המשותף המקסימלי**1.3.1 הגדרת המחלק המשותף המקסימלי**

הגדרה 1.12 יהיו $n, m \in \mathbb{Z}$. מספר d נקרא **מחלק משותף מקסימלי** של n, m אם הוא מקסימלי לגבי יחס החלוקה בין כל המחלקים המשותפים. כלומר, d מחלק את n ואת m , ומתחלק בכל מחלק משותף אחר.

ע'א לא e-כריורי, לא ברור שתאיז קיים מספר כזה.

תרגיל 1.13 ()** אם d הוא מחלק משותף מקסימלי של a, b , ו- $a' \sim a, b' \sim b, d' \sim d$, אז d' הוא מחלק משותף מקסימלי של a', b' (במלים אחרות, אפשר לומר שמחלקת החברות $[d]$ היא מחלק משותף מקסימלי של מחלקות החברויות $[a], [b]$).

תרגיל 1.14 ()** הוכח שאם קיים מחלק משותף מקסימלי של n ו- m , אז הוא יחיד עד כדי חברות.

1.3.2 כחוג ראשי \mathbb{Z}

הגדרה 1.15 לכל a, b שלא שניהם אפס, נסמן ב- (a, b) את המספר הגדול ביותר בקבוצת המחלקים המשותפים של a ו- b (גדול ביותר לגבי יחס הסדר הרגיל).

תרגיל 1.16 (+)** קיים לכל a, b שאינם שניהם אפס.

משפט 1.17 לכל $n, m \in \mathbb{Z}$, קיימים $\alpha, \beta \in \mathbb{Z}$ כך ש- $\alpha n + \beta m = (n, m)$.

תרגיל 1.18 (*)** הוכח את המשפט. **הדרכה.** נסמן ב- e את המינימום של הקבוצה $I_0 = \{x > 0 \mid \exists \alpha, \beta : x = \alpha n + \beta m\}$ ו- $d = (a, b)$. $d \mid e$ כי צירוף ליניארי של a, b . כתוב $a = qe + r$, והראה $r = 0$, ולכן $a \mid e$; בדומה $b \mid e$; לכן $e \leq d$. מכאן $d = e \in I_0$.

1.3.3 אלגוריתם אוקלידס

תרגיל 1.19 ()** אם $a = qb + r$ אז $(a, b) = (b, r)$.

תרגיל 1.20 (*)** תאר אלגוריתם הנעזר בחילוק עם שארית כדי לחשב את המחלק המשותף המקסימלי של שני מספרים נתונים.

תרגיל 1.21 ()** נסמן $d = (n, m)$. אם $n = qm + r$ ו- $\alpha m + \beta r = d$ אז $\beta n + (\alpha - \beta q)m = d$.

תרגיל 1.22 (*)** תאר אלגוריתם לחישוב המחלק המשותף המקסימלי של זוג מספרים, והצגה שלו כצירוף שלם שלהם.

1.3.4 מספרים זרים

הגדרה 1.23 המספרים n, m הם **זרים** אם $(n, m) = 1$.

טענה 1.24 אם a, b זרים ו- $a \mid bc$, אז $a \mid c$.

תרגיל 1.25 ()** הוכח את הטענה. **הדרכה.** כתוב $\alpha a + \beta b = 1$.

1.3.5 תרגילים נוספים

1.4 ראשוניים ופירוק לגורמים

הגדרה 1.26 מספר $p \in \mathbb{Z}$ הוא ראשוני אם הוא אינו יכול לחלק מכפלה בלי לחלק את אחד הגורמים שלה.

הגדרה 1.27 מספר $p \in \mathbb{Z}$ הוא אי-פריק, אם בכל פירוק $p = ab$, בהכרח $a \sim 1$ או $b \sim 1$.

כל מספר מתחלק בהפיכים ובחברים שלו, ולכן אלו נקראים 'מחלקים טריוויאליים'.

תרגיל 1.28 (*) התכונות הבאות שקולות:

1. p אי-פריק.

2. אם $p = ab$ אז $a \sim p$ או $b \sim p$.

3. אם $a | p$ אז $a \sim 1$ או $a \sim p$.

תרגיל 1.29 (**-) כל ראשוני הוא אי-פריק.

תרגיל 1.30 (*) אם p אי-פריק, אז לכל n , $p | n$ או $(p, n) = 1$.

תרגיל 1.31 (**+) כל אי-פריק הוא ראשוני. **הדרכה.** יהי p אי-פריק, ונניח $p | ab$ אם $p \nmid a$ אז $(p, a) = 1$ לפי תרגיל 1.30, ולפי 1.24, $p | b$.

תרגיל 1.32 (**+) הראה ש- $p \in \mathbb{Z}$ ראשוני אם ורק אם אין לו אף מחלק לא טריוויאלי.

תרגיל 1.33 (**-) כל מספר טבעי אפשר להציג כמכפלה של גורמים ראשוניים. **הדרכה.** אינדוקציה שלמה.

משפט 1.34 הפירוק של מספר טבעי לגורמים ראשוניים הוא יחיד עד-כדי סדר.

תרגיל 1.35 (**-*) הוכח את המשפט.

תרגיל 1.36 (**+) תן קריטריון לכך ש- $n = p_1^{a_1} \cdots p_t^{a_t}$ יחלק את $n' = p_1^{a'_1} \cdots p_t^{a'_t}$ (כאשר $a_i, a'_i \geq 0$), ונוסחה למחלק המשותף המקסימלי.

1.5 שקילות מודולו n

יהי $n \in \mathbb{Z}$, $n \neq 0$ קבוע. נגדיר יחס על המספרים השלמים:

הגדרה 1.37 a' שקול ל- b מודולו n (כותבים: $a \equiv b \pmod{n}$) אם $n | (a - b)$.

תרגיל 1.38 (*) הוכח ששקילות מודולו n היא יחס שקילות (כלומר, טרנזיטיבית, סימטרית ורפלקסיבית).

טענה 1.39 אם $a \equiv a' \pmod{n}$ ו- $b \equiv b' \pmod{n}$, אז $a + b \equiv a' + b' \pmod{n}$ ו- $ab \equiv a'b' \pmod{n}$.

פירושו של דבר הוא שפעולות החיבור והכפל של מחלקות שקילות מודולו n , המבוצעות על נציגים, מוגדרות היטב. עובדה זו תהיה לנו לעזר רב בהמשך.

1.5.1 משפט השאריות הסיני

משפט 1.40 (משפט השאריות הסיני) יהיו n, m זרים. לכל a, b , קיים x יחיד מודולו nm כך ש-
 $x \equiv a \pmod{n}$ ו- $x \equiv b \pmod{m}$.

תרגיל 1.41 (*)** הוכח את המשפט. **הדוכה.** נניח ש- $\alpha n + \beta m = 1$. הראה ש- $x = \alpha n b + \beta m a$ פתרון. את היחידות הוכח לפי ספירה.

2 חבורות למחצה ומונוידים

מושגים: פעולה אסוציאטיבית, חבורה למחצה, איבר יחידה, איבר אפס; מונויד, איבר הפיך.

2.1 חבורות למחצה

פעולה בינרית על קבוצה A היא פונקציה $*$: $A \times A \rightarrow A$. שימו לב שלפי ההצגה, הפעולה "מאגרת היטב", כלומר, לכל $x, y \in A$ איברים יש ערך יחיד $x * y$ ו"סגורה" - הערך הזה שייך ל- A .
 פעולה $*$ היא אסוציאטיבית אם $a * (b * c) = (a * b) * c$.

הגדרה 2.1 חבורה למחצה היא מערכת מתמטית הכוללת קבוצה עם פעולה אסוציאטיבית עליה.

תרגיל 2.2 (*)** הראה שאם הפעולה אסוציאטיבית, אז החזקה מוגדרת היטב (כלומר, כל הדרכים להכפיל איבר x בעצמו n פעמים מביאות לאותה תוצאה).

תרגיל 2.3 (*) תהי X קבוצה. האוסף X^X של פונקציות $X \rightarrow X$, עם פעולת ההרכבה של פונקציות, הוא חבורה למחצה.

הגדרה 2.4 איזומורפיזם של חבורות למחצה $(X, *)$, (Y, \circ) הוא פונקציה חד-חד-ערכית ועל $f: X \rightarrow Y$, כך ש- $f(x * x') = f(x) \circ f(x')$. אם קיים איזומורפיזם בין החבורות למחצה, אומרים שהן איזומורפיות, ומסמנים $X \cong Y$.

תרגיל 2.5 ()** איזומורפיות היא תכונה טרנזיטיבית, סימטרית ורפלקסיבית. **מסקנות** המבט של תורת הקבוצות האקסיומטית יש כאן אי-דיוק מסויים, אבל אפשר לומר שאיזומורפיות היא יחס שקילות.

הגדרה 2.6 איבר e בחבורה למחצה S הוא איבר יחידה אם לכל $x \in S$, $xe = xe = x$.

תרגיל 2.7 (*) אם יש בחבורה למחצה איבר יחידה, אז הוא יחיד.

2.2 מונוידים

הגדרה 2.8 חבורה למחצה עם איבר יחידה נקראת מונויד.

תרגיל 2.9 ()** תהי A קבוצה. הוכח ש- $M = A^A = \{f: A \rightarrow A\}$ עם פעולת ההרכבה הוא מונויד.

תרגיל 2.10 ()** הראה שכל חבורה למחצה S אפשר להרחיב למונויד $S' = S \cup \{e\}$, אם נגדיר את e להיות איבר היחידה במבנה החדש.

תרגיל 2.11 ()** תאר את המונויד המתקבל לאחר חזרה n פעמים על הבניה של תרגיל 2.10, כשמתחילים ממונויד האפס $M = \{0\}$.

הגדרה 2.12 יהי M מונויד עם איבר היחידה 1. איבר $a \in M$ הוא הפיך אם קיים $b \in M$ כך ש-
 $ab = ba = 1$.

תרגיל 2.13 ()** אם a הפיך, אז האיבר b שמספקת ההגדרה הוא יחיד.

לכן, אם a הפיך, מוצדק לקרוא לאיבר b המקיים $ab = ba = 1$ **ההפכי** של a , בהא הידיעה, ולסמן אותו בסימון a^{-1} .

תרגיל 2.14 (*) אם a הפיך, אז גם a^{-1} הפיך, ו- $(a^{-1})^{-1} = a$.

תרגיל 2.15 ()** אם a, b הפיכים, אז גם ab הפיך, ו- $(ab)^{-1} = b^{-1}a^{-1}$.

הגדרה 2.16 את אוסף האיברים ההפיכים במונויד M מסמנים ב- $U(M)$.

טענה 2.17 לכל מונויד M , $U(M)$ הוא חבורה.

3 חבורות ותת-חבורות

מושגים: מונויד עם צמצום, חבורה. איזומורפיזם. סדר של חבורה. \mathbb{Z}_n חבורות אוילר. החבורות הסימטריות. החבורות הדיהדרליות. החבורה הליניארית הכללית. חבורה אבלית. מכפלה ישירה חיצונית. תת-חבורה.

3.1 חבורות

הגדרה 3.1 חבורה היא מונויד שבו כל האיברים הפיכים. במלים אחרות, חבורה היא מערכת מתמטית הכוללת קבוצה G , פעולה אסוציאטיבית $*$: $G \times G \rightarrow G$ ואיבר יחידה $1 \in G$, כך שכל האיברים של G הפיכים.

כל קבוצה עם איבר אחד (ופעולת הכפל ההכרחית) היא חבורה. כל החבורות האלה איזומורפיות, ונקראות **החבורה הטריטיואלית**. לפעמים, במקום לסמן חבורה זו ב- $G = \{1\}$, נכתוב פשוט $G = 1$.

תרגיל 3.2 (*) אם G חבורה אז $U(G) = G$.

הגדרה 3.3 למונויד יש תכונת הצמצום משמאל אם $ab = ac$ גורר $b = c$. באופן דומה מוגדר גם צמצום מימין.

משפט 3.4 מונויד סופי עם צמצום משמאל הוא חבורה.

תרגיל 3.5 (*)** הוכח את המשפט.

הגדרה 3.6 אם יש איזומורפיזם בין חבורות, אומרים שהן איזומורפיות (בציוק כמו במקרה של חבורות לאחצה או מוניזים).

תרגיל 3.7 (*) הראה שבחבורה בת יותר מאיבר אחד.

3.2 סדר של חבורה

הגדרה 3.8 הסדר של חבורה הוא מספר האיברים בחבורה.

פריט האיזע החשוב ביותר על חבורה סופית הוא הסדר שלה. בהמשך נראה שאפשר ללמוד הרבה על חבורה מיזיעת הסדר שלה לבידול, אם כי בדרכ-כלל יש כמה חבורות לא איזומורפיות מאותו סדר. אומרים שאיברים $a, b \in G$ בחבורה הם מתחלפים אם $ab = ba$.

3.3 דוגמאות לחבורות

3.3.1 החבורות הציקליות \mathbb{Z} ו- \mathbb{Z}_n :

החבורה האינסופית הפשוטה ביותר היא $(\mathbb{Z}, +, 0)$. אם 'מקפלים' את החבורה הזו למחלקות שקילות, מקבלים חבורה אחת מכל סדר. נקבע $n \geq 1$.

תרגיל 3.9 (*) הראה שיש בדיוק n מחלקות שקילות מודולו n . הדרכה. הראה שכל מספר שקול לאחד מבין $0, 1, \dots, n-1$, ושאלה אינם שקולים זה לזה.

תרגיל 3.10 (***) הזכר בטענה 1.39, והראה שפעולת החיבור $[a] + [b] = [a + b]$ מוגדרת היטב.

כשמציינים העתקה מקבוצה לקבוצה (ופעולה בינרית בכלל זה), עולה לפעמים צורך להוכיח שהפעולה מוגדרת היטב. ישנם שני מצבים שכיחים. הראשון, אם $f: A \rightarrow B$, מציינים את $f(\alpha)$ באופן מסוים, וצריך לוודא שאכן $f(\alpha) \in B$. המקרה השני הוא כאשר A אוסף של מחלקות שקילות ובהצגות $f(\alpha)$ מציינים בחירה (בדרכ כלל של נציג מהמחלקה α). לדוגמה, בפעולת החיבור כתבנו " $[x] + [y] = [x + y]$ ", במקום "יהיו α, β מחלקות נבחר נציגים x, y כך ש- $[x] = \alpha, [y] = \beta$, נציג $[x + y] = \alpha + \beta$ ". צריך לוודא שבחירת נציגים x', y' עם אותן תכונות תביא לאותה תוצאה.

תרגיל 3.11 (***) הראה שאוסף המחלקות $[0], \dots, [n-1]$ הוא חבורה ביחס לחיבור:

1. הראה שהפעולה אסוציאטיבית.

2. הראה שיש איבר יחידה (מהו?).

3. הראה שלכל איבר קיים הפכי. מהו איבר היחידה? מהו ההפכי של $[a]$?

הגדרה 3.12 החבורה של מחלקות השקילות מודולו n , ביחס לפעולת החיבור, נקראת \mathbb{Z}_n (וגם $\mathbb{Z}/n\mathbb{Z}$, מסיבות שיובררו בסעיף 5.4).

3.3.2 חבורות אוילר U_n :

כמקודם, נקבע $n \geq 1$.

תרגיל 3.13 ()** הזכר בטענה 1.39, והראה שפעולת הכפל $[a] \cdot [b] = [a \cdot b]$ מוגדרת היטב.

תרגיל 3.14 (*) המחלק המשותף המקסימלי תלוי רק במחלקת השקילות מודולו n במלים אחרות, אם $a \equiv a' \pmod{n}$ אז $(a, n) = (a', n)$.

תרגיל 3.15 (*)** איבר $[a] \in \mathbb{Z}_n$ הוא הפיך ביחס לכפל אם ורק אם $(a, n) = 1$.

תרגיל 3.16 (*)** אם $(a, n) = (b, n) = 1$ אז $(ab, n) = 1$.

הגדרה 3.17 חבורת אוילר מסדר n , U_n , היא אוסף מחלקות השקילות מודולו n , של מספרים הזרים ל- n , עם פעולת הכפל.

תרגיל 3.18 ()** הראה ש- U_n היא חבורה:

1. הראה שהפעולה אסוציאטיבית.

2. הראה שיש איבר יחידה (מהו?).

3. הראה שלכל איבר קיים הפכי. מהו ההפכי של $[a]$?

מספר האיברים בחבורה הזו אינו n אלא

$$\varphi(n) = |\{1 \leq a \leq n : (a, n) = 1\}|;$$

הפונקציה φ נקראת פונקציית אוילר.

תרגיל 3.19 ()** הוכח:

$$1. U_6 \cong U_4 \cong U_3 \cong \mathbb{Z}_2$$

$$2. U_{10} \cong U_5 \cong \mathbb{Z}_4$$

$$3. U_9 \cong U_7 \cong \mathbb{Z}_6$$

3.3.3 החבורות הסימטריות S_n

הגדרה 3.20 פונקציה חד-חד-ערכית ועל מקבוצה לעצמה, $\sigma : X \rightarrow X$, נקראת תמורה.

תרגיל 3.21 (*) S_X , עם פעולת הרכבת הפונקציות, היא חבורה.

תרגיל 3.22 (*) הוכח ש- $|S_n| = n!$.

הגדרה 3.23 אם $1 \leq r_1, \dots, r_t \leq n$ שונים זה מזה, תמורה σ המעבירה $r_1 \mapsto r_2 \mapsto \dots \mapsto r_t \mapsto r_1$ (וקובעת את שאר האברים) נקראת מחזור. ומסמנים $\sigma = (r_1 r_2 \dots r_t)$. הסדר של המחזור הוא האורך שלו, $o(\sigma) = t$.

הקבוצה $\{r_1, \dots, r_t\}$ נקראת התומך של המחזור; מחזוריים זרים הם מחזוריים שהתומכים שלהם זרים.

תרגיל 3.24 ()** מחזוריים זרים - מתחלפים.

משפט 3.25 כל תמורה ב- S_n אפשר לכתוב כמכפלה של מחזוריים זרים.

3.3.4 החבורות הדיהדרליות D_n

יהי $n \geq 2$. החבורה הסימטרית S_n היא אוסף כל הדרכים לערבב את העצמים $1, \dots, n$. אם נטיל מגבלות על סוגי הערבוב המותרים, נקבל חבורות קטנות יותר. למשל, החבורה D_n מוגדרת כאוסף הדרכים לפעול על מצולע בן n צלעות, כך שיתפוס בסוף הפעולה את אותו המקום במרחב. יש שתי פעולות יסודיות: סיבוב ימינה ב- $\frac{1}{n}$ המעגל (שנסמן באות σ), ושיקוף בציר קבוע כלשהו העובר דרך מרכז המצולע ואחד הקודקודים (שנסמן באות τ).

תרגיל 3.26 ()** בדוק שהפעולות מקיימות את היחסים $\sigma^n = 1$, $\tau^2 = 1$, $\tau\sigma\tau^{-1} = \sigma^{-1}$.

הגדרה 3.27 החבורה הדיהדרלית מסדר n , D_n , היא הקבוצה

$$\{\sigma^i \tau^j : i = 0, \dots, n-1, j = 0, 1\},$$

$$\text{עם הפעולה } \sigma^i \tau^j \cdot \sigma^{i'} \tau^{j'} = \sigma^{i+(-1)^j i' \pmod n} \tau^{j+j' \pmod 2}$$

3.3.5 חבורות המטריצות הקלאסיות

יהי F שדה.

הגדרה 3.28 $\text{GL}_n(F) = \{A \in M_n(F) : \det(A) \neq 0\}$

3.4 אבליות

הגדרה 3.29 אברים x, y בחבורה מתחלפים אם $xy = yx$. אם כל שני אברים בחבורה מתחלפים, אומרים שהיא אבלית.

פעולת החבורה נקראת בזרק כלל 'כפל', ומסומנת בהתאם. בחבורות אבליות אפשריים מעשים להשתמש בסימון חיבורי. אם מצוה בקבוצה של מספרים, למשל, (שמוצרות עליה מראש פעולות חיבור וכפל), יתכן שיהיה עלינו להבהיר האם מצוה בחבורה ביחס לחיבור או לכפל.

תרגיל 3.30 (*) הוכח: $(xy)^2 = x^2 y^2$ לכל x, y אם ורק אם החבורה אבלית.

3.5 מכפלה ישרה חיצונית

הגדרה. אם G_1, G_2 חבורות, מגדירים על הקבוצה $G_1 \times G_2$ של כל הזוגות הסדורים פעולה לפי רכיבים, $(g_1, g_2)(g'_1, g'_2) = (g_1 g'_1, g_2 g'_2)$. החבורה המתקבלת היא המכפלה הישרה החיצונית של G_1, G_2 .

תרגיל 3.31 (*) $G_1 \times G_2$ היא חבורה. איבר היחידה הוא $(1_{G_1}, 1_{G_2})$, וההפכי של איבר נתון על-ידי $(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$.

3.6 תת-חבורות

תהי G חבורה.

הגדרה 3.32 תת-קבוצה לא ריקה $H \subseteq G$ היא תת-חבורה של G אם היא סגורה לכפל ולהיפוך, כלומר, לכל $x, y \in H$ מתקיים $xy \in H$ ו- $x^{-1} \in H$. במקרה זה H עצמה היא חבורה (עם הכפל המצומצם מ- G , ואותו איבר יחידה), מסמנים $H \leq G$.

תרגיל 3.33 (*) אם $N \leq H, H \leq G$ אז $N \leq G$.

4 משפט לגרנז'

מושגים. יוצרים ותת-החבורה הנוצרת. קוסט. מחזור, חילוף. סדר של איבר. משפט פרמה, משפט אוילר, שאריות ריבועיות. חבורה ציקלית. כפל של תת-חבורות.

4.1 יוצרים של חבורה ותת-החבורה הנוצרת

טענה 4.1 החיתוך של משפחה כלשהי של תת-חבורות של G הוא תת-חבורה.

תרגיל 4.2 (**). הוכח את הטענה.

תהי $X \subset G$ תת-קבוצה כלשהי של אברים בחבורה.

תרגיל 4.3 (**). הוכח שהחיתוך של כל תת-החבורות של G המכילות את X הוא תת-החבורה הקטנה ביותר המכילה את X (כלומר, זוהי תת-חבורה המכילה את X , ומוכלת בכל תת-חבורה אחרת המכילה את X).

תרגיל 4.4 (**). הוכח שהאוסף של כל המכפלות הסופיות ב- G של אברים מ- X או מ- $X^{-1} = \{x^{-1} : x \in X\}$, הוא תת-החבורה הקטנה ביותר המכילה את X .

הגדרה 4.5 תת-החבורה שהוגדרה בכל אחד משני התרגילים הקודמים נקראת **תת-החבורה הנוצרת על-ידי** X , ומסמנים אותה ב- $\langle X \rangle$. אם $G = \langle X \rangle$, אומרים ש- X היא **קבוצת יוצרים של** G .

תרגיל 4.6 (***) הוכח שתת-החבורה $\langle (1234), (13) \rangle$ של S_4 איזומורפית ל- D_4 .

4.1.1 יוצרים של S_n

הגדרה 4.7 מחזור באורך 2 ב- S_n נקרא **חילוף**. כלומר, החילופים הם איברים מהצורה (ij) .

איבר $x \neq 1$ בחבורה הוא (מסדר 2) אם $x^2 = 1$ (ראה סעיף 4.3).

תרגיל 4.8 (*) כל חילוף הוא איבר מסדר 2.

תרגיל 4.9 (**). S_n נוצרת על-ידי כל החילופים (ij) .

תרגיל 4.10 (***) S_n נוצרת על-ידי כל החילופים $(1j)$.

4.2 קוסטים ומשפט לגרנז'

תהינה G חבורה ו- $H \leq G$ תת-חבורה. לכל $x \in G$, אנו מסמנים $Hx = \{hx : h \in H\}$ ו- $xH = \{xh : h \in H\}$.

הגדרה 4.11 הקבוצות Hx נקראות קוסטים שמאליים של H , והקבוצות xH - קוסטים ימניים של H .

נגדיר יחס שקילות על החבורה G : $x \equiv_H y$ אם $xy^{-1} \in H$.

תרגיל 4.12 (**). הוכח שהיחס \equiv_H הוא יחס שקילות.

תרגיל 4.13 (*). מחלקות השקילות של היחס \equiv_H הן מהצורה Hx .
הסק: כמחלקות שקילות, שתי מחלקות Hx, Hy הן או שוות או נחתכות באופן ריק (קל להוכיח זאת כמובן גם באופן ישיר).

תרגיל 4.14 (**). Hy היא קבוצת האיברים $x \in G$ שעבורם $y \in Hx$.

תרגיל 4.15 (**). לכל $x, y \in G$, $|Hx| = |Hy|$, ובפרט $|Hx| = |H|$.

הגדרה 4.16 האינדקס (השמאלי) של H ב- G הוא מספר הקוסטים השמאליים של H בחבורה. את האינדקס מסמנים ב- $[G:H]$.

תרגיל 4.17 (**+). האינדקס הימני של H ב- G הוא מספר הקוסטים הימניים. הוכח שהאינדקס הימני תמיד שווה לשמאלי. **הדרכה.** חשוב על הפונקציה $Hx \mapsto x^{-1}H$ (מדוע לא $Hx \mapsto xH$?)

משפט 4.18 (משפט לגרנז') אם $H \leq G$ חבורות סופיות, אז $|H|$ מחלק את $|G|$.

תרגיל 4.19 (**). הראה ש- $|G| = |H| \cdot [G:H]$, והסק את משפט לגרנז'.

4.3 סדר של איבר

הגדרה 4.20 יהי $a \in G$. הסדר של האיבר a הוא $n > 0$ הקטן ביותר שעבורו $a^n = 1$, אם קיים כזה; אחרת אומרים שהסדר הוא אינסוף. אנו מסמנים את הסדר ב- $o(a)$.

תרגיל 4.21 (**). הוכח שהסדר של a שווה לסדר של תת-החבורה הנוצרת, $\langle a \rangle$.

תרגיל 4.22 (*). הסדר של איבר $a \in G$ מחלק את סדר החבורה.

טענה 4.23 $x^n = 1$ אם ורק אם $n \mid o(x)$.

תרגיל 4.24 (**). אם $x, y \in G$ מתחלפים ו- $(o(x), o(y)) = 1$, אז $o(xy) = o(x)o(y)$.

תרגיל 4.25 (**-). הסדר של (x, y) בחבורה $G \times H$ הוא הכפולה המשותפת המינימלית $[o(x), o(y)]$. **הדרכה.** הראה ש- $o(xy) \mid o(x)o(y)$, ומצא הצבה מתאימה כדי להוכיח $o(x)o(y) \mid o(xy)$.

תרגיל 4.26 (**). מצא ב- S_7 איבר מסדר 5, 6, 7, 10. למה אין איבר מסדר 8?

4.4 יישומים בתורת המספרים

תרגיל 4.27 (*) אם p ראשוני אז $\varphi(p) = p - 1$ ו- $|U_p|$.

נזכיר ששדה הוא מבנה אלגברי F עם חיבור וכפל, שבו $(F, +, 0)$ חבורה אבלית, $(F - \{0\}, \cdot, 1)$ חבורה אבלית, והכפל דיסטריוטיבי ביחס לחיבור.

תרגיל 4.28 (***) אם p ראשוני, אז \mathbb{Z}_p (עם החיבור והכפל מודולו p) הוא שדה.

תרגיל 4.29 (**+) מצא את האברים מסדר 2 ב- U_p .

משפט 4.30 (משפט פרמה הקטן) אם p ראשוני, אז לכל a זר ל- p , $a^{p-1} \equiv 1 \pmod{p}$.

תרגיל 4.31 (***) הוכח את המשפט, על-ידי התבוננות בסדר של $[a] \in U_p$.

משפט 4.32 (משפט אוילר) לכל n , אם a זר ל- n , $a^{\phi(n)} \equiv 1 \pmod{n}$.

4.4.1 פונקציית אוילר

4.4.2 שאריות ריבועיות

4.4.3 בדיקת ראשוניות

4.5 שימושים להצפנה

4.5.1 RSA

4.5.2 שיטת רבין

4.6 חבורות ציקליות

4.33 הגדרה חבורה הנוצרת על-ידי איבר יחיד נקראת חבורה ציקלית.

במילים אחרות, חבורה G היא ציקלית אם יש איבר $x \in G$ כך שכל איבר בחבורה הוא חזקה של x .

תרגיל 4.34 (***) כל חבורה מסדר ראשוני היא ציקלית.

תרגיל 4.35 (*) הוכח שחבורה ציקלית היא אבלית.

תרגיל 4.36 (**+) הוכח שחבורה מסדר n היא ציקלית אם ורק אם יש בה איבר מסדר n .

4.6.1 יחידות

תרגיל 4.37 (*) הראה שכל החבורות \mathbb{Z}_n ציקליות. הראה שהחבורה \mathbb{Z} ציקלית.

משפט 4.38 כל חבורה ציקלית מסדר n איזומורפית ל- \mathbb{Z}_n ; כל חבורה ציקלית מסדר אינסופי איזומורפית ל- \mathbb{Z} .

4.6.2 תת-חבורות של חבורה ציקלית

תרגיל 4.39 (+)** כל תת-חבורה של \mathbb{Z} היא מהצורה $n\mathbb{Z}$ עבור n מתאים. **הזרנה.** הזכר בהוכחה של משפט 1.17.

טענה 4.40 כל תת-חבורה של חבורה ציקלית היא ציקלית.

תרגיל 4.41 (+)** הסדר של a , כאיבר בחבורה \mathbb{Z}_n , הוא $\frac{n}{(n,a)}$.

משפט 4.42 בחבורה ציקלית מסדר n יש תת-חבורה יחידה מכל סדר $d \mid n$.

תרגיל 4.43 (-)** הוכח את המשפט. **הזרנה.** תהי H תת-חבורה מסדר d . מכיוון שהיא ציקלית, יש בה $\varphi(d)$ אברים מסדר d , וזה מספרם בחבורה כולה.

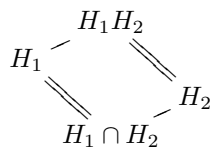
4.6.3 מכפלה של חבורות ציקליות

משפט 4.44 $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$ אם ורק אם $(n, m) = 1$.

תרגיל 4.45 (*)** הוכח את המשפט. **הזרנה.** לכיוון " \Leftarrow " העזר בקיום איבר מסדר nm בחבורה \mathbb{Z}_{nm} . לכיוון " \Rightarrow " הפעל את משפט 1.17.

4.7 כפל תת-חבורות

משפט 4.46 המכפלה $H_1 H_2$ של תת-חבורות H_2, H_1 היא תת-חבורה אם ורק אם $H_1 H_2 = H_2 H_1$.



טענה 4.47 אם $H_1, H_2 \leq G$ תת-חבורות מתחלפות, אז $[H_1 H_2 : H_1] = [H_2 : H_1 \cap H_2]$.

במלים אחרות (כאשר $H_1 H_2$ סופיות), $|H_1 H_2| = \frac{|H_1| \cdot |H_2|}{|H_1 \cap H_2|}$.

תרגיל 4.48 (-)** הוכח את הטענה. **הזרנה.** הגדר פונקציה $f: H_1 \times H_2 \rightarrow H_1 H_2$.

5 הומומורפיזמים ותת-חבורות נורמליות

מושגים: הומומורפיזם. גרעין ותמונה. תת-חבורה נורמלית. חבורת מנה. משפט האיזומורפיזם הראשון.

5.1 הומומורפיזמים

הגדרה 5.1 תהינה G ו- H חבורות. הומומורפיזם (של חבורות) $\phi: G \rightarrow H$ הוא פונקציה המקיימת את האקסיומות $\phi(xy) = \phi(x)\phi(y)$, $\phi(1_G) = \phi(1_H)$, ו- $\phi(x^{-1}) = \phi(x)^{-1}$ לכל $x, y \in G$.

5.2 גרעין ותמונה

יהי $\phi: G \rightarrow H$ הומומורפיזם.

הגדרה 5.2 הגרעין של ϕ הוא אוסף האיברים $\text{Ker}(\phi) = \{g \in G: \phi(g) = 1\}$. התמונה של ϕ הוא אוסף האיברים $\text{Im}(\phi) = \{\phi(x): x \in G\}$.

תרגיל 5.3 ()** לכל הומומורפיזם $\phi: G \rightarrow H$, $\text{Ker}(\phi)$ היא תת-חבורה של G , ו- $\text{Im}(\phi)$ היא תת-חבורה של H .

תרגיל 5.4 ()** נניח ש- G נוצרת על-ידי קבוצת יוצרים X . אם שני הומומורפיזמים $\phi, \phi': G \rightarrow H$ מסכימים על X , אז הם מתלכדים.

הגדרה 5.5 הומומורפיזם $\phi: G \rightarrow H$ נקרא מונומורפיזם (או: שיכון) אם הוא חד-חד-ערכי, ואפימורפיזם אם הוא על.

5.3 תת-חבורה נורמלית

תרגיל 5.6 (*) אם H תת-חבורה של G , אז לכל $g \in G$ גם gHg^{-1} תת-חבורה.

משפט 5.7 התכונות הבאות של תת-חבורה $H \leq G$ שקולות:

$$1. \quad g \in G \text{ לכל } gHg^{-1} \subseteq H$$

$$2. \quad g \in G \text{ לכל } gHg^{-1} = H$$

$$3. \quad g \in G \text{ לכל } gH = Hg$$

4. כל קוסט ימני הוא גם קוסט שמאלי.

5. כל קוסט שמאלי הוא גם קוסט ימני.

הגדרה 5.8 במקרה ש- $H \leq G$ מקיימת את התכונות שבמשפט, אומרים שהיא תת-חבורה נורמלית, ומסמנים $H \triangleleft G$.

תרגיל 5.9 ()** הגרעין של כל הומומורפיזם $G \rightarrow H$ הוא תת-חבורה נורמלית של G (ראה משפט 5.17).

תרגיל 5.10 ()** אם $[G:H] = 2$ אז H נורמלית ב- G .

הגדרה 5.11 חבורה G היא פשוטה אם אין לה תת-חבורות נורמליות.

תרגיל 5.12 ()** נתון ש $G_1 \subseteq G_2 \subseteq \dots \subseteq G_n \subseteq \dots$ חבורות פשוטות. הוכח שגם $G = \bigcup_n G_n$ פשוטה.

5.4 חבורת מנה

כפל של קוסטים מוגדר כפי שמוגדר בסעיף 4.7 כפל של כל שתי תת-קבוצות.

משפט 5.13 המכפלה של כל שני קוסטים שמאליים של H היא קוסט שמאלי, אם ורק אם H נורמלית.

הוכחה. אם $H \triangleleft G$ אז $Hx \cdot Hy = H(xH)y = HHxy = Hxy$. בכיוון ההפוך נניח שלכל x, y יש z כך ש- $HxHy = Hz$; נבחר $y = 1$, אז לכל x יש z כך ש- $xH = Hz$. ואז $xH \subseteq HxH = Hz$ ואז H נורמלית (תרגיל).

□

תרגיל 5.14 (*)** תת-חבורה $H \leq G$ היא נורמלית אם ורק אם הפעולה $(Ha, Hb) \mapsto Hab$ על קבוצת הקוסטים השמאליים מוגדרת היטב.

תרגיל 5.15 ()** אם $N \triangleleft G$, הקבוצה G/N של הקוסטים של N ב- G , עם הפעולה $Na \cdot Nb = Nab$, היא חבורה, שאיבר היחידה שלה הוא N . האיבר ההפכי מחושב על-ידי $(Na)^{-1} = Na^{-1}$.

הגדרה 5.16 אם $N \triangleleft G$, החבורה G/N נקראת **חבורת המנה**, או **מודולו N** .

משפט 5.17 תת-חבורה $H \leq G$ היא נורמלית אם ורק אם היא גרעין של הומומורפיזם מ- G לחבורה כלשהי.

תרגיל 5.18 ()** יהי F שדה. נסמן ב- $B_n(F)$ את חבורת המטריצות המשולשיות-עליונות ההפיכות מעל F , ב- $U_n(F)$ את החבורה של מטריצות ב- $B_n(F)$ שרכיבי האלכסון שלהן כולם 1, וב- $T_n(F)$ את אוסף המטריצות הסקלריות ההפיכות. הוכח ש- $U_n(F) \triangleleft B_n(F)$, $U_n(F) \triangleleft T_n(F)$, $B_n(F)/U_n(F) \cong T_n(F)$, $U_n(F)T_n(F) = B_n(F)$, ו- $U_n(F) \cong \text{SL}_n(F)$. $T_n(F) = \text{GL}_n(F)$

תרגיל 5.19 ()** נסמן $B = \{A \in M_2(\mathbb{R}) : \det(A) = \pm 1\}$. הוכח ש- $B \triangleleft \text{GL}_n(\mathbb{R})$ ו- $\text{GL}_n(\mathbb{R})/B \cong \mathbb{R}^\times / \langle -1 \rangle \cong (\mathbb{R}^+)^{\times}$

5.5 משפט האיזומורפיזם הראשון

משפט 5.20 (משפט האיזומורפיזם הראשון) יהי $\varphi : G \rightarrow H$ הומומורפיזם של חבורות. אז $G/\text{Ker}(\varphi) \cong \text{Im}(\varphi)$.

משפט האיזומורפיזם הראשון שימושי כל-כך, עד שמעתה, אם נרצה להוכיח שחבורת מנה G/N איזומורפית לחבורה אחרת, כמעט לעולם לא נעשה זאת באופן ישיר, במקום זה, נבנה איזומורפיזם מ- G אל החבורה המבוקשת ש- N היא הגרעין שלו.

תרגיל 5.21 (*)** הוכח את המשפט.

תרגיל 5.22 (*) אם $\varphi : G \rightarrow H$ על, אז $H \cong G/\text{Ker}(\varphi)$, כלומר: H איזומורפית ל-חבורת מנה של G .

6 סריג תת-החבורות

מושגים: חיתוך, מכפלה. תת-חבורות משלימות. קומוטטורים. מכפלה ישרה פנימית. משפט האיזומורפיזם השני. משפט האיזומורפיזם השלישי. סריג, מודולריות. משפט ההתאמה.

6.1 חיתוך ומכפלה של תת-חבורות

תרגיל 6.1 ()** אם $H \leq G$ ו- $N \triangleleft G$, אז $N \cap H \triangleleft H$. מצא דוגמה נגדית ל- $N \cap H \triangleleft N$.

תרגיל 6.2 ()** אם $N_1, N_2 \triangleleft G$, אז גם $N_1 \cap N_2 \triangleleft G$.

תרגיל 6.3 (*) תהינה $H_1, H_2 \leq G$.
 א. אם H_1 או H_2 נורמלית, אז $H_1 H_2$ תת-חבורה של G .
 ג. אם שתיהן נורמליות, אז $H_1 H_2 \triangleleft G$.

6.2 מכפלה ישרה פנימית

תת-חבורות $H, K \leq G$ הן **משלימות** אם $H \cap K = 1$ ו- $HK = G$.

תרגיל 6.4 (*) הראה שאם H, K משלימות אז $HK = KH$.

תרגיל 6.5 (*) נניח ש- H, K משלימות. אז לכל איבר $g \in G$ יש הצגה יחידה בצורה $g = hk$ עבור $h \in H$ ו- $k \in K$.

איבר מהצורה $[x, y] = xyx^{-1}y^{-1}$ נקרא **קומוטטור** (משום שהוא מודד באיזו מידה x ו- y מתחלפים, או אינם מתחלפים, זה עם זה).

תרגיל 6.6 (*) $[x, y] = 1$ אם ורק אם $xy = yx$.

הגדרה 6.7 תהינה $A, B \leq G$. $[A, B]$ היא תת-חבורה של G הנוצרת על-ידי הקומוטטורים $[a, b]$ עבור $a \in A, b \in B$.

תרגיל 6.8 (*) $[A, B] = 1$ אם ורק אם כל איבר $a \in A$ מתחלף עם כל איבר $b \in B$.

הגדרה 6.9 G היא **מכפלה ישרה פנימית של תת-חבורות** H, K אם H, K משלימות, ו- $[H, K] = 1$.

תרגיל 6.10 (*) אם G אבלית ו- H, K משלימות, אז G היא מכפלה ישרה שלהן.

תרגיל 6.11 ()** תהינה H, K תת-חבורות משלימות. הוכח: $[H, K] = 1$ אם ורק אם $H, K \triangleleft G$.

משפט 6.12 אם G מכפלה ישרה פנימית של H, K , אז $G \cong H \times K$.

תרגיל 6.13 ()** הוכח את המשפט. **הזרקה.** הגדר $\varphi: H \times K \rightarrow G$ לפי $\varphi(h, k) = hk$.

6.2.1 מכפלה ישרה של כמה תת-חבורות

6.3 משפטי האיזומורפיזם

בתרגילים לעיל הוכחנו שאם $H \leq G$ ו- $N \triangleleft G$, אז NH חבורה, $N \triangleleft NH$, ו- $N \cap H \triangleleft H$.
משפט 6.14 (משפט האיזומורפיזם השני) תהי G חבורה עם תת-חבורה H ותת-חבורה נורמלית N . אז $NH/N \cong H/N \cap H$.

תרגיל 6.15 ()** הוכח את המשפט. **הדרכה.** הגדר $\varphi: H \rightarrow NH/N$ לפי $\varphi(h) = hN$.

משפט 6.16 (משפט האיזומורפיזם השלישי) תהיינה $K \leq N$ תת-חבורות נורמליות של חבורה G . אז $(G/K)/(N/K) \cong G/N$.

תרגיל 6.17 ()** הוכח את המשפט. **הדרכה.** הגדר $\varphi: G/K \rightarrow G/N$ לפי $\varphi(gK) = gN$.

6.4 סריג תת-החבורות

6.4.1 סריגים

הגדרה 6.18 קבוצה Λ עם יחס סדר חלש \leq נקראת **סריג** אם לכל $a, b \in \Lambda$ יש חסם עליון וחסם תחתון לקבוצה $\{a, b\}$. במלים אחרות, מקסימום לקבוצה $\{x: x \leq a, x \leq b\}$, ומינימום לקבוצה $\{x: a \leq x, b \leq x\}$. את הראשון מסמנים $a \wedge b$ ואת השני $a \vee b$.

6.4.2 הסריג של תת-החבורות

טענה 6.19 אוסף תת-החבורות של חבורה, עם יחס ההכלה, הוא סריג.

6.4.3 מודולריות

6.5 אינדקס של תת-חבורות

תרגיל 6.20 (*)** תהיינה $A, B \leq G$ תת-חבורות.

$$1. [A: A \cap B] \leq [G: B]. \text{ הדרכה. הגדר } f: A \rightarrow \{aB: a \in A\} \text{ על.}$$

$$2. [A: A \cap B] = [G: B] \text{ אם ורק אם } G = AB.$$

$$3. \text{הסק ש- } [G: A \cap B] \leq [G: A] \cdot [G: B].$$

$$4. \text{אם } AB \leq G \text{ (בפרט, אם } A \triangleleft G \text{ או } B \triangleleft G), \text{ אז } [AB: A \cap B] = [AB: A] \cdot [AB: B].$$

6.6 משפט ההתאמה

משפט 6.21 יהי $\varphi: G \rightarrow H$ הומומורפיזם, עם גרעין $K = \text{Ker}(\varphi)$. נסמן ב- \mathcal{L}_G את אוסף תת-החבורות של G המכילות את K , וב- \mathcal{L}_H את אוסף כל תת-החבורות של $\text{Im} \varphi$. אז קיימת התאמה חד-חד-ערכית ועל $\alpha: \mathcal{L}_G \rightarrow \mathcal{L}_H$, המקיימת:

$$1. \text{(מונוטוניות) עבור } G_1, G_2 \in \mathcal{L}_G \text{ אם ורק אם } G_1 \leq G_2 \text{ אז } \alpha(G_1) \leq \alpha(G_2).$$

$$2. \text{(שמירה על חיתוך) } \alpha(G_1 \cap G_2) = \alpha(G_1) \cap \alpha(G_2).$$

3. $\alpha(G_1G_2) = \alpha(G_1)\alpha(G_2)$ (שמירה על מכפלה)
4. $[G_1:G_2] = [\alpha(G_1):\alpha(G_2)]$ או $G_2 \subseteq G_1$ אם $G_2 \subseteq G_1$ (שמירה על אינדקס)
5. $\alpha(N) \triangleleft \alpha(H)$ אם ורק אם $N \triangleleft H, N, H \in \mathcal{L}_2$ (שמירה על נורמליות)
6. $H/N \cong \alpha(H)/\alpha(N)$ או $N \triangleleft H$ מקיימות $N, H \in \mathcal{L}_1$ (שמירה על מנות)

7 הצמדה ומחלקות הצמידות

מושגים: מרָפֵז. הקוטרניונים. מרָפֵז של איבר ושל תת-חבורה. מחלקת צמידות. שוויון המחלקות.

7.1 המרָפֵז

הגדרה 7.1 תהי G חבורה. המרָפֵז $Z(G) = \{z \in G : \forall x \in G : zx = xz\}$ הוא אוסף האיברים המתחלפים עם כל אברי G .

תרגיל 7.2 (*) $Z(G) \triangleleft G$

תרגיל 7.3 (**). תהי G חבורה. אם $G/Z(G)$ חבורה ציקלית, אז G אבליית.

7.1.1 המרָפֵז של S_n

טענה 7.4 שני מחזוריים $\sigma, \tau \in S_n$ מתחלפים אם ורק אם הם (כלומר - התומכים שלהם) זרים.

תרגיל 7.5 (**). נניח $n \geq 3$ אז $Z(S_n) = 1$

7.2 מרָפֵזים

7.2.1 מרָפֵז של איבר

תהי G חבורה עם איבר $a \in G$.

הגדרה 7.6 המרָפֵז של a הוא אוסף האיברים $C_G(a) = \{x \in G : xa = ax\}$

תרגיל 7.7 (*) הראה ש- $C_G(a)$ היא תת-חבורה של G .

תרגיל 7.8 (**). $C_G(gxg^{-1}) = g \cdot C_G(x) \cdot g^{-1}$

7.2.2 מרָפֵז של תת-חבורה

תהי $H \leq G$ תת-חבורה.

הגדרה 7.9 המרָפֵז של H ב- G הוא $C_G(H) = \{g \in G : (\forall h \in H) gh = hg\}$

תרגיל 7.10 (*) $C_G(H)$ תת-חבורה של G .

תרגיל 7.11 (**). אם $A \subseteq B$ אז $C_G(B) \subseteq C_G(A)$

תרגיל 7.12 (**). $H \subseteq C_G(C_G(H))$

תרגיל 7.13 (**). לכל תת-חבורה $H \leq G$, $C_G(C_G(C_G(H))) = C_G(H)$

7.3 מחלקות צמידות

הגדרה 7.14 אברים $x, y \in G$ הם צמודים אם קיים $g \in G$ כך ש- $y = gxg^{-1}$. במקרה זה מסמנים $x \sim y$.

תרגיל 7.15 (*) יחס הצמידות \sim הוא יחס שקילות. (המחלקות נקראות מחלקות צמידות, ומסמנים אותן ב-[x]).

משפט 7.16 לכל $a \in G$, $|[a]|$ שווה לאינדקס $[G : C_G(a)]$.

7.3.1 מחלקות צמידות ב- S_n

הגדרה 7.17 תהי $\sigma \in S_n$ מכפלה של מחזורים זרים מאורכים n_1, \dots, n_t , כאשר $n_1 \leq \dots \leq n_t$, $n_1 + \dots + n_t = n$. מבנה המחזורים של σ הוא הוקטור $[n_1, \dots, n_t]$. אם ערך מסויים חוזר על עצמו, נשתמש בסימון החזקה למען הקיצור.

לדוגמא, מבנה המחזורים של הזהות הוא $[1, \dots, 1]$, אז $[1^n]$. מבנה המחזורים של $(1234)(56)(78) \in S_9$ הוא $[4, 2^2, 1]$ (ולא $[4, 2^2]$ - המטרה היא שאפשר יהיה לקרוא את n מתוך מבנה המחזורים).

משפט 7.18 תמורות הן צמודות ב- S_n אם ורק אם יש אותו מבנה מחזורים.

תרגיל 7.19 (***) הוכח את הכיוון הראשון של המשפט: תהי σ תמורה עם מבנה מחזורים $[n_1, \dots, n_t]$. הראה של- $\tau\sigma\tau^{-1}$ אותו מבנה מחזורים.

תרגיל 7.20 (***) הוכח את הכיוון השני: אם ל- σ ו- τ אותו מבנה מחזורים, אז הן צמודות. **הדרכה.** כתוב את התמורות זו מעל זו, בהתאמה למבנה המחזורים.

7.3.2 מחלקות צמידות בתת-חבורה

7.4 שוויון המחלקות

שוויון המחלקות של חבורה G הוא השוויון

$$|G| = |Z(G)| + \sum_{C \subseteq G, |C| \neq 1} |C|,$$

כאשר הסכום הוא על כל מחלקות הצמידות הלא-טריביואליות של החבורה.

תרגיל 7.21 (**) הוכח את שוויון המחלקות. **הדרכה.** פרק את החבורה למחלקות צמידות.

7.4.1 חבורות- p

הגדרה 7.22 יהי p ראשוני. חבורת- p (סופית) היא חבורה מסדר p^t ל- t כלשהו.

משפט 7.23 המרכז של חבורת- p אינו טריביואלי.

תרגיל 7.24 (***) הוכח את המשפט. **הדרכה.** שוויון המחלקות; הגודל של כל מחלקת צמידות הוא חזקה של p .

תרגיל 7.25 (**) כל חבורה מסדר p^2 היא אבלית. **הדרכה.** תרגיל 7.3.

תרגיל 7.26 (**) כל חבורה מסדר p^2 איזומורפית ל- \mathbb{Z}_{p^2} או ל- $\mathbb{Z}_p \times \mathbb{Z}_p$. **הדרכה.** אם יש איבר מסדר p^2 סיימנו. אחרת קח שני איברים מסדר p , x, y , כך ש- $\langle x \rangle \not\subseteq \langle y \rangle$, והראה ש- $G = \langle x, y \rangle \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

8 אוטומורפיזמים

מושגים: אוטומורפיזם, אוטומורפיזם פנימי. חבורת האוטומורפיזמים, חבורת האוטומורפיזמים הפנימיים, חבורת האוטומורפיזמים החיצוניים. גרף קיילי. המנרמל. משפט N/C . תת-חבורות צמודות. תת-חבורה קרקטריסטית. חבורה פשוטה.

8.1 חבורת האוטומורפיזמים

הגדרה 8.1 איזומורפיזם מחבורה אל עצמה נקרא אוטומורפיזם.

הגדרה 8.2 אוסף האוטומורפיזמים של חבורה G נקרא 'חבורת האוטומורפיזם של G ', ומסמנים אותו בסימון $\text{Aut}(G)$.

תרגיל 8.3 (*) $\text{Aut}(G)$ היא אכן חבורה.

תרגיל 8.4 ()** הוכח ש- $\text{Aut}(\mathbb{Z}_n) \cong U_n$. **הזרקה.** הגדר $\Phi: \text{Aut}(\mathbb{Z}_n) \rightarrow U_n$ לפי $\Phi(\phi) = \phi(1)$.

8.1.1 אוטומורפיזמים פנימיים

לא תמיד קל לבנות ולגלות אוטומורפיזמים. עם זאת, יש אוטומורפיזמים שהחבורה תורמת במו ידיה, והם קושרים אל חבורת האוטומורפיזמים מושגים שפגשנו בפרקים הקודמים.

הגדרה 8.5 לכל $g \in G$, נגדיר $\gamma_g: G \rightarrow G$ לפי $\gamma_g(h) = ghg^{-1}$. נקרא אוטומורפיזם פנימי, או אוטומורפיזם של הצמדה.

תרגיל 8.6 (*) $\gamma_g \in \text{Aut}(G)$.

תרגיל 8.7 ()** $\gamma_g \circ \gamma_h = \gamma_{gh}$.

תרגיל 8.8 (*)** נגדיר $\Gamma: G \rightarrow \text{Aut}(G)$ לפי $\Gamma(g) = \gamma_g$.
א. הוכח ש- Γ הומומורפיזם.

ב. הראה ש- $\text{Ker } \Gamma = Z(G)$, והסק ש- $\text{Inn}(G) \cong G/Z(G)$.

תרגיל 8.9 (*) לכל $\varphi \in \text{Aut}(G)$ ו- $g \in G$, $\varphi \circ \gamma_g \circ \varphi^{-1} = \gamma_{\varphi(g)}$.
הסק ש- $\text{Inn}(G) = \{\gamma_g : g \in G\}$ היא תת-חבורה נורמלית של $\text{Aut}(G)$.

8.1.2 העלאה בחזקה

לחבורה יש 'יותר' אוטומורפיזמים של הצמדה ככל שהיא 'פחות' אבלית, וכאשר החבורה אבלית אין בכלל אוטומורפיזמים כאלה. מאידך, יש מקור אספקה אחר לאוטומורפיזמים של לחבורות אבליות, שחשיבותו תתברר כשנחקור את המבנה של החבורות האלה.

הגדרה 8.10 לכל $m \in \mathbb{Z}$, נסמן $\mu_m: G \rightarrow G$ לפי $\mu_m: g \mapsto g^m$.

תרגיל 8.11 (*) אם G אבלית אז $\mu_m: G \rightarrow G$ היא הומומורפיזם.

תרגיל 8.12 ()** אם G אבלית ו- $(m, |G|) = 1$, אז $\mu_m \in \text{Aut}(G)$.

8.1.3 אוטומורפיזמים של גרפים

8.2 המנרמל

תהי H תת-חבורה של G .

תרגיל 8.13 (*) אם $H \triangleleft G$ ורק אם $\gamma_g(H) = H$ לכל $g \in G$.

הגדרה 8.14 המנרמל של H ב- G הוא $N_G(H) = \{g \in G : gHg^{-1} = H\}$.

תרגיל 8.15 (*) $N_G(H)$ היא תמיד תת-חבורה של G .

תרגיל 8.16 (*) $H \triangleleft N_G(H)$.

תרגיל 8.17 (***) $N_G(H)$ היא תת-החבורה הגדולה ביותר של G שבה H נורמלית. יתרה מזו, אם $H' \leq H \leq G$, אז $H \triangleleft H'$ אם ורק אם $N_G(H) \subseteq N_G(H')$.

משפט 8.18 (משפט N/C) תהי $H \leq G$. קיים שיכון $N_G(H)/C_G(H) \hookrightarrow \text{Aut}(H)$.

תרגיל 8.19 (***) הוכח את המשפט. **הדרכה.** הגדר $\varphi : N_G(H) \rightarrow \text{Aut}(H)$ לפי $\varphi : g \mapsto \gamma_g$. הוכח שהפונקציה הזו מוגדרת היטב (לשם כך הגדרנו את המנרמל!), וחשב את הגרעין שלה.

8.2.1 תת-חבורות צמודות

הזכר בתרגיל 5.6, שלפיו כל תת-חבורה $H \leq G$ מוקפת בענף של תת-חבורות צמודות מהצורה gHg^{-1} . אלו תת-החבורות הצמודות ל- H .

תרגיל 8.20 (*) אם H_1, H_2 צמודות, אז הן איזומורפיות.

תרגיל 8.21 (*) $N_G(gHg^{-1}) = gN_G(H)g^{-1}$.

תרגיל 8.22 (*) $C_G(gHg^{-1}) = gC_G(H)g^{-1}$.

תרגיל 8.23 (***) $C_G(H) \triangleleft N_G(H)$.

משפט 8.24 מספר תת-החבורות של G הצמודות ל- H שווה ל- $[G : N_G(H)]$.

9 חבורות של תמורות

מושגים: משפט קיילי, העידון שלו. סימן של תמורה. חבורת התמורות הזוגיות. הלמה של Burnside.

9.1 משפט קיילי

בסעיף זה נראה שכל חבורה היא למעשה חבורה של תמורות.

משפט 9.1 (משפט קיילי) כל חבורה G איזומורפית לתת-חבורה של החבורה הסימטרית S_G .

זכור שאם G חבורה סופית, מסדר n , אז $S_G \cong S_n$. כלומר, המשפט נותן שיכון $G \hookrightarrow S_n$, כאשר $n = |G|$.

תרגיל 9.2 (***) הוכח את המשפט. **הדרכה.** הגדר $\Psi : G \rightarrow S_G$ לפי $\Psi(g) : x \mapsto gx$. הראה ש- $\Psi(gh) = \Psi(g)\Psi(h)$ והסק ש- Ψ מוגדרת היטב **כלומר**, בהקשר הנכחי, היא אחזירה תמונות ולא סתם פונקציות $G \rightarrow G$.

9.1.1 העידון של משפט קיילי

9.2 הסימן של תמורה

תהי $\sigma \in S_n$ תמורה. נאמר שהזוג (i, j) מפרסדר אם $i < j$ ו- $\sigma i > \sigma j$.

הגדרה 9.3 הסימן של $\sigma \in S_n$ מוגדר לפי הזוגיות של מספר הפרות הסדר ביחס ל- σ : $\text{sgn}(\sigma) = (-1)^{|\{i, j : i < j, \sigma i > \sigma j\}|}$.

טענה 9.4 העתקת הסימן $\text{sgn} : S_n \rightarrow \{\pm 1\}$ היא הומומורפיזם.

תרגיל 9.5 (*)** הוכח את טענה 9.4, כלומר, הראה ש- $\text{sgn}(\sigma\tau) = \text{sgn}(\sigma)\text{sgn}(\tau)$. **הדרכה.** חלק את הזוגות (i, j) שבהם $i < j$ לארבע קבוצות, לפי התכונות $\tau(i) < \tau(j)$ ו- $\sigma\tau(i) < \sigma\tau(j)$, וחשב את התרומה של כל זוג לכל אחד מהסימנים.

תרגיל 9.6 ()** יהי $\tau = (ab)$ חילוף. הוכח ש- $\text{sgn}(\tau) = -1$. בפרט, sgn היא על, לכל $n \geq 2$.

9.2.1 הסימן והדיסקרימיננטה

9.2.2 חבורת התמורות הזוגיות

בתרגיל 4.9 ראינו שכל תמורה אפשר לכתוב כמכפלה של חילופים.

טענה 9.7 הזוגיות של מספר החילופים בהצגה של תמורה σ היא קבועה. כלומר, אם $\sigma = \tau_1 \cdots \tau_k = \nu_1 \cdots \nu_t$ (כאשר τ_i, ν_j חילופים), אז $k \equiv t \pmod{2}$.

תרגיל 9.8 (*)** הוכח את הטענה. **הדרכה.** $\text{sgn}(\sigma) = (-1)^k = (-1)^t$.

הגדרה 9.9 $A_n = \text{Ker}(\text{sgn})$ היא חבורת התמורות הזוגיות. התמורות נקראות כק-של-ספ מספר החילופים בהצגות שלהן.

תרגיל 9.10 (*) $[S_n : A_n] = 2$.

תרגיל 9.11 ()** תן שלושה נימוקים לכך ש- $A_n \triangleleft S_n$. **הדרכה.** האינדקס שלה הוא 2; היא גרעין של הומומורפיזם; וכן ישירות מן ההגדרה.

9.2.3 יוצרים של A_n

תרגיל 9.12 (*)** A_n נוצרת על-ידי כל המחזורים מאורך 3. **הדרכה.** חשב את $(ijk)(jkt)$.

9.2.4 חבורה פשוטה A_n

9.3 תמורות מקריות

9.3.1 הלמה של Burnside

10 חבורות אבליות

מושגים: תת-חבורת הקומוטטורים. משפט קושי. אקספוננט. פירוק פרימרי. צורה קנונית של חבורה אבלית סופית. פיתול וחוסר פיצול. בסיס של חבורה אבלית.

10.1 תת-חבורת הקומוטטורים

הגדרה 10.1 תהי G חבורה. תת-חבורת הקומוטטורים של G היא תת-החבורה הנוצרת על-ידי הקומוטטורים; את תת-חבורת הקומוטטורים מסמנים G' .

משפט 10.2 G/G' היא המנה האבלית המקסימלית של G . ביתר פירוט:

- $G' \triangleleft G$.
- G/G' חבורה אבלית.
- לכל תת-חבורה $N \triangleleft G$, $N \subseteq G'$ (ואז G/N חבורת מנה של G/G').

10.1.1 יוצרים של חבורות קומוטטורים**10.2 משפט קושי**

משפט 10.3 יהי p ראשוני המחלק את הסדר של חבורה G . אז יש ב- G איבר מסדר p .

תרגיל 10.4 ()** הוכח את משפט קושי לחבורה סופית G כלשהי באמצעות פעולת הסיבוב על $X = \{(g_1, \dots, g_p) \in G^p : g_1 \cdots g_p = 1\}$. **הזרקה.** ראשית, $|X| = |G|^{p-1}$ מתחלק ב- p . וקטור אינו משתנה תחת סיבוב בדיוק כאשר $g_1 = \dots = g_p = 1$ ומספר הקטורים האלה מוכרח להתחלק ב- p .

10.3 האקספוננט

הגדרה 10.5 **האקספוננט של חבורה G** הוא המספר הקטן ביותר N כך ש- $a^N = 1$ לכל $a \in G$. מסמנים מספר זה ב- $\exp(G)$.

תרגיל 10.6 (*) האקספוננט של G הוא הכפולה המשותפת המינימלית של סדרי האיברים בה.

תרגיל 10.7 (*) $\exp(\mathbb{Z}/n\mathbb{Z}) = n$.

תרגיל 10.8 ()** $\exp(G)$ מחלק את $|G|$.

תרגיל 10.9 ()** ל- $\exp(G)$ יש אותם גורמים ראשוניים כמו ל- $|G|$.

תרגיל 10.10 (-)** $\exp(A \times B) = [\exp(A), \exp(B)]$.

תרגיל 10.11 (+)** אם G חבורה אבלית עם $\exp(G) = |G|$, אז היא ציקלית. **הזרקה.** פרק את $|G|$ לגורמים והפעל את תרגיל 4.24.

10.4 הפירוק הפרימרי

הזכר בהגדרה 8.10: אם A חבורה אבלית, $\mu_n: A \rightarrow A$ המוגדרת לפי $\mu_n(a) = a^n$ היא הומומורפיזם.

הגדרה 10.12 תהי A חבורה אבלית ויהי $\mu_n: A \rightarrow A$ הומומורפיזם של העלאה בחזקה. נסמן $A^n = \text{Im}(\mu_n) = \{a^n : a \in A\}$ ו- $A_n = \text{Ker}(\mu_n) = \{a \in A : a^n = 1\}$. אין קשר בין הסימון A_n לחבורת התאורות הצוליות של הצורה 9.9.

תרגיל 10.13 ()** תהי $A = \mathbb{Z}_n$. הראה שלכל $d | n$, $A_d \cong \mathbb{Z}_d$ ו- $A^d \cong \mathbb{Z}_n/d$. חשב את A_m ואת A^m עבור m כלשהו.

תרגיל 10.14 (+)** $\exp(A_n) | n$.

תרגיל 10.15 ()** נניח ש- $\exp(A) | nm$. אז $A^n \subseteq A_m$.

תרגיל 10.16 ()** אם $\exp(A) = nm$ ו- n, m זרים, אז $A^n = A_m$.

משפט 10.17 אם $\exp A = nm$ כאשר n, m זרים, אז $A \cong A_n \times A_m$.

תרגיל 10.18 (*)** הוכח את המשפט. **הזרנה.** כתוב $1 = \alpha n + \beta m$ והראה ש- $A_n \cap A_m = 1$ ו- $A \subseteq A^n A^m \subseteq A_n A_m$.

10.19 הגדרה חבורה שהסדר של כל איבר בה הוא חוקה של אותו ראשוני p , נקראת **חבורת- p** .

תרגיל 10.20 (*)** חבורה סופית היא חבורת- p אם ורק אם הסדר שלה הוא חזקה של p , אם ורק אם האקספוננט שלה חזקת- p .

משפט 10.21 כל חבורה אבלית סופית היא מכפלה ישרה של חבורות- p , שהן יחידות עדיכדי איזומורפיזם.

תרגיל 10.22 ()** הוכח את המשפט. **הזרנה.** קיום הפירוק באינדוקציה על משפט 10.17, לפי תרגיל 10.14.

10.5 חבורות p -אבליות

טענה 10.23 בחבורת- p יש איבר שסדרו שווה לאקספוננט.

תרגיל 10.24 ()** הוכח את הטענה. **הזרנה.** אחרת הסדר של כל האברים מחלק את $\exp(A)/p$.

משפט 10.25 אם g הוא איבר מסדר השווה לאקספוננט בחבורת- p אבלית A , אז תת-החבורה הציקלית שהוא יוצר היא מחובר ישר ב- A .

תרגיל 10.26 (*)** הוכח את המשפט. **הזרנה.** באינדוקציה. נניח ש- $A = \langle g \rangle$. ראשית, קיים מחוץ ל- H איבר x מסדר p , לפי משפט קושי על A/H והשוואת $x^p = g^i$. כעת $Q = \langle x \rangle$ מקיים $Q \cap H = 1$ ו- $\exp(A/Q) = \exp(A)$ כי $HQ/Q \cong H$. באינדוקציה קיים $Q \subseteq K \leq A$ כך ש- $A/Q = (HQ/Q) \oplus K/Q$ מכפלה ישרה, ואז $HK = HQK = A$ ו- $H \cap K \subseteq H \cap Q = 1$.

תרגיל 10.27 (*)** תהי $G = \mathbb{Z}_{p^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_t}}$. הראה ש- $[p^{m-1}G : p^m G] = p^{|\{i: \alpha_i = m\}|}$. בפרט, אפשר לקרוא את קבוצת הערכים $\alpha_1, \dots, \alpha_t$ מתוך G .

משפט 10.28 לכל חבורת- p אבלית סופית יש פירוק יחיד לסכום ישר של חבורות ציקליות, $G = \mathbb{Z}_{p^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_t}}$ כאשר $\alpha_1 \leq \cdots \leq \alpha_t$.

תרגיל 10.29 ()** הוכח את המשפט. **הזרנה.** הקיום באינדוקציה לפי משפט 10.25, והיחידות היא תרגיל 10.27.

10.6 משפט המיון לחבורות אבליות סופיות

משפט 10.30 כל חבורה אבלית סופית אפשר להציג באופן יחיד בצורה

$$\mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_t},$$

כאשר $d_1 \mid \cdots \mid d_t$.

צורה זו של החבורה נקראת הצורה הקנונית.

תרגיל 10.31 (*)** הוכח את המשפט. **הזרנה.** קיום: פרק את החבורה למכפלה של חבורות- p לפי משפט 10.21, ופרק כל אחת מאלה לסכום של t חבורות ציקליות לפי משפט 10.28. אסוף ל- \mathbb{Z}_{d_t} (תרגיל 4.44) את המרכיב הגדול ביותר בכל קבוצה, וכן הלאה. יחידות: הראה ש- $t = \max |A/pA|$, כאשר המקסימום על-פני כל הראשוניים המחלקים את $|A|$; הראה ש- $d_1 \mid p^\ell$ אם ורק אם $\log_p |p^{\ell-1}A/p^\ell A| = t$.

תרגיל 10.32 ()** הראה ש- $m\mathbb{Z}_n \cong \mathbb{Z}_{\frac{n}{(n,m)}}$.

תרגיל 10.33 ()** הראה שאם $A = \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_t}$, אז לכל m , הצורה הקנונית של mA היא $\mathbb{Z}_{\frac{d_1}{(d_1,m)}} \oplus \cdots \oplus \mathbb{Z}_{\frac{d_t}{(d_t,m)}}$.

תרגיל 10.34 (*)** הוכח את יחידות ההצגה באינדוקציה על הסדר. **פתרון.** חתי A חבורה אבלית, עם הצגה קנונית $\mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_t}$ (שאולי אינה יחידה). נניח, באינדוקציה, שמספר המרכיבים $\ell(B)$ בהצגה הקנונית של B מוגדר היטב לכל חבורה B מסדר קטן משל A . הראה (בעזרת תרגיל 10.33) ש- d_1 הוא הערך הקטן ביותר של m שעבורו $mA \subset A$ ו- $\ell(mA) < t$. נניח שיש שתי הצגה קנונית נוספת $\mathbb{Z}_{d'_1} \oplus \cdots \oplus \mathbb{Z}_{d'_t}$ עם $t \leq t'$ או $d_1 \mid d'_1$ ולכן המספרים $d_1/d'_1, \dots, d_t/d'_1$ ו- d'_1/d_1 ואלו שווים זה לזה בהתאמה; מכיון שבעני המקרים לחבורה אחוה סדר. גם מספר הערכים השווים ל- d'_1 שווה, ומכאן שההצגות שוות.

10.6.1 חבורות אוילר

10.7 חבורות אבליות אינסופיות

10.7.1 חבורות שאינן נוצרות סופית

11 מבוא לחוגים

מושגים: חוג, חוג קומוטטיבי, אידיאל שמאלי וימני, אידיאל. הומומורפיזם של חוגים, חוג מנה, משפט האיזומורפיזם הראשון. שדה, חוג פשוט. אידיאל ראשוני, אידיאל מקסימלי. מחלק אפס, תחום שלמות, שדה שברים. יחס החלוקה, חבורות. איבר אי-פריק ואיבר ראשוני. אידיאל ראשי, חוג ראשי. חוג אוקלידי, חוג פולינומים.

11.1 חוגים, תת-חוגים ואידיאלים

הגדרה 11.1 חוג (עם יחידה) הוא מבנה אלגברי הכולל קבוצה R עם פעולות חיבור וכפל, כך ש- $\langle R, +, 0 \rangle$ חבורה אבלית, $\langle R, \cdot, 1 \rangle$ מונוידי, ו- $a(b+c) = ab+ac$, $(a+b)c = ac+bc$.

אם R חוג, אזי $\langle R, +, 0 \rangle$ נקראת החבורה החיבורית של החוג, ו- $\langle R, \cdot, 1 \rangle$ המונויד הכפלי של החוג.

תרגיל 11.2 (*) \mathbb{Z} ו- \mathbb{Z}_n (לכל n טבעי) הם חוגים.

הגדרה 11.3 חוג הוא קומוטטיבי אם הכפל קומוטטיבי, כלומר $ab = ba$ לכל $a, b \in R$.

הגדרה 11.4 תת-חבורה חיבורית $S \subseteq R$ הכוללת את איבר היחידה וסגורה לכפל, נקראת תת-חוג.

הגדרה 11.5 המכפלה של תתי-קבוצות $A, B \subseteq R$ מוגדרת כאוסף כל הסכומים הסופיים $A \cdot B = \{a_1 b_1 + \dots + a_n b_n : a_1, \dots, a_n \in A, b_1, \dots, b_n \in B\}$.

הגדרה 11.6 תת-חבורה חיבורית $L \subset R$ היא אידיאל שמאלי אם $RL \subseteq L$, ואידיאל ימני אם $LR \subseteq L$. תתי-קבוצה שהיא אידיאל שמאלי וימני נקראת אידיאל. מסמנים, בהתאמה, $L \leq_\ell R$, $L \leq_r R$ ו- $L \triangleleft R$.

תרגיל 11.7 (*) תת-חבורה חיבורית $L \subset R$ היא אידיאל שמאלי אם ורק אם היא סגורה לכפל שמאלי מבחוץ, כלומר, לכל $a \in R$ ו- $x \in L$, $ax \in L$. נסח תנאי דואלי לאידיאלים ימניים.

תרגיל 11.8 (**-) לכל $a \in R$, $Ra = \{xa : x \in R\}$ הוא אידיאל שמאלי (או החוג R כולו).

תרגיל 11.9 (***) אם $I, J \triangleleft R$, אז $I + J \triangleleft R$ (או $I + J = R$) ו- $IJ \triangleleft R$ ו- $I \cap J \triangleleft R$.

תרגיל 11.10 (***) אם $L \leq_\ell R$ ו- $T \leq_r R$, אז $LT \triangleleft R$.

11.2 הומומורפיזמים וחוגי מנה

לכל תת-חבורה חיבורית $S \subseteq R$, מוגדרת חבורת המנה R/S ביחס לפעולת החיבור.

תרגיל 11.11 (***) (השווה לתרגיל 5.14) פעולת הכפל על R/I מוגדרת היטב אם ורק אם $I \triangleleft R$ (או $I = R$).

הגדרה 11.12 אם $I \triangleleft R$, החוג R/I ביחס לפעולות החיבור והכפל של קוסטים, נקרא חוג המנה ביחס ל- I .

תרגיל 11.13 (*) $n\mathbb{Z} \triangleleft \mathbb{Z}$ ו- $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ כחוגים.

הגדרה 11.14 פונקציה $\phi: R \rightarrow S$ היא הומומורפיזם (של חוגים) אם $\phi(1_R) = 1_S$ ו- $\phi(x+y) = \phi(x) + \phi(y)$ ו- $\phi(xy) = \phi(x)\phi(y)$.

איזומורפיזם, מונומורפיזם, אפימורפיזם, אנדומורפיזם ואוטומורפיזם של חוגים מוגדרים באותו אופן שהם מוגדרים לחבורות.

הגדרה 11.15 התמונה של הומומורפיזם ϕ היא תתי-קבוצה $\text{Im}(\phi) = \{\phi(x) : x \in R\}$. הגרעין הוא תתי-קבוצה $\text{Ker}(\phi) = \{x \in R : \phi(x) = 0\}$.

אלו הם למעשה התמונה והגרעין של ההומומורפיזם, כהומומורפיזם בין החבורות החיבוריות

תרגיל 11.16 (*) $\text{Im}(\phi)$ הוא תת-חוג של S , ו- $\text{Ker}(\phi)$ הוא אידיאל של R (שים לב ש- $\text{Ker}(\phi) \neq R$).

משפט 11.17 (משפט האיזומורפיזם הראשון) יהיו R, S חוגים, ו- $\phi: R \rightarrow S$ הומומורפיזם. אז $R/\text{Ker}(\phi) \cong \text{Im}(\phi)$.

הערה כמובן *Cauchy 5.20*.

תרגיל 11.18 (*)** נסח גרסאות של משפטי האיזומורפיזם השני והשלישי לחוגים.

11.3 אידיאלים בחוג קומוטטיבי

11.3.1 שדות

איבר a של חוג R הוא **הפיך** אם הוא הפיך במונויד הכפלי, כלומר, קיים $b \in R$ כך ש- $ab = ba = 1$.

הגדרה 11.19 שדה הוא חוג קומוטטיבי, שבו כל האיברים השונים מאפס הפיכים.

11.3.2 אידיאל ראשוני ומקסימלי

הגדרה 11.20 אידיאל $M \triangleleft R$ הוא **מקסימלי** אם אין אידיאלים $M \subset M' \triangleleft R$.

טענה 11.21 בחוג קומוטטיבי, $M \triangleleft R$ אם ורק אם R/M שדה.

הגדרה 11.22 יהי R חוג קומוטטיבי. אידיאל $P \triangleleft R$ הוא **ראשוני** אם לכל $A, B \triangleleft R$, אם $AB \subseteq P$ אז $A \subseteq P$ או $B \subseteq P$.

תרגיל 11.23 (*)** ראשוני P אם ורק אם לכל $a, b \in R$, אם $ab \in P$ אז $a \in P$ או $b \in P$.

הגדרה 11.24 איבר $a \in R$, $a \neq 0$ נקרא **מחלק אפס** אם קיים $b \neq 0$ כך ש- $ab = 0$.

הגדרה 11.25 חוג קומוטטיבי ללא מחלקי אפס נקרא **תחום שלמות**.

תרגיל 11.26 (*) כל שדה הוא תחום שלמות.

תרגיל 11.27 ()** כל תת-חוג של תחום שלמות הוא תחום שלמות.

משפט 11.28 יהי R חוג קומוטטיבי. $P \triangleleft R$ הוא ראשוני אם ורק אם R/P תחום שלמות.

תרגיל 11.29 ()** כל אידיאל מקסימלי הוא ראשוני.

11.3.3 אידיאלים ראשיים

11.30 הגדרה אידיאל מהצורה Ra של חוג קומוטטיבי R נקרא **אידיאל ראשי**. במקרה זה, a הוא יוצר של האידיאל.

למרות הצמיח בשמות, אין קשר בין ראשוניות וראשיות של אידיאלים. לפעמים מסמנים את Ra בסימון $\langle a \rangle$. בדומה לתרגיל 4.3, מסמנים ב- $\langle S \rangle$ את האידיאל הקטן ביותר המכיל את הקבוצה S .

משפט 11.31 כל האידיאלים של \mathbb{Z} הם ראשיים.

תרגיל 11.32 ()** הוכח את המשפט. **הדרכה.** תרגיל 4.39.

תרגיל 11.33 ()** $n\mathbb{Z}$ אידיאל ראשוני אם ורק אם $n\mathbb{Z}$ מקסימלי, אם ורק אם n ראשוני.

11.4 תחומי שלמות**11.4.1 שדה השברים**

בתרגיל 11.27 הראינו שכל תת-חוג של שדה הוא תחום שלמות.

משפט 11.34 כל תחום שלמות הוא תת-חוג של שדה.

תרגיל 11.35 ()** יהי D תחום שלמות. הוכח שהיחס $(a, b) \sim (a', b')$ אם ורק אם $ab' = ba'$ הוא יחס שלמות על הקבוצה $\{(a, b) : a, b \in D, b \neq 0\}$.

את מחלקות השקילות של תרגיל 11.35 נסמן $a/b = [(a, b)]$. **שדה השברים** של D הוא קבוצת מחלקות השקילות, שאותה מסמנים ב- $q(D)$.

תרגיל 11.36 (*)** בסימונים אלה, הראה שהפעולות $a/b + c/d = (ad + bc)/bd$ ו- $a/b \cdot c/d = ac/bd$ מוגדרות היטב.

תרגיל 11.37 (*)** הוכח את המשפט. **הדרכה.** הראה ש- $q(D)$ הוא שדה, וש- $a \mapsto a^{-1}$ הוא שיכון של חוגים $D \rightarrow q(D)$.

11.4.2 אברים בתחומי שלמות

נקבע תחום שלמות R .

תרגיל 11.38 (*) הפיך אם ורק אם $Ra = R$.

הגדרה 11.39 אומרים ש- $a | b$ (a' מחלק את b) אם קיים $c \in R$ כך ש- $b = ac$. (השווה להגדרה 1.2)

תרגיל 11.40 (*) $a | b$ ב- R אם ורק אם $Rb \subseteq Ra$.

הגדרה 11.41 a ו- b חברים אם $a | b$ ו- $b | a$.

תרגיל 11.42 (*) $a | b$ ב- R אם ורק אם $Rb = Ra$.

תרגיל 11.43 ()** הוכח שיחס החברות הוא יחס שקילות על האיברים השונים מאפס ב- R .

תרגיל 11.44 ()** הוכח שיחס החלוקה הוא יחס סדר חלש על מחלקות החבורות.

כל איבר $a \in R$ אפשר לפרק $a = au^{-1} \cdot u$, כאשר u הפיך. פירוק כזה, שבו אחד הגורמים הפיך, נקרא **פירוק טריוויאלי**.

11.45 הגדרה איבר $p \in R$ (שאינו אפס ואינו הפיך) נקרא **אי-פריק** אם אין לו פירוקים לא-טריוויאליים.

11.46 הגדרה איבר $p \in R$ (שאינו אפס ואינו הפיך) הוא **ראשוני** אם $p \mid ab$ נובע ש- $p \mid a$ או $p \mid b$.

תרגיל 11.47 (+)** כל איבר ראשוני הוא אי-פריק.

תרגיל 11.48 ()** האיבר p ראשוני אם ורק אם האידיאל Rp ראשוני.

תרגיל 11.49 (+)** האיבר p אי-פריק אם ורק אם Rp הוא מקסימלי בקבוצת האידיאלים הראשיים.

לסיכום נושא זה:

$$\Leftarrow Rp \text{ מקסימלי}$$

$$Rp \text{ ראשוני} \iff p \text{ ראשוני} \Leftarrow$$

$$p \text{ אי-פריק} \iff Rp \text{ מקסימלי בקבוצת האידיאלים הראשיים.}$$

טענה 11.50 אם יש לאיבר a בחוג R פירוק לגורמים ראשוניים, אז זהו הפירוק היחיד בין כל הפירוקים שלו לגורמים אי-פריקים.

תרגיל 11.51 (-)** הוכח את הטענה. כלומר: נניח ש- $a = x_1 \cdots x_n = y_1 \cdots y_m$ הם שני פירוקים של a לגורמים אי-פריקים בחוג R . אם כל הגורמים x_i ראשוניים, הראה ש- $m = n$ ושעד כדי סדר, כל y_i הוא חבר של x_i . **הדרכה.** x_n מחלק מכפלה, ולכן את אחד הגורמים שלה, נניח y_m ; אבל y_m אי-פריק ולכן $y_m \sim x_n$. צמצם והמשך באינדוקציה על n .

11.4.3 חוגים ראשיים

11.52 הגדרה תחום שלמות שבו כל האידיאלים ראשיים נקרא **חוג ראשי**.

תרגיל 11.53 (*) \mathbb{Z} הוא חוג ראשי.

טענה 11.54 בחוג ראשי, אם a אי-פריק אז הוא ראשוני.

תרגיל 11.55 (-)** הוכח את הטענה. **הדרכה.** אם a אי-פריק אז Ra מקסימלי בקבוצת האידיאלים הראשיים לפי תרגיל 11.49; אבל מכיוון שהחוג ראשי, Ra מקסימלי, ולפי תרגיל 11.48 הוא ראשוני. לפי תרגיל 11.29, a ראשוני.

משפט 11.56 בחוג ראשי, כל איבר (שונה מאפס, לא הפיך) אפשר לפרק למכפלה של איברים אי-פריקים.

תרגיל 11.57 (*)** הוכח את המשפט. **הדרכה.** נסמן ב- P את קבוצת האברים שהם מכפלות של איברים אי-פריקים; כך P סגורה לכפל. נניח, בשלילה, שקיים $a_0 \neq 0$ לא הפיך שאינו ב- P . בנה באינדוקציה סדרה $a_{n+1} | a_n$ (מחלק ממש) של איברים שאינם ב- P . אז $d \in R$ כך ש- $I = Rd \subseteq Ra_n$ ו- $d \in Ra_n$ ואז $d \in Ra_{n+1} \subseteq I = Rd \subseteq Ra_n$ ולכן קיים $d \in R$ כך ש- $I = Rd \subseteq Ra_n$ ו- $d \in Ra_{n+1} \subseteq I = Rd \subseteq Ra_n$ ולכן קיים $d \in R$ כך ש- $I = Rd \subseteq Ra_n$ ו- $d \in Ra_{n+1} \subseteq I = Rd \subseteq Ra_n$.

משפט 11.58 בחוג ראשי, כל איבר (שונה מאפס, לא הפיך) מתפרק לגורמים אי-פריקים באופן יחיד.

תרגיל 11.59 ()** הוכח את המשפט. **הדרכה.** משפט 11.56 וטענה 11.50.

11.4.4 חוגים אוקלידיים

גם אם תכונת פירוק היחיד לגורמים, המתקיימת בכל חוג ראשי, מוצאת חן בעינינו מאד, נותרה לנו בעיה קשה: כיצד להוכיח שחוג מסויים הוא ראשי?

הגדרה 11.60 יהי R תחום שלמות. פונקציה $d: R \rightarrow \mathbb{N} \cup \{-\infty\}$ המקיימת $d(0) < d(x)$ לכל $x \neq 0$ נקראת פונקציה אוקלידית אם

$$(E1) \quad d(a) \leq d(b) \text{ לכל } a | b, \text{ וכן}$$

$$(E2) \quad \text{לכל } b \neq 0 \text{ ולכל } a \text{ קיימים } q, r \text{ כך ש-} a = qb + r \text{ ו-} d(r) < d(b).$$

תחום שלמות שמוגדרת עליו פונקצייה אוקלידית נקרא תחום אוקלידי.

תרגיל 11.61 (*) $d: R \rightarrow \mathbb{N} \cup \{-\infty\}$ המקיימת $d(0) < d(x)$ לכל $x \neq 0$ ואת התנאי (E1) היא אוקלידית, אם ורק אם לכל $b \neq 0$ ולכל a קיים q כך ש- $d(a - qb) < d(b)$.

תרגיל 11.62 (*)** כל חוג אוקלידי הוא ראשי. **הדרכה.** העזר בהוכחה של משפט 1.17: אם $0 \neq I \triangleleft R$ אידיאל, אז $0 \neq a \in I$ עם $d(a)$ מינימלי הוא יוצר של I .

11.4.5 פולינומים מעל שדה

הגדרה 11.63 יהי R חוג קומוטטיבי. החוג $R[x] = \{a_0 + \dots + a_n x^n : a_0, \dots, a_n \in R\}$ עם הפעולות הרגילות, נקרא חוג הפולינומים מעל R .

תרגיל 11.64 (-)** $R[x]$ הוא אכן חוג, המכיל עותק של R .

מגדירים את הדרגה $\deg: R[x] - \{0\} \rightarrow \mathbb{N}$ כמקובל, $\deg(a_0 + \dots + a_n x^n) = n$ אם $a_n \neq 0$.

תרגיל 11.65 (+)** אם R תחום שלמות, אז $\deg(fg) = \deg(f) + \deg(g)$ לכל $f, g \in R[x]$.

תרגיל 11.66 ()** אם R תחום שלמות אז גם $R[x]$ הוא תחום שלמות.

תרגיל 11.67 ()** האברים ההפיכים ב- $R[x]$ הם אלו ההפיכים כבר ב- R .

משפט 11.68 יהי F שדה. אז חוג הפולינומים $F[x]$ הוא חוג אוקלידי.

תרגיל 11.69 (*)** הוכח את המשפט. **הדרכה.** הצע אלגוריתם לחילוק עם שארית.

תרגיל 11.70 (*) לכל שדה F , $F[x]$ הוא תחום ראשי.

משפט 11.71 כל פולינום מעל שדה F מתפרק לגורמים אי־פריקים באופן יחיד.

תרגיל 11.72 ()** הוכח את המשפט. **הדרכה.** ראשי לפי תרגיל 11.70, ולכן הטענה הראשונה נובעת מתרגיל 11.58.

משפט 11.73 אם $f \in F[x]$ פולינום אי־פריק, או $\langle f \rangle \mid F[x]$ הוא שדה.

תרגיל 11.74 ()** הוכח את המשפט. **הדרכה.** $\langle f \rangle$ מקסימלי בקבוצת האידיאלים הראשיים לפי תרגיל 11.49; אבל מכיוון שהחוג ראשי, R_f מקסימלי, ולכן חוג המנה ביחס אליו הוא שדה, משפט 11.21.

תרגיל 11.75 ()** לכל פולינום $f \in F[x]$, $F[x]/\langle f \rangle$ מכיל עותק של F , והוא מרחב וקטורי מעליו, ממימד $\deg(f)$.

12 מבוא לשדות סופיים

מושגים: שורש של פולינום. גזירה פורמלית. תת־שדה. פולינום מינימלי. מאפיין של שדה.

12.1 שורשים של פולינומים

יהי F שדה. אם $f = \sum_{i=0}^n a_i x^i \in F[x]$ ו־ $a \in F$, אז $f(a) = \sum_{i=0}^n a_i a^i$.

הגדרה 12.1 איבר $a \in F$ הוא שורש כל $f \in F[x]$ אם $f(a) = 0$.

תרגיל 12.2 (*)** a הוא שורש של f אם ורק אם $(x-a) \mid f(x)$. **הדרכה.** חילוק עם שארית: כתוב $f(x) = (x-a)q(x) + r(x)$; $\deg(r) < \deg(x-a) = 1$; ולכן $r(x) \in F$. הצב $x = a$ וקבל $r = 0$.

משפט 12.3 לפולינום ממעלה n מעל שדה יש לכל היותר n שורשים.

תרגיל 12.4 (*)** הוכח את המשפט. **הדרכה.** לפולינום יש פירוק יחיד לגורמים. יש שורש יחיד לכל גורם $x-a$ בפירוק הזה, ומספרם של אלו אינו עולה על n לפי תרגיל 11.65.

תרגיל 12.5 (*)** תת־חבורה כפלית סופית של שדה היא ציקלית.

הגדרה 12.6 מגדירים גזירה פורמלית של פולינומים, לפי $(\sum a_i x^i)' = \sum i a_i x^{i-1}$.

תרגיל 12.7 ()** הראה ש־ $(f+g)' = f' + g'$ ו־ $(fg)' = fg' + f'g$.

תרגיל 12.8 ()** אם $f \mid g^2$ אז $f \mid f'$.

תרגיל 12.9 ()** אם $f' = -1$, אז כל השורשים של f שונים זה מזה.

12.2 שדות

12.10 הגדרה תת-חוג F של שדה K הוא תת-שדה אם F סגור (בנוסף לחיבור, לחיסור וכפל, גם ל)חילוק.

12.11 תרגיל (*) אם $F \subseteq K$ תת-שדה, אז K הוא מרחב וקטורי מעל F .

את הממד של K מעל תת-השדה F מסמנים ב- $[K:F]$.

12.12 תרגיל ()** יהי F תת-שדה של K , ויהי $a \in K$. אז $\Phi_a: F[x] \rightarrow K$ המוגדר לפי $\Phi_a(f) = f(a)$ הוא הומומורפיזם של חוגים.

12.13 תרגיל ()** אם $[K:F] < \infty$ אז Φ_a כנ"ל אינו חד-חד-ערכי.

12.14 הגדרה יהיו $F \subseteq K$ שדוץ ו- $a \in K$. הפולינום המינימלי של a מעל F הוא הפולינום בעל המעלה הקטנה ביותר מעל F המאפס את a , אם קיים כזה.

12.15 תרגיל ()** אם F, K, a כנ"ל, אז הפולינום המינימלי h הוא מינימלי גם לגבי יחס החילוק, כלומר, הוא מחלק כל פולינום מעל F המאפס את a . **הזרחה.** $\text{Ker}(\Phi_a) = \langle h \rangle$.

12.16 תרגיל (*)** אם F, K, a כנ"ל, אז h אי-פריק ו- $\text{Im}(\Phi_a) = F[a]$ שדה. **הזרחה.** $F[a] \subseteq K$ ו- $\text{Im}(\Phi_a) \cong F[x]/\langle h \rangle$, ולכן הוא תחום שלמות; לפי h ראשוני, אבל מכיון ש- $F[x]$ ראשי, $\langle h \rangle$ מקסימלי, ולכן חוג המנה הוא שדה.

12.17 תרגיל ()** $[F[a]:F] = \deg(h)$

12.2.1 שורשים ופיצול

12.18 משפט יהי $p \in F[x]$ פולינום אי-פריק. אז קיים שדה המכיל את F , ממימד $\deg(p)$ מעליו, שבו יש שורש ל- p .

12.19 תרגיל (*)** הוכח את המשפט. **הזרחה.** קח $K = F[x]/\langle f \rangle$. הוא מכיל עותק של F וממדו מעליו $\deg(p)$ לפי תרגיל 12.75; הקוסט $x + \langle f \rangle$ מקיים $x + \langle f \rangle = f(x) + \langle f \rangle = f(x + \langle f \rangle)$ שהוא איבר האפס של K , ולכן $x + \langle f \rangle \in K$ שורש.

12.20 הגדרה אומרים ששדה K מפצל את $f \in F[x]$, אם הפירוק של f בחוג $K[x]$ הוא לגורמים ליניאריים.

12.21 משפט לכל פולינום מעל שדה F יש שדה מפצל.

12.22 תרגיל (*)** הוכח את המשפט. **הזרחה.** באינדוקציה על המעלה. קח גורם אי-פריק p של הפולינום; לפי משפט 12.18 יש שדה $F \subseteq K$ ובו שורש של p , ולכן של f . מעל K אפשר לכתוב $f(x) = (x - \alpha)f_1(x)$ עם $\deg(f_1) < \deg(f)$, ולפי הנחת האינדוקציה יש שדה $K_1 \subseteq K$ המפצל את f_1 , ולכן גם את f .

12.2.2 המאפיין של שדה

הגדרה 12.23 המאפיין של חוג R הוא המספר הקטן ביותר n כך שהסכום $1 + 1 + \dots + 1$ של n עותקים של היחידה, שווה לאפס - אם יש כזה, ואפס אחרת.

תרגיל 12.24 ()** לכל חוג R יש הומומורפיזם $\phi: \mathbb{Z} \rightarrow R$ המוגדר היטב על-ידי ההנחה $1 \mapsto 1_R$.

תרגיל 12.25 ()** המאפיין של R הוא יוצר של הגרעין של ϕ של תרגיל 12.24.

תרגיל 12.26 ()** המאפיין של תחום שלמות (ובכלל זה שדה) הוא ראשוני, או אפס.

תרגיל 12.27 ()** כל שדה ממאפיין p מכיל עותק של \mathbb{Z}_p .

תרגיל 12.28 ()** כל שדה ממאפיין 0 מכיל עותק של הרציונליים \mathbb{Q} .

תרגיל 12.29 (*)** בשדה ממאפיין p ראשוני, $(a + b)^p = a^p + b^p$. **הדרכה.** הבינום של בינום.

תרגיל 12.30 ()** בשדה ממאפיין p ראשוני, $(a + b)^{p^n} = a^{p^n} + b^{p^n}$. **הדרכה.** אינדוקציה.

תרגיל 12.31 (*)** בשדה ממאפיין p ראשוני, $x \mapsto x^p$ הוא אוטומורפיזם. **הדרכה.** זהו הומומורפיזם לפי תרגיל 12.29, והגרעין טריוויאלי כי $x^p = 0$ גורר $x = 0$.

12.3 שדות סופיים

תרגיל 12.32 (*) לשדה סופי יש מאפיין חיובי.

תרגיל 12.33 (*)** כל שדה סופי הוא מסדר p^n עבור p ראשוני ו- n מתאים. **הדרכה.** יהי F שדה סופי. לפי תרגיל 12.32 המאפיין שלו הוא ראשוני p , ולפי תרגיל 12.27 הוא מכיל עותק של \mathbb{Z}_p . לפי תרגיל 12.11 הוא מרחב וקטורי מעל \mathbb{Z}_p , וממדו כמובן סופי. לכן $F \cong \mathbb{Z}_p^n$ כמרחבים וקטוריים, ומכאן $|F| = p^n$.

משפט 12.34 יש שדה מסדר $p^n = q$.

תרגיל 12.35 (*)** הוכח את המשפט. **הדרכה.** לפולינום $f = x^q - x$ יש שדה מפצל L לפי משפט 12.21. אוסף השורשים $L_0 = \{a \in L : a^q = a\}$ סגור לחיבור וכפל לפי תרגיל 12.30, ולחילוק לפי $a^{-1} = a^{q-2}$. לכן L_0 שדה. הוא מפצל את f כי כל שורשי f נמצאים בו. לבסוף, $|L_0| = q$ לפי תרגיל 12.9.

משפט 12.36 השדה מסדר q הוא יחיד עד-כדי איזומורפיזם.

כדי להוכיח את המשפט הזה, יש להראות ש'שדה פיצול', שהוא שדה מפצל מינימלי, הוא יחיד עד-כדי איזומורפיזם.

משפט 12.37 יש פולינום אי-פריק מכל מעלה מעל \mathbb{F}_p .

תרגיל 12.38 (*)** הוכח את המשפט. **הדרכה.** נניח $q = p^n$. אם $F_q^\times = \langle \alpha \rangle$ לפי תרגיל 12.5, אז $\mathbb{F}_q = F_p[\alpha]$ ולכן המעלה של הפולינום המינימלי של α מעל \mathbb{F}_p היא n ($[\mathbb{F}_q : \mathbb{F}_p] = n$ (תרגיל 12.17), והרי הפולינום הזה אי-פריק).