התחלקות - הגדרות בלבד

תורת המספרים האלמנטרית - 80115

מרצה: אהוד (אודי) דה-שליט

מתרגל: גיא ספיר

סוכם ע"י: שריה אנסבכר

סמסטר ב' תשפ"ג, האונ' העברית

תוכן העניינים

אשמח לקבל הערות והארות על הסיכומים על מנת לשפרם בעתיד,
כל הערה ולו הפעוטה ביותר (אפילו פסיק שאינו במקום או רווח מיותר) תתקבל בברכה;
אתם מוזמנים לכתוב לי לתיבת הדוא"ל: sraya.ansbacher@mail.huji.ac.il.

לסיכומים נוספים היכנסו לאתר:
אקסיומת השלמות - סיכומי הרצאות במתמטיקה
https://srayaa.wixsite.com/math

1 יחס החלוקה

הגדרה 1.1. יהיו $a,b\in\mathbb{Z}$, נאמר ש-a מחלק את b (או ש-b הוא כפולה של a) ונסמן $a\mid b$ אם קיים $q\in\mathbb{Z}$ כך ש-$b=a\cdot q$.

♣ מהגדרה נובע שאם $a\mid b$ אז $a\neq 0$.

משפט. יהיו $a_1,a_2,\dots,a_n\in\mathbb{Z}$, מתקיימים שני הפסוקים הבאים:

- אם קיים $r\geq i\in\mathbb{N}$ כך ש-$a_i\neq 0$ אז קיים $d\in\mathbb{N}$ יחיד כך ש-$d\mid a_i$ לכל $n\geq i\in\mathbb{N}$ ובנוסף לכל $q\in\mathbb{Z}$ המחלק את כולם ($q\mid a_i$ לכל $n\geq i\in\mathbb{N}$) מתקיים $q\mid d$.
- אם $a_i\neq 0$ לכל $n\geq i\in\mathbb{N}$ אז קיים $l\in\mathbb{N}$ כך ש-$a_i\mid l$ לכל $n\geq i\in\mathbb{N}$ ובנוסף לכל $m\in\mathbb{Z}$ המתחלק בכולם ($a_i\mid m$ לכל $n\geq i\in\mathbb{N}$) מתקיים $l\mid m$.

הגדרה 1.2. מחלק משותף מקסימלי וכפולה משותפת מינימלית
יהיו $a_1,a_2,\dots,a_n\in\mathbb{Z}$,

- אם קיים $n\geq i\in\mathbb{N}$ כך ש-$a_i\neq 0$ אז נסמן ב-$\gcd(a_1,a_2,\dots,a_n)$ את אותו d יחיד שמקיים את התנאים במשפט שלעיל, ונקרא לו המחלק המשותף המקסימלי של $a_1,a_2,\dots,a_n$.
- אם $a_i\neq 0$ לכל $n\geq i\in\mathbb{N}$ אז נסמן ב-$\operatorname{lcm}(a_1,a_2,\dots,a_n)$ את אותו m יחיד שמקיים את התנאים במשפט שלעיל ונקרא לו הכפולה המשותפת המינימלית של $a_1,a_2,\dots,a_n$.

♣ הגדרות שקולות ל-gcd ול-lcm הן:

- המחלק המשותף המקסימלי הוא הטבעי הגדול ביותר שמחלק את $a_1,a_2,\dots,a_n$.
- הכפולה המשותפת המינימלית היא הטבעי הקטן ביותר שמתחלק ב-$a_1,a_2,\dots,a_n$.

הסיבה להגדרה דווקא בצורה הנ"ל היא שהגדרה זו תופסת בכל חוג חילופי[1].

הגדרה 1.3. יהיו $a,b\in\mathbb{Z}$, נאמר ש-a ו-b זרים זה לזה אם $\gcd(a,b)=1$ (לפעמים אומרים גם "ראשוניים זה ביחס לזה", אנחנו לא נעשה זאת בגלל הבלבול עם הראשוניים).

הגדרה 1.4. יהיו $a_1,a_2,\dots,a_n\in\mathbb{Z}$, נאמר שהם זרים זה לזה בזוגות אם $\gcd(a_i,a_j)$ לכל $n\geq i,j\in\mathbb{N}$ כך ש-$i\neq j$.

סימון: לכל $a\in\mathbb{Z}$ נסמן $(a):=a\cdot\mathbb{Z}$ (כזכור $a\cdot\mathbb{Z}:=\{a\cdot q\mid q\in\mathbb{Z}\}$), כלומר (a) היא קבוצת כל הכפולות של a.

הגדרה 1.5. אידיאל
קבוצה $I\subseteq\mathbb{Z}$ תקרא אידיאל אם מתקיימים שלושת התנאים הבאים:

1. $0\in I$.
2. לכל $a,b\in I$ מתקיים $a+b\in I$.
3. לכל $a\in I$ ולכל $q\in\mathbb{Z}$ מתקיים $q\cdot a\in I$.

♣ זוהי ההגדרה של אידיאל בכל חוג חילופי, בחוג השלמים ניתן היה להסתפק בסגירות לחיבור ולחיסור מפני שניתן להמיר כל כפל שלמים לחיבור וחיסור[2].

[1] חוג חילופי (קומוטטיבי) הוא קבוצה שעליה מוגדרות פעולות חיבור וכפל המקיימת את כל אקסיומות השדה מלבד קיום הופכי.
[2] לעומת זאת אין שום אפשרות להמרת כפל רציונליים בחיבור וזו הסיבה לכך שנזקקנו לשתי פעולות בשדה.

2 המספרים הראשוניים

2.1 התחלה

יהי $0 \neq p \in \mathbb{Z}$ כך ש-$p \neq \pm 1$.

הגדרה 2.1. נאמר ש-p הוא מספר אי-פריק אם אין לו מחלקים שונים מ-± 1 ו-$\pm p$, כלומר לכל $a, b \in \mathbb{Z}$ כך ש-$p = ab$ מתקיים $a = \pm p$ (וממילא $b = \pm 1$) או ש-$a = \pm 1$ (וממילא $b = \pm p$).

הגדרה 2.2. נאמר ש-p הוא מספר ראשוני אם לכל $a, b \in \mathbb{Z}$ המקיימים $p \mid ab$ מתקיים $p \mid a$ או ש-$p \mid b$.

♣ היה קל יותר לו היינו מגדירים את הראשוניים והאי-פריקים כטבעיים גדולים מ-1 המקיימים את התכונות הנ"ל ביחס לטבעיים.

♣ בחוג השלמים אלו הגדרות שקולות (נראה זאת בהמשך) אך ישנם חוגים אחרים שבהם המצב שונה.

♣ בסיכומי קורס זה אסמן ב-Prime את קבוצת הראשוניים (ב-$\mathbb{N}$ או ב-$\mathbb{Z}$ ע"פ ההקשר).

הגדרה 2.3. נאמר ששני מספרים $a, b \in \mathbb{Z}$ הם מספרים ידידים אם ניתן להציג את האחד כמכפלה של האחר באיבר הפיך.

♣ בחוג השלמים האיברים ההפיכים היחידים הם ± 1 אך ישנם חוגים אחרים (למשל חוג הפולינומים[3] וחוג השלמים של גאוס המופיע בהגדרה הבאה) שבהם המצב שונה.

2.2 חוג השלמים של גאוס

הגדרה 2.4. חוג השלמים של גאוס
נסמן $\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ ונקרא ל-$\mathbb{Z}[i]$ חוג השלמים של גאוס.

♣ הרעיון מאחורי הסימון $\mathbb{Z}[i]$ הוא כמו הסימון $\mathbb{F}[x]$ שסימן את חוג הפולינומים בעלי מקדמים בשדה $\mathbb{F}$ אלא שכעת המשתנה אינו x עלום אלא i, ואכן כל הצבה של i בפולינום עם מקדמים שלמים ניתן להציג בצורה $a + bi$; רעיון זה מופיע גם בסימון $\mathbb{Z}\left[\sqrt{-5}\right]$ שבאחת ההערות בקובץ הטענות.

♣ יחס החלוקה, ראשוניות ואי-פריקות מוגדרים בחוג השלמים של גאוס באותה צורה שהוגדרו בשלמים, גם בחוג השלמים של גאוס יש שקילות בין ראשוניות לאי-פריקות ולכן המשפט היסודי של האריתמטיקה תקף גם בו.

הגדרה 2.5. הנורמה (בחוג השלמים של גאוס) היא פונקציה $N : \mathbb{Z}[i] \to \mathbb{N}_0$ המוגדרת ע"י $N(a + bi) = a^2 + b^2$[4].

[3] בליניארית 2 הגדרנו פולינום הפיך אם קיים פולינום אחר כך שמכפלתם היא הפולינום 1, לפי זה הפולינומים ההפיכים הם אלו שדרגתם 0.
[4] כלומר הריבוע של הנורמה ב-$\mathbb{C}$, הסיבה לשימוש בריבוע היא כדי להישאר בחוג השלמים.

2.3 המשפט היסודי של האריתמטיקה

הגדרה 2.6. הריבוי של מספר ראשוני $p \in \mathbb{Z}$ בפירוק של מספר שלם $0 \neq n \in \mathbb{Z}$ לראשוניים הוא[5]:

$$\mathrm{Ord}_p(n) := \max\{e \in \mathbb{N}_0 : p^e \mid n\}$$

♣ ניתן להבחין ש-$\mathrm{Ord}_p(n)$ הוא החזקה שבה הופיע p[6] בהצגה:

$$n = \mathrm{sgn}(n) \cdot \prod_{i=1}^{r} p_i^{e_i}$$

כאשר $p_1, p_2, \ldots, p_r \in \mathbb{N}$ הם מספרים ראשוניים המקיימים $p_1 < p_2 < \ldots < p_r$ ו-$e_1, e_2, \ldots, e_r \in \mathbb{N}$.

הגדרה 2.7. מספר שלם $n \in \mathbb{Z}$ יקרא מספר ריבועי אם קיים $m \in \mathbb{Z}$ כך ש-$n = m^2$.

♣ מהגדרה מספר ריבועי הוא אי-שלילי[7].

הגדרה 2.8. נאמר שמספר שלם $n \in \mathbb{Z}$ חופשי מריבועים אם לא קיים מספר ריבועי $1 \neq m \in \mathbb{N}$ כך ש-$m \mid n$.

♣ מה שמייחד מספרים חופשיים מריבועים היא העובדה שכל ראשוני מופיע בפירוק שלהם פעם אחת לכל היותר.

♣ 1 הוא מספר ריבועי וגם מספר חופשי מריבועים!

2.4 שכיחות המספרים הראשוניים

הגדרה 2.9. תהא $(M_n)_{n=1}^{\infty}$ סדרה המוגדרת ע"י $M_n = 2^n - 1$, האיברים בסדרה זו נקראים מספרי מרסן; אם M_n הוא מספר ראשוני נאמר שהוא ראשוני מרסן.

הגדרה 2.10. תהא $(F_n)_{n=1}^{\infty}$ סדרה המוגדרת ע"י $F_n = 2^n + 1$, האיברים בסדרה זו נקראים מספרי פרמה; אם F_n הוא מספר ראשוני נאמר שהוא ראשוני פרמה.

---

[5] נשים לב שמהגדרה הקבוצה $\{e \in \mathbb{N}_0 : p^e \mid n\}$ אינה ריקה שהרי $p^0 = 1 \mid n$ והיא חסומה מלעיל מפני ש-$|p| \geq 2$ ולכן קיים $e \in \mathbb{N}$ כך ש-$|p^e| > n$ והרי ערכו המוחלט של המחלק קטן מזה של המחולק.

[6] כמובן שהריבוי של $-p$ זה לזה של p, אם הראשוני אינו מופיע אז הריבוי הוא 0.

[7] בהעברית וויקיפדיה הגדירו מספר ריבועי כמספר שלם **וחיובי** המקיים את הנ"ל, בעוד שבוויקיפדיה האנגלית וב-MathWorld הגדירו כפי שהגדרנו כאן.