קירובים דיופנטיים - 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

תודתי נתונה לאורטל פלדמן על הסיכום שכתב בשנת הלימודים תשע"ו,
נעזרתי בו רבות על מנת לכתוב את הסיכום שלפניכם.

* * *

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 התחלה

♣ "בתורת המספרים, קירוב דיופנטי של מספר ממשי נתון הוא מספר רציונלי קרוב אל המספר המבוקש. האנליזה הדיופנטית עוסקת, בין השאר, בקיומם של קירובים דיופנטיים, בטיב הקירוב האפשרי, ובהכללות של הבעיה היסודית. התחום נקרא על שמו של דיופנטוס שהציג בעיות שהפתרונות שלהן דווקא במספרים שלמים." (ציטוט מהערך "קירוב דיופנטי" בוויקיפדיה העברית)

הגדרה 1.1. מספר $z\in\mathbb{C}$ יקרא מספר אלגברי אם קיים פולינום $P\in\mathbb{Z}\left[x\right]$ כך ש-z הוא שורש של P, אחרת יקרא מספר טרנסצנדנטי (או טרנסצנדנטלי).

♣ יש המחליפים את $\mathbb{Z}\left[x\right]$ ב-$\mathbb{Q}\left[x\right]$ אך זה שקול מפני שניתן להכפיל במכנה המשותף של כל המקדמים ולקבל פולינום מתאים ב-$\mathbb{Z}\left[x\right]$.

♣ קבוצת המספרים האלגבריים היא בת-מנייה שכן $\mathbb{Z}\left[x\right]$ בת-מנייה, ולכן העוצמה של קבוצת המספרים הטרנסצנדנטיים היא עוצמת הרצף, כלומר במונחים של עוצמה ישנם הרבה יותר מספרים טרנסצנדנטיים מאשר מספרים אלגבריים.

♣ קשה מאד להוכיח שמספרים כמו e ו-π הם אכן טרנסצנדנטיים, לעומתם נראה בהמשך דרך לבנות מספרים טרנסצנדנטיים שאינם מועילים במיוחד (בטח בהשוואה ל-e ו-π).

הגדרה 1.2. יהי $\alpha\in\mathbb{C}$ מספר אלגברי, הדרגה הקטנה ביותר של פולינום ב-$\mathbb{Z}\left[x\right]$ ש-α הוא שורש שלו ($\min\left\{ \deg P\mid P\in\mathbb{Z}\left[x\right],\ P\left(\alpha\right)=0\right\}$) תקרא הדרגה של α ואז נאמר ש-α הוא מספר אלגברי מדרגה/מעלה זו.

2 סדרות פרי (Farey)

הגדרה 2.1. סדרות פרי (Farey)[1]

לכל $n\in\mathbb{N}$ סדרת פרי ה-n-ית (מסומנת ב-$\mathcal{F}_n$) היא סדרה סופית שבה כל הרציונליים בקטע $[0,1]$ שהמכנה שלהם (בהצגה מצומצמת) קטן או שווה ל-n כשהם מסודרים בסדר עולה; כלומר:

$$\begin{aligned}
\mathcal{F}_1 &:= \left(\frac{0}{1},\frac{1}{1}\right)\\
\mathcal{F}_2 &:= \left(\frac{0}{1},\frac{1}{2},\frac{1}{1}\right)\\
\mathcal{F}_3 &:= \left(\frac{0}{1},\frac{1}{3},\frac{1}{2},\frac{2}{3},\frac{1}{1}\right)\\
\mathcal{F}_4 &:= \left(\frac{0}{1},\frac{1}{4},\frac{1}{3},\frac{1}{2},\frac{2}{3},\frac{3}{4},\frac{1}{1}\right)\\
\mathcal{F}_5 &:= \left(\frac{0}{1},\frac{1}{5},\frac{1}{4},\frac{1}{3},\frac{2}{5},\frac{1}{2},\frac{3}{5},\frac{2}{3},\frac{3}{4},\frac{4}{5},\frac{1}{1}\right)\\
&\vdots
\end{aligned}$$

[1] ערך בוויקיפדיה האנגלית: John Farey.

3 שברים משולבים

אינטואיציה: יהי $x \in \mathbb{R}$ ונסמן $r_0 := \lfloor x \rfloor$ ו-$a_0 := x - r_0$, א"כ $0 \leq r_0 < 1$ וגם $x = a_0 + r_0$; אם נסמן $x_1 := \frac{1}{r_0} > 1$ נקבל:

$$x = a_0 + r_0 = a_0 + \frac{1}{x_1}$$

כעת ניתן לחזור על התהליך ולסמן $r_1 := \lfloor x_1 \rfloor$, $a_1 := x_1 - r_1$ ו-$x_2 := \frac{1}{r_1}$ ולקבל:

$$x = a_0 + \frac{1}{a_1 + \frac{1}{x_2}}$$

וכך ניתן לחזור על התהליך כמה פעמים שנרצה:

$$x = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{x_3}}}$$

$$x = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ldots a_{n-1} + \frac{1}{x_n}}}}$$

טוב, האמת היא שלא תמיד אפשר להמשיך את התהליך לנצח, אם היה i שעבורו $r_i = 0$ התהליך היה נעצר משום שאז לא היה ניתן להגדיר $x_{i+1} := \frac{1}{r_i}$; אנחנו נראה שכצפוי זה קורה אם"ם $x \in \mathbb{Q}$.

הגדרה 3.1. שבר משולב סופי

שבר משולב סופי הוא ביטוי מהצורה:

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ldots \frac{1}{a_n}}}}$$

כאשר $0 \leq a_0 \in \mathbb{R}$ ו-$0 < a_i \in \mathbb{R}$ לכל $n \geq i \in \mathbb{N}$.

מכיוון שהביטוי הנ"ל אינו נוח לכתיבה מקובלים שני כתיבים נוספים עבור אותו ביטוי[2]:

$$\langle a_0, a_1, \ldots, a_n \rangle$$

$$a_0 + \frac{1}{a_1+}\frac{1}{a_2+}\frac{1}{a_3+}\ldots\frac{1}{a_{n-1}+}\frac{1}{a_n}$$

הגדרה 3.2. שבר משולב אינסופי

שבר משולב אינסופי הוא ביטוי מהצורה:

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{\ldots}}}}$$

כאשר $0 \leq a_0 \in \mathbb{R}$ ו-$0 < a_i \in \mathbb{R}$ לכל $i \in \mathbb{N}$ והכוונה היא לגבול[3] של הסדרה $(b_n)_{n=0}^{\infty}$ המוגדרת ע"י (לכל $n \in \mathbb{N}$):

$$b_0 := \langle a_0 \rangle, \ b_n := \left\langle a_0, a_1, a_2, \ldots, a_{n-1} + \frac{1}{a_n} \right\rangle$$

אם זו מתכנסת אומרים גם שהשבר המשולב מתכנס.

[2] יש המשתמשים בסוגריים מרובעים במקום המשולשים.

[3] אם הוא קיים, אחרת מדובר בביטוי פורמלי בלבד.

4 משוואות פל (Pell)

♣ הסיבה היחידה לכך שפרק זה מופיע בקבצים העוסקים בקירובים דיופנטיים היא שההוכחה ללמה 4.5 (ראו בקובצי הטענות וההוכחות) משתמשת בטענה שלמספר ממשי יש אינסוף קירובים שונים מסדר שני (ראו טענה 2.6 בקובצי הטענות וההוכחות).

יהי $n\in\mathbb{N}$ שאינו ריבוע ונסמן $R:=\mathbb{Z}\left[\sqrt{n}\right]:=\left\{ x+\sqrt{n}y\mid x,y\in\mathbb{Z}\right\}$ ו-$F:=\mathbb{Q}\left[\sqrt{n}\right]:=\left\{ r+\sqrt{n}\cdot s\mid r,s\in\mathbb{Q}\right\}$.

למה 4.1. R הוא חוג ו-F הוא שדה (עם פעולות החיבור והכפל המושרות מ-$\mathbb{R}$).

הגדרה 4.2. נגדיר את <u>הנורמה</u> ב-R וב-F ע"י $N\left(a+\sqrt{n}b\right):=\left(a+\sqrt{n}b\right)\left(a-\sqrt{n}b\right)$ לכל $a+\sqrt{n}b$ ב-R ו/או ב-F.

הגדרה 4.3. <u>משוואות פל</u>[4] הן משוואות דיופנטיות מהצורה $x^{2}-Dy^{2}=N$ כאשר $D\in\mathbb{N}$ אינו ריבוע ו-$0\neq N\in\mathbb{Z}$.

♣ כלומר משוואת פל שואלת אם קיים איבר בחוג $R:=\left\{ x+\sqrt{D}y\mid x,y\in\mathbb{Z}\right\}$ כך ש-N הוא הנורמה של אותו איבר.

♣ קיימות משוואות פל שאין להן פתרון, כך למשל למשוואה $x^{2}-3y^{2}=2$ אין פתרון מודולו 3 ולכן אין לה גם פתרון בשלמים.

למה. הנורמה (ב-R וב-F) כפלית.

מסקנה. לכל $a,b\in\mathbb{Z}$ מתקיים: $a+\sqrt{D}\cdot b$ הפיך ב-R אם"ם $a^{2}-D\cdot b^{2}=\pm1$.

♣ מסקנה זו היא הסיבה העיקרית לעניין במשוואות פל.

[4] ערך בוויקיפדיה: ג'ון פל.