תורת המספרים

משה קמנסקי

18 באפריל 2022

1 מבוא

רוב התחומים במתמטיקה (ובפרט רוב הקורסים בתואר ראשון) מתמקדים בשיטה או צורת מחשבה אחת: באנליזה חוקרים אי-שוויונות ממשיים, באלגברה מבנים אלגבריים, וכדומה. תורת המספרים שונה מהבחינה הזו מיתר התחומים: היא מוגדרת כחקר שאלות על המבנה הכי טבעי שקיים, המספרים הטבעיים, ועושה זאת במגוון שיטות. למרות שאת המספרים הטבעיים קל מאד לתאר, מסתבר שהשאלות בו נוטות להיות קשות, והפתרון להן, במידה שקיים, יכול להגיע כמעט מכל תחום במתמטיקה: אלגברה, גאומטריה, אנליזה ממשית ומרוכבת, הסתברות, טופולוגיה ועוד. ישנן השערות שקל מאוד לנסח, ואיננו יודעים את התשובה עליהן כבר מאות שנים, ביניהן השערת גולדבאך (כל מספר זוגי הוא סכום של שני ראשוניים) ואינסופיות הראשוניים התאומים (ראשוניים שההפרש ביניהם הוא 2). השערה מפורסמת נוספת שהייתה כלולה ברשימה זו היא "המשפט האחרון של פרמה", שהוכח על ידי אנדרו ווילס באמצע שנות התשעים של המאה ה-20. ההוכחה עשתה שימוש בכלים מכל התחומים שהוזכרו לעיל (וכלים נוספים). המטרה שלנו בקורס הזה היא לבדוק מה ניתן לעשות באמצעות כלים אלמנטריים, איפה הם מפסיקים לעבוד, ואיך כלים שונים יכולים לעזור.

1.1 ראשוניים

כמה מהכלים ניתן לראות כבר בהוכחות השונות של אחד המשפטים המפורסמים של אוקלידס:

משפט א׳ (אוקלידס). *לכל מספר ראשוני יש ראשוני גדול ממנו*

נזכיר את ההוכחה של אוקלידס, שהיא אלמנטרית לגמרי:

הוכחה. נניח ש-p ראשוני ונסתכל על $n = p! + 1$, כאשר $p!$ מכפלת הטבעיים החיוביים עד p. אם q גורם ראשוני של n, אז $q > p$, כי אחרת הוא מחלק את $p!$ וגם את n, ולכן את $1 = n - p!$. $\square$

נסמן ב-p_i את הראשוני ה-i, ב-$\mathbb{P}$ את קבוצת כל הראשוניים. המשפט אומר שזו היא סדרה אינסופית, אבל ההוכחה נותנת קצת יותר מזה: אנחנו יודעים שלכל i מתקיים $p_{i+1} \leqslant p_i! + 1$. למעשה, אפשר להחליף את $p_i!$ במכפלת *הראשוניים* עד p_i, וההוכחה עובדת באותה מידה.

תרגיל 1.1.1. הוכיחו שלכל $i \geqslant 0$ מתקיים $p_i \leqslant 2^{2^i}$

אפשר לקבל תוצאות יותר טובות באמצעות שיטות אנליטיות:

משפט ב׳ (אוילר). *הסכום* $\sum_{p\in\mathbb{P}}\frac{1}{p}$ *מתבדר*

כמובן שנובע מהמשפט שיש אינסוף ראשוניים, אבל ההתבדרות של הטור אומרת שהסדרה p_i גדלה לאט:

תרגיל 1.1.2. הסיקו מהמשפט שלכל ממשי $c>1$ קיים קיימים אינסוף טבעיים i כך ש- $p_i<i^c$

לפני שנוכיח את המשפט, נקבע את המוסכמה הבאה למשך כל הקורס: p *תמיד מסמל מספר ראשוני*.

נזכיר את העובדות הבאות על טורים:

1. טור a_n *מתכנס בהחלט* אם הטור $|a_n|$ מתכנס. בפרט, אם $a_n\geqslant 0$ לכל n, שני המושגים מתלכדים
2. אם אחד הטורים a_n או b_n מתכנס בהחלט, אז טור המכפלה מתכנס למכפלת הגבולות.
3. אם $|c|<1$ אז הטור c^n מתכנס (בהחלט) ל-$\frac{1}{1-c}$.

הוכחת משפט ב׳. אם S קבוצה סופית של ראשוניים, אז התזכורת לעיל נותנת:

$$\prod_{p\in S}\frac{1}{1-\frac{1}{p}}=\prod_{p\in S}(1+\frac{1}{p}+\dots)=\sum_{n\in N(S)}\frac{1}{n}\tag{1.1}$$

כאשר $N(S)$ קבוצת כל הטבעיים שכל הגורמים הראשוניים שלהם ב-S. בפרט, אם $S=S_k$ היא קבוצת הראשוניים הקטנים מ-$k+1$, אז כל הטבעיים הקטנים מ-$k+1$ שייכים ל-$N(S)$, ואנחנו מקבלים

$$\prod_{p\leqslant k}\frac{1}{1-\frac{1}{p}}\geqslant\sum_{n\leqslant k}\frac{1}{n}\geqslant\log(k)$$

כאשר הסכום שמופיע במרכז הוא סכום חלקי של *הטור ההרמוני*, והחסם בצד ימין נובע מהשוואה לאינטגרל. כיוון ששני הצדדים חיוביים (ו-log פונקציה עולה), אפשר להפעיל log על שני הצדדים ולקבל

$$\sum_{p\leqslant k}-\log(1-\frac{1}{p})\geqslant\log(\log(k))$$

אבל עבור $0\leqslant c\leqslant\frac{1}{2}$ (ובפרט עבור $c=\frac{1}{p}$)

$$-\log(1-c)=\sum_{i>0}\frac{c^i}{i}\leqslant c+c^2$$

ולכן

$$\log(\log(k))\leqslant\sum_{p\leqslant k}\frac{1}{p}+\frac{1}{p^2}=\sum_{p\leqslant k}\frac{1}{p}+\sum_{p\leqslant k}\frac{1}{p^2}$$

כיוון ש-$\sum_{p\leqslant k}\frac{1}{p^2}<\sum_{n\geqslant 2}\frac{1}{n^2}<1$, מקבלים $\sum_{p\leqslant k}\frac{1}{p}\geqslant\log(\log(k))-1$. בפרט, הטור מתבדר. $\square$

החלק המעניין ביותר בהוכחה הזו נמצא *ממש* בהתחלה, במשוואה (1.1). למעשה הוא כולל הוכחה יותר פשוטה של אינסופיות הראשוניים: אם יש רק מספר סופי שלהם, אפשר לקחת את S להיות קבוצת *כל* הראשוניים. במקרה זה, בצד ימין של המשוואה מופיע הטור ההרמוני, ומקבלים סתירה לכך שהוא מתבדר. להוכחה יש ערך מוסף שנותן אי השוויון שהוכחנו, אבל בכיוון אחר אפשר לנסות בכל זאת להכליל את המשוואה הזו לכל הראשוניים. כיוון ששוב מקבלים את הטור ההרמוני בצד ימין, זה בלתי אפשרי ישירות, אבל השוויון נותר בעינו אם מעלים את $\frac{1}{p}$ (בצד שמאל) ואת n (בצד ימין) באותה חזקה s. עבור $s > 1$ ממשי, $\zeta(s) = \sum_{n>0} \frac{1}{n^s}$ מתכנס, ואפשר לחשוב על הביטוי כעל פונקציה של s. פונקציה זו נקראת *פונקציית זיטא* של רימן. היא הוגדרה על-ידי אוילר, אבל רימן הבין שכדאי לחשוב עליה כפונקציה של ערכים *מרוכבים* s. אחת הבעיות הפתוחות המפורסמות במתמטיקה היא להוכיח את השערת רימן, שהיא טענה על הערכים בהם הפונקציה הזו מתאפסת. פונקציית זיטא

1.2 החשיבות של הראשוניים

הראשוניים מהווים את אבני הבניין של המספרים השלמים. במקרים רבים, כדי להוכיח טענה על כל השלמים, מספיק להוכיח אותה לראשוניים. נראה מספר דוגמאות לזה בהמשך, ושתיים כבר עכשיו:

תרגיל 1.2.1. "המשפט האחרון של פרמה" אומר שעבור $n > 2$, לא קיימים שלמים חיוביים a, b, c כך ש-$a^n + b^n = c^n$. הוכיחו שאם הטענה נכונה ל-$n = 4$ ול-n ראשוני, אז היא נכונה

תרגיל 1.2.2. נסמן ב-T את קבוצת הטבעיים שהם סכום $a^2 + b^2$ עבור a, b שלמים. הוכיחו שאם n מכפלה של ראשוניים ששייכים ל-T, אז גם $n \in T$.

באופן קצת מפתיע, מסתבר שלשאלות על ראשוניים יש נגיעה גם בחיי היום-יום. נניח ש-X היא קבוצה סופית של הודעות. מערכת הצפנת מפתח פומבי על X היא קבוצת פונקציות הפיכות $E : X \to X$ עם התכונה שהידיעה של E לא מאפשרת לחשב בקלות את ההפכית שלה D, ללא מידע נוסף. הפונקציה E נקראת פונקציית ההצפנה, ו-D פונקציית הפיענוח. היא מאפשר למי שמכיר את E ואת D לפרסם את E בפומבי, ולהסתיר את D, וכך לאפשר לכל אחד להצפין הודעות בלי שהם יוכלו לפענח. באופן יותר קונקרטי, אפשר תמיד לחשוב על X כקבוצת הטבעיים שקטנים ממספר מספיק גבוה N, ועל $E = E_k$ ו-$D = D_l$ כמקודדות על-ידי מספרים טבעיים k ו-l. ההנחה היא לכן שמתוך הידיעה של k לא ניתן לחשב בקלות את l ("לחשב בקלות" אומר למשל במספר צעדים פולינומי ב-$\log(k)$).

שאלה 1.2.3. *האם קיימת מערכת הצפנת מפתח פומבי?*

התשובה לשאלה הזו לא ידועה, אבל קיימות מערכות שמשערים שהן כאלה. הראשונה והמפורסמת ביותר נקראת RSA. בשיטה הזו, המצפין בוב בוחר שני מספרים ראשוניים גדולים p, q ומספר e שאין לו גורמים משותפים עם $(p-1)(q-1)$. המפתח הפומבי של בוב מורכב מהמכפלה $n = pq$ (אבל לא מהגורמים עצמם!), ומהמספר e. כדי לשלוח לבוב גרסה מוצפנת של ההודעה x, אליס משתמשת במידע הזה כדי לחשב את השארית, ביחס ל-n, של x^e. זוהי ההודעה המוצפנת $y = E(x)$. כאשר בוב מקבל את ההודעה המוצפנת, הוא יכול לפענח אותה על-ידי חישוב השארית של y^d ביחס ל-n, כאשר d הוא מספר עם התכונה ש-$de - 1$ מתחלק ב-$(p-1)(q-1)$.

לכן, המפתח הסודי, שקובע את D, נתון על-ידי המידע של p ו-q (וגם d, אבל אותו קל לחשב). בהמשך נסביר למה התהליך הזה אכן נותן את ההודעה המקורית x (בהנחה ש-$x < n$). בשלב זה, נשים לב מהן השאלות הנוספות שיש לענות עליהן כדי להבין האם זו מערכת מפתח פומבי טובה:

1. כמה קל לייצר מספרים ראשוניים גדולים?

2. כמה קל לבדוק האם מספר הוא ראשוני?

3. בהינתן $n = pq$, כמה קל למצוא את p, q?

4. כמה קל למצוא מספר d כמו בתיאור של ההצפנה (בהנחה ש-p, q ידועים)

5. כמה קל לחשב שארית של חזקה (כלומר, כמה קל להצפין ולפענח בשיטה הזו)?

נראה בקרוב ששתי הבעיות האחרונות הן יחסית קלות. ההנחה שהפירוק של n ל-p, q הוא קשה הוא החלק המרכזי בהשערה ש-RSA הצפנת מפתח פומבי טובה, שכן הפירוק הזה הוא המפתח הסודי. נציין שגם אם הבעיה הזו קשה, לא ידוע שלא ניתן לפרוץ את ההצפנה בדרך אחרת. השאלה השנייה לא מופיעה ישירות בהצפנה, אבל היא רלוונטית לשאלה הראשונה: דרך אחת לייצר ראשוניים היא לבחור מספר מתוך קבוצה שמכילה הרבה ראשוניים, ואז לבדוק שהוא אכן כזה. באופן קצת מפתיע, מסתבר שאפשר לבדוק יחסית מהר אם מספר הוא ראשוני, בעיקר אם מרשים שיטות הסתברותיות, אבל אנחנו לא נעסוק בזה.

נתייחס עכשיו לשאלה הראשונה, מזווית ספציפית: האם אפשר למצוא פונקציה ש"מייצרת" ראשוניים, כלומר, פונקציה (קלה לחישוב) $f : \mathbb{N} \to \mathbb{N}$ עם התכונה ש-$f(n)$ ראשוני לכל $n \in \mathbb{N}$ (או לפחות לכל n בקבוצה שקל לתאר).

נתבונן ראשית בפונקציות לינאריות, $f(n) = an + b$, כאשר $a, b \in \mathbb{N}$. אם מספר $c > 1$ מחלק את a ואת b, אז הוא מחלק גם את $f(n)$ לכל n, ולכן סדרה כזו בהכרח לא תכלול הרבה ראשוניים. מאידך, אם זה לא המצב, ישנו המשפט המפורסם הבא של דיריכלה:

משפט ג' (דיריכלה). *בסדרה $an + b$ עבור $a, b \in \mathbb{N}$ זרים יש אינסוף ראשוניים.*

אנחנו נחזור אל המשפט הזה בהמשך. כמובן שדוגמא אחת היא המקרה $a = 1$ ו-$b = 0$, כלומר סדרת כל הטבעיים, אז המשפט הזה מכליל את המשפט של אוקלידס, אבל זה גם מראה שהמשפט לא מועיל מאד במציאת ראשוניים מהר.

פונקציה לינארית היא פולינום ממעלה 1. מה קורה אם מגדילים את המעלה?

תרגיל 1.2.4. נגדיר $p(n) = n^2 + n + 41$. מיצאו 10 ערכים טבעיים שונים n עבורם $p(n)$ ראשוני. האם $p(n)$ ראשוני לכל n?

תרגיל 1.2.5. הוכיחו שאם p פולינום כלשהו עם מקדמים שלמים, ו-M מספר שלם כך ש-$p(n)$ ראשוני לכל $n \geqslant M$ אז p קבוע

אז לא קיים פולינום במשתנה אחד שמייצר ראשוניים. מה אם מרשים יותר משתנים?

משפט ד'. *קיים פולינום $p(x_1, \dots, x_k)$ עם מקדמים שלמים שכל ערך חיובי שלו על מספרים טבעיים $n_1, \dots, n_k$ הוא ראשוני*

המשפט הזה הוא מקרה פרטי של הפתרון של הבעייה העשירית של הילברט, על-ידי מטיאסביץ', ג'וליה רובינסון ואחרים. ההוכחה נותנת את הפולינום באופן מפורש, אבל השימוש בו לייצור ראשוניים אינו יעיל.

מה לגבי פונקציות שאינן פולינום? מרסן התעניין בראשוניים מהצורה 2^n-1. האבחנה הראשונה היא:

תרגיל 1.2.6. הוכיחו שאם 2^n-1 ראשוני אז גם n ראשוני

מרסן חשב שגם הכיוון ההפוך נכון: אם n ראשוני אז גם 2^n-1 ראשוני, אבל מסתבר שזו טעות: $2^{11}-1=2047=23\cdot 89$. ראשוני מהצורה הזו נקרא *ראשוני מרסן*. ראשוני מרסן

שאלה 1.2.7. *האם יש אינסוף ראשוניי מרסן?*

נסיון נוסף נתון על-ידי הסדרה $F(n)=2^{2^n}+1$. מספרים מהצורה הזו נקראים *מספרי פרמה*. פרמה שיער שהם תמיד ראשוניים, אבל אוילר הוכיח ש-$F(5)$ מתחלק ב-641 (שימו לב ש-$F(5)=2^{32}+1$ אז הטענה לא טריוויאלית בעידן ללא מחשב!). למעשה, לא ידועים ערכים $n>4$ עבורם $F(n)$ ראשוני, ולא ידוע אם יש אינסוף כאלה. מספרי פרמה

למרות זאת, מספרי פרמה נותנים הוכחה נוספת לאינסופיות הראשוניים:

תרגיל 1.2.8.
1. נניח ש-F_n סדרה אינסופית של מספרים טבעיים גדולים מ-1 עם התכונה: עבור $m>n$, המספרים F_m, F_n זרים (כלומר, אין מספר ראשוני שמחלק את שניהם). הסיקו שיש אינסוף ראשוניים
2. נסמן ב-F_n את מספר פרמה ה-n. הוכיחו שלכל $n>1$ מתקיים $F_n=F_0\cdot\dots\cdot F_{n-1}+2$.
3. הסיקו מהסעיף שעבור $m>n$ המספרים F_n, F_m הם זרים, ולכן שיש אינסוף ראשוניים

1.3 המספרים הטבעיים

נסיים את המבוא עם תזכורת על מה אנחנו מדברים, כלומר, מהם המספרים הטבעיים. ההנחה היא שהפרטים מוכרים מקורסים אחרים. לקבוצת הטבעיים יש מספר מבנים מעניים: חיבור, כפל, סדר ועוד. מסתבר שכל המבנה נקבע באופן יחיד כבר על-ידי הסדר. במלים אחרות, הטבעיים מאופיינים על-ידי התכונות הבאות:

הגדרה 1.3.1. קבוצת הטבעיים היא קבוצה סדורה לא ריקה $(\mathbb{N},\leqslant)$, עם התכונות הבאות:

1. לכל איבר שאינו מינימום יש קודם מיידי
2. ב-$\mathbb{N}$ אין איבר מירבי
3. לכל תת-קבוצה לא ריקה יש מינימום.

מהתכונות הללו נובע בקלות שהסדר הוא מלא, ושלכל איבר יש עוקב מיידי. המינימום של $\mathbb{N}$ עצמה מסומן ב-0, ולכל $n\in\mathbb{N}$ העוקב מסומן ב-$s(n)$. מהתכונות נובעות גם שתי הצורות של הוכחה באינדוקציה:

טענה 1.3.2 (אינדוקציה). *אם* $A \subseteq \mathbb{N}$ *תת-קבוצה כך ש-*$0 \in A$ *ולכל* $n \in A$ *גם* $s(n) \in A$ *אז* $A = \mathbb{N}$.

טענה 1.3.3 (אינדוקציה שלמה). *אם* $A \subseteq \mathbb{N}$ *מקיימת: לכל* $n \in \mathbb{N}$*, אם* $m \in A$ *לכל* $m < n$ *אז* $n \in A$*, אז* $A = \mathbb{N}$.

תרגיל 1.3.4. הוכיחו את שתי הטענות

עובדה קרובה היא האפשרות להגדיר פונקציות ברקורסיה:

טענה 1.3.5 (משפט הרקורסיה). *נניח ש-*A *קבוצה,* $a \in A$ *איבר בה, ו-*$f : A \to A$ *פונקציה. אז קיימת פונקציה יחידה* $g : \mathbb{N} \to A$ *כך ש-*$g(0) = a$ *ו-*$g(s(n)) = f(g(n))$ *לכל* $n \in \mathbb{N}$.

העובדה שהתכונות של הטבעיים מאפיינות אותם ניתנת לניסוח מדויק באופן הבא:

תרגיל 1.3.6. נניח ש-M קבוצה סדורה נוספת המקיימת את התכונות בהגדרת הטבעיים. הוכיחו שקיימת פונקציה הפיכה יחידה $t : \mathbb{N} \to M$ ששומרת על הסדר (כלומר, אם $n > m$ אז $t(n) > t(m)$). הוכיחו שהפונקציה ההפוכה שומרת על הסדר אף היא.

ההגדרות והתכונות של הכפל והחיבור נובעות אף הן מהטענות הללו. למשל, תהי A קבוצת הפונקציות מ-$\mathbb{N}$ לעצמה, $a \in A$ פונקציית הזהות, ו-$f : A \to A$ הפונקציה הנתונה על-ידי $f(u) = s \circ u$, כאשר $s \in A$ פונקציית העוקב. לפי משפט הרקורסיה, קיימת פונקציה $g : \mathbb{N} \to A$ כך ש-$g(0)$ היא הזהות, ו-$g(s(n)) = s \circ g(n)$. במלים אחרות, $g(n)$ היא הפונקציה שמוסיפה לקלט שלה את n, וניתן להגדיר: $n + m = g(n)(m)$. מההגדרה הזו אולי לא ברור מיד שזו יוצאת פעולה חילופית (כלומר, ש-$g(n)(m) = g(m)(n)$), אבל ניתן להוכיח זאת באינדוקציה. ההגדרה והתכונות של הכפל מתקבלים באופן דומה. סוף הרצאה 1, 19 באוק

2 פירוק לראשוניים

2.1 המשפט היסודי

בכל ההוכחות לאינסופיות הראשוניים שראינו בסעיף הקודם, היו (לפחות) שני חורים: הראשון הוא שלא הגדרנו מהו ראשוני. נעשה זאת כעת:

הגדרה 2.1.1. מספר טבעי n הוא *פריק* אם ניתן לרשום אותו כמכפלה $n = mk$ כאשר m, k שונים שניהם מ-1. הוא נקרא *אי-פריק* אם אינו פריק ושונה מ-1. הוא נקרא *ראשוני* אם הוא שונה מ-1, ולכל שני מספרים m, k, אם n מחלק את mk אז הוא מחלק את m או את k. פריק אי-פריק ראשוני

תרגיל 2.1.2. הוכיחו שראשוני שונה מ-0 הוא אי-פריק

הכיוון ההפוך של התרגיל האחרון גם נכון, אבל יותר קשה. זה יהיה אחד השלבים בהוכחת המשפט הבא. כרגיל, אנחנו מסמנים ב-p_i את הראשוני ה-i.

משפט 2.1.3 (המשפט היסודי של האריתמטיקה). *כל מספר טבעי חיובי* n *אפשר לרשום כמכפלה (סופית)* $n = p_1^{k_1} \dots p_i^{k_i}$*, עבור סדרה יחידה* k_i *של טבעיים*

פורמלית, הסדרה k_i היא תמיד אינסופית (כדי שהיחידות תתקיים), אבל כיוון שהמכפלה היא סופית, $k_i = 0$ לכמעט כל i.

המשפט נובע ישירות משלוש הטענות הבאות:

טענה 2.1.4. *כל מספר טבעי חיובי הוא מכפלה של מספרים אי-פריקים*

טענה 2.1.5. *אם עבור שתי סדרות k_i ו-l_i מתקיים* $p_1^{k_1} \cdots = p_1^{l_1} \dots$ *אז* $k_i = l_i$ *לכל* i.

טענה 2.1.6. *כל מספר אי-פריק הוא ראשוני*

ההוכחה של טענה 2.1.4 היא תרגיל קלאסי באינדוקציה שלמה:

הוכחת טענה 2.1.4. נניח ש-n טבעי חיובי, ונניח שהטענה נכונה לכל $m < n$. אם n אי-פריק או 1 אין מה להוכיח, אז נניח ש-$n = mk$ פריק. אז $0 < m, k < n$ ולכן לפי ההנחה כל אחד מהם הוא מכפלה סופית של אי-פריקים, ולכן גם n. לפי משפט האינדוקציה השלמה, הטענה נכונה לכל מספר טבעי. □

הוכחת היחידות משתמשת ישירות באקסיומות הסדר. נשים לב שמאינדוקציה נובע שאם p ראשוני ו-$m_1, \dots, m_k$ הם מספרים ש-p מחלק את מכפלתם, אז p מחלק אחד מהם.

הוכחת טענה 2.1.5. נניח בשלילה שהטענה שגויה. כאמור, בסדרה k_i כמו שמופיעה בטענה כמעט כל הערכים הם 0. לכן הסכום m של ה-k_i-ים והסכום n של ה-l_i-ים הוא מספר טבעי, ואפשר להניח ש-m מינימלי. אם i הוא מספר עבורו $l_i > 0$ אז p_i מחלק את אחד ה-p_j-ים עבור $k_j > 0$, ולכן $i = j$ (כי p_j אי פריק). אבל אז אפשר לחלק ב-p_i, וזו סתירה למינימליות של m. □

כדי להשלים את הוכחת המשפט, נותר להוכיח שכל אי-פריק הוא ראשוני. לשם כך, נשתמש בהגדרה הבאה:

המחלק המשותף המירבי

הגדרה 2.1.7. אם A קבוצה של טבעיים שכוללת לפחות איבר חיובי אחד, *המחלק המשותף המירבי* של A הוא המקסימום $\gcd(A)$ של קבוצת המספרים הטבעיים שמחלקים את כל המספרים ב-A. אם $A = \{n_1, \dots, n_k\}$ סופית נרשום לפעמים $\gcd(n_1, \dots, n_k)$ במקום $\gcd(A)$.

נשים לב שזה מוגדר היטב, משום שקבוצת המחלקים לא ריקה (כוללת לפחות את 1) וחסומה (על-ידי כל אחד מהאיברים החיוביים של A), ולכל קבוצה כזו יש מקסימום ב-$\mathbb{N}$. בהמשך כשנדבר על $\gcd(A)$ תמיד נניח שהיא מקיימת את הנחת ההגדרה. התרגיל הבא מראה שתמיד אפשר להתמקד בקבוצות סופיות:

תרגיל 2.1.8. הוכיחו שאם $A \subseteq B$ קבוצות לא ריקות של טבעיים חיוביים, אז $\gcd(B) \leqslant \gcd(A)$. הסיקו שלכל קבוצה לא ריקה של טבעיים חיוביים A יש תת-קבוצה לא ריקה וסופית B כך ש-$\gcd(A) = \gcd(B)$.

מספרים זרים

במונחים אלה, שני מספרים n, m הם *מספרים זרים* אם ורק אם $\gcd(n, m) = 1$. המחלק המשותף המירבי מעניין בעיקר בזכות הטענה הבאה:

טענה 2.1.9 (האלגוריתם של אוקלידס). *לכל שני טבעיים חיוביים* n, m *קיימים מספרים שלמים* a, b *כך ש-*$na + mb = \gcd(n, m)$

נשים לב ש-a, b הם *שלמים*, לאו דווקא אי-שליליים (לרוב, אחד מהם יהיה שלילי). זה אחד המקומות בהם משתלם לעבור לעבוד עם כלל השלמים.

תרגיל 2.1.10. נניח ש-$n, m \in \mathbb{N}$ ו-$m > 0$

1. הוכיחו שאם d מחלק את m ואת n, אז d מחלק את $\gcd(n, m)$
2. הוכיחו שאם k טבעי נוסף, אז $\gcd(n, m, k) = \gcd(n, \gcd(m, k))$

הוכחת טענה 2.1.6. נניח ש-n אי-פריק, ונניח ש-n מחלק את mk. כיוון ש-$\gcd(m, n)$ מחלק את n ו-n אי-פריק, $\gcd(m, n) = n$ או $\gcd(m, n) = 1$. באפשרות הראשונה n מחלק את m וסיימנו. באפשרות השנייה האלגוריתם של אוקלידס נותן a, b שלמים כך ש-$am + bn = 1$. נכפיל את שני הצדדים ב-k ונקבל $kam + kbn = k$. לפי ההנחה, n מחלק את צד שמאל ולכן את k. □

הוכחת הטענה מסיימת את הוכחת המשפט הבסיסי של האריתמטיקה, אבל עלינו עדיין להציג את האלגוריתם של אוקלידס. לשם כך, נזכיר מושג בסיסי נוסף, חלוקה עם שארית:

טענה 2.1.11. *אם n, m מספרים טבעיים ו-$m > 0$, קיים טבעיים k, r יחידים כך ש-$0 \leqslant r < m$ ו-$n = km + r$.*

המספר r מהטענה נקרא *השארית* של n בחלוקה ב-m. השארית

הוכחה. הקבוצה של הטבעיים i כך ש-$im \leqslant n$ היא סופית ולא ריקה. לכן, יש בה איבר מירבי k. נסמן $r = n - km$. אז $r \geqslant 0$ כי $n \geqslant km$ ו-$r < m$ כי אחרת $(k+1)m \leqslant n$, בסתירה למירביות של k. □

תרגיל 2.1.12. נניח ש-$n, m > 0$, ו-r השארית של n בחלוקה ב-m. הוכיחו ש-$\gcd(n, m) = \gcd(m, r)$.

הוכחת טענה 2.1.9. אפשר להניח ש-$n > m > 0$ ונוכיח באינדוקציה (שלמה) על m. תהי r השארית של n בחלוקה ב-m. אז $g = \gcd(n, m) = \gcd(n, r)$ לפי התרגיל, ו-$r < m$ לפי הגדרת השארית. לכן, לפי הנחת האינדוקציה קיימים c, d שלמים כך ש-$g = cn + dr = cn + d(n - km) = (c + d)n - dkm$. לכן $a = c + d$ ו-$b = -dk$ (כאשר $n = km + r$) פותרים את הבעיה. □

סיימנו את הוכחת המשפט. נשים לב שההוכחה אכן נותנת אלגוריתם לחישוב המחלק המשותף המירבי והצירוף השלם שנותן אותו.

לפי המשפט היסודי, לכל מספר $n > 0$ ולכל ראשוני p יש מספר טבעי יחיד $v_p(n)$ כך ש-$n = \prod_p p^{v_p(n)}$, כלומר, $v_p(n)$ הוא החזקה של p בהצגה של n כמכפלת ראשוניים. $v_p(n) \in \mathbb{N}$ נקרא לפעמים *הריבוי* של p ב-n. קיבלנו לכן, לכל ראשוני p, פונקציה $v_p : \mathbb{N}_+ \to \mathbb{N}$ (כאשר $\mathbb{N}_+$ הטבעיים החיוביים). הריבוי

תרגיל 2.1.13. הוכיחו את הטענות הבאות לכל $n, m \neq 0$ ולכל ראשוני p

1. $v_p(nm) = v_p(n) + v_p(m)$
2. $v_p(n+m) \geqslant \min(v_p(n), v_p(m))$. הראו מקרה בו אין שוויון
3. n מחלק את m אם ורק אם $v_p(n) \leqslant v_p(m)$ לכל p
4. $v_p(\gcd(m,n)) = \min(v_p(m), v_p(n))$
5. אם $A \subseteq \mathbb{N}$ תת-קבוצה כלשהי, *כפולה משותפת* של A היא מספר שכל איברי A מחלקים. אם A סופית, *הכפולה המשותפת המינימלית* של A מסומנת ב-$\operatorname{lcm}(A)$ (למה היא קיימת?). הוכיחו ש-$v_p(\operatorname{lcm}(n,m)) = \max(v_p(n), v_p(m))$
6. הוכיחו ש-$\operatorname{lcm}(n,m) \cdot \gcd(n,m) = nm$

כפולה משותפת

הכפולה המשותפת המינימלית

2.2 שלשות פיתגוריות

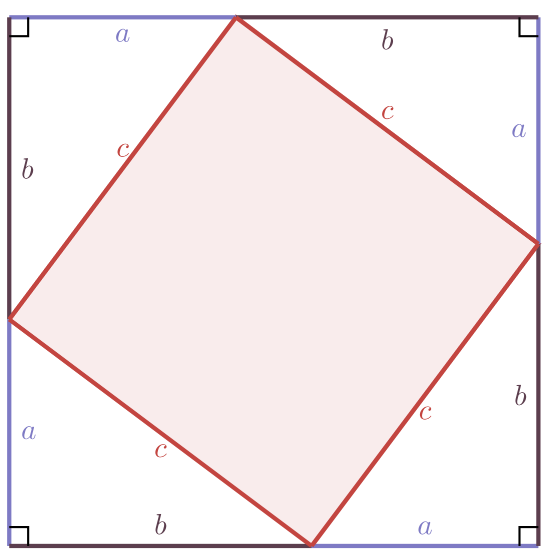
הגדרה 2.2.1. שלושה מספרים טבעיים $a, b, c > 0$ נקראים *שלשה פיתגורית* אם קיים משולש ישר זווית שאורכי צדדיו a, b, c

שלשה פיתגורית

כיוון שדמיון משולשים שומר על היות המשולש ישר זווית, הגדרה זו לא תלויה במידת האורך שבחרנו. כיוון שאנחנו מניחים שכל המספרים חיוביים, אורך היתר בשלשה כזו יהיה הגדול מבין שלושתם. כדי לקבל תיאור קצת יותר אלגברי של השלשות הללו, נזכיר את

משפט 2.2.2 (משפט פיתגורס). *אם a, b, c אורכי הצלעות של משולש ישר זווית, כאשר c אורך היתר, אז* $c^2 = a^2 + b^2$

גרסא של אחת ההוכחות היפות של המשפט מיוחסת לג'יימס גארפילד, הנשיא ה-20 של ארה"ב. ההוכחה כולה כלולה בציור הבא:



שאלה 2.2.3. *האם קיימות שלשות פיתגוריות?*

התשובה היא שכן: המספרים $3, 4, 5$ מהווים שלשה פיתגורית. השאלה הבאה שאפשר לשאול היא כמה שלשות פיתגוריות יש, למשל האם יש אינסוף. לשאלה הזו יש תשובה לא מעניינת: אם אפשר להכפיל את כל איברי השלשה הקודמת באותו מספר. למשל, $6, 8, 10$ היא גם שלשה פיתגורית. מבחינה גאומטרית, מקבלים משולש דומה למשולש הקודם. לכן, שאלה יותר מעניינת היא אולי: האם יש אינסוף מחלקות דמיון שונות של משולשים שמיוצגות על-ידי שלשות פיתגוריות? מבחינה אלגברית, יש לפחות שתי דרכים לנסח את הבעיה בצורה מעניינת. הראשונה היא לחלק בריבוע היתר: אם $a^2 + b^2 = c^2$, אז $(\frac{a}{c})^2 + (\frac{b}{c})^2 = 1$ כאשר $r = \frac{a}{c}$ ו-$s = \frac{b}{c}$ מספרים רציונליים. אם מכפילים את כל האיברים באותו מספר, המספרים r, s לא משתנים. בכיוון ההפוך, אם r, s הם מספרים רציונליים עבורם $r^2 + s^2 = 1$, אז על-ידי כפל במכנה המשותף אפשר לקבל שלשה פיתגורית. לכן, אנחנו מחפשים פתרונות רציונליים של המשוואה $x^2 + y^2 = 1$. מבחינה גאומטרית, אנחנו מחפשים נקודות עם קואורדינטות רציונליות על מעגל היחידה. אנחנו נחזור לנקודת המבט הזו בהמשך.

הגישה השנייה היא פשוט להוסיף את התנאי שהרכיבים יהיו זרים:

הגדרה 2.2.4. *שלשה פיתגורית פרימיטיבית* היא שלשה פיתגורית בה אורכי הניצבים זרים שלשה פיתגורית פרימיטיבית

כמובן שבמצב הזה, גם אורך היתר זר לכל אחד מהניצבים. ישנן עוד שתי שאלות שקשורות לשאלה מהן השלשות הפיתגוריות: איזה מספרים טבעיים יכולים להופיע בתור יתר של שלשה פיתגורית, ושאלת ביניים מעניינת בפני עצמה:

שאלה 2.2.5. *איזה מספרים טבעיים הם סכום של שני ריבועים?*

כדי לנסות לענות על השאלה הזו, נתבונן בשאלה דומה אך יותר פשוטה: איזה מספרים הם הפרש של שני ריבועים? ראשית, התרגיל הבא מרמז שכדאי להתמקד בראשוניים:

תרגיל 2.2.6. הוכיחו שאם m, n הם הפרש של ריבועים, אז גם mn הוא כזה

נניח שראשוני p הוא הפרש של שני ריבועים: $p = a^2 - b^2$. אז $p = (a-b)(a+b)$. אבל זהו פירוק של p, וכיוון ש-p ראשוני, נובע מזה ש-$a - b = 1$ ו-$a + b = p$, כלומר, $p = 2b + 1$ ו-$b = \frac{p-1}{2}$. אם p אי-זוגי, הביטוי הזה הוא מספר טבעי, והוא נותן פתרון לבעיה. זה פותר את הבעיה (בצורה קצת מסובכת) לכל האי-זוגיים. הפתרון הכללי הוא לא קשה באופן דומה, כמו שנראה בתרגיל הבא, אבל פחות רלוונטי לעניינו כרגע:

תרגיל 2.2.7. הוכיחו שמספר טבעי הוא הפרש של שני ריבועים אם ורק אם השארית שלו בחלוקה ב-4 שונה מ-2

האם אפשר להשתמש בשיטה דומה על-מנת לענות על שאלה 2.2.5? כמו בשאלה על ההפרש, כדאי להתמקד ראשית במקרה של ראשוניים. ההבדל הוא שאם $p = a^2 + b^2$, הביטוי בצד ימין לא ניתן לפירוק כמכפלה, לפחות לא במספרים השלמים. אבל הוא כן ניתן לביטוי כזה אם היה לנו מספר i עם התכונה $i^2 = -1$: אז $p = (a+ib)(a-ib)$. אז כדי להשתמש בשיטות דומות, עלינו להבין את התשובה למספר שאלות: האם קיים עולם מספרים בו יש שורש i ל--1? האם יש בו משמעות לפירוק לראשוניים? האם p ראשוני שם?

2.3 חוגים

המסקנה מהסעיף הקודם היא שאנחנו מחפשים מבנה יותר כללי מהמספרים הטבעיים שבו יש משמעות למושגים שדיברנו עליהם. במספרים הטבעיים הפעולות שעניינו אותנו היו כפל וחיבור, אבל ראינו כבר שנוח לדבר גם על חיסור. זה מוביל להגדרה הבאה:

הגדרה 2.3.1. *חוג* נתון על-ידי קבוצה A ושתי פעולות $+$ ו-$\cdot$ על A (שנקראות חיבור וכפל), המקיימות את התכונות הבאות: חוג

1. לכל $a,b,c\in A$ מתקיים $(a\cdot b)\cdot c=a\cdot(b\cdot c)$ ו-$(a+b)+c=a+(b+c)$ (חוק הקיבוץ)
2. קיים איבר $0\in A$ כך ש-$0+a=a$ לכל $a\in A$, וקיים איבר $1\in A$ כך ש-$1\cdot a=a\cdot 1=a$
3. לכל $a,b\in A$ מתקיים $a+b=b+a$
4. לכל $a\in A$ קיים $b\in A$ כך ש-$a+b=b+a=0$
5. לכל $a,b,c\in A$ מתקיים $a\cdot(b+c)=a\cdot b+a\cdot c$ ו-$(b+c)\cdot a=b\cdot a+c\cdot a$ (חוקי הפילוג)

החוג הוא *חוג חילופי* אם $a\cdot b=b\cdot a$ לכל $a,b\in A$ חוג חילופי

לפני שנראה דוגמאות, נציין תכונות בסיסיות:

תרגיל 2.3.2. הוכיחו שלכל חוג A:

1. האיברים 0 ו-1 כפי שנדרשים בהגדרה הם יחידים
2. $0=1$ אם ורק אם זהו האיבר היחיד ב-A
3. לכל $a\in A$ יש איבר יחיד $b\in A$ כך ש-$a+b=0$. איבר זה נקרא *האיבר הנגדי* ל-a, ומסומן $-a$. הסכום $c+(-a)$ מסומן כ-$c-a$, וכד'. האיבר הנגדי
4. תת-קבוצה B של A הכוללת את $0,1$, סגורה תחת הפעולות $+,\cdot,-$ (מהסעיף הקודם) היא בעצמה חוג. תת-קבוצה כזו נקראת *תת-חוג* של A. תת-חוג

אם a,b איברים של חוג, נכתוב לרוב ab במקום $a\cdot b$.

דוגמא 2.3.3. הקבוצה $\mathbb{Z}$ של השלמים, עם הפעולות הרגילות של חיבור וכפל, היא חוג חילופי.

דוגמא 2.3.4. הקבוצה $\mathbb{Z}[x]$ של פולינומים עם מקדמים ב-$\mathbb{Z}$ היא חוג חילופי עם פעולות הכפל והחיבור הרגילות של פולינומים. באופן יותר כללי, אם A חוג חילופי כלשהו, ניתן ליצור את חוג הפולינומים $A[x]$ מעל A, כלומר, פולינומים עם מקדמים ב-A, ועם פעולות הכפל והחיבור הרגילות של פולינומים. זהו שוב חוג חילופי

ביתר פירוט, $A[x]$ הוא קבוצת הביטויים הפורמליים $a_0+a_1x+\dots a_kx^k$, כאשר $a_i\in A$, ו-$a_k\neq 0$ אם $k>0$. על כל ביטוי כזה נוח לחשוב כסדרה אינסופית a_i שכמעט כל איבריה 0 (ואז k הוא המספר הגדול ביותר עבורו $a_k\neq 0$, נקרא *דרגת הפולינום*). הפעולות בחוג הזה מוגדרות, במונחים של סדרות כאלה, על-ידי

דרגת הפולינום

$$(a_i)+(b_i)=(a_i+_A b_i)$$
$$(a_i)\cdot(b_i)=(\sum_{j=0}^{i}a_j\cdot_A b_{i-j})$$

כאשר סימן הסכום $\sum$ הוא במובן של החיבור ב-A (המשמעות של זה ברורה בגלל קיבוציות החיבור)

תרגיל 2.3.5. בידקו שפעולות אלה אכן מגדירות חוג חילופי

על מנת לתת דוגמאות נוספות, נגדיר הגדרה נוספת:

הגדרה 2.3.6. איבר a בחוג A הוא *איבר הפיך* אם קיים $b\in A$ כך ש-$1=ab=ba$. חוג חילופי A הוא *שדה* אם $1\neq 0$, ולכל $a\in A$ שונה מ-0 יש הפכי.

איבר הפיך

שדה

דוגמאות לשדות כוללות את הרציונליים $\mathbb{Q}$, הממשיים $\mathbb{R}$ והמרוכבים $\mathbb{C}$. אלה, לכן גם דוגמאות של חוגים, אבל הם נותנים גם דוגמאות לחוגים שאינם חילופיים דרך אלגברה לינארית:

דוגמא 2.3.7. נניח ש-$\Bbbk$ שדה, ו-V מרחב לינארי מעל $\Bbbk$. נסמן ב-$A=\mathrm{End}(V)$ את קבוצת ההעתקות הלינאריות (מעל $\Bbbk$) מ-V לעצמו. הסכום של שני איברים של A הוא שוב העתקה לינארית, וגם ההרכבה, ושתי הפעולות הללו הופכות את A לחוג. אם המימד של V הוא מספר סופי n, אפשר לזהות את A עם קבוצת המטריצות הריבועיות בגודל n מעל $\Bbbk$, עם פעולות של חיבור וכפל מטריצות. באלגברה לינארית מראים שאם המימד גדול מ-1 אז: החוג אינו חילופי, קיימים איברים $t,s\in A$ שונים מ-0 עבורם $ts=0$, קיים איבר $t\in A$ שונה מ-0 ו-1 עבורו $t^2=t$.

דוגמא 2.3.8. אם A_1 ו-A_2 שני חוגים, עם פעולות $+_1,\cdot_1$ ו-$+_2,\cdot_2$ בהתאמה, אפשר להגדיר מבנה של חוג על המכפלה הקרטזית $A=A_1\times A_2$ של הקבוצות הללו על-ידי:

$$\langle a_1,a_2\rangle+\langle b_1,b_2\rangle=\langle a_1+_1 b_1,a_2+_2 b_2\rangle$$
$$\langle a_1,a_2\rangle\cdot\langle b_1,b_2\rangle=\langle a_1\cdot_1 b_1,a_2\cdot_2 b_2\rangle$$

תרגיל 2.3.9. הוכיחו שזה אכן חוג. הוכיחו שאם $A_1,A_2\neq 0$, אז ב-$A_1\times A_2$ יש איבר $t\neq 0,1$ כך ש-$t^2=t$.

דוגמא 2.3.10. נניח ש-A חוג חילופי. נסמן $A[i]=\{a+bi\mid a,b\in A\}$ (פורמלית, $A[i]=A^2$ כקבוצה, ואנחנו רושמים את $\langle a,b\rangle$ כ-$a+bi$). נגדיר חיבור כמו ב-A^2, וכפל על-ידי הנוסחא $(a+bi)(c+di)=ac-bd+(ad+bc)i$.

תרגיל 2.3.11. 1. הוכיחו שההגדרות לעיל הופכות את $A[i]$ לחוג חילופי.

2. נניח שב-A יש איבר a עם התכונה ש-$a^2=-1$. הוכיחו שקיימים $x,y\in A[i]$ שונים מ-0 כך ש-$xy=0$ (איברים x,y עם התכונה הזו נקראים *מחלקי אפס*)

מחלקי אפס

עבור $A=\mathbb{R}$ מקבלים בבנייה הזו את המספרים המרוכבים. עבור הבעיה שהעלינו בסעיף הקודם נתעניין במקרה $A=\mathbb{Z}$. החוג $\mathbb{Z}[i]$ שמתקבל נקרא *חוג השלמים של גאוס*. חוג השלמים של גאוס

תרגיל 2.3.12. נניח ש-A חוג חילופי, ו-$a\in A$. נגדיר העתקה $l_a:A\to A$ על-ידי: $l_a(b)=ab$.

1. הוכיחו ש-a מחלק אפס אם ורק אם $a\neq 0$ ו-l_a אינה חד-חד-ערכית
2. הוכיחו ש-a הפיך אם ורק אם l_a היא על
3. עד סוף השאלה נתמקד בדוגמא $A=\Bbbk[i]$, כאשר $\Bbbk$ שדה. הוכיחו ש-A מרחב וקטורי ממימד 2 מעל $\Bbbk$, כאשר החיבור נתון על-ידי החיבור של A, והכפל בסקלר נתון על-ידי $c(a+bi)=ca+cbi$.
4. הוכיחו שלכל $x\in A$, ההעתקה l_x היא לינארית. הסיקו שאם ב-A אין מחלקי אפס, אז A שדה.
5. חשבו את הדטרמיננטה של l_x, כאשר $x=a+bi\in A$. הסיקו שב-A יש מחלקי אפס אם ורק אם ל--1 יש שורש ב-$\Bbbk$.

סוף הרצאה 2, 22 באוק

המטרה הבאה שלנו היא להבין איזה מההגדרות והטענות שהוכחנו עבור הטבעיים ניתן להכליל ל-$\mathbb{Z}[i]$ ולחוגים יותר כלליים. כיוון שרוב החוגים שנעסוק בהם יהיו חילופיים, נניח מעכשיו *שכל החוגים שלנו הם חילופיים*, אלא אם נאמר אחרת.

נשים לב שקבוצת הטבעיים לא מהווה חוג. החוג הרלוונטי במקרה הזה הוא חוג השלמים $\mathbb{Z}$, שכולל אותו מידע, אבל במעבר מ-$\mathbb{N}$ ל-$\mathbb{Z}$ צריך לעדכן כמה הגדרות. כדי לראות זאת, נשים לב למשל שב-$\mathbb{Z}$ אין כמעט איברים אי-פריקים בהגדרה שלנו: אם $n\in\mathbb{Z}$, אז $n=-1\cdot -n$. מאותה סיבה, לא יכול להיות פירוק יחיד לראשוניים. באופן יותר כללי, הבעיות שגורם -1 יכולות להיגרם על-ידי כל איבר הפיך. לכן, בהקשר הזה ההגדרה הנכונות הן כאלה:

הגדרה 2.3.13. יהי A חוג.

1. איבר $a\in A$ *מחלק* איבר אחר b אם קיים $c\in A$ כך ש-$b=ac$ מחלק
2. איבר $a\in A$ הוא *איבר פריק* אם $a=bc$ עבור b,c שאינם הפיכים. אם a לא הפיך ולא פריק, הוא נקרא *איבר אי-פריק* איבר פריק איבר אי-פריק
3. איבר a הוא *איבר ראשוני* אם הוא לא הפיך, ולכל שני איברים $b,c\in A$, אם a מחלק את bc אז a מחלק את b או את c איבר ראשוני

ראינו שבחוגים כלליים עשויים להיות מחלקי אפס. בחוגים כאלה, למושגים הללו עשויות להיות תכונות קצת לא מוכרות. למשל:

תרגיל 2.3.14. הוכיחו ש-0 הוא ראשוני בחוג A אם ורק אם אין ב-A מחלקי אפס

מהסיבות הללו נצמצם את העניין שלנו לחוגים ללא מחלקי אפס:

הגדרה 2.3.15. החוג החילופי A נקרא *תחום שלמות* (או לפעמים פשוט *תחום*) אם אין ב-A מחלקי אפס תחום שלמות תחום

חשיבות *מעשית* אחת של ההנחה הזו נתונה בעובדה שבתחום אפשר "לבטל" איבר שונה מ-0 שמופיע בשני צידי מכפלה:

תרגיל 2.3.16. הוכיחו שאם A תחום שלמות, $a \in A$ שונה מ-0, ועבור $b, c \in A$ מתקיים $ab = ac$, אז $b = c$. הראו שזה לא נכון אם A אינו תחום.

תרגיל 2.3.17. הוכיחו ששני התנאים הבאים שקולים עבור איברים $a, b \in A$ בתחום שלמות:

1. קיים איבר הפיך $u \in A$ כך ש-$a = ub$
2. a מחלק את b ו-b מחלק את a

הוכיחו שהתנאים הללו מגדירים יחס שקילות על איברי A. הוכיחו גם שאם a שקול ל-b ו-$a = xb \neq 0$ אז x הפיך.

תרגיל 2.3.18. נניח ש-$\mathbb{k}$ שדה, ונתבונן בחוג הפולינומים $A = \mathbb{k}[x]$

1. מי הם האיברים ההפיכים ב-A?
2. הוכיחו ש-A תחום שלמות
3. הוכיחו שאם עבור $b \in \mathbb{k}$ ועבור $p(x) \in A$ מדרגה גדולה מ-1 מתקיים $p(b) = 0$ אז p פריק (רמז: חילוק עם שארית של פולינומים)

הטיעון שמראה שראשוני הוא אי-פריק בהקשר של הטבעיים (תרגיל 2.1.2) עובד לתחום כללי, וכך גם ההוכחה של טענה 2.1.5:

טענה 2.3.19. *אם $p_1 \dots p_k = q_1 \dots q_l$ שתי מכפלות של איברים ראשוניים בתחום שלמות, אז $k = l$, ואחרי שינוי סדר הגורמים, לכל i קיים איבר הפיך u_i כך ש-$p_i = u_i q_i$*

במלים אחרות, המחלקה של ה-p_i ביחס לשקילות מתרגיל 2.3.17 נקבעת ביחידות, עד כדי סדר.

תרגיל 2.3.20. הוכיחו את הטענה (ההוכחה למקרה של הטבעיים עובדת, אבל שימו לב איפה משתמשים בכך שהחוג הוא תחום, ומאיפה מופיעים ה-u_i)

שני החלקים האחרים בהוכחת המשפט היסודי לא מתקיימים בחוג כללי, ולכן הם הופכים להגדרה:

הגדרה 2.3.21. תחום A נקרא *תחום פריקות יחידה* אם כל איבר שאינו 0 ואינו הפיך הוא *מכפלה של איברים אי-פריקים*, וכל איבר אי-פריק הוא ראשוני תחום פריקות יחידה

שוב, כמו במקרה של הטבעיים, התנאי הזה גורר שכל איבר שונה מ-0 ניתן לרשום באופן יחיד כמכפלה של ראשוניים, אבל היחידות היא במובן שהזכרנו.

איך אפשר להוכיח שחוג הוא תחום פריקות יחידה? ראשית, צריך להוכיח שהוא תחום. לשם כך, נוח להשתמש באבחנה הבאה:

תרגיל 2.3.22. הוכיחו שכל תת-חוג של תחום שלמות הוא תחום שלמות. בפרט, תת-חוג של שדה הוא תחום שלמות. הסיקו (בעזרת תרגיל 2.3.12) ש-$\mathbb{Z}[i]$ הוא תחום.

מלבד היחידות, כל אחד מהשלבים בהם השתמשנו בהוכחת משפט 2.1.3 יכול להיכשל בחוגים יותר כלליים. אחד השלבים העיקריים היה השימוש במחלק המשותף המירבי. על-מנת להגדיר אותו השתמשנו בסדר על הטבעיים, אבל השימוש היה דרך האלגוריתם של אוקלידס, שהטענה שלו לא מזכירה את הסדר. במילים אחרות, המחלק המשותף המירבי איפשר לנו להוכיח שהשלמים הם תחום ראשי, במובן הבא:

תחום ראשי

הגדרה 2.3.23. תחום A נקרא *תחום ראשי* אם לכל תת-קבוצה $B \subseteq A$ קיים $d \in A$ שמחלק את כל איברי B, וכך שקיימים $a_1, \dots, a_k \in A$ ו-$b_1, \dots, b_k \in B$ עבורו $d = \sum_i a_i b_i$.

במלים אחרות, d הוא "צירוף לינארי" של איברי B, עם מקדמים מ-A. ההוכחה שתחום ראשי הוא תחום פריקות יחידה דומה מאד למקרה של הטבעיים:

טענה 2.3.24. *כל תחום ראשי הוא תחום פריקות יחידה*

הוכחה. ההוכחה שכל אי-פריק הוא ראשוני זהה לגמרי למקרה של השלמים: נניח ש-a איבר אי-פריק שמחלק את bc. לפי ההנחה, קיים איבר d שמחלק את a, b, וכך ש-$d = ra + sb$ עבור איברים $r, s \in A$. כיוון ש-a אי-פריק ו-d מחלק אותו, d הוא הפיך או ש-$a = ud$ עבור איבר הפיך u. במקרה השני סיימנו, משום שאז a מחלק את b, ולכן אפשר להניח ש-d הפיך, עם הפכי e. אז $c = ced = ce(ra + sb) = cera + cesb$, וצד ימין הוא סכום של שני איברים שמתחלקים ב-a.

נותר להוכיח שכל איבר a הוא מכפלה סופית של אי-פריקים. נניח שזה לא כך. בפרט, $a = a_1 b_1$ עבור איברים a_1, b_1 שאינם הפיכים. לפי ההנחה, לפחות אחד מהם אינו מכפלה סופית של אי-פריקים, נניח שזה a_1. אז $a_1 = a_2 b_2$, כאשר a_2, b_2 לא הפיכים. באופן כזה, מקבלים סדרה אינסופית a_i של איברי a, כאשר לכל $i \leqslant j$, האיבר a_j מחלק את a_i (ו-$a_0 = a$). נתבונן בקבוצה $A = \{a_i \mid i \in \mathbb{N}\}$. לפי ההנחה, קיים איבר d שהוא צירוף לינארי של ה-a_i, ושמחלק את כל ה-a_i. אם j הוא המספר הגדול ביותר עבורו a_j מופיע בצירוף, אז a_j מחלק את כל האיברים האחרים בסכום, ובפרט את d. לכן, a_j מחלק את a_i לכל i. זו סתירה לכך ש-b_{j+1} אינו הפיך. □

סוף הרצאה 3, 26 באוק

איך אפשר להוכיח שתחום A הוא ראשי? עבור השלמים, הגדרנו את המחלק המשותף המירבי, והוכחנו את הראשיות באמצעות חלוקה עם שארית. שני המושגים הללו משתמשים בסדר על השלמים. בחוג כללי, אין לנו סדר, אבל לפעמים יש תכונה חלשה יותר, שמספיקה גם היא:

תחום אוקלידי

הגדרה 2.3.25. תחום A נקרא *תחום אוקלידי* אם קיימת פונקציה $\alpha : A \backslash \{0\} \to \mathbb{N}$, עם התכונה שלכל $a, b \in A$ כך ש-$b \neq 0$ קיימים $d, r \in A$ כך ש-$a = db + r$, ואם $r \neq 0$ אז $\alpha(r) < \alpha(b)$.

פונקציה אוקלידית

פונקציה α כזו נקראת *פונקציה אוקלידית*.

במקרה של הטבעיים לא ראינו את α כי היא הייתה הזהות, אבל אם היינו מנסחים את ההוכחה במונחים של החוג $\mathbb{Z}$, אז פונקציית הערך המוחלט היא אוקלידית. דוגמא חשובה נוספת היא חוג הפולינומים מעל שדה:

תרגיל 2.3.26. הוכיחו שאם $\Bbbk$ שדה, פונקציית הדרגה היא פונקציה אוקלידית על החוג $\Bbbk[x]$ של פולינומים במשתנה אחד x מעל $\Bbbk$

הפונקציה האוקלידית מאפשרת לנו לחזור על האלגוריתם של אוקלידס במקרה היותר כללי, בדיוק באותו אופן:

טענה 2.3.27. *כל תחום אוקלידי הוא ראשי*

הוכחה. נניח ש-B_0 תת-קבוצה של A, ונסמן ב-B את קבוצת הצירופים הלינאריים של איברים ב-B_0:

$$B = \{\sum_i a_i b_i \mid a_i \in A, b_i \in B_0\}$$

עלינו להוכיח שיש $d \in B$ שמחלק את כל האיברים ב-B (שימו לב ש-$B_0 \subseteq B$, אז זה מספיק, אבל למעשה ברור שהתנאים שקולים). אם $B = \{0\}$ אז $d = 0$ מקיים את התנאי. אחרת, קבוצת הערכים $\alpha(b)$ עבור $b \in B$ שונה מאפס היא תת-קבוצה לא ריקה של $\mathbb{N}$, ולכן יש לה מינימום. נבחר $d \in B$ איבר כלשהו עבורו $\alpha(d)$ שווה למינימום הזה (בפרט, $d \neq 0$). לפי ההנחה, לכל $b \in B$ קיימים k ו-r כך ש-$b = kd + r$, ו-$\alpha(r) < \alpha(d)$ אם $r \neq 0$. כיוון ש-b, d שייכים ל-B, כך גם $r = b - kd$, ולכן אם $r \neq 0$ נקבל סתירה למזעריות של $\alpha(d)$. □

השתמשנו כבר מספר פעמים בקבוצת "הצירופים הלינאריים" מעל A של תת-קבוצה של A. זה מושג לחלוטין לא מעניין אם A הוא שדה, אבל מעניין מאד לחוג כללי:

הגדרה 2.3.28. תת-קבוצה I של חוג A נקראת *אידיאל* אם לכל $x, y \in I$ ולכל $a, b \in A$, גם $ax + by \in I$ אידיאל

נדבר על אידיאלים בקרוב. כעת רק נשים לב שאם $a \in A$, הקבוצה $(a) = \{ab \mid b \in A\}$ היא אידיאל. אידיאל מהצורה הזו נקרא *אידיאל ראשי*, ואת ההגדרה של תחום ראשי אפשר לנסח כך: אידיאל ראשי

תרגיל 2.3.29. הוכיחו שתחום הוא ראשי אם ורק אם כל אידיאל בו הוא ראשי.

הערה 2.3.30. הוכחנו שאם תחום הוא אוקלידי אז הוא ראשי, ואם תחום הוא ראשי אז הוא תחום פריקות יחידה. הגרירות הללו הן גרירות ממש: הכיוון ההפוך אינו נכון. בפועל, ברוב המקרים בהם מוכיחים שתחום הוא ראשי הוא על-ידי מציאת פונקציה אוקלידית, אבל אפשר למצוא דוגמאות של תחומים ראשיים שאינם אוקלידיים. מה שיותר חשוב, יש "הרבה יותר" תחומי פריקות יחידה מאשר תחומים ראשיים, וישנם גם תחומים שאינם תחומי פריקות יחידה, כפי שנראה מיד

תרגיל 2.3.31. הוכיחו שחוג הפולינומים $\mathbb{Z}[x]$ אינו תחום ראשי (מצד שני, זו עובדה שאם A תחום פריקות יחידה, אז כך גם $A[x]$)

דוגמא 2.3.32. החוג $A = \mathbb{Z}[\sqrt{-5}] = \{n + m\sqrt{-5} \mid n, m \in \mathbb{Z}\}$ הוא תחום שאינו תחום פריקות יחידה (כאשר החיבור והכפל מוגדרים באופן דומה ל-$\mathbb{Z}[i]$). אז 2 אינו ראשוני: הוא מחלק את $6 = (1 + \sqrt{-5})(1 - \sqrt{5})$, אבל בבירור לא את הגורמים (וברור ש-2 אינו הפיך ב-A). מצד שני, בתרגיל 2.4.17 נראה ש-2 אינו פריק ב-A.

2.4 פריקות בחוג גאוס

נראה עכשיו איך הפריקות נראית בדוגמא שהתחלנו איתה, חוג השלמים של גאוס $\mathbb{Z}[i]$. בתור התחלה, נזכיר שראינו בתרגיל 2.3.12 ש-$K = \mathbb{Q}[i]$ הוא שדה, ולכל $x \in \mathbb{Q}[i]$ התאמנו העתקה לינארית l_x של K לעצמו, כמרחב וקטורי מעל $\mathbb{Q}$. לכל העתקה כזו אפשר להסתכל על הדטרמיננטה, ולקבל איבר $N(x)$, שאנו קוראים לו *הנורמה* של x. מנקודת המבט הזו ברור שהנורמה היא כפלית: נורמה

טענה 2.4.1. *לכל* $x, y \in \mathbb{Q}[i]$ *מתקיים* $N(xy) = N(x)N(y)$.

הוכחה. לכל x, y מתקיים $l_{xy} = l_x l_y$, אז הטענה נובעת מכפליות הדטרמיננטה $\square$

מאידך, חישבנו באותו תרגיל שאם $x = a + bi$, אז $N(x) = x\bar{x} = a^2 + b^2$, כאשר $\bar{x} = a - bi$ הצמוד המרוכב של x. הנוסחה הזו חשובה מכמה סיבות: ראשית, היא מראה שהתמונה של הצמצום שלה ל-$\mathbb{Z}[i]$ מוכלת ב-$\mathbb{Z}$. שנית, זהו בדיוק הביטוי שהתעניינו בו בהקשר של השלשות הפיתגוריות. במלים אחרות,

מסקנה 2.4.2. *מספר טבעי הוא סכום של שני ריבועים אם ורק אם הוא מהצורה* $N(x)$ *עבור* $x \in \mathbb{Z}[i]$

בצירוף עם הטענה הקודמת, אנחנו מקבלים פתרון פשוט של תרגיל 1.2.2: קבוצת האיברים שניתן להציג כסכום שני ריבועים סגורה תחת כפל.

לבסוף, הנה הקישור לפריקות יחידה:

טענה 2.4.3. *פונקציית הנורמה היא פונקציה אוקלידית על* $A = \mathbb{Z}[i]$*. בפרט, זהו תחום ראשי ובעל פריקות יחידה.*

הוכחה. נניח ש-$a, b \in A$ ו-$b \neq 0$. קבוצת הנורמות של איברים בקבוצה $\{a - kb \mid k \in A\}$ היא קבוצה לא ריקה של טבעיים, ולכן יש לה מינימום. נבחר k עבורו מתקבל המינימום. עלינו להוכיח ש-$N(a - kb) < N(b)$. כיוון שהנורמה מוגדרת וכפלית על כל $\mathbb{Q}[i]$, זה שקול לטענה ש-$N(\frac{a}{b} - k) < 1$.

במלים אחרות, נתון לנו המספר המרוכב $z = \frac{a}{b}$, ו-k הוא איבר של A שנמצא במרחק מינימלי מ-z. עלינו להראות שהמרחק הזה קטן מ-1. אם S הריבוע שאורך צלעו 1 ומרכזו z, יש בריבוע הזה לפחות איבר אחד מ-A, ומאידך, הריבוע מוכל בעיגול היחידה סביב z, אז סיימנו. $\square$

השלב הבא הוא להבין משהו על ההפיכים והראשוניים בחוג גאוס.

מסקנה 2.4.4. *נסמן* $A = \mathbb{Z}[i]$

1. *האיברים ההפיכים ב-A הם* $1, -1, i, -i$.

2. *מספר שלם n הוא ראשוני כאיבר של A אם ורק אם הוא ראשוני ב-$\mathbb{Z}$ ואינו מהצורה $N(x)$ עבור* $x \in A$.

3. *אם $x \in A$ אינו שלם, אז x ראשוני אם ורק אם $N(x)$ ראשוני כמספר שלם*

הוכחה. 1. ברור שהאיברים המצוינים הם הפיכים. מצד שני, אם $u \in A$ הוא איבר הפיך, אז $N(u) \in \mathbb{N}$ איבר הפיך (כי אם $uv = 1$ ב-A אז $1 = N(uv) = N(u)N(v)$), כלומר $N(u) = 1$. לכן u חייב להיות כאמור.

2. אם n אינו ראשוני ב-$\mathbb{Z}$ אז פירוק שלו ב-$\mathbb{Z}$ הוא גם פירוק לא טריוויאלי ב-A (כי אין הפיכים חדשים). אם $n = N(x) = a^2 + b^2 = (a - bi)(a + bi)$ אז השוויון מראה פירוק של n, שהוא פירוק ממש אם n אינו הפיך (ולא השתמשנו פה בכך ש-n ראשוני). מאידך, אם $p = xy$ ב-A, אז $p^2 = N(p) = N(xy) = N(x)N(y)$. אם x, y אינם הפיכים, אז בהכרח $N(x) = N(y) = p$.

3. נסמן $n = N(x) = x\bar{x}$. אם x ראשוני אז גם $\bar{x}$ ראשוני (ושניהם לא ב-$\mathbb{Z}$ לפי ההנחה), אז אם n אינו ראשוני ב-$\mathbb{Z}$, קיבלנו איבר שמתפרק לראשוניים בשתי צורות שונות. מאידך, אם x אינו ראשוני, אז $x = rs$ ב-A, ולכן $N(x) = N(r)N(s)$ פירוק לא טריוויאלי של $N(x)$ ב-$\mathbb{Z}$. □

לסיכום, הוכחנו שאם p ראשוני ב-$\mathbb{Z}$, אז או שהוא ראשוני ב-$\mathbb{Z}[i]$, או שהוא מכפלה של שני ראשוניים צמודים (ולא שלמים), וכל הראשוניים ב-$\mathbb{Z}[i]$ מתקבלים באופן הזה. השאלה שנותרה, כדי למיין בצורה מפורשת את הראשוניים, היא: בהינתן ראשוני שלם, איך להחליט האם הוא ראשוני ב-$\mathbb{Z}[i]$? ראינו שזה קורה אם ורק אם הוא לא מהצורה $N(x)$, אבל אנחנו רוצים תשובה יותר מפורשת.

הפתרון הוא להסתכל על השארית של הראשוני $p \in \mathbb{Z}$ ביחס ל-4. כיוון שעבור $p = 2$ התשובה פשוטה, אפשר להניח ש-p אי-זוגי. במקרה זה, השארית יכולה להיות 1 או 3. כיוון אחד הוא פשוט:

תרגיל 2.4.5. הוכיחו שאם $n + 1$ מתחלק ב-4, אז הוא אינו סכום של שני ריבועים. בפרט, אם n כזה הוא ראשוני, אז הוא נשאר ראשוני גם ב-$\mathbb{Z}[i]$

הכיוון השני הוא משפט של פרמה שנובע בקלות מהטענה הבאה, אותה נוכיח בקרוב.

טענה 2.4.6 (הלמה של לגרנז'). *אם p שלם ראשוני עבורו $p - 1$ מתחלק ב-4, אז p מחלק מספר מהצורה $n^2 + 1$*

מסקנה 2.4.7 (פרמה). *אם $p - 1$ מתחלק ב-4, אז הוא אינו ראשוני ב-$\mathbb{Z}[i]$*

הוכחה. אפשר להניח ש-p ראשוני ב-$\mathbb{Z}$. אז לפי הלמה של לגרנז', p מחלק את $m^2 + 1 = (m - i)(m + i)$ עבור איזשהו m שלם. אם p ראשוני, אז p מחלק את אחד מהגורמים, אבל זה בבירור לא יתכן. □

לסיכום:

מסקנה 2.4.8. *1. כל ראשוני מהצורה $4k + 3$ ב-$\mathbb{Z}$ הוא ראשוני ב-$\mathbb{Z}[i]$*

2. כל ראשוני אחר ב-$\mathbb{Z}$ הוא מכפלה של שני ראשוניים שונים ב-$\mathbb{Z}[i]$

3. כל הראשוניים ב-$\mathbb{Z}[i]$ הם מהצורה הנ"ל, וכל איבר ב-$\mathbb{Z}[i]$ הוא מכפלה סופית של איבר מהצורה הזו, יחידה עד כדי סדר והפיכים.

תרגיל 2.4.9. 1. מיצאו פירוק לגורמים ראשוניים של $56, 3 + 5i, 9 + i \in \mathbb{Z}[i]$

2. מצאו מחלק משותף מירבי של $6 - 17i, 18 + i$, ורישמו אותו כצירוף לינארי של איברים אלה מעל $\mathbb{Z}[i]$.

סוף הרצאה 4, 29 באוק

הנה המסקנה לגבי מספרים טבעיים שהם סכום של שני ריבועים:

מסקנה 2.4.10. *מספר טבעי n הוא סכום של שני ריבועים אם ורק אם לכל ראשוני p עבורו $p+1$ מתחלק ב-4 החזקה $v_p(n)$ היא זוגית.*

הוכחה. העובדה שכל מספר מהצורה הזו הוא סכום של שני ריבועים נובעת ישירות מהעובדות הנ"ל.

בכיוון ההפוך, נניח ש-$n = N(x) = x\bar{x}$. הפירוק של x לראשוניים הוא מהצורה $r_1 \dots r_k s_1 \dots s_l$, כאשר r_i ראשוניים ב-$\mathbb{Z}$ שהשארית שלהם 3 בחלוקה ב-4, ו-s_i אינם ב-$\mathbb{Z}$ (אולי עם חזרות). אז $n = x\bar{x} = r_1^2 \dots r_k^2 \cdot s_1\bar{s_1} \dots s_l\bar{s_l}$, כאשר כל $s_i\bar{s_i} = N(s_i)$ הוא ראשוני ב-$\mathbb{Z}$ עם שארית שונה מ-3 בחלוקה ב-4. זה מה שרצינו להוכיח. □

והנה מסקנה עבור שלשות פיתגוריות:

תרגיל 2.4.11. הוכיחו שראשוני הוא היתר של משולש ישר זווית עם ניצבים שלמים (חיוביים) אם ורק אם השארית שלו בחלוקה ב-4 היא 1

כמובן שכל שלשה פיתגורית בה היתר הוא ראשוני היא פרימיטיבית. מה לגבי שלשות פרימיטיביות בהן היתר אינו ראשוני?

טענה 2.4.12. *מספר טבעי חיובי c הוא היתר בשלשה פיתגורית פרימיטיבית אם ורק אם הוא מכפלה של ראשוניים שהשארית שלהם בחלוקה ב-4 היא 1*

לפני ההוכחה, נשים לב ראשית:

תרגיל 2.4.13. הוכיחו שריבוע זוגי לא יכול להיות סכום של שני ריבועים אי-זוגיים.

הוכחת טענה 2.4.12. לפי התרגיל, אפשר להניח ש-c אי-זוגי (ולכן אחד הניצבים זוגי והשני אי-זוגי). אם c מתחלק בראשוני p שהשארית שלו 3, ו-$c^2 = N(x) = x\bar{x}$, אז כיוון ש-p ראשוני ב-$\mathbb{Z}[i]$, הוא מחלק את x, ולכן את הרכיבים שלו, וזו סתירה לפרימיטיביות.

נותר להוכיח שכל מכפלה n של ראשוניים עם שארית 1 היא יתר בשלשה פרימיטיבית. אנחנו כבר יודעים ש-$n = N(x)$ עבור $x \in A$, כלומר $n^2 = N(x^2)$, והמטרה שלנו היא להראות שזו שלשה פרימיטיבית. נשים לב שזה בדיוק אומר ש-x^2 לא מתחלק באף גורם ראשוני p של n (ב-$\mathbb{Z}$). נוכיח זאת בשני שלבים:

ראשית, נניח ש-p ראשוני ב-$\mathbb{Z}$, כך ש-$p = N(x)$ ב-$\mathbb{Z}[i]$. אז לכל k מתקיים $p^k = N(x^k) = a^2 + b^2$. אנחנו טוענים ש-p לא מחלק את a, b. אחרת, $p = x\bar{x}$ מחלק את x^k, כלומר $\bar{x}$ מחלק את x^{k-1}. אבל זה לא יתכן, כי $x, \bar{x}$ ראשוניים שונים ב-$\mathbb{Z}[i]$.

כיוון ש-n מכפלה של חזקות של ראשוניים מהשלב הראשון, כדי לסיים את ההוכחה מספיק להראות שאם $m = N(x), n = N(y)$ שלמים זרים, והרכיבים של x ושל y זרים (כלומר, x, y לא מתחלקים באיבר לא הפיך של $\mathbb{Z}$), אז גם הרכיבים של xy זרים. נשאיר את זה כתרגיל. □

תרגיל 2.4.14. השלימו את ההוכחה: הוכיחו שאם $x = a + bi$ עבור רכיבים a, b זרים ו-$y = c + di$ עבור c, d זרים, ו-$m = N(x), n = N(y)$ גם הם זרים, אז גם הרכיבים של $x \cdot y$ זרים.

ההוכחה נותנת קצת יותר: אם c היתר בשלשה פרימיטיבית, אז הוא מהצורה $N(x)$, כאשר הרכיבים u,v של $x=u+vi$ זרים (ב-$\mathbb{Z}$), ובמקרה הזה, $N(x^2)=c^2$ נותן את השלשה. כיוון ש-$x^2=u^2-v^2+2uvi$, הניצבים בשלשה נתונים על-ידי u^2-v^2 ו-$2uv$, והיתר נתון על-ידי $c=u^2+v^2$. מאידך, ברור שכל u,v טבעיים זרים נותנים שלשה פיתגורית פרימיטיבית בצורה הזו, ולכן קיבלנו:

מסקנה 2.4.15. *כל שלשה פיתגורית פרימיטיבית היא מהצורה* $\langle u^2-v^2,2uv,u^2+v^2\rangle$, *עבור* u,v *זרים יחידים.*

את המסקנה האחרונה אפשר להוכיח גם בצורה גאומטרית. ראינו שניתן לזהות שלשות פיתגוריות עם נקודות על מעגל היחידה שהקואורדינטות שלהן רציונליות (ליתר דיוק, עם הנקודות על המעגל שנמצאות ברביע הראשון). כיוון שהנקודה $P=\langle -1,0\rangle$ לא מעניינת מבחינתו, אפשר להסתכל על המעגל ללא נקודה זו, ואז אפשר לזהות את הנקודות על המעגל ללא P עם הישר הממשי דרך *ההטלה הסטריאוגרפית*: דרך כל נקודה $Q\neq P$ עובר ישר יחיד, והוא נחתך בנקודה יחידה $\langle 0,t\rangle$ עם ציר ה-y. זו העתקה רציפה הפיכה, וחישוב פשוט מראה שהמספר t מתאימה לנקודה $Q(t)=\langle\frac{1-t^2}{1+t^2},\frac{2t}{1+t^2}\rangle$ על המעגל. בפרט, אם t רציונלי, אז גם הנקודה, וקיבלנו שלשה פיתגורית. בכיוון השני, אם התחלנו עם נקודה רציונלית על המעגל, t מתקבלת מפעולות לינאריות על הנקודות הרציונליות P,Q, אז t חייב להיות רציונלי. אז $Q(t)$ מתאימה באופן חד-חד-ערכי ועל בין שלשות פיתגוריות פרימיטיביות לנקודות רציונליות t בין 0 ל-1.

אם נרשום $t=\frac{u}{v}$, נקבל את הנקודה $\langle\frac{v^2-u^2}{v^2+u^2},\frac{2uv}{v^2+u^2}\rangle$ שקיבלנו לעיל. את העובדות האחרות שקיבלנו לעיל יותר קשה לקבל באופן הזה. ניצלנו כאן את העובדה שלמרות שחיפשנו פתרונות במספרים טבעיים, ניתן לתרגם את הבעיה לפתרונות בשברים, וזה לעתים הרבה יותר קל.

ההצגה שקיבלנו עבור שלשות פיתגוריות מאפשרת לנו להוכיח את המקרה $n=4$ של משפט פרמה (שבמקרה זה אכן הוכח על-ידי פרמה). למעשה, יותר קל להוכיח טענה יותר חזקה:

מסקנה 2.4.16. *לא קיים פתרון בשלמים חיוביים למשוואה* $x^4+y^4=z^2$

סוף הרצאה 5, 2 בנוב

הוכחה. נניח שקיים פתרון, ונבחר כזה עבורו z מינימלי. אז x,y,z זרים בזוגות, ולכן $\langle x^2,y^2,z\rangle$ שלשה פיתגורית פרימיטיבית. לפי מסקנה 2.4.15,

$$x^2=u^2-v^2$$
$$y^2=2uv$$
$$z=u^2+v^2$$

עבור u,v זרים. לכן $\langle x,v,u\rangle$ שלשה פיתגורית פרימיטיבית, ולפי אותה טענה,

$$x=n^2-m^2$$
$$v=2nm$$
$$u=n^2+m^2$$

עבור n, m זרים. בפרט, $y^2 = 4nm(n^2+m^2)$. כיוון ש-n, m, n^2+m^2 זרים בזוגות, נובע מזה ש-$m = r^2, n = s^2$, ו-$n^2+m^2 = t^2$ ריבועים. לכן $t^2 = s^4 + r^4$, אבל $0 < t \leqslant t^2 = u < z$, בסתירה למינימליות של z. □

השיטות שהשמשנו בהן כדי לחקור את חוג גאוס, מאפשרות לנו לחקור גם חוגים אחרים, כגון $\mathbb{Z}[\sqrt{-5}]$, אבל כפי שכבר הזכרנו בדוגמא 2.3.32, התשובה עשוי להיות שונה:

תרגיל 2.4.17. נגדיר את הנורמה על $A = \mathbb{Z}[\sqrt{-5}]$ באופן דומה להגדרה עבור חוג גאוס. הוכיחו שההפיכים ב-A הם $1, -1$. הוכיחו ש-2 ו-3 אינם פריקים ב-A. מיצאו דוגמה שמראה ש-N במקרה הזה אינה פונקציה אוקלידית.

3 מנות ושאריות

3.1 העתקות של חוגים

נניח שנתונה מערכת משוואות פולינומיות $P(\bar{x}) = 0$ (בכמה משתנים) עם מקדמים שלמים, ואנחנו רוצים להראות שאין למערכת פתרון שלם. נניח שנתונה לנו פונקציה $f : \mathbb{Z} \to A$ לחוג A. אז אפשר להפעיל את f על המקדמים של הפולינומים P, ולקבל מערכת משוואות P_f עם מקדמים ב-A. יתכן שאת המערכת P_f הרבה יותר קל לפתור או לנתח מאשר את המערכת המקורית.

אם $\bar{a}$ פתרון שלם של המערכת המקורית, אז אפשר להפעיל גם עליו את f, ולקבל סדרה סופית $f(\bar{a})$ של איברים ב-A. האם הסדרה הזו מהווה פתרון של P_f? התשובה היא "כן" אם f *הומומורפיזם*:

הומומורפיזם
העתקה של חוגים

הגדרה 3.1.1. פונקציה $f : A \to B$ בין שני חוגים (לא בהכרח חילופיים) נקראת *הומומורפיזם* (או *העתקה של חוגים*) אם לכל $a, b \in A$:

1. $f(a+b) = f(a) + f(b)$
2. $f(ab) = f(a)f(b)$
3. $f(1_A) = 1_B$

איזומורפיזם
אנדומורפיזם
אוטומורפיזם

הומומורפיזם $f : A \to B$ נקרא *איזומורפיזם* אם קיים הומומורפיזם $g : B \to A$ כך ש-$g \circ f$ ו-$f \circ g$ פונקציות הזהות. הומומורפיזם מ-A ל-A נקרא *אנדומורפיזם* של A, ואיזומורפיזם מ-A ל-A נקרא *אוטומורפיזם* של A.

תת-חוג

תת-חוג של חוג B הוא תת-קבוצה A של B עבורה העתקת ההכלה היא הומומורפיזם.

דוגמא 3.1.2. לכל חוג A (לא בהכרח חילופי) קיים הומומורפיזם יחיד f מ-$\mathbb{Z}$ ל-A, שנתון על-ידי $f(n) = n \cdot 1_A$ עבור n טבעי, כאשר $n \cdot 1_A$ הוא הסכום של 1_A עם עצמו n פעמים.

דוגמא 3.1.3. העתקת ההצמדה $x \mapsto \bar{x}$ היא אוטומורפיזם של חוג השלמים של גאוס (וגם של שדה המרוכבים)

דוגמא 3.1.4. נניח ש-A חוג (חילופי), $\bar{a} = \langle a_1, \dots, a_n \rangle \in A^n$. אז ההעתקה $t_{\bar{a}} : A[x_1, \dots, x_n] \to A$ הנתונה על-ידי $t_{\bar{a}}(p) = p(\bar{a})$ היא הומומורפיזם.

נשים לב שהתנאי $f(1)=1$ בהגדרת ההומומורפיזם הוא הכרחי: למשל, אם $B=\mathbb{Z}\times\mathbb{Z}$ כמו בדוגמא 2.3.8, תת-הקבוצה $A=\{\langle x,0\rangle \mid x\in\mathbb{Z}\}\subseteq B$ של B היא חוג עם פעולות הכפל והחיבור המצומצמות מ-B, אבל היא לא תת-חוג בהגדרה שלנו.

תרגיל 3.1.5. נניח ש-$f:A\to B$ העתקה של חוגים, ונסמן ב-$C=f(A)$ את התמונה של f. הוכיחו את הטענות הבאות:

1. $f(0)=0$ ו-$f(-a)=-f(a)$ לכל $a\in A$
2. C הוא תת-חוג
3. אם A חילופי או שדה, אז גם C כזה
4. הוכיחו ש-f חד-חד-ערכית ועל אם ורק אם היא איזומורפיזם

המוטיבציה בה התחלנו נתונה בתרגיל הבא:

תרגיל 3.1.6. נניח ש-A חוג חילופי, ו-$p(\bar{x})=\sum a_{\bar{i}}\bar{x}^{\bar{i}}$ פולינום עם מקדמים $a_{\bar{i}}$ ב-A. נניח שנתונה העתקה $f:A\to B$ לחוג B. הוכיחו שאם $\bar{a}$ פתרון של המשוואה $p(\bar{x})=0$ ב-A, אז $f(\bar{a})$ פתרון של המשוואה $p_f(\bar{x})=0$ ב-B, כאשר $p_f(\bar{x})=\sum f(a_{\bar{i}})\bar{x}^{\bar{i}}$.

תרגיל 3.1.7. הוכיחו שלא קיים הומומורפיזם מ-$\mathbb{Z}[\sqrt{-5}]$ לחוג השלמים של גאוס

בפרט, אם אנחנו רוצים להוכיח שלמערכת של משוואות דיאופנטיות (כלומר, משוואות פולינומיות מעל השלמים) אין פתרון, מספיק למצוא העתקה מ-$\mathbb{Z}$ לחוג כלשהו A בו לתמונה של המערכת אין פתרונות. ראינו בדוגמא 3.1.2 שלכל חוג יש העתקה יחידה מ-$\mathbb{Z}$, ולכן מציאת העתקה כזו שקולה למציאת חוג מתאים A. איזה חוגים עשויים להיות מעניינים בהקשר הזה? בדוגמא הבאה השתמשנו בהקשר של שלשות פיתגוריות:

דוגמא 3.1.8. נסמן $A=\{0,1,2,3\}$, ונגדיר חיבור ב-A על-ידי $x+y=z$ אם z השארית של הסכום הרגיל של x,y בשלמים בחלוקה ב-4, ובאופן דומה לכפל. קל לבדוק שהפעולות הללו מגדירות מבנה של חוג, וההעתקה היחידה מ-$\mathbb{Z}$ אל A היא העתקת השארית בחלוקה ב-4. בדיקה ישירה מראה שהריבוע של כל איבר ב-A הוא 0 או 1. בפרט, סכום של שני ריבועים בהכרח שונה מ-3, ולכן מספר שלם שהוא סכום של שני ריבועים אינו מהצורה $4k+3$.

3.2 מנות

העתקות כמו בדוגמא האחרונה שימושיות מאד כדי להראות שלמשוואה אין פתרונות (לפחות מצורה מסוימת), אבל האופן שבו הגדרנו את A לא נוח מבחינות מסוימות: כדי לחשב סכומים ומכפלות צריך לעבור לשלמים, והוכחה של תכונות החוג (כמו חוק הקיבוץ) היא מסורבלת. מעבר לזה, הגדרה כזו לא מאפשרת לחשב את כל האפשרויות השונות להעתקות כאלה, ולא ברור איך להכליל אותה להעתקות מחוגים שאינם $\mathbb{Z}$ (בייחוד כאלה שאינם אוקלידיים).

נשים לב שמנקודת המבט של פתרון משוואות, אנחנו מתעניינים רק בתמונה של ההעתקה, ולכן אפשר להניח שההעתקה שאנחנו מחפשים היא על. לכן, אנחנו מנסים לענות בצורה יותר שיטתית על השאלה: בהינתן חוג A, עבור איזה חוגים B קיימת העתקה $f:A\to B$ שהיא על, ואיך עשויה

להיראות העתקה כזו? ראינו לעיל שאם f היא בנוסף חד-חד-ערכית אז היא איזומורפיזם. זה אומר ש-B הוא אותו חוג כמו A, עד כדי "שינוי שמות". לרוב, העתקה כזו לא באמת מפשטת את הבעיה, אלא רק מעבירה אותה (אולי) לשפה אחרת. לכן, מה שמעניין אותנו בעיקר זה באיזה אופנים f עשויה להיות לא חד-חד-ערכית.

נזכיר שאם $f : A \to Q$ היא העתקה של קבוצות, אפשר "למדוד" באיזו מידה f לא חד-חד-ערכית באמצעות יחס שקילות על A: האיבר $a, b \in A$ הם שקולים אם $f(a) = f(b)$. למשל, f חד-חד-ערכית אם ורק אם היחס הזה הוא יחס השוויון. אם f היא על, אפשר לזהות את Q (באופן יחיד) עם המנה ביחס השקילות הזה, ואת f עם העתקת המנה. מצד שני, אם מתחילים ביחס שקילות כלשהו, העתקת המנה אל קבוצת המנה היא על. במלים אחרות, לתת העתקה מ-A על קבוצה כלשהי Q שקול ללתת יחס שקילות על A.

כל זה נכון בפרט אם A ו-Q הם מרחבים וקטוריים מעל שדה כלשהו $\Bbbk$, אבל אם f היא בנוסף העתקה לינארית, אפשר להגיד יותר: מחלקת השקילות U של $0 \in A$ נקראת במקרה זה הגרעין של f, וניתן לתאר את יחס השקילות הנ"ל במונחים של U: האיברים $a, b \in A$ הם שקולים אם ורק אם $a - b \in U$. גם כאן, אם U תת-מרחב כלשהו של A, אז קיימת העתקה לינארית $f : A \to A/U$ על מרחב A/U, מרחב המנה, שהגרעין שלה הוא U, והעתקה זו נקבעת ביחידות. במלים אחרות, לתת העתקה לינארית מ-A על מרחב Q שקול ללתת תת-מרחב U של A.

המטרה שלנו היא לתת תיאור דומה במקרה של חוגים. לשם כך, נתאר ראשית את הגרעין של העתקה בין חוגים:

הגדרה 3.2.1. אם $f : A \to B$ העתקה של חוגים, *הגרעין של ההעתקה* f הוא הקבוצה $\operatorname{Ker}(f) = \{a \in A \mid f(a) = 0\}$. גרעין של העתקה

לגרעין יש מבנה שכבר הזכרנו:

תרגיל 3.2.2. הוכיחו שהגרעין של כל העתקה בין חוגים הוא אידיאל

נראה, לכן, סביר לצפות שהעתקות מ-A על חוגים אחרים מתוארות על-ידי אידיאלים ב-A. זה אכן המצב:

טענה 3.2.3. *נניח ש-A חוג (חילופי), I אידיאל ב-A, ו-$g : A \to B$ העתקה של חוגים כך ש-$g(I) = 0$. אז:*

1. *קיים חוג A/I והעתקה של חוגים $\pi : A \to A/I$ שהיא על והגרעין שלה I*
2. *יש העתקה יחידה $h : A/I \to B$ כך ש-$h \circ \pi = g$.*
3. *הגרעין של h הוא $\pi(J)$ כאשר J הגרעין של g, והתמונה של h שווה לתמונה של g. בפרט, אם g היא על והגרעין שלה הוא I, אז h איזומורפיזם*

מסקנה אחת של הסעיף השלישי היא שהחוג A/I וההעתקה π כמו בסעיף הראשון הם יחידים, עד כדי איזומורפיזם יחיד. במקרה ש-I נוצר על-ידי איבר אחד a, נרשום לעתים A/a במקום A/I.

הוכחה. 1. נגדיר יחס $\sim$ על A על-ידי: $a \sim b$ אם $a - b \in I$. כיוון ש-I סגור לחיבור, זהו יחס שקילות על A. נגדיר את A/I להיות קבוצת המנה, ואת π להיות העתקת המנה. האיברים

$0,1$ של המנה מוגדרים להיות $\pi(0), \pi(1)$, בהתאמה. אז π על, וברור ש-$\pi(a)=0$ אם ורק אם $a\in I$. נותר להגדיר את הפעולות על $Q={}^{A}/_{I}$ באופן ש-π יהיה העתקה של חוגים.

כיוון ש-π היא על, יש רק אפשרות אחת להגדיר את הפעולות: $\pi(a)+\pi(b)=\pi(a+b)$ ו-$\pi(a)\cdot\pi(b)=\pi(a\cdot b)$. עלינו להראות שזה מוגדר היטב, כלומר: אם $\pi(a)=\pi(a')$ ו-$\pi(b)=\pi(b')$ אז $\pi(a+b)=\pi(a'+b')$ ו-$\pi(ab)=\pi(a'b')$. כיוון ש-$\pi(a)=\pi(a')$, ההפרש $c=a-a'$ שייך ל-I, באופן דומה $d=b-b'\in I$. אז $a+b-(a'+b')=c+d\in I$, ו-$ab-a'b'=a(b-b')+(a-a')b'=ad+cb'\in I$. זה מראה שהפעולות מוגדרות היטב. העובדה שהפעולות הללו מקיימות את הגדרת החוג נובעת ישירות מזה ש-π מכבדת את הפעולות הללו, ונשאיר זאת בתור תרגיל.

2. היחידות נובעת אוטומטית מהנוסחה $g=h\circ\pi$ ומהעובדה ש-π היא על. הקיום של h נובע מכך שאם $a\sim b$ אז $g(a)=g(b)$. העובדה ש-h היא העתקה של חוגים שוב נובעת מהנוסחה (תרגיל).

3. תרגיל $\square$

תרגיל 3.2.4. השלימו את ההוכחה

תרגיל 3.2.5. נניח ש-$\Bbbk$ שדה, $a\in\Bbbk$, ו-$t_a:\Bbbk[x]\to\Bbbk$ ההעתקה מדוגמא 3.1.4. חשבו את הגרעין של t_a.

סוף הרצאה 6, 5 בנוב

בפרט, אנחנו מקבלים מיון של כל המנות של $\mathbb{Z}$:

מסקנה 3.2.6. *אם $f:\mathbb{Z}\to A$ העתקה על, אז A איזומורפי ל-${}^{\mathbb{Z}}/_{n}$, עבור טבעי n*

בפרט, אם f אינה איזומורפיזם (כלומר $n>0$), אז A סופי, בגודל n.

הוכחה. ל-f מתאים אידיאל ב-$\mathbb{Z}$, וראינו שכל אידיאל ב-$\mathbb{Z}$ הוא ראשי, כאשר $(n)=(m)$ אם ורק אם $|n|=|m|$ $\square$

לכל $n>0$, לכל איבר של ${}^{\mathbb{Z}}/_{n}$ יש נציג יחיד שהוא שארית בחלוקה ב-n, כלומר איבר $0\leqslant r<n$, ולעתים נוח לחשוב על המנה במונחים אלה, אבל תיאור כזה לא קיים באופן כללי לחוגים אחרים, אפילו אם הם אוקלידיים.

לעובדה שחוג הוא סופי יש יתרון מהסוג שכבר ראינו:

תרגיל 3.2.7. נניח ש-a איבר בחוג A. הוכיחו ש-a ראשוני אם ורק אם ${}^{A}/_{a}$ תחום שלמות.

הוכיחו שאם חוג סופי הוא תחום שלמות אז הוא שדה. הסיקו ש-${}^{\mathbb{Z}}/_{n}$ הוא שדה אם ורק אם $n>0$ ראשוני.

השדה הראשוני

השדה ${}^{\mathbb{Z}}/_{p}$, עבור p ראשוני, נקרא *השדה הראשוני* ממציין p ומסומן ב-$\mathbb{F}_p$. חצי מהשם מוסבר על-ידי ההגדרה הבאה.

הגדרה 3.2.8. לכל חוג A, הגרעין של ההעתקה היחידה מ-$\mathbb{Z}$ ל-A הוא מהצורה (n) עבור מספר טבעי יחיד n. המספר הזה נקרא *המציין* של A.

מציין

מהתכונות הבסיסיות של המנה נובע לכן שאם A הוא חוג ממציין p אז הוא מכיל עותק יחיד של השדה $\mathbb{F}_p$. במובן הזה $\mathbb{F}_p$ הוא ראשוני.

3.3 יוצרים

על מנת להקל על התיאור של העתקות, נוח לדבר על קבוצות יוצרים של חוג, שמקבילות לקבוצות פורשות במרחבים וקטוריים:

הגדרה 3.3.1. תת-קבוצה S של חוג A נקראת *קבוצת יוצרים* אם לא קיים תת-חוג *ממש* של A שמכיל את S. קבוצת יוצרים

דוגמא 3.3.2. אם A חוג כלשהו, אז חוג הפולינומים $A[x_1,\dots,x_n]$ נוצר על-ידי $A\cup\{x_1,\dots,x_n\}$ (או באופן יותר כללי, על-ידי כל קבוצה $S\cup\{x_1,\dots,x_n\}$, כאשר S יוצרת את A)

תרגיל 3.3.3. הוכיחו ש-A נוצר על-ידי הקבוצה הריקה אם ורק אם הוא מנה של $\mathbb{Z}$.

תרגיל 3.3.4. הוכיחו שחוג השלמים של גאוס נוצר על-ידי $\{i\}$

אם T ו-S שתי העתקות לינאריות ממרחב וקטורים U למרחב אחר V, והן מסכימות על תת-קבוצה פורשת של U, אז הן שוות. המצב דומה עבור חוגים:

תרגיל 3.3.5. נניח ש-$f,g:A\to B$ הומומורפיזמים. הוכיחו שהקבוצה $\{a\in A\mid f(a)=g(a)\}$ היא תת-חוג של A. הסיקו שאם S קבוצת יוצרים של A, ו-$f(a)=g(a)$ לכל $a\in S$, אז $f=g$.

המשמעות של המסקנה האחרונה היא שכדי לתאר העתקה מ-A לאיזשהו חוג, מספיק לומר לאן הולכים יוצרים. הנה דוגמא חשובה:

טענה 3.3.6. *נניח ש-$a_1,\dots,a_n\in A$ איברים של חוג A. אז קיימת העתקה יחידה $f:\mathbb{Z}[x_1,\dots,x_n]\to A$ כך ש-$f(x_i)=a_i$.*

הוכחה. על-מנת להוכיח קיום, נשים לב שלכל $p(\bar{x})\in\mathbb{Z}[\bar{x}]$ ניתן לחשב את הערך $p(\bar{a})$ של הפולינום $p(\bar{x})$ על האיבר $\bar{a}$, איבר ב-A. נגדיר $f(p)=p(\bar{a})$. קל לראות (כמו בתרגיל 3.1.4) שזהו הומומורפיזם, והוא מקיים $f(x_i)=a_i$. היחידות נובעת מכך ש-$\{x_1,\dots,x_n\}$ יוצרים את $\mathbb{Z}[x_1,\dots,x_n]$. □

קבוצות יוצרים רלוונטיות גם כשהן מופיעות בטווח:

תרגיל 3.3.7. נניח ש-$f:A\to B$ העתקה של חוגים, וש-$S\subseteq B$ יוצרת את B. הוכיחו שאם S מוכלת בתמונה של f, אז f היא על.

בפרט, אנחנו מקבלים את התיאור הבא של חוג השלמים:

דוגמא 3.3.8. לפי טענה 3.3.6, קיימת העתקה יחידה f מ-$\mathbb{Z}[x]$ לחוג השלמים ששולחת את x ל-i. כיוון ש-i יוצר את חוג השלמים, העתקה זו היא על. מהו הגרעין של f? הפולינום x^2+1 נמצא בגרעין כיוון ש-$f(x^2+1)=f(x)^2+1=i^2+1=0$, ולכן גם כל האידיאל שנוצר על-ידו. כדי להראות שזהו כל הגרעין, נניח ש-$f(p(x))=0$. חלוקה עם שארית ב-$\mathbb{Q}[x]$ מאפשרת לנו לרשום $p(x)=q(x)(x^2+1)+r(x)$, כאשר q,r פולינומים מעל $\mathbb{Q}$, ו-r לינארי. אם m המכנה המשותף של כל המקדמים, אז $mp(x)=q'(x)(x^2+1)+r'(x)$, כאשר q',r' עם מקדמים ב-$\mathbb{Z}$. נפעיל את f על שני הצדדים ונקבל $0=f(m)f(p(x))=f(mp(x))=f(q'(x)(x^2+1))+f(r'(x))=f(r'(x))=ai+b$

כאשר $r'(x) = ax + b$. ביטוי כזה יכול להיות שווה ל-0 ב-$\mathbb{Z}[i]$ רק אם $a = b = 0$, כלומר, $p(x) = q(x)(x^2 + 1)$. השוואת המקדמים מראה שהמקדמים של q חייבים להיות ב-$\mathbb{Z}$.

תרגיל 3.3.9. נסמן $A = \mathbb{Z}[i]$, ונניח ש-p ראשוני ב-$\mathbb{Z}$. הוכיחו ש-$\mathbb{k} = A/(p)$ חוג שמכיל את $\mathbb{F}_p$, בעל p^2 איברים.

נסמן ב-r את השארית של p ביחס ל-4. הוכיחו:

1. אם $r = 3$ אז $\mathbb{k}$ שדה
2. אם $r = 1$ אז $\mathbb{k}$ הוא חוג עם מחלקי אפס
3. אם $r = 2$ (כלומר $p = 2$) אז יש ב-$\mathbb{k}$ איבר $\epsilon \neq 0$ כך ש-$\epsilon^2 = 0$

3.4 שאריות

נתמקד עכשיו בחוגי מנה של $\mathbb{Z}$, בפרט בשדות $\mathbb{F}_p$, עבור ראשוני $p > 0$. כזכור, אמרנו שהחוג A הוא ממציין p אם הוא מכיל את $\mathbb{F}_p$. לחוגים כאלה יש מבנה נוסף:

טענה 3.4.1. *אם A חוג ממציין $p > 0$, ההעתקה $\mathrm{Fr} : A \to A$ הנתונה על-ידי $\mathrm{Fr}(a) = a^p$ היא אנדומורפיזם של A.*

האנדומורפיזם הזה נקרא *העתקת הפרובניוס* **העתקת הפרובניוס**

הוכחה. העובדה ש-Fr כפלית ברורה ולא תלויה במציין, צריך להוכיח שהיא שומרת על חיבור. משפט הבינום אומר שלכל $a, b \in A$,

$$\mathrm{Fr}(a+b) = (a+b)^p = \sum_{0 \leqslant i \leqslant p} \binom{p}{i} a^i b^{p-i}$$

כאשר $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ המקדם הבינומי. המונה מתחלק ב-p, אבל כאשר $0 < i < p$ המכנה לא, אז המקדם כולו מתחלק ב-p במקרה זה. כיוון שהמציין של A הוא p, המספר הזה שווה ל-0 ב-A, ולכן הסכום כולו הוא $a^p + b^p = \mathrm{Fr}(a) + \mathrm{Fr}(b)$. □

ראינו בתרגיל 3.3.5 שקבוצת האיברים $E = \{a \in A \mid f(a) = g(a)\}$ בחוג A ששני ההומומורפיזמים $f, g : A \to B$ ממנו מסכימים עליהם, היא תת-חוג. קל לראות שאם איבר של E הוא הפיך ב-A, אז ההופכי שלו גם שייך ל-E, ובפרט, אם A שדה אז גם E שדה. במקרה ש-A חוג ממציין p אפשר להתבונן במקרה הפרטי ש-$B = A$, וההעתקות הן הזהות והפרובניוס. אנחנו מקבלים:

מסקנה 3.4.2. *בכל חוג A ממציין $p > 0$, תת-הקבוצה $A^{\mathrm{Fr}} = \{a \in A \mid a^p = a\}$ היא תת-חוג של A. אם A שדה, אז תת-החוג הזה הוא $\mathbb{F}_p$.*

תת-החוג A^{Fr} נקרא *חוג השבת* של Fr (או *שדה השבת*, אם A שדה). **חוג השבת** **שדה השבת**

הוכחה. החלק הראשון נובע מהדיון לעיל. לגבי החלק השני, אנחנו כבר יודעים ששדה השבת מכיל את $\mathbb{F}_p$, אבל כל איבר בשדה השבת הוא פתרון של המשוואה $x^p - x = 0$, וזו משוואה פולינומית ממעלה p, אז בשדה יש לה לכל היותר p פתרונות. □

עבור השדה $\mathbb{F}_p$ עצמו, המסקנה היא שהאיברים הם בדיוק השורשים של הפולינום $x^p - x$. מנקודת המבט של השלמים, אנחנו מקבלים:

מסקנה 3.4.3 (המשפט הקטן של פרמה). *לכל מספר שלם n וראשוני p, המספר $n^p - n$ מתחלק ב-p*

עבור $x \in \mathbb{F}_p$ שונה מ-0, אפשר לחלק ב-x ולקבל $x^{p-1} - 1 = 0$. לכן השורשים של הפולינום הזה ב-$\mathbb{F}_p$ הם בדיוק האיברים ההפיכים שם (כל אחד בריבוי אחד), כלומר $\prod_{\alpha \in \mathbb{F}_p^\times}(x - \alpha) = x^{p-1} - 1$. בפרט, עבור $x = 0$ מקבלים:

מסקנה 3.4.4 (משפט ווילסון). *לכל $p > 0$ ראשוני, $\prod_{\alpha \in \mathbb{F}_p^\times} \alpha = -1$. בפרט, p מחלק את $(p-1)! + 1$.*

עכשיו אפשר להחזיר חוב ולהוכיח את הלמה של לגרנז':

הוכחת טענה 2.4.6. נניח ש-$p = 4k + 1$. לפי משפט ווילסון, p מחלק את $(4k)! + 1$, אז מספיק להראות שיש m כך של-m^2 ול-$(4k)!$ אותה שארית ביחס ל-p. אבל ב-$\mathbb{F}_p$, לכל i מתקיים $4k + 1 - i = -i$ ולכל $1 \leqslant i \leqslant 2k$ יש מספר יחיד מהצורה $4k + 1 - i$ בין $2k + 1$ ל-$4k$. לכן ב-$\mathbb{F}_p$

$$(4k)! = (2k)! \cdot (-1)^{2k}(2k)! = (2k)!^2$$

כלומר, $m = (2k)!$ פותר את הבעיה (שימו לב שהשוויון $(4k)! = (2k)!^2$ נכון ב-$\mathbb{F}_p$, לרוב לא ב-$\mathbb{Z}$!) □

סוף הרצאה 7, 9 בנוב

נעבור עכשיו לדיון על החוג $A = \mathbb{Z}/n$ כאשר $n > 0$ אינו ראשוני. נניח ש-$n = mk$. האם יש קשר בין $\mathbb{Z}/n$ ל-$\mathbb{Z}/m$ ו-$\mathbb{Z}/k$? נשים לב ראשית שיש העתקה טבעית מ-$\mathbb{Z}/n$ ל-$\mathbb{Z}/m$: העתקת המנה (או השארית) מ-$\mathbb{Z}$ ל-$\mathbb{Z}/m$ שולחת את n ל-0, ולכן לפי טענה 3.2.3 משרה העתקה $r_1 : \mathbb{Z}/n \to \mathbb{Z}/m$. במלים פשוטות, השארית של מספר ביחס ל-m, במקרה הזה, תלויה רק בשארית שלו ביחס ל-n. מאותה סיבה, ישנה העתקה $r_2 : \mathbb{Z}/n \to \mathbb{Z}/k$, וביחד מקבלים העתקה $r : \mathbb{Z}/n \to \mathbb{Z}/m \times \mathbb{Z}/k$. בכלל, המידע של $r(a)$, עבור $a \in \mathbb{Z}/n$ לא מאפשר לשחזר את a: למשל, אם $m = k$, אז שני הרכיבים של r זהים, וכל אחד מהם מכיל פחות מידע מאשר a עצמו. אבל אם m, k זרים, המצב הוא אחר.

טענה 3.4.5 (משפט השאריות הסיני). *נניח ש-$n_1, \ldots, n_k$ מספרים טבעיים זרים בזוגות. אז ההעתקה הטבעית*

$$r : \mathbb{Z}/n_1 \ldots n_k \to \mathbb{Z}/n_1 \times \ldots \times \mathbb{Z}/n_k$$

היא איזומורפיזם

הוכחה. אם a בגרעין של r, אז הוא מתחלק בכל ה-n_i. כיוון שה-n_i זרים בזוגות, זה אומר שהוא מתחלק במכפלה שלהם, ולכן הוא 0 בחוג המקורי. זה מראה ש-r חד-חד-ערכית, אבל שני הצדדים הם קבוצות סופיות באותו גודל, אז r גם על. לפי תרגיל 3.1.5, r איזומורפיזם. $\square$

את הטענה אפשר לנסח גם בשפה של פתרון משוואות: נניח ש-$n_1,\dots,n_k$ זרים בזוגות, ו-r_i שאריות ביחס ל-n_i (כלומר $0 \leqslant r_i < n_i$). אנחנו מחפשים מספר m עם התכונה שהשארית של m ביחס לכל n_i היא r_i. אז המשפט אומר ש-m כזה קיים, וכל שני פתרונות נבדלים בכפולה של $n_1 \cdot \dots \cdot n_k$.

למשפט ישנה המסקנה הבאה:

מסקנה 3.4.6. *איבר של $\mathbb{Z}/n$ הוא הפיך אם ורק אם הוא זר ל-n*

הוכחה. אם m אינו זר ל-n, יש ראשוני p שמחלק את שניהם. אז $m \cdot \frac{n}{p} = \frac{m}{p} \cdot n = 0$ ב-$\mathbb{Z}/n$, כלומר m הוא מחלק אפס.

מאידך, אם m זר ל-n, אז לפי משפט השאריות הסיני אפשר למצוא מספר טבעי x עם שארית 1 ביחס ל-n ו-0 ביחס ל-m. אז x מתחלק ב-m, נניח $x = my$, כלומר השארית של my ביחס ל-n היא 1. אז y הוא ההפכי של m ביחס ל-n. $\square$

תרגיל 3.4.7. נניח ש-$n = pq$ מכפלה של שני ראשוניים שונים. הוכיחו שיש מספרים $1 < e < f < n$ כך ש: השארית של e^2 ביחס ל-n היא e, השארית של f^2 היא f, המכפלה ef מתחלקת ב-n ו-$e + f - 1$ גם מתחלק ב-n. הוכיחו ש-e, f כאלה יחידים. מיצאו את e, f עבור $n = 65$.

תרגיל 3.4.8. נניח ש-$p \in \mathbb{Z}$ ראשוני מהצורה $4k + 1$. הוכיחו ש-$\mathbb{Z}[i]/p$ איזומורפי ל-$\mathbb{F}_p^2$

להשלמת התמונה, נתאר את קבוצת האיברים ההפיכים ב-$\mathbb{Z}/p^m$ עבור $m > 0$ כלשהו.

טענה 3.4.9. *איבר של $\mathbb{Z}/p^n$ עבור $n \geqslant 1$ הוא הפיך אם ורק אם השארית שלו ב-$\mathbb{Z}/p$ שונה מ-0.*

בהוכחה נוח לחשוב על כפולות של p ב-$\mathbb{Z}/p^n$ כעל איברים "קטנים". זה סביר, כי כל איבר כזה ϵ מקיים $\epsilon^m = 0$ עבור m מספיק גדול.

הוכחה. באינדוקציה על n. עבור $n = 1$ הטענה נכונה כי $\mathbb{Z}/p$ שדה. עבור $n \geqslant 1$ כלשהו, נוכיח שאיבר x של $\mathbb{Z}/p^{n+1}$ הוא הפיך אם ורק אם התמונה שלו $\bar{x}$ ב-$\mathbb{Z}/p^n$ הפיכה. כיוון של-x ול-$\bar{x}$ אותה שארית ב-$\mathbb{Z}/p$, זה יוכיח את הטענה. בכיוון אחד, אם x הפיך עם הפכי y, אז $\bar{y}$ הפכי של $\bar{x}$.

בכיוון השני, נשים לב ראשית שאם $\epsilon = ap^n \in \mathbb{Z}/p^{n+1}$, אז $\epsilon^2 = 0$, ואז $1 + \epsilon$ הפיך: האיבר $1 - \epsilon$ הפכי שלו, משום ש-$(1+\epsilon)(1-\epsilon) = 1 - \epsilon^2 = 1$. עכשיו, נניח ש-$x$ איבר עבורו $\bar{x}$ הפיך, כך שעבור איבר $y \in \mathbb{Z}/p^{n+1}$ מתקיים $\bar{x}\bar{y} = 1$. אז $xy = 1 + ap^n$, ו-$y' = y(1 - ap^n)$ הוא ההפכי של x. $\square$

לכל טבעי n, מספר הטבעיים שקטנים או שווים ל-n וזרים לו מסומן ב-$\varphi(n)$, והפונקציה $n \mapsto \varphi(n)$ נקראת *פונקציית אוילר*. הניתוח לעיל נותן את נוסחאות מפורשות עבורה: פונקציית אוילר

מסקנה 3.4.10. *פונקציית אוילר φ היא בעלת התכונות הבאות:*

1. *אם m ו-n זרים אז* $\varphi(mn)=\varphi(m)\varphi(n)$

2. $\varphi(p^n)=(p-1)p^{n-1}$ *לכל ראשוני p וטבעי* $n>0$

הוכחה. נסמן ב-U_n את קבוצת האיברים ההפיכים של $\mathbb{Z}/n$. ראינו במסקנה 3.4.6 שהגודל של U_n הוא $\varphi(n)$.

1. לפי משפט השאריות הסיני, $\mathbb{Z}/nm$ איזומורפי ל-$\mathbb{Z}/m\times\mathbb{Z}/n$ ולכן יש העתקה הפיכה מ-U_{nm} לקבוצת ההפיכים ב-$\mathbb{Z}/m\times\mathbb{Z}/n$. אבל הקבוצה הזו היא קבוצת הזוגות בהם כל אחד מהרכיבים הפיך, כלומר $U_m\times U_n$.

2. יש לנו העתקה מ-$\mathbb{Z}/p^n$ על $\mathbb{F}_p$, וגודל כל אחד מהסיבים הוא p^{n-1}. ראינו שאיבר של $\mathbb{Z}/p^n$ הוא הפיך בדיוק אם הוא נמצא באחד הסיבים שאינם הגרעין, וישנם $p-1$ כאלה. $\square$

תרגיל 3.4.11. הוכיחו שלכל $n>0$ שהמחלקים הראשוניים שלו הם $p_1,\dots,p_k$ מתקיים $\frac{\varphi(n)}{n}=(1-\frac{1}{p_1})\dots(1-\frac{1}{p_k})$

4 הצפנות

בסעיף זה נראה שתי שיטות הצפנת מפתח פומבי, ונסביר למה הן עובדות. הכלי העיקרי הוא סוג נוסף של מבנה אלגברי, חבורות.

4.1 חבורות

הגדרה 4.1.1. חבורה היא קבוצה G עם פעולה $\cdot$ המקיימת:

1. $(a\cdot b)\cdot c=a\cdot(b\cdot c)$ לכל $a,b,c\in G$.

2. קיים איבר $e\in G$ כך ש-$ae=ea=a$ לכל $a\in G$

3. לכל איבר $a\in G$ יש איבר $a^{-1}\in G$ כך ש-$aa^{-1}=a^{-1}a=e$.

חבורה חילופית
חבורה אבלית
העתקה של חבורות
הומומורפיזם של חבורות

החבורה G נקראת *חבורה חילופית* (או *חבורה אבלית*) אם $ab=ba$ לכל $a,b\in G$.

העתקה של חבורות (או *הומומורפיזם של חבורות*) הוא פונקציה $f:G\to H$ מהחבורה G לחבורה H כך ש-$f(gh)=f(g)f(h)$ לכל $g,h\in G$. איזומורפיזם, אוטומורפיזם וכו' מוגדרים בצורה מקבילה להגדרה בחוגים.

זה תרגיל בסיסי שאיבר e כמו בהגדרה הוא יחיד, ולכן התנאי בסעיף האחרון מוגדר היטב. התורה של חבורות חילופיות קלה בהרבה מזו של חבורות כלליות, ואנחנו נזדקק בעיקר למקרה הזה, אבל את ההתחלה אפשר לפתח באותה קלות ללא התנאי הזה.

ישנן שתי חבורות שמופיעות כבר בהגדרה של חוג:

דוגמא 4.1.2. אם A חוג כלשהו, אז A עם פעולת החיבור היא חבורה חילופית. קבוצת האיברים ההפיכים ב-A היא חבורה תחת פעולה הכפל של A, והחבורה היא חילופית אם A חוג חילופי.

הסיבה המרכזית לעניין בחבורות היא שהן מקודדות סימטריה. בהינתן סוג מסוים של אובייקטים (למשל: חוגים, מרחבים וקטוריים, מרחבים גאומטריים, וכו), יש ביניהם לרוב מושג של העתקות, ששומרות על המבנה. הרכבה של העתקות כאלה היא שוב העתקה עם אותן תכונות, והעתקה נקראת הפיכה אם יש העתקה בכיוון ההפוך כך שההרכבה שלהן היא הזהות בשני הכיוונים. בפרט, אוסף ההעתקות ההפיכות $\mathrm{Aut}(X)$ מאובייקט כזה X לעצמו הוא חבורה, כאשר הפעולה נתונה על-ידי הרכבת העתקות. על כל העתקה כזו אפשר לחשוב כעל "סימטריה" של X, אז החבורה הזו מקודדת אלגברית את מבנה הסימטריה של X.

דוגמא 4.1.3. אם $\Bbbk$ שדה (או באופן יותר כללי, חוג חילופי) ו-n טבעי, אוסף המטריצות ההפיכות בגודל n מעל $\Bbbk$ היא חבורה תחת הפעולה של כפל מטריצות. החבורה הזו מסומנת ב-$\mathrm{GL}(n,\Bbbk)$. הפעולה הלינארית של מטריצות כאלה על איברי $X=\Bbbk^n$ מזהה את החבורה הזו כחבורת האוטומורפיזמים של X, כמרחב לינארי מעל $\Bbbk$.

דוגמא 4.1.4. לכל קבוצה X, קבוצת כל התמורות (העתקות הפיכות מ-X לעצמה) היא חבורה תחת הרכבה, שמסומנת ב-$\mathrm{Sym}(X)$. כאשר $X=\{1,\dots,n\}$, החבורה מסומנת גם ב-S_n, ונקראת חבורת התמורות ה-n.

אם G חבורה, תת-קבוצה H של G היא *תת-חבורה* אם לכל $g,h\in H$ גם $gh\in H$, ואם H עצמה היא חבורה עם הפעולה הזו. נובע מכך שאיבר היחידה של G שייך ל-H (תרגיל). תת-חבורה

אנחנו בשלב זה מתעניינים בחבורות סופיות. עבור חבורות כאלה מעניין לשאול כמה איברים יש בהן. מספר האיברים בחבורה נקרא *הסדר של החבורה*. המשפט הבא הוא הכלי הבסיסי ביותר בחקר חבורות סופיות. הסדר של החבורה

טענה 4.1.5 (משפט לגרנז'). *אם G חבורה סופית ו-H תת-חבורה של G, אז הסדר של H מחלק את הסדר של G.*

הוכחה. נגדיר יחס $\sim$ על G על-ידי: $g_1\sim g_2$ אם $g_1=hg_2$ עבור איזשהו $h\in H$. אנחנו טוענים:

1. $\sim$ הוא יחס שקילות

2. יש העתקה הפיכה בין כל שתי מחלקות שקילות של $\sim$

(כל זה נכון גם בלי ההנחה ש-G סופית). הטענה הראשונה היא תרגיל. בשביל החלק השני, אם $g_1,g_2\in G$, נגדיר $t_{g_1,g_2}:G\to G$ על-ידי $t_{g_1,g_2}(g)=gg_1^{-1}g_2$. אם g שקול ל-g_1 אז $gg_1^{-1}\in H$ ולכן $t_{g_1,g_2}(g)$ שקול ל-g_2. כיוון ש-t_{g_2,g_1} הפכית ל-t_{g_1,g_2}, זה מוכיח את החלק השני.

נשים לב שמחלקת השקילות של e היא בדיוק H. עכשיו, אם G סופית, הגודל שלה הוא סכום גדלי מחלקות השקילות. כיוון שיש העתקה הפיכה בין כל מחלקה ל-H, הגודל של כולן הוא H, אז הגודל של G הוא מכפלת הגודל של H במספר מחלקות השקילות. $\square$

לפעמים אפשר לתאר בצורה מפורשת את קבוצת המחלקות, ולקבל מידע יותר מדויק על הסדרים:

תרגיל 4.1.6. עבור $G=S_n$, חבורת התמורות מדוגמא 4.1.4, הוכיחו שתת-הקבוצה $H=\{g\in S_n\mid g(n)=n\}$ היא תת-חבורה, וש-$g_1\sim g_2$ אם ורק אם $g_1^{-1}(n)=g_2^{-1}(n)$ (כאשר $\sim$ כמו בהוכחת משפט לגרנז'). הסיקו שהסדר של S_n הוא $n!$.

והנה דוגמא נוספת:

מסקנה 4.1.7. *אם G חבורה סופית ו-$f : G \to H$ הומומורפיזם, אז הסדר של $f(G)$ מחלק את הסדר של G. בפרט, אם G, H חבורות סופיות שהסדרים שלהן זרים, אין הומומורפיזמים לא טריוויאליים ביניהן.*

הוכחה. נסמן $K = \operatorname{Ker} f = \{g \in G \mid f(g) = e\}$. אז K תת-חבורה של G, ולכל $g_1, g_2 \in G$ מתקיים $f(g_1) = f(g_2)$ אם ורק אם $g_1 \sim g_2$ עבור היחס $\sim$ כמו בהוכחת משפט לגרנז' (עבור תת-החבורה K). לכן, גודל התמונה של f הוא כמספר מחלקות השקילות, וראינו שהוא $|G|/|K|$. החלק השני נובע משום ש-$f(G)$ היא תת-חבורה שהסדר שלה מחלק את הסדרים של G ושל H. $\square$

החיתוך של אוסף כלשהו של תתי-חבורות של חבורה G הוא תת-חבורה, ובפרט לכל תת-קבוצה S של G קיימת תת-חבורה קטנה ביותר של G שמכילה את S (קטנה ביותר במובן שהיא מוכלת בכל תת-חבורה אחרת כזו). תת-החבורה הזו נקראת *תת-החבורה שנוצרת על-ידי* S (כדאי להשוות לסעיף 3.3). תת-החבורה שנוצרת על-ידי S

בפרט, לכל איבר g של החבורה G יש תת-חבורה קטנה ביותר $\langle g \rangle$ שכוללת אותו. במפורש, זוהי תת-החבורה $\{g^n \mid n \in \mathbb{Z}\}$. הסדר של תת-החבורה הזו (אם היא סופית) נקרא גם הסדר של האיבר g. זהו המספר החיובי הקטן ביותר n עבורו $g^n = e$. אנחנו מקבלים:

מסקנה 4.1.8. *הסדר של כל איבר בחבורה סופית מחלק את סדר החבורה, ואם $f : G \to H$ העתקה של חבורות ו-$g \in G$ מסדר סופי, אז הסדר של $f(g)$ מחלק את הסדר של g.*

תרגיל 4.1.9. הוכיח שבחבורה $\mathrm{GL}(2, \mathbb{F}_3)$ יש איברים מסדר 4 ו-3, אבל אין איבר מסדר 5.

סוף הרצאה 8, 12 בנוב

4.2 הצפנת RSA

בסעיף זה נתאר את הצפנת המפתח הפומבי הראשונה שפורסמה. הצפנה זו קרויה RSA על שם שלושת ממציאיה, רון ריבסט, עדי שמיר וליאונרד אדלמן. נזכיר שבהצפנת מפתח פומבי המפתח מורכב משני חלקים, חלק פומבי וחלק סודי. שיטת ההצפנה מאפשרת לכל אחד להצפין בקלות הודעות, אבל לא לפענח הודעות שהוצפנו על-ידי אותו מפתח. על-מנת לפענח, יש לדעת את המפתח הסודי (או להיפך).

נזכיר בצורה יותר מדויקת מה אנחנו מחפשים. אנחנו מתעניינים בקבוצה סופית S של "הודעות". לשם הפשטות, נניח ש-S כוללת גם את ההודעות הגלויות וגם המוצפנות. הבעלים של המפתח, בוב, מפרסם את S (כלומר, את האופן שבו הודעות בשפה הטבעית מקודדות למטרות ההצפנה) ואת פונקציית ההצפנה $e : S \to S$ בה כל שחקן אחר (למשל, אליס) יכול להשתמש כדי להצפין הודעה $x \in S$. בנוסף, בידי בוב מצוי מפתח סודי $d : S \to S$ שהוא הפונקציה ההפוכה ל-e. כאשר בוב מקבל את ההודעה המוצפנת y, הוא מפעיל עליה את d כדי לקבל את ההודעה המקורית. על מנת שהעסק יעבוד, אנחנו רוצים ש:

1. יהיה קל לחשב את $e(x)$ ואת $d(y)$
2. יהיה קשה מאד לחשב את d מתוך ידיעת e

3. *יהיה לא כל-כך קשה לייצר את e, d ו-S (אבל יכול להיות משמעותית יותר קשה מהחישובים בסעיף הראשון, משום שעקרונית, כל שחקן צריך לעשות זאת רק פעם אחת)*

מה המשמעות של "קשה" או "קל"? אם אנחנו מעוניינים, למשל, להצפין הודעות של 1000 ספרות בינאריות, קבוצת ההודעות שלנו היא בגודל $n = 2^{1000}$. "גודל הקלט", בהקשר הזה, הוא אורך ההודעה, כלומר מספר k בין 0 ל-1000. תהליך שרץ במספר לינארי ב-k של צעדים הוא מהיר, אז סביר למשל בתור זמן ריצה של הצפנה או פיענוח. מאידך, תהליך שלוקח מספר לינארי של צעדים ב-$n = 2^k$ לא יסיים לרוץ בשום זמן סביר. זו (עשויה להיות) המשמעות של "קשה" עבור חישוב המפתח הסודי מתוך הפומבי. זמני ריצה בסעיף השלישי יכולים למשל להיות פולינומיים ב-k: לרוב יותר איטי מלינארי ב-k, אבל עדיין לאין שיעור יותר מהיר מלינארי ב-n. ההבדל הגדול בין סדרי הגודל מאפשר לנו לקיים דיון לא מאוד מדויק בזמני הריצה. למשל, ערכי ה-log של מספר m, עבור בסיסים שונים של ה-log, נבדלים בקבוע כפלי אחד מהשני, וזהו הבדל חסר משמעות מבחינת הניתוח הנ"ל (שינוי הבסיס הזה רלוונטי למשל אם רוצים לשנות את האלפבית ממנו נלקחות ההודעות).

הרעיון הבסיסי הוא ב-RSA (ובשיטות אחרות) הוא לחשוב על ההודעות (הגלויות והמוצפנות) כעל איברי חבורה סופית G. זה מאפשר שימוש במבנה החבורה, ופונקציית ההצפנה תהיה אוטומורפיזם של G. המטרה שלנו היא למצוא מחלקה של חבורות ואוטומורפיזמים שלהן, כך שידיעת האוטומורפיזם $e : G \to G$ לא מאפשרת לחשב בקלות את ההפכי $d : G \to G$.

בתור נסיון ראשון, אפשר לנסות חבורות מהצורה $G = \mathbb{Z}/n$. על מנת להבין למה זה לא עובד, נחשב את חבורת האוטומורפיזמים של חבורה כזו, ונתחיל משאלה יותר כללית, איך נראות העתקות מ-$\mathbb{Z}/n$ לחבורה כללית:

טענה 4.2.1. *לכל חבורה G, יש התאמה טבעית בין העתקות (של חבורות) מ-$\mathbb{Z}/n$ ל-G לאיברים ב-G שהסדר שלהם מחלק את n, שנתונה על-ידי $f \mapsto f(1)$. תחת ההתאמה הזו, ההעתקות החד-חד-ערכיות מתאימות לאיברים שהסדר שלהם בדיוק n.*

הוכחה. הסדר של $1 \in \mathbb{Z}/n$ הוא n, אז אם $g = f(1)$, ראינו במסקנה 4.1.8 שהסדר k של g מחלק את n. אז $f(k) = e$, ואם $k < n$, אז f אינה חח"ע. מאידך, אם f אינה חח"ע, אז $g^k = f(k) = e$ עבור $0 < k < n$, אז הסדר של g קטן מ-n. לבסוף, אם $g \in G$ הוא איבר שהסדר שלו מחלק את n, נגדיר $h : \mathbb{Z} \to G$ על-ידי $h(i) = g^i$. כיוון שהסדר של g מחלק את n, לכל m שמתחלק ב-n מקבלים $h(m) = e$, אז h משרה העתקה מ-$\mathbb{Z}/n$ ל-G. □

עבור $G = \mathbb{Z}/n$, אנחנו מקבלים:

מסקנה 4.2.2. *לכל $k \in \mathbb{Z}/n$ יש אנדומורפיזם יחיד ששולח את 1 ל-k. זהו אוטומורפיזם אם ורק אם k זר ל-n.*

תרגיל 4.2.3. הוכיחו שלכל d שמחלק את n יש ל-$\mathbb{Z}/n$ תת-חבורה אחת מסדר d. הסיקו את הנוסחא $\sum_{d|n} \varphi(d) = n$ (הסכום הוא על כל המחלקים)

הטענה האחרונה נותנת תיאור של קבוצת האוטומורפיזמים כקבוצה, אבל אוסף האוטומורפיזמים הוא חבורה (עם הרכבה), אז אפשר לשאול מהו מבנה החבורה כאן. התשובה שקיבלנו מזהה את הקבוצה עם קבוצת האיברים ההפיכים, אז סביר לצפות שזו שמבנה החבורה גם

הוא מגיע משם. כדי להוכיח זאת, נשים לב ראשית שאם A חבורה חילופית, אז האוסף $\mathrm{End}(A)$ של כל האנדומורפיזמים של A הוא חוג (לא בהכרח חילופי):

הגדרה 4.2.4. נניח ש-$\langle A, +\rangle$ חבורה חילופית. *חוג האנדומורפיזמים* של A הוא החוג $\mathrm{End}(A) = \{f : A \to A \mid f \text{ אנדומורפיזם}\}$, עם הפעולות: **חוג האנדומורפיזמים**

$$(f+g)(a) = f(a) + g(a)$$
$$(f \cdot g)(a) = f(g(a))$$

עכשיו נשים לב:

טענה 4.2.5. *אם A חוג כלשהו, לכל איבר $a \in A$ ההעתקה $l_a : A \to A$ הנתונה על ידי $l_a(b) = ab$ היא אנדומורפיזם של החבורה החיבורית של A. ההעתקה $a \mapsto l_a$ היא הומומורפיזם חד-חד-ערכי של חוגים מ-A ל-$\mathrm{End}(A)$. בפרט, לכל איבר הפיך a, ההעתקה l_a היא אוטומורפיזם.*

תרגיל 4.2.6. הוכיחו את הטענה

מסקנה 4.2.7. *לכל n, חבורת האוטומורפיזמים של החבורה החיבורית של $\mathbb{Z}/n$ היא U_n, חבורת האיברים ההפיכים שם.*

הוכחה. הטענה האחרונה נותנת העתקה חד-חד-ערכית של חבורות מ-U_n לחבורת האוטומורפיזמים, וראינו לפני כן שההעתקה הזו היא על. $\square$

מה כל זה אומר לגבי בעיית ההצפנה? אם נרצה לחשוב על קבוצת ההודעות כחבורה החיבורית $G = \mathbb{Z}/n$, ופונקציית ההצפנה e היא אוטומורפיזם של G, אז היא נתונה על ידי $e(x) = ax$ עבור a זר ל-n (והכפל הוא ב-$\mathbb{Z}/n$). פונקציית הפיענוח היא לכן מאותה צורה, $d(x) = bx$, כאשר b ההפכי של a ב-$\mathbb{Z}/n$. כדי להצפין הודעות, המצפין צריך לדעת את a ואת n, אז השאלה היא: האם מתוך המידע של a ו-n, אפשר לחשב ביעילות את ההפכי b של a ביחס ל-n? התשובה היא כן: כיוון ש-a ו-n זרים, האלגוריתם של אוקלידס נותן מספרים x, y כך ש-$ax + ny = 1$, אז x הוא ההפכי של a. כמה צעדים דורש האלגוריתם של אוקלידס? אחרי שלב אחד, מחליפים את n, a ב-a, r, כאשר $r < \frac{n}{2}$. לכן, האלגוריתם דורש לכל היותר $\log(n)$ צעדים. כזכור, עבורינו אלגוריתם הוא מהיר אם הוא דורש מספר פולינומי של צעדים ב-$\log(n)$ (שהוא גודלו של הקלט, בספרות).

הלקח הוא שכדאי לחפש חבורות יותר מורכבות מהחבורה החיבורית של $\mathbb{Z}/n$. יש עוד חבורה שהחוג הזה מספק לנו: החבורה הכפלית U_n של האיברים ההפיכים. כיוון שזו אינה, לרוב, חבורה חיבורית של חוג, לא נוכל לחשב את חבורת האוטומורפיזמים כמו קודם. אבל רעיון דומה עובד לכל חבורה חילופית:

טענה 4.2.8. *לכל חבורה חילופית G, ההעתקה $t_d : G \to G$ הנתונה על-ידי $t_d(g) = g^d$, היא אנדומורפיזם, לכל $d \in \mathbb{Z}$. אם G סופית מסדר m, ו-d זר ל-m, אז t_d אוטומורפיזם. ההעתקה $d \mapsto t_d$ היא העתקה של חבורות מ-U_m לחבורת האוטומורפיזמים $\mathrm{Aut}(G)$ של G.*

ההעתקה $d \mapsto t_d$ לא חייבת להיות חד-חד-ערכית או על. למעשה:

תרגיל 4.2.9. הוכיחו את הטענה. הוכיחו שאם k הוא הסדר הגבוה ביותר של איבר ב-G, אז יש העתקה חד-חד-ערכית של חבורות מ-U_k ל-$\mathrm{Aut}(G)$. הוכיחו של-U_{15} יש אוטומורפיזם שאינו חזקה

למרות זאת, אפשר להתבונן באוטומורפיזמים מהצורה הזו. נניח ראשית ש-$G = U_p$, כאשר p ראשוני. אנחנו יודעים שסדר החבורה הזו הוא $p-1$, ולכן מפתח ההצפנה צריך להיות מספר a שזר ל-$p-1$. על מנת להצפין הודעה $x \in U_p$, יש לחשב את השארית של x^a ביחס ל-p. בכמה צעדים ניתן לעשות זאת? נאיבית, צריך לעשות a הכפלות, כאשר a הוא מסדר הגודל של x או p, כלומר נראה שזו פעולה יקרה. אבל אם a זוגי, אז $x^a = (x^{\frac{a}{2}})^2$, וכיוון שכל הפעולות מתחלפות עם מעבר לשאריות, בגישה הזו יש לנו כ-$\frac{a}{2} + 1$ פעולות. חזרה על אותו רעיון מספר כלשהו של פעמים מראה שניתן לחשב את החזקה בכ-$\log(a)$ צעדים. לכן, הצפנת (ופענוח) הודעות אינן פעולות יקרות. הבעיה היא ששוב קל לחשב את המפתח הסודי: הראשוני p הינו חלק מהמפתח הפומבי, ולכן גם $p-1$, והמפתח הסודי הוא ההפכי (הכפלי) של a ביחס ל-$p-1$, חישוב שכבר ראינו שהוא קל.

למעשה, את U_p, עבור p ראשוני, אפשר להבין קצת יותר טוב:

תרגיל 4.2.10. בתרגיל זה נוכיח שבחבורה כפלית של שדה סופי F בעל p^k איברים, יש איבר מסדר $p^k - 1$ (בפרט, ב-U_p יש איבר מסדר $p-1$), ולכן היא איזומורפית ל-$\mathbb{Z}/p^k-1$. איבר עם התכונה הזו נקרא *שורש יחידה פרימיטיבי* שורש יחידה פרימיטיבי

במהלך התרגיל, נתייחס לתכונה הבאה M של חבורה G:

> החבורה G היא סופית מסדר n וחילופית, ולכל $k \in \mathbb{N}$ יש לכל היותר k איברים $g \in G$ עבורם $g^k = e$.

אנחנו נוכיח שכל חבורה בעלת התכונה הזו היא איזומורפית ל-$\mathbb{Z}/n$ (חבורה כזו נקראת *חבורה מעגלית*). חבורה מעגלית

1. הוכיחו שהחבורה הכפלית של F מקיימת את תכונה M.
2. נניח שהסדר של חבורה חילופית G הוא $n = p^l m$, כאשר m מספר זר ל-p. הוכיחו שהפונקציה $t : G \to G$ הנתונה על-ידי $t(g) = g^{p^l}$ היא העתקה של חבורות, שהגרעין שלה G_p הוא קבוצת האיברים ב-G שהסדר שלהם מחלק את p^l, והתמונה שלה היא קבוצת האיברים G^p שהסדר שלהם זר ל-p.
3. הוכיחו שהפונקציה $f : G_p \times G^p \to G$ הנתונה על-ידי $f(g, h) = gh$ היא איזומורפיזם של חבורות. הסיקו שאם G_p ו-G^p מעגליות, אז גם G מעגלית
4. נניח ש-G_p מקיימת את תכונה M. הוכיחו שהיא מעגלית (רמז: הסתכלו על איבר עם סדר מירבי ב-G)
5. הוכיחו שכל חבורה עם תכונה M היא מעגלית, והסיקו שהחבורה הכפלית של שדה היא כזו

מה קורה עבור U_n כאשר n אינו ראשוני? נניח ש-$n = pq$, מכפלה של שני ראשוניים. שוב המפתח הפומבי נתון על-ידי מספר a שזר לגודל $\varphi((p-1)(q-1))$ של U_n. הנימוק לעיל מראה גם פה שהצפנה ופענוח ניתן לבצע ביעילות. המפתח הפומבי מורכב במקרה זה מ-a ו-n. על-מנת לחשב את המפתח הסודי בשיטה הקודמת, עלינו לחשב את ההפכי של a ביחס ל-$\varphi(n)$. זה קל, בהנחה שהפורץ יודע את $\varphi(n)$. כמה קל לחשב את $\varphi(n)$?

טענה 4.2.11. *אם $n = pq$, אז ניתן לחשב בקלות את $\varphi(n)$ אם ורק אם ניתן לחשב בקלות את p, q מתוך n.*

הוכחה. בהנתן p, q, אפשר לחשב ישירות את $\varphi(n) = (p-1)(q-1)$. בכיוון השני, נתונים לנו המכפלה $n = pq$ והסכום $m = p + q = n - \varphi(n) + 1$, ולכן p, q הם הפתרונות של המשוואה הריבועית $x^2 - mx + n = 0$, וניתן לחשבם בעזרת הנוסחא לפתרון של משוואה כזו. $\square$

אז הדרך הישירה למציאת המפתח הסודי מתוך המפתח הפומבי דורשת יכולת לפרק מספר שלם לגורמים ראשוניים מהר. השאלה האם זו אכן בעיה קשה היא פתוחה, למרות שהאמונה הרווחת היא שכן. לסיכום, אפשר לתאר את שלבי העבודה באופן הבא:

1. בעל המפתח בוב בוחר שני מספרים ראשוניים גדולים p, q, ומספר e שזר ל-$\varphi(n) = (p-1)(q-1)$. הוא מפרסם את $n = pq$ ואת e.

2. בוב מחשב, באמצעות האלגוריתם של אוקלידס, את ההפכי d של e ביחס ל-$\varphi(n)$. המספרים d ו-$\varphi(n)$ הם המפתח הסודי.

3. כאשר אליס רוצה להצפין הודעה $x \in U_n$, היא מחשבת את השארית y של x^e ביחס ל-n. ראינו שניתן לעשות זאת ביעילות.

4. כאשר בוב צריך לפענח את ההודעה y, הוא מחשב את $y^e = x^{de} = x$ באותו אופן.

ניתן להשתמש באותה מערכת גם עבור חתימות דיגיטליות: בוב שולח לאליס הודעה x ביחד עם עותק מוצפן $y = x^d$ שלה (כרגיל, פעולת החזקה היא ב-$\mathbb{Z}/n$). המפתח הסודי d נדרש על-מנת לבצע פעולה זו. כאשר אליס מקבלת את ההודעה x ואת העותק המוצפן $y = x^d$, היא מחשבת את $y^e = x^{de} = x$ ומוודאת שקיבלה את ההודעה המקורית. נושא חשוב שלא דיברנו עליו: על מנת לייצר את המערכת, צריך למצוא את שני המספרים הראשוניים p, q. כמה זה קל? לא נתעכב על זה, אבל נעיר שבכל מקרה זו פעולה שעושים "אחת ולתמיד", ולכן לא נורא אם היא תהיה יקרה משמעותית מההצפנה והפיענוח.

כפי שהזכרנו, ההצפנה הזו אכן עובדת רק אם פירוק מספר לגורמים הוא קשה. אולם יש בעיה נוספת: לא הוכחנו שהקושי של פריצת ההצפנה *שקול* לפירוק לגורמים. במלים אחרות, יתכן שניתן לפרוץ את ההצפנה (לחשב את המפתח הסודי) אפילו בלי לפרק לגורמים. הבעיה הזו נפתרת בשיטה הבאה שנראה.

סוף הרצאה 9, 16 בנוב

4.3 הצפנת רבין

שיטה זו דומה להצפנת ה-RSA, בכך שקבוצת ההודעות היא עדיין U_n עבור $n=pq$, מכפלה של שני ראשוניים. אולם פונקציית ההצפנה היא תמיד $E(x)=x^2$. כיוון שסדר החבורה U_n הוא $(p-1)(q-1)$, מספר זוגי, ההעתקה הזו אינה חח"ע: ראינו ש-U_n איזומורפית ל-$U_p \times U_q$, וב-U_p יש שני איברים בגרעין של E (זו החבורה הכפלית של שדה). לכן, כל הודעה מוצפנת מתקבלת מארבע הודעות מקוריות.

הבעיה של היפוך הפונקציה הזו היא בדיוק הבעיה של חישוב שורש ריבועי ב-U_n. בקרוב נעסוק בבעיה הזו בהרחבה, ובפרט נוכיח במלואה את הטענה הבאה:

טענה 4.3.1 (נוסחת אוילר). *נניח ש-p ראשוני אי-זוגי, ו-$t \in U_p$. אז קיים $s \in U_p$ עבורו $s^2=t$ אם ורק אם $t^{\frac{p-1}{2}}=1$. אם זה המצב, ואם p מהצורה $4k-1$, אז s כזה נתון על-ידי $s=t^k$.*

הוכחה. כאמור, את הטענה העיקרית נוכיח בהמשך. בשלב זה נוכיח את נוסחת השורש: אם t ריבוע, אז

$$(t^k)^2=t^{2k}=t^{\frac{p+1}{2}}=t\cdot t^{\frac{p-1}{2}}=t$$

משום ש-$t^{\frac{p-1}{2}}=1$. □

בינתיים נשתמש בטענה על מנת להוכיח:

טענה 4.3.2. *דרגת הקושי של חישוב שורשים ב-U_n שווה לדרגת הקושי של הפירוק של n לראשוניים*

לשם הפשטות נוכיח את הטענה בהנחה של-p ול-q יש שארית 3 בחלוקה ב-4. ההוכחה קצת יותר קשה למקרה הכללי, אבל בכל מקרה נראה בקרוב שההנחה הזו לא מגבילה מאד.

הוכחה. נרשום $ap+bq=1$. תחת האיזומורפיזם מ-U_n ל-$U_p \times U_q$ במשפט השאריות הסיני, איבר זה הולך לאיבר $\langle bq, ap\rangle = \langle 1,1\rangle$, כלומר $bq=1$ ב-$\mathbb{F}_p$ ו-$ap=1$ ב-$\mathbb{F}_q$. השורשים של $1 \in U_p \times U_q$ הם $\langle \pm 1, \pm 1\rangle$, ולכן מתאימים ל-$\pm ap \pm bq$ ב-U_n.

אם אנחנו יודעים לחשב את ההפכית (הרב-ערכית) D של E, אז $D(1)$ היא בדיוק ארבעת האיברים הללו, ומתוכם אפשר לחשב את ap ואת bq. כיוון שאנחנו יודעים גם את $n=pq$, האלגוריתם של אוקלידס נותן לנו את p ואת q.

בכיוון ההפוך, אם הפירוק של n ידוע, מספיק לדעת לחשב שורש ריבועי ב-U_p וב-U_q. הנחנו ש-$p=4k-1$, ולכן השורש נתון על-ידי הנוסחא בטענה 4.3.1. □

תרגיל 4.3.3. נסמן $n=77$ ו-$e=7$

1. הצפינו את ההודעה 20 באמצעות מפתח ה-RSA הנתון על-ידי n ו-e
2. חשבו את המפתח הסודי עבור e, n הנ"ל, וודאו שהפיענוח של ההודעה המוצפנת הוא 20
3. הצפינו את אותה הודעה באמצעות הצפנת רבין (עם אותו n)

4. חשבו את כל ההודעות האחרות m עבורן $E(m)=E(20)$ (כאשר E הצפנת רבין ביחס ל-n)

הערה 4.3.4. בשימוש בשיטה זו, עדיין יש צורך להבדיל בין ארבעת ההודעות האפשריות שנותנות אותה הודעה מוצפנת. בהנחה ששני הראשוניים שנבחרו הם משארית 3 ביחס ל-4, דרך אחת לעשות זאת, עקרונית, היא לצמצם את מרחב ההודעות לקבוצת האיברים S של U_n שהם עצמם ריבועים. כפי שראינו (ונזכיר שוב בקרוב), ל--1 אין שורש ב-U_p וב-U_q, ולכן בדיוק אחת מארבע ההודעות שנותנות אותו ערך תחת E היא בעצמה ריבוע. במלים אחרות, הצמצום של E לקבוצה S הוא פונקציה הפיכה. גישה זו דורשת חישוב נוסף, על מנת לוודא שההודעה נמצאת ב-S.

5 הדדיות ריבועית

5.1 שורשים בשדות סופיים

נזכיר שראינו שיתר של שלשה פיתגורית הוא בהכרח מכפלה של ראשוניים מהצורה $4k+1$. האם יש אינסוף כאלה? נשים לב ראשית שהתשובה עבור הסדרה המשלימה היא די פשוטה:

תרגיל 5.1.1. הוכיחו שיש אינסוף ראשוניים מהצורה $4n+3$ (רמז: אם לא, מה השארית ביחס ל-4 של מכפלת כל הראשוניים שאינם מהצורה $4n+1$?)

ראינו במסקנה 2.4.8 שראשוני $p>2$ הוא מהצורה $4n+1$ בדיוק אם אינו ראשוני ב-$\mathbb{Z}[i]$. כיוון ש-$i^2=-1$, אנחנו מקבלים:

טענה 5.1.2. *בשדה $\mathbb{F}_p$ אין שורשים ל--1 אם ורק אם p הוא מהצורה $4k+3$*

הוכחה. נסמן $A={}^{\mathbb{Z}[i]}/_{p}$, חוג ממציין p. נניח שב-$\mathbb{F}_p$ יש שורש a ל--1. אז התמונה של i ב-A היא שורש שונה מ-a ומ-$-a$. לכן A אינו שדה, ולכן לפי תרגיל 3.3.9 אינו מהצורה $4k+3$.

מאידך, אם ב-$\mathbb{F}_p$ אין שורש ל--1 אז הפולינום x^2+1 אי-פריק מעל $\mathbb{F}_p$, וכיוון ש-$\mathbb{F}_p[x]$ תחום פריקות יחידה, הוא ראשוני בחוג זה. יש לנו העתקה של חוגים מ-$\mathbb{F}_p[x]$ על A, שהגרעין שלה מכיל את x^2+1. כיוון ש-x^2+1 ראשוני, המנה ${}^{\mathbb{F}_p[x]}/_{x^2+1}$ היא תחום שלמות, ולכן שדה (כי היא סופית). לכן גם A שדה (ושווה למנה זו). שוב לפי תרגיל 3.3.9, p הוא מהצורה $4k+3$. $\square$

סוף הרצאה 10, 19 בנוב

נשים לב שהטענה נובעת גם מנוסחת אוילר (טענה 4.3.1), אולם אותה עדיין לא הוכחנו. כדי להראות שיש אינסוף ראשוניים עם שארית 1 ביחס ל-4 מספיק לכן להוכיח:

טענה 5.1.3. *יש אינסוף ראשוניים p עבורם ב-$\mathbb{F}_p$ יש שורש ל--1.*

הוכחה. נניח שיש רק מספר סופי, ונסמן ב-n את המכפלה של כולם. אז כל המספרים n, אינו שורש של -1 בשום $\mathbb{F}_p$: בכל $\mathbb{F}_p$ בו שורש כזה קיים, $n=0$. כלומר n^2+1 שונה מ-0 בכל $\mathbb{F}_p$, ולכן $n^2+1=1$ (ב-$\mathbb{Z}$), וזו סתירה. $\square$

הטענה הזו מדגימה שני דברים: השאלה האם למספר יש שורש ב-$\mathbb{F}_p$ היא שאלה מעניינת, והתשובה נקבעת על ידי השייכות של p לסדרות חשבוניות מסוימות (במקרה הזה, $4n+1$ או $4n+3$). ראינו כבר סיבה נוספת לחשיבות של שורשים בשדות כאלה בהצפנת רבין, והנוסחא

לשורשי משוואה ריבועית מראה שפתרון כל המשוואות הריבועיות תלויה בקיומם של שורשים. משפט ההדדיות הריבועית נותן מענה (מסוים) על השאלה: האם למספר n יש שורש ריבועי ב-$\mathbb{F}_p$.

על מנת לנסח את הטענה, נוח להגדיר את הסימון הבא:

סימן לז'נדר

הגדרה 5.1.4. *סימן לז'נדר* $\left(\frac{n}{p}\right)$ עבור ראשוני אי זוגי p ומספר שלם n הוא המספר k כך של-n יש $k+1$ שורשים ריבועיים ב-$\mathbb{F}_p$

במלים אחרות, $\left(\frac{n}{p}\right)=0$ אם n מתחלק ב-p, ואחרת הוא 1 אם ל-n יש שורש ב-$\mathbb{F}_p$ ו--1 אחרת.

האבחנה הבאה מראה, בין היתר, שמעניין במיוחד להסתכל על המקרה ש-n הוא ראשוני:

טענה 5.1.5. *סימן לז'נדר הוא כפלי: לכל* $n,m\in\mathbb{Z}$ *מתקיים* $\left(\frac{nm}{p}\right)=\left(\frac{n}{p}\right)\left(\frac{m}{p}\right)$

הטענה הזו היא מסקנה ישירה של טענה 4.3.1, שהחלק הראשון שלה אומר במונחים אלה: לכל ראשוני אי-זוגי p השוויון $\left(\frac{n}{p}\right)=n^{\frac{p-1}{2}}$ מתקיים ב-$\mathbb{F}_p$ (זוהי נוסחת אוילר).

הוכחת טענה 4.3.1. הטענה ברורה אם n מתחלק ב-p, אז אפשר להניח $n\in U_p$. נתבונן בהעתקה $h:U_p\to U_p$ הנתונה על-ידי $h(n)=n^{\frac{p-1}{2}}$. אם $t=h(n)$ אז $t^2=1$ ולכן $t=1$ או $t=-1$. הגרעין של h לא יכול להיות כל U_p, כי למשוואה $x^{\frac{p-1}{2}}=1$ יש לכל היותר $\frac{p-1}{2}$ פתרונות. לכן, גודל הגרעין הוא בדיוק $\frac{p-1}{2}$. אם $n=m^2$ אז $h(n)=h(m^2)=m^{p-1}=1$, כלומר כל הריבועים נמצאים בגרעין. מאידך, ההעתקה $x\mapsto x^2$ גם היא הומומורפיזם, שהגרעין שלו $\{-1,1\}$, אז התמונה היא בגודל $\frac{p-1}{2}$, כלומר הגרעין של h הוא בדיוק קבוצת הריבועים. □

משפט ההדדיות נותן קשר בין ערכי $\left(\frac{p}{q}\right)$ ו-$\left(\frac{q}{p}\right)$ עבור ראשוניים אי-זוגיים p,q:

משפט 5.1.6 (משפט ההדדיות הריבועית). *לכל שני ראשוניים אי-זוגיים* p,q *מתקיים:* $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{(p-1)(q-1)}{4}}$

על מנת לחשב את $\left(\frac{n}{p}\right)$ ל-n כלשהו, צריך בנוסף לדעת את הערכים עבור $n=-1$ ו-$n=2$. את המקרה הראשון כבר ראינו:

טענה 5.1.7. *ל--1 אין שורש ב-$\mathbb{F}_p$ אם ורק אם p מהצורה $4n+3$. לכן,* $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$

במקרה השני צריך לטפל בנפרד:

טענה 5.1.8. *לכל ראשוני אי-זוגי p, ל-2 יש שורש ב-$\mathbb{F}_p$ אם ורק אם השארית של p ביחס ל-8 היא 1 או -1.*

אפשר גם להרחיב את סימן לז'נדר על-ידי כפליות במכנה: $\left(\frac{n}{mk}\right)=\left(\frac{n}{m}\right)\left(\frac{n}{k}\right)$ לכל n שלם ו-$m,k>0$. לפי הגדרה, הערך של $\left(\frac{n}{m}\right)$ תלוי רק בשארית של n ביחס ל-m, והעובדה הזו,

ביחד עם משפט ההדדיות מראים שאפשר לחשב ערך זה במהירות (באופן דומה למחלק המשותף המירבי). זה חשוב לשימושים בהצפנות (כפי שראינו), בבדיקת ראשוניות ועוד.

כדאי להזכיר גם את הפרשנות במונחים של סדרות חשבוניות: לפי משפט ההדדיות, לכל ראשוני p יש איחוד סופי S של סדרות חשבוניות כך של-p יש שורש ב-$\mathbb{F}_q$ אם ורק אם $q \in S$.

מסקנה נוספת נוגעת למקרה (כמעט) הכי פשוט של *עקרון הסה*: ראינו שאחת הדרכים הכי פשוטות להראות שלמשוואה דיאופנטית אין פתרון היא למצוא שדה סופי בו למשוואה אין פתרון. הכיוון ההפוך לרוב אינו נכון (כפי שמיד נראה): תתכן משוואה שיש לה פתרון בכל שדה שארית סופי, אבל לא ב-$\mathbb{Z}$. אבל למשוואות ריבועיות זה לא המצב:

תרגיל 5.1.9. 1. הוכיחו שמספר שלם הוא ריבוע אם ורק אם השארית שלו בכל שדה $\mathbb{F}_p$ היא ריבוע.

2. הוכיחו שמשוואה ריבועית $x^2 + bx + c = 0$ עם מקדמים שלמים b, c היא פתירה ב-$\mathbb{Z}$ אם ורק אם היא פתירה בכל שדה $\mathbb{F}_p$.

3. הוכיחו שלמשוואה $(x^2-2)(x^2-3)(x^2-6) = 0$ יש פתרון בכל $\mathbb{F}_p$ אבל לא בשלמים

לעקרון ההדדיות יש מבחר הוכחות. ההוכחה שאנחנו נראה תהיה יחסית פשוטה מבחינה קומבינטורית, אבל תשתמש בכלי חשוב, *התמרת פורייה*, אותו נציג כעת.

5.2 תזכורת על אלגברה לינארית

נזכיר כמה עובדות על אלגברה לינארית. המטרה שלנו כפולה: בהמשך נזדקק לחלק מהעובדות הללו, וחלקן מהוות מוטיבציה ואנאלוגיה לבניות דומות שנבצע עבור חבורות. מומלץ מאד להוכיח את כל הטענות פה כתרגיל.

נקבע שדה $\Bbbk$. אם V ו-U מרחבים וקטוריים מעל $\Bbbk$, נסמן ב-$\mathrm{Hom}_{\Bbbk}(U,V)$ את קבוצת ההעתקות הלינאריות מ-U ל-V. לקבוצה זו עצמה יש מבנה של מרחב וקטורי מעל $\Bbbk$, שנתון על-ידי חיבור העתקות לינאריות וכפל שלהן בקבועים מהשדה. בפרט, עבור $V = \Bbbk$, אנחנו מקבלים מרחב וקטורי $\check{U} = \mathrm{Hom}_{\Bbbk}(U, \Bbbk)$ שנקרא *המרחב הדואלי* של U. איברי $\check{U}$ נקראים לפעמים *פונקציונלים* על U. המרחב הדואלי פונקציונלים

אם W מרחב נוסף, ו-$T : U \to W$ העתקה לינארית, ההעתקה $s \mapsto s \circ T$ היא העתקה לינארית מ-$\mathrm{Hom}_{\Bbbk}(W,V)$ ל-$\mathrm{Hom}_{\Bbbk}(U,V)$. בפרט, T קובעת העתקה $\check{T} : \check{W} \to \check{U}$. הטענה הבאה מנוסחת מטעמי נוחות עבור המרחבים הדואליים, אבל נכונה באופן יותר כללי למרחבי העתקות.

עובדה 5.2.1. *נניח ש-U, V, W מרחבים לינאריים מעל $\Bbbk$ ו-$S : U \to V$ ו-$T : V \to W$ העתקות לינאריות. אז*

1. $\widecheck{T \circ S} = \check{S} \circ \check{T}$

2. *אם S חד-חד-ערכית אז $\check{S}$ על*

3. *אם T על אז $\check{T}$ חד-חד-ערכית*

בפרט, T חד-חד-ערכית אם ורק אם $\check{T}$ על, T היא על אם ורק אם $\check{T}$ חד-חד-ערכית, ו-T איזומורפיזם אם ורק אם $\check{T}$ איזומורפיזם

לכל מרחב V, המרחב $\check{V}$ גם הוא לינארי, ולכן ניתן להסתכל על המרחב הדואלי שלו, $\check{\check{V}}$. ישנה העתקה לינארית טבעית i_V מ-V ל-$\check{\check{V}}$, שנתונה על-ידי: $i_V(v)(\phi)=\phi(v)$ לכל $v\in V$ ו-$\phi\in\check{V}$. בשל העובדה הבאה, אנחנו יכולים לחשוב על V כעל תת-מרחב של $\check{\check{V}}$:

עובדה 5.2.2. *נניח ש-V מרחב לינארי*

1. *ההעתקה $i_V : V\to\check{\check{V}}$ היא חד-חד-ערכית*
2. *אם $T:U\to V$ העתקה, אז $\check{\check{T}}\circ i_U = i_V\circ T$ (כלומר, אחרי הזיהוי של U עם התמונה שלו תחת i_U, הצמצום של $\check{\check{T}}$ ל-U הוא T)*
3. *אם V ממימד סופי, אז $\check{V}$ מרחב מאותו מימד. בפרט, במצב הזה i_V איזומורפיזם.*

אם B בסיס של מרחב V, כל העתקה לינארית מ-V למרחב W נקבעת ביחידות על-ידי צמצומה ל-B, וכל פונקציה מ-B ל-W ניתן להרחיב להעתקה לינארית מ-V ל-W. במלים אחרות, אפשר לזהות את המרחב הלינארי $\mathrm{Hom}_{\Bbbk}(V,W)$ עם מרחב הפונקציות W^B מ-B ל-W. בפרט, ניתן לזהות את $\check{V}$ עם $\Bbbk^B$, מרחב הפונקציות מ-B ל-$\Bbbk$.

לכל קבוצה B קיים מרחב וקטורי $\Bbbk[B]$ מעל $\Bbbk$ שמכיל את B כבסיס: על מנת לראות זאת, מספיק למצוא מרחב שמכיל את B ובו B קבוצה בלתי תלויה (כי אז אפשר לקחת את תת-המרחב ש-B יוצרת). דוגמא אחת למרחב כזה היא מרחב כל הפונקציות $\Bbbk^B$ מ-B ל-$\Bbbk$, כאשר אנחנו מזהים כל איבר $b\in B$ עם *הפונקציה המציינת* $\delta_b\in\Bbbk^B$ הנתונה על-ידי $\delta_b(a)=1$ אם $a=b$ ו-0 אחרת (כדאי לבדוק שפונקציות מציינות אלה בלתי-תלויות לינארית). נדגיש שזו רק בניה אפשרית אחת של מרחב כזה, ואנחנו לא נשתמש בבנייה זו (או בכל בנייה אחרת) אלא רק בקיומו של מרחב כזה (כל שני מרחבים כאלה איזומורפיים קאנונית, כי B בסיס בשניהם). כיוון ש-B בסיס של $\Bbbk[B]$, המרחב הדואלי נתון על-ידי $\widecheck{\Bbbk[B]}=\Bbbk^B$. הפונקציה המציינת

אם $B\subseteq V$ תת-קבוצה של מרחב וקטורי, ניתן לצמצם כל איבר $\phi\in\check{V}$ לקבוצה B, ולקבל פונקציה (של קבוצות) $\phi_0 : B\to\Bbbk$. תהליך הצמצום הזה מגדיר העתקה לינארית r_B מ-$\check{V}$ למרחב $\Bbbk^B$. זוהי ההעתקה הדואלית להעתקה מ-$\Bbbk[B]$ ל-V שנקבעת על-ידי שליחת איברי הבסיס B לעצמם ב-V. לכן, בשילוב עם העובדות הקודמות אנחנו מקבלים:

עובדה 5.2.3. *במצב הנ"ל, B בלתי תלויה לינארית אם ורק אם r_B היא על ו-B פורשת את V אם ורק אם r_B חד-חד-ערכית. בפרט, r_B איזומורפיזם אם ורק אם B בסיס של V.*

5.3 דואליות פונטריאגין

אנחנו מעוניינים לקבל דואליות דומה לדואליות הנ"ל עבור חבורות, כלומר, לייצר מחבורה G חבורה דואלית $\check{G}$, עם תכונות דומות לדואליות במרחבים וקטוריים. אפשר לנסות, בדומה למקרה של מרחבים וקטוריים, להגדיר $\check{G}=\mathrm{Hom}(G,\mathbb{T})$, כאשר הפעם Hom מסמל העתקות

של חבורות, עבור חבורה מתאימה $\mathbb{T}$. מה יכולה להיות החבורה הזו? ראשית, ראינו כבר שאם $\mathbb{T}$ חבורה חילופית, הקבוצה של ההעתקות מהווה חבורה, תחת כפל איבר-איבר ב-$\mathbb{T}$, וקל לראות שתנאי החילופיות הוא גם הכרחי. מאידך, אם $\mathbb{T}$ אכן חילופית, אז כל העתקה מ-G ל-$\mathbb{T}$ תשלח את האיברים gh ו-hg לאותו איבר ב-$\mathbb{T}$. לכן, אין סיכוי בדואליות כזו לשחזר את ההבדל בין שני איברים כאלה, ואנחנו צריכים להגביל מראש את תשומת הלב לחבורות חילופיות.

יתכן ש-$\mathbb{T} = \mathbb{Z}$ נראית כמו בחירה טבעית עבור $\mathbb{Z}$, אבל נשים לב שב-$\mathbb{Z}$ אין איברים מסדר סופי (מלבד הטריוויאלי) ולכן כל איבר מסדר סופי ב-G יהיה חייב ללכת ליחידה תחת כל הומומורפיזם. בפרט, לכל חבורה סופית ישנו רק ההומומורפיזם הטריוויאלי ל-$\mathbb{Z}$. מכאן, ש-$\mathbb{T}$ צריכה לכלול איברים מכל סדר סופי. מסתבר שהבחירה הנכונה עבור $\mathbb{T}$ היא חבורת המעגל, שנוח לחשוב עליה כקבוצה הנתונה על-ידי התנאי $|z| = 1$ במישור המרוכב. זו תהיה ההגדרה שלנו (לפחות בגרסה הראשונה).

הגדרה 5.3.1. *חבורת המעגל* $\mathbb{T}$ היא חבורת המספרים המרוכבים מנורמה 1 (עם כפל של מרוכבים). חבורת המעגל
לכל חבורה G, *החבורה הדואלית* ל-G היא החבורה $\breve{G} = \mathrm{Hom}(G, \mathbb{T})$ של הומומורפיזמים של חבורות, תחת כפל של פונקציות החבורה הדואלית

הגדרה זו שימושית כמו שהיא, אבל רק אם מעשירים את $\breve{G}$ במבנה נוסף, של חבורה טופולוגית. אנחנו נזדקק רק למקרה הפרטי בו החבורה G היא סופית, ובמקרה זה הטופולוגיה אינה נדרשת. לכן, מעכשיו נניח שאנחנו עוסקים בחבורה חילופית סופית G (ניתן להשוות תנאי זה לסופיות המימד של המרחב הוקטורי). סוף הרצאה 11, 23 בנוב

דוגמא 5.3.2. נניח ש-G היא החבורה החיבורית $\mathbb{Z}/n$. ראינו שהעתקות מחבורה זו לכל חבורה אחרת מתאימות באופן טבעי לאיברים מסדר המחלק את n. בפרט, $\breve{\mathbb{Z}/n}$ היא החבורה $\mu_n = \{z \in \mathbb{C} \mid z^n = 1\}$. כיוון ש-$\mathbb{C}$ סגור אלגברית וממציין 0, בחבורה זו n איברים.

דוגמא 5.3.3. נניח ש-$G = \mu_n$. התמונה של כל העתקה מ-μ_n ל-$\mathbb{T}$ מוכלת ב-μ_n, ולכן $\breve{\mu_n}$ היא קבוצת האנדומורפיזמים של μ_n (עדיין עם הפעולה של כפל פונקציות!). ראינו שכל איבר i של $\mathbb{Z}/n$ מגדיר אנדומורפיזם כזה, $z \mapsto z^i$, וזה מגדיר העתקה $\mathbb{Z}/n \to \breve{\mu_n}$. בקרוב נראה שזהו איזומורפיזם

אם H היא תת-חבורה של החבורה G, ניתן לצמצם כל העתקה מ-G ל-$\mathbb{T}$ ל-H. הצמצום של מכפלת העתקות הוא מכפלת הצמצומים, ולכן אנחנו מקבלים העתקה r של חבורות מ-$\breve{G}$ ל-$\breve{H}$. הגרעין של העתקה זו הוא, על-פי הגדרה, ההעתקות מ-G ל-$\mathbb{T}$ שהן טריוויאליות על H (כלומר, שהגרעין שלהן מכיל את H). העתקות כאלה ניתן לזהות עם העתקות מהמנה G/H ל-$\mathbb{T}$ (על פי הגדרת המנה). במלים אחרות, ניתן לזהות את הגרעין של r עם החבורה $\breve{G/H}$. הטענה הבאה מראה, בין היתר, ש-r היא על (כדאי להשוות לעובדה 5.2.1)

טענה 5.3.4. *נניח ש-G חבורה סופית חילופית, H תת-חבורה ו-$\chi : H \to \mathbb{T}$ העתקה. אז יש $\frac{|G|}{|H|}$ דרכים להרחיב את χ להעתקה $\tilde{\chi} : G \to \mathbb{T}$. בפרט,* $|G| = |\breve{G}|$.

הוכחה. נוכיח ראשית שקיימת לפחות הרחבה אחת. אפשר להניח באינדוקציה ש-G נוצרת על-ידי H ואיבר נוסף $a \in G$. כיוון ש-G סופית, יש $k > 0$ עבורו $b = a^k \in H$, ואפשר להניח ש-k הוא מינימלי עם התכונה הזו. אז לכל איבר של G יש הצגה יחידה בצורה $a^m h$ כאשר $h \in H$

ו-$m \in \mathbb{Z}/k$. נבחר פתרון α של המשוואה $x^k = \chi(b)$ ב-$\mathbb{T}$, ונגדיר $\widetilde{\chi}(a^m h) = \alpha^m \chi(h)$. ברור שזוהי הרחבה כפי שרצינו.

את הטענה על מספר ההרחבות נוכיח באינדוקציה שלמה על $|G|$. קבוצת ההרחבות של χ היא בדיוק הסיב $r^{-1}(\chi)$, כאשר r העתקת הצמצום שנידונה לפני ההוכחה. החלק הראשון מראה שקבוצה זו אינה ריקה, ולכן הגודל שלה הוא כגודל הגרעין של r. ראינו לפני ההוכחה שניתן לזהות גרעין זה עם $\widecheck{G/H}$, ולכן אם H אינה טריוויאלית, הטענה נובע באינדוקציה. יתר על-כן, אם H טריוויאלית אבל קיימת תת-חבורה ממש לא טריוויאלית H_1 של G, כל איבר של $\breve{G}$ הוא הרחבה של איבר של $\breve{H_1}$, באינדוקציה ישנם $|H_1|$ איברים כאלה, ולכל אחד $|G/H_1| = \frac{|G|}{|H_1|}$ הרחבות, אז בסה"כ $|G|$ איברים, כפי שרצינו.

נותר לטפל במקרה בו ל-G אין תת-חבורה ממש לא טריוויאלית, כלומר במקרה בו G נוצרת על-ידי איבר אחד a. במקרה זה, G איזומורפית ל-$\mathbb{Z}/n$, כאשר $n = |G|$ (על-ידי ההעתקה ששולחת את $1 \in \mathbb{Z}/n$ ל-a), וראינו את הטענה בדוגמא 5.3.2. $\square$

החבורה $\breve{G}$ היא חילופית וסופית, ולכן יש לה חבורה דואלית $\breve{\breve{G}}$. יש לנו העתקה טבעית של חבורות, הנתונה על-ידי $g(\chi) = \chi(g)$, בדיוק כמו במקרה הלינארי. הטענה הבאה מקבילה לטענה שלמרחב ולדואלי שלו אותו מימד במקרה הסוף מימדי (עובדה 5.2.2).

מסקנה 5.3.5. *ההעתקה הטבעית מ-G ל-$\breve{\breve{G}}$ היא איזומורפיזם*

הוכחה. על מנת להוכיח שההעתקה חד-חד-ערכית, צריך להראות שאם $g \in G$ איבר כך ש-$g(\chi) = 1$ לכל $\chi \in \breve{G}$, אז $g = e$. אבל $g(\chi) = \chi(g)$, אז צריך להראות שאם g אינו הזהות, אז יש χ עבורו $\chi(g) \neq 1$, וזה חלק מהטענה האחרונה. זה מראה שההעתקה היא חד-חד-ערכית, והיא על כי שוב לפי הטענה האחרונה, יש בשתי החבורות אותו מספר איברים. $\square$

בפרט, החבורה הדואלית ל-μ_n היא אכן $\mathbb{Z}/n$.

דואליות פונטריאגין

לדואליות שבמסקנה קוראים *דואליות פונטריאגין*. כאמור, היא רחבה יותר מההקשר הסופי שלנו, אבל ההרחבה דורשת מושגים מטופולוגיה. לדואליות זו תכונות נחמדות רבות, בדומה למרחבים וקטוריים. למשל:

טענה 5.3.6. *אם $t : G \to H$ הומומורפיזם בין שתי חבורות חילופיות סופיות, אז קיים הומומורפיזם $\breve{t} : \breve{H} \to \breve{G}$, עם התכונה ש-$\breve{t}(\phi)(g) = \phi(t(g))$ לכל $\phi \in \breve{H}$ ו-$g \in G$. לאחר הזיהוי של כל חבורה עם הדואלית הכפולה שלה, $\breve{\breve{t}} = t$.*

תרגיל 5.3.7. הוכיחו את הטענה. הוכיחו גם ש-t חד-חד-ערכית אם ורק אם $\breve{t}$ היא על (בדומה לעובדה 5.2.1 ו 5.2.2)

תרגיל 5.3.8. הוכיחו שאם G, H חבורות חילופיות סופיות, אז $\widecheck{G \times H}$ איזומורפית ל-$\breve{G} \times \breve{H}$. הסיקו שאם k, l זרים אז μ_{kl} איזומורפית ל-$\mu_k \times \mu_l$.

5.4 התמרת פורייה

התחלנו את הדיון בדואליות פונטריאגין מההקבלה למצב עבור מרחבים וקטוריים. בסעיף זה נראה שיש קשר שהוא מעבר להקבלה. לפני שנמשיך, נעיר שבמקרה הכללי של חבורות טופולוגיות, החשיבות של הבחירה ב-$\mathbb{T}$ להיות מעגל היחידה נובעת מהתכונות הטופולוגיות של חבורה זו. בהקשר הסופי, האיברים היחידים של $\mathbb{T}$ שמשחקים תפקיד הם האיברים מסדר סופי (במלים אחרות, *שורשי היחידה*), וגם ביניהם, רק אלה שהסדר שלהם אינו זר לסדר החבורה. לכן, מעכשיו נקבע שדה סגור אלגברית $\Bbbk$, שהמציין שלו p זר לכל סדרי החבורות שנדבר עליהן (או 0), ו-$\mathbb{T}$ תהיה חבורת שורשי היחידה ב-$\Bbbk$. אם n זר ל-p, יש בחבורה זו n איברים שונים שהסדר שלהם מחלק את n (ובפרט, כפי שראינו, זו חבורה מעגלית). אם $\Bbbk=\mathbb{C}$, אז $\mathbb{T}$ מוכלת בחבורת המעגל, ומכילה את התמונה של כל האיברים בחבורה הדואלית, וזה המקרה שכדאי לחשוב עליו במהלך רוב הדיון, אבל נזכה להשתמש גם בשדה ממציין חיובי בקרוב.

שורשי היחידה

סוף הרצאה 12, 26 בנוב

נניח עכשיו ש-G חבורה חילופית סופית. אם נתעלם לרגע ממבנה החבורה ונחשוב על G כקבוצה, נזכרנו בסעיף 5.2 שקיים מרחב לינארי $\Bbbk[G]$ שמכיל את G כבסיס, ושהמרחב הדואלי שלו הוא $\Bbbk^G$, מרחב כל הפונקציות מ-G ל-$\Bbbk$. כיוון ש-G חבורה חילופית סופית, יש לה חבורה דואלית $\breve{G}$, שמורכבת לפי הגדרתה מפונקציות מ-G ל-$\mathbb{T}$, תת-קבוצה של $\Bbbk$. בפרט, אפשר לחשוב על $\breve{G}$ כתת-קבוצה של $\Bbbk^G=\widetilde{\Bbbk[G]}$. לפי טענה 5.3.4, הגודל של $\breve{G}$ הוא בדיוק המימד של מרחב זה, ולכן סביר לתהות האם קבוצה זו מהווה בסיס. לפי עובדה 5.2.3 (עבור $V=\Bbbk^G$ ו-$B=\breve{G}$), על מנת להוכיח זאת מספיק להראות שההעתקה מ-$\widetilde{\Bbbk^G}$ ל-$\Bbbk^{\breve{G}}$ היא איזומורפיזם. כיוון ש-$\Bbbk^G$ הוא המרחב הדואלי ל-$\Bbbk[G]$ והמימד סופי, התחום של העתקה זו הוא $\Bbbk[G]$, והצבה בהגדרות מראה ישירות, שההעתקה שמדובר עליה היא ההרחבה על-ידי לינאריות של ההעתקה $G\to\breve{\breve{G}}\subseteq\Bbbk^{\breve{G}}$ שנתונה על-ידי דואליות פונטריאגין. מסיבות שנראה מיד, נהוג להרכיב בהקשר הזה עם ההעתקה $g\mapsto g^{-1}$ (שהיא אוטומורפיזם של החבורה G), אז ההעתקה שאנחנו מעוניינים בה נתונה בהגדרה הבאה:

התמרת פורייה

הגדרה 5.4.1. אם G חבורה חילופית סופית, *התמרת פורייה* עבור G היא ההעתקה הלינארית $\mathcal{F}:\Bbbk[G]\to\Bbbk^{\breve{G}}$ שמרחיבה את הפונקציה $\mathcal{F}_0:G\to\Bbbk^{\breve{G}}$ הנתונה על-ידי $\mathcal{F}_0(g)(\chi)=\chi(g^{-1})$.

כאמור, אנחנו רוצים להראות ש-$\mathcal{F}$ איזומורפיזם. לשם כך, נגדיר העתקה בכיוון ההפוך. המרחב $\Bbbk^{\breve{G}}$ נפרש באופן חופשי על-ידי הפונקציות δ_χ (הפונקציות המציינות) עבור $\chi\in\breve{G}$. נגדיר $\widetilde{\mathcal{F}}:\Bbbk^{\breve{G}}\to\Bbbk[G]$ על-ידי $\widetilde{\mathcal{F}}(\delta_\chi)=\sum_{g\in G}\chi(g)g$ לכל $\chi\in\breve{G}$. למען הנוחות, נרשום במפורש את ההעתקות על איברים כלליים:

$$\mathcal{F}(\sum_{g\in G}a_g g)(\phi)=\sum_{g\in G}a_g\phi(g^{-1}) \tag{5.1}$$

$$\widetilde{\mathcal{F}}(t)=\sum_{\chi\in\breve{G}}t(\chi)\sum_{g\in G}\chi(g)g=\sum_{g\in G}(\sum_{\chi\in\breve{G}}t(\chi)\chi(g))g \tag{5.2}$$

לכל $a_h\in\Bbbk$, $\phi\in\breve{G}$ ו-$t:\breve{G}\to\Bbbk$. נשים לב, בפרט, שלכל פונקציה t כזו, הסכום $\sum_{\chi\in\breve{G}}t(\chi)$ המקדם של e ב-$\widetilde{\mathcal{F}}(t)$.

שתי ההעתקות שהגדרנו הן לא בדיוק הפוכות, אבל קרוב מספיק:

טענה 5.4.2. *לכל* $v\in\Bbbk[G]$ *ולכל* $h\in\Bbbk^{\breve{G}}$ *מתקיים* $\widetilde{\mathcal{F}}(\mathcal{F}(v))=|G|v$ *ו-*$\mathcal{F}(\widetilde{\mathcal{F}}(h))=|G|h$

כמובן נובע מזה ש-$\frac{1}{|G|}\widetilde{\mathcal{F}}$ הופכית ל-$\mathcal{F}$, ובפרט $\mathcal{F}$ איזומורפיזם (אבל פה אנחנו משתמשים בכך ש-$\Bbbk$ ממציין זר ל-$|G|$). ישנן נורמליזציות נוספות, למשל לחלק את שתי הפונקציות ב-$\sqrt{|G|}$.

הוכחה. מלינאריות, מספיק להוכיח את השוויון השני כאשר $h=\delta_\chi$, עבור $\chi\in\breve{G}$. עבור χ כזה, ההגדרה נותנת לכל $\psi\in\breve{G}$

$$\mathcal{F}(\widetilde{\mathcal{F}}(\delta_\chi))(\psi)=\mathcal{F}(\sum_{g\in G}\chi(g)g)(\psi)=\sum_{g\in G}\chi(g)\mathcal{F}(g)(\psi)=\sum_{g\in G}\chi(g)\psi(g^{-1})$$

עלינו להוכיח שצד ימין הוא 0 אם $\chi\neq\psi$ ו-$|G|$ אם $\chi=\psi$. טענה זו חשובה מסיבות נוספות, ולכן נוכיח אותה בנפרד למטה. השוויון הראשון נכון משום שלפי מה שראינו, לשני המרחבים יש אותו מימד $|G|=|\breve{G}|$, או באמצעות חישוב דומה. $\square$

להשלמת ההוכחה, עלינו להוכיח את הטענה הבאה:

טענה 5.4.3. *לכל* $\chi,\psi\in\breve{G}$ *ולכל* $g,h\in G$ *מתקיים*

$$\sum_{g\in G}\chi(g)\psi(g^{-1})=\begin{cases}|G| & \chi=\psi\\ 0 & \chi\neq\psi\end{cases} \tag{5.3}$$

$$\sum_{\chi\in\breve{G}}\chi(g)\chi(h^{-1})=\begin{cases}|G| & g=h\\ 0 & g\neq h\end{cases} \tag{5.4}$$

הוכחה. השוויון השני מתקבל מהראשון על-ידי דואליות. את השוויון הראשון מספיק להוכיח למקרה $\psi=1$ (הפונקציה הקבועה 1) כי $\chi=\psi$ אם ורק אם $\chi\psi^{-1}=1$. אם $\chi=1$ אז הטענה ברורה. אחרת, ישנו $h\in G$ עבורו $\chi(h)\neq 1$. אז $\sum_{g\in G}\chi(g)=\sum_{g\in G}\chi(hg)=\chi(h)\sum_{g\in G}\chi(g)$, וכיוון ש-$\chi(h)\neq 1$, הסכום הוא 0. $\square$

הטענה גם מראה סיבה אחת לכך שהרכבנו עם העתקת ההפכי. סוף הרצאה 13,
את הטענה על הפיכות העתקת פורייה אפשר לנסח גם בדרך הבאה: 30 בנוב

מסקנה 5.4.4. *איברי* $\breve{G}$ *מהווים בסיס של* $\Bbbk^G$. *מטריצת המעבר מבסיס זה לבסיס הנתון על-ידי הפונקציות המציינות* δ_g *נתונה על-ידי* $\frac{1}{|G|}(\chi^{-1}(g))_{\chi\in\breve{G},g\in G}$

תרגיל 5.4.5. הוכיחו את המסקנה

בניסוח אחר, המסקנה אומרת שניתן לזהות את $\Bbbk^G$ עם $\Bbbk[\breve{G}]$, ואת התמרת פורייה ניתן לראות כאיזומורפיזם $\mathcal{F}:\Bbbk[G]\to\breve{\Bbbk[\breve{G}]}$.

תרגיל 5.4.6. עם הזיהוי שהוזכר, נסמן ב-$\mathcal{F}_G:\Bbbk[G]\to\breve{\Bbbk[\breve{G}]}$ את התמרת פורייה עבור G, וב-$\mathcal{F}_{\breve{G}}:\Bbbk[\breve{G}]\to\breve{\Bbbk[G]}$ את התמרת פורייה עבור החבורה $\breve{G}$ (כאשר זיהינו את G עם $\breve{\breve{G}}$). הוכיחו ש-$\mathcal{F}_{\breve{G}}=\breve{\mathcal{F}_G}$, כאשר צד ימין הוא ההעתקה הדואלית

תרגיל 5.4.7. לכל תת-קבוצה $A \subseteq G$ נסמן $A^{\perp} = \{\chi \in \breve{G} \mid \forall a \in A\ \chi(a) = 1\}$. עבור $B \subseteq \breve{G}$ אנחנו חושבים על $B^{\perp}$ כעל תת-קבוצה של G, תחת הזיהוי הרגיל של G עם $\breve{\breve{G}}$.

1. הוכיחו ש-$A^{\perp}$ תת-חבורה של $\breve{G}$.
2. הוכיחו ש-$(A^{\perp})^{\perp}$ היא תת-החבורה של G שנוצרת על-ידי A (בפרט, אם A תת-חבורה אז $(A^{\perp})^{\perp} = A$)
3. נניח ש-A תת-חבורה ו-$\chi \in \breve{G}$. הוכיחו:

$$\sum_{g \in A} \chi(g) = \begin{cases} |A| & \chi \in A^{\perp} \\ 0 & \text{אחרת} \end{cases}$$

4. נניח שוב ש-A תת-חבורה, ונסמן $a = \sum_{g \in A} g$, איבר של $\Bbbk[G]$. הוכיחו ש-$\mathcal{F}(a) = |A|\delta_{A^{\perp}}$, כאשר לכל תת-קבוצה δ_X היא הפונקציה המציינת של X (כלומר, $\delta_X(a) = 1$ אם $a \in X$ ו-0 אחרת).

עבור השימוש שלנו, נזדקק למבנה נוסף. לתחום ולטווח של התמרת פורייה יש מבנה של חוג: הכפל על $\Bbbk[G]$ מתקבל מהכפל ב-G (כפל זה נקרא לעתים *קונבולוציה*), והכפל ב-$\Bbbk^{\breve{G}}$ הוא הכפל הרגיל של פונקציות. אפשר לחשוב על $\Bbbk$ כעל תת-חוג שני החוגים, על-ידי הזיהוי של $a \in \Bbbk$ עם ae, כאשר e היחידה של החבורה המתאימה. אנחנו טוענים: קונבולוציה

טענה 5.4.8. *התמרת פורייה היא העתקה של חוגים:* $\mathcal{F}(u * v) = \mathcal{F}(u)\mathcal{F}(v)$ *ו-*$\mathcal{F}(a) = a$ *לכל* $a \in \Bbbk$.

כפי שראינו, נובע מזה שגם ההפכית $\frac{1}{|G|}\widetilde{\mathcal{F}}$ של $\mathcal{F}$ היא העתקה של חוגים.

הוכחה. מלינאריות, מספיק לבדוק זאת על הבסיס G של $\Bbbk[G]$, ועל בסיס זה $\mathcal{F}$ היא פשוט האיזומורפיזם של G עם $\breve{\breve{G}}$, מורכבת עם ההעתקה $g \mapsto g^{-1}$ (שהיא אוטומורפיזם של G, כי G חילופית). □

תרגיל 5.4.9. נסמן $G = \mathbb{Z}/12$ ו-$H = \mathbb{Z}/2 \times \mathbb{Z}/6$. הוכיחו ש-$G$ ו-H אינן איזומורפיות, אבל החוגים $\mathbb{C}[H]$ ו-$\mathbb{C}[G]$ איזומורפיים

תרגיל 5.4.10. נסמן $G = \mathbb{Z}/4$ ו-$H = \mathbb{Z}/2 \times \mathbb{Z}/2$.

1. רשמו במפורש איזומורפיזם מ-$\mathbb{C}[G]$ ל-$\mathbb{C}[H]$
2. הוכיחו שאין איזומורפיזם מ-$\mathbb{R}[G]$ ל-$\mathbb{R}[H]$ (רמז: הוכיחו שבחבורה הכפלית של $\mathbb{R}[H]$ אין איברים מסדר 4)

סוף הרצאה 14, 3 בדצמ

ההערה האחרונה שנזדקק לה נוגעת להעתקות. נניח ש-$f:X\to Y$ העתקה בין קבוצות. כיוון ש-Y תת-קבוצה של $\Bbbk[Y]$, ניתן לחשוב על f כעל פונקציה (של קבוצות) מ-X ל-$\Bbbk[Y]$. לפי הגדרת $\Bbbk[X]$, יש העתקה לינארית יחידה $T_f:\Bbbk[X]\to\Bbbk[Y]$ שמרחיבה את f. מאידך, פונקציה כזו משרה העתקה $C_f:\Bbbk^Y\to\Bbbk^X$ של חוגים (ושל מרחבים וקטוריים מעל $\Bbbk$), הנתונה על-ידי $C_f(t)(x)=t(f(x))$ לכל $t\in\Bbbk^Y$ ו-$x\in X$ (במלים אחרות, $C_f(t)=t\circ f$).

תרגיל 5.4.11. במצב לעיל, הוכיחו שאם $g:Y\to Z$ פונקציה נוספת, אז $T_{g\circ f}=T_g\circ T_f$ ו-$C_{g\circ f}=C_f\circ C_g$. בפרט, אם f הפיכה, אז גם T_f ו-C_f הפיכות.

נניח עכשיו ש-G,H חבורות, ו-σ העתקה של חבורות. עבור $f=\sigma$ בפסקה הקודמת, אנחנו מקבלים העתקה לינארית $T_\sigma:\Bbbk[G]\to\Bbbk[H]$, וכיוון ש-$\sigma$ העתקה של חבורות, T_σ העתקה של חוגים (לפי לינאריות, מספיק לבדוק זאת על הבסיס G של $\Bbbk[G]$). אם G,H סופיות וחילופיות, ההעתקה σ משרה העתקה $\breve{\sigma}:\breve{H}\to\breve{G}$ (כמו בטענה 5.3.6), ועבור $f=\breve{\sigma}$ נקבל מהפסקה הקודמת $C_{\breve{\sigma}}:\Bbbk^{\breve{G}}\to\Bbbk^{\breve{H}}$. הקשר בין שתי ההעתקות הללו נתון על-ידי התמרת פורייה:

טענה 5.4.12. *לכל העתקה $\sigma:G\to H$ בין חבורות חילופיות סופיות מתקיים $C_{\breve{\sigma}}\circ\mathcal{F}_G=\mathcal{F}_H\circ T_\sigma$ (כאשר ההעתקות $C_{\breve{\sigma}}$ ו-T_σ הוגדרו לעיל).*

תרגיל 5.4.13. השלימו את הפרטים בהוכחה

אנחנו נתעניין בטענה 5.4.12 בעיקר במקרה $G=H$ ו-σ אוטומורפיזם של G. במקרה זה, לפי תרגיל 5.4.11 גם T_σ ו-$C_{\breve{\sigma}}$ העתקות לינאריות הפיכות. אחד היתרונות של מעבר מ-G ל-$\Bbbk[G]$ (ומ-σ ל-T_σ) הוא שגם אם ל-σ אין נקודות שבת מעניינות (כלומר, אם $\sigma(g)\neq g$ לכל $g\neq e$), ל-T_σ עשויים להיות וקטורים עצמיים מעניינים. לגבי וקטורים כאלה, מקבלים מטענה 5.4.12 את המסקנה הבאה:

מסקנה 5.4.14. *אם $v\in\Bbbk[G]$ וקטור עצמי של T_σ עבור אוטומורפיזם σ של G, אז $\mathcal{F}(v)$ וקטור עצמי של $C_{\breve{\sigma}}$, עם אותו ערך עצמי*

איך אפשר לבנות וקטור עצמי עבור אוטומורפיזם σ? התרגיל הבא נותן שיטה כללית שתהיה רלוונטית בהקשר של הוכחת חוק ההדדיות.

תרגיל 5.4.15. בשאלה זו:

1. $\Bbbk$ שדה ממציין אפס
2. G חבורה חילופית סופית
3. $H=\mathrm{Aut}(G)$ חבורת האוטומורפיזמים של G
4. $\theta:H\to\Bbbk^\times$ העתקה של חבורות

נניח ש-$g\in G$ איבר עם התכונה: **לכל** $h\in H$, **אם** $h(g)=g$ **אז** $\theta(h)=1$.

הוכיחו שהאיבר $v=\sum_{h\in H}\theta(h^{-1})h(g)\in\Bbbk[G]$ הוא וקטור עצמי של T_h לכל $h\in H$, עם ערך עצמי $\theta(h)$ (שימו לב שוקטור עצמי הוא בפרט שונה מ-0)

הדרכה: הוכיחו קודם את המקרה הפרטי בו $h(g)\neq g$ לכל h שאינו הזהות (זה יהיה המקרה שלנו)

הערה 5.4.16. נניח ש-S קבוצה של העתקות לינאריות הפיכות ממרחב וקטורי V לעצמו. אם $v \in V$ וקטור עצמי של כל ההעתקות ב-S, אז הוא וקטור עצמי של כל ההרכבות של איברים של S ושל ההפכיות שלהן (במלים אחרות, של כל איברי תת-החבורה של $GL(V)$ שנוצרת על-ידי S, כאשר $GL(V)$ חבורת האוטומורפיזמים של V כמרחב וקטורי). נניח ש-S סגורה תחת הרכבות והעתקות הפוכות (כלומר שהיא כבר תת-חבורה). לכל $t \in S$ נסמן ב-$\theta(t)$ את הערך העצמי המתאים ל-v. אז לכל $r, t \in S$ מתקיים $\theta(r \circ t) = \theta(r)\theta(t)$, כלומר θ הומומורפיזם מ-S ל-$\Bbbk^\times$. משום כך, בהינתן חבורה כזו S והומומורפיזם $\theta : S \to \Bbbk^\times$, טבעי לשאול האם יש וקטור עצמי משותף של כל איברי S שהערכים העצמיים שלו נתונים על-ידי θ. התרגיל האחרון עונה על השאלה הזו במקרה הפרטי ש-$V = \Bbbk[G]$ ו-S חבורת ה-T_h, עבור $h \in \mathrm{Aut}(G)$.

5.5 הוכחת משפט ההדדיות

נתונים שני ראשוניים אי-זוגיים שונים p, q. אפשר להניח ש-$p < q$. נתבונן בחבורה החיבורית $G = \mathbb{Z}/q$. כיוון שאיברי G נראים כמו איברי השדה $\Bbbk$, נסמן ב-$[i]$ את האיבר ב-$\Bbbk[G]$ שמתאים ל-i.

ראינו במסקנה 4.2.7 שחבורת האוטומורפיזמים $\mathrm{Aut}(G)$ במקרה זה היא $U_q = \mathbb{F}_q{}^\times$. העובדה שסימן לז'נדר $\left(\frac{i}{q}\right)$ כפלי ב-i ותלוי רק בשארית של i ביחס ל-q אומרת שאפשר לחשוב עליו כעל העתקה של חבורות מ-U_q ל-$\Bbbk^\times$. נסמן $v = \sum_{i \in G} \left(\frac{i}{q}\right) [i] \in \Bbbk[G]$: זהו הוקטור שמתקבל מתרגיל 5.4.15 עבור $\theta(i) = \left(\frac{i}{q}\right)$ ו-$g = 1 \in G$, ולכן הוא וקטור עצמי של T_m לכל איבר $m \in U_q$, עם ערך עצמי $\left(\frac{m}{q}\right)$ (אפשר גם לבדוק זאת ישירות בתור תרגיל. במקרה שלנו אין הבדל בין m להפכי שלו ב-U_q, משום שלשניהם אותו ערך תחת θ). במילים אחרות, $T_m(v) = \left(\frac{m}{q}\right) v$ לכל $m \in U_q$ (וכמובן שזה נכון גם עבור $m = 0$).

ראינו שהחבורה הדואלית של G היא μ_q, חבורת שורשי היחידה מסדר q. נסמן ב-$g = \mathcal{F}(v)$ את התמרת הפורייה של v. אז g היא פונקציה מ-μ_q ל-$\Bbbk$. הערכים $g(\xi) = \sum_{i \in \mathbb{Z}/q} \left(\frac{i}{q}\right) \xi^{-i}$ (עבור $\xi \neq 1$) נקראים *סכומי גאוס*. לפי מסקנה 5.4.14, g הוא וקטור עצמי של $C_m : \Bbbk^{\mu_q} \to \Bbbk^{\mu_q}$, עם ערך עצמי $\left(\frac{m}{q}\right)$ לכל האיברים m ב-U_q. הפעולה של U_q על μ_q נתונה עבור $m \in U_q$ על-ידי $\xi \mapsto \xi^m$, ולכן $g(\xi^m) = \left(\frac{m}{q}\right) g(\xi)$ לכל $\xi \in \mu_q$ ולכל m שלם (גם פה, הנוסחא נכונה גם עבור $m = 0$ מסיבות שנראה מיד). סכומי גאוס

סוף הרצאה 15, 10 בדצמ

טענה 5.5.1. *לכל* $\xi \neq 1$ *מתקיים* $g(\xi)^2 = \left(\frac{-1}{q}\right) q$ *(ו-*$g(1) = 0$*)*

הוכחה. ראשית, $g(1) = \sum_{i \in G} \left(\frac{i}{q}\right) = 0$ משום שבדיוק חצי מהאיברים ב-G הם ריבועים. לכל אוטומורפיזם $l \in U_q$ מתקיים

$$C_l(g^2) = C_l(g)^2 = \left(\frac{l}{q}\right)^2 g^2 = g^2$$

לכן, לכל $l \in U_q$ ולכל $\xi \in \mu_q$ מתקיים $g^2(\xi^l) = g^2(\xi)$. לכן, הערך של g^2 על האיברים ששונים מ-1 הוא קבוע. כדי לחשב מהו ערך זה, מספיק לחשב את $\sum_{\xi \in \mu_q} g^2(\xi)$. ראינו בנוסחא (5.2) שערך זה הוא המקדם של $0 \in \mathbb{Z}/q$ ב-$\widetilde{\mathcal{F}}(g^2)$. מאידך,

$$\widetilde{\mathcal{F}}(g^2) = \widetilde{\mathcal{F}}(\mathcal{F}(v)^2) = \widetilde{\mathcal{F}}(\mathcal{F}(v * v)) = q \cdot v * v$$

ולכן הערך שאנחנו מחפשים הוא המקדם של 0 ב-$q \cdot v * v$. לפי ההגדרה, ערך זה הוא $q \sum_{i \in \mathbb{Z}/q} \left(\frac{i}{q}\right) \left(\frac{-i}{q}\right) = q(q-1) \left(\frac{-1}{q}\right)$, שוב לפי הכפליות. אז זהו סכום הערכים, וכיוון שיש $q-1$ איברים בסכום, זו התוצאה שחיפשנו[1] ☐

נניח עכשיו שהמציין של $\mathbb{k}$ הוא p. בפרט, השוויון מהטענה האחרונה מראה ש-g היא פונקציה קבועה (מחוץ ל-1), שהערך הקבוע שלה הוא ב-$\mathbb{F}_p$.

הוכחת משפט ההדדיות (משפט 5.1.6). נבחר $\xi \in \mu_q$ לא טריוויאלי כלשהו, ונסמן $b = g(\xi)$. מהטענה האחרונה (עם שימוש באותם מונחים), נקבל

$$b^p = b \cdot b^{p-1} = b \cdot (b^2)^{\frac{p-1}{2}} = b \cdot (\left(\frac{-1}{q}\right) q)^{\frac{p-1}{2}} = b(-1)^{\frac{q-1}{2}\frac{p-1}{2}} \left(\frac{q}{p}\right)$$

כאשר השוויון האחרון נובע ממשוואת אוילר (נזכיר שאנחנו עובדים ב-$\mathbb{F}_p$). כיוון ש-$b \neq 0$, אפשר לצמצם ולקבל

$$b^{p-1} = (-1)^{\frac{q-1}{2}\frac{p-1}{2}} \left(\frac{q}{p}\right)$$

מאידך, כיוון שאנחנו עובדים בשדה ממציין p, והמקדמים $\left(\frac{i}{q}\right)$ בביטוי עבור b הם ב-$\mathbb{F}_p$, הפעולה של p על b נתונה על-ידי חזקה p: $b^p = g(\xi)^p = g(\xi^p) = \left(\frac{p}{q}\right) b$, והפעם הצמצום נותן $b^{p-1} = \left(\frac{p}{q}\right)$. הצירוף של שני השוויונות נותן את המשפט. ☐

על-מנת לקבל את התמונה המלאה, עלינו עדיין לחשב את $\left(\frac{2}{p}\right)$ לכל ראשוני אי-זוגי p. החישוב דומה מאד, ונשאיר אותו בתור תרגיל:

תרגיל 5.5.2. חיזרו על הוכחת משפט ההדדיות עבור $q = 8$ במקום ראשוני אי-זוגי. הסיקו את טענה 5.1.8.

5.6 כפל מהיר של פולינומים

נתבונן שוב בחוג החבורה $\mathbb{k}[G]$ כאשר $G = \mathbb{Z}/n$. אם נרשום את איבר הבסיס $i \in \mathbb{Z}/n$ כ-x^i, אפשר לזהות את $\mathbb{k}[G]$ עם קבוצת הפולינומים ממעלה קטנה מ-n, והכפל נקבע על-ידי הנוסחא $x^i * x^j = x^{i+j}$, כאשר החיבור במעריך הוא חיבור שאריות ביחס ל-n. לכן, עבור $0 \leqslant i < n$

[1] לפחות בהנחה ש-$q \neq 1$ ב-$\mathbb{k}$!

האיבר x^i הוא אכן החזקה ה-i של $x = x^1$, ואנחנו מזהים את x^n עם $x^0 = 1$. במלים אחרות, החוג $\Bbbk[G]$ איזומורפי ל-$\Bbbk[x]/x^n-1$.

אם ξ שורש יחידה n, אז $\xi^n = 1$ ולכן הערך $p(\xi)$ של פולינום $p(x)$ ב-$\Bbbk[G]$ על שורש יחידה כזה ξ מוגדר היטב. במלים אחרות, כל איבר של $\Bbbk[G]$ ניתן לראות כפונקציה מ-μ_n ל-$\Bbbk$, איבר של $\Bbbk^{\check{G}}$. עד-כדי מעבר להפכי, זוהי בדיוק התמרת פורייה: אם $p(x) = \sum_{i\in\mathbb{Z}/n} a_i x^i$, אז $\mathcal{F}(p(x))(\xi) = \sum_{i\in\mathbb{Z}/n} a_i\xi^{-i} = p(\xi^{-1})$. במלים אחרות, התמרת פורייה מעבירה פולינום מהייצוג שלו על-ידי המקדמים של המונומים לייצוג שלו על-ידי ערכיו על שורשי היחידה (והטענה על הפיכות התמרת פורייה היא במקרה זה הטענה שכל פונקציה מ-n ערכים שונים ל-$\Bbbk$ מיוצגת על-ידי פולינום יחיד ממעלה קטנה מ-n). כפי שציפינו מטענה 5.4.8, כפל פולינומים עובר לכפל פונקציות בצד השני.

כמה צעדים נדרשים על-מנת לבצע כפל כזה? אם p, q שני פולינומים ממעלה $n-1$, נתונים כל אחד על-ידי n מקדמים, כל מקדם דורש n מכפלות וסכומים, וישנו סדר גודל של n מקדמים, אז הכפל בשיטה זו מתבצע בזמן ריבועי (בקירוב) במעלת הפולינום. האם אפשר לעשות יותר טוב? אם הפולינומים נתונים על-ידי הערכים שלהם (למשל על μ_n), הכפל לוקח סדר גודל של n צעדים (צריך לעבור על איברי μ_n ולכפול). לכן, אם יש שיטה לחשב מהר את התמרת פורייה (ואת ההתמרה ההפוכה), נקבל כפל מהיר של פולינומים.

מסתבר ששיטות כאלה אכן קיימות. הנפוצה ביותר נקראת Cooley–Tukey (אבל הייתה ידועה לגאוס), ודומה לרעיון של העלאה מהירה בחזקה. לשם הפשטות, נניח ש-$n = 2^k$ עבור k טבעי. אז עבור פולינום $p(x)$ ממעלה n,

$$\mathcal{F}(p)(\xi^{-1}) = \sum_{i<2^k} a_i\xi^i = \sum_{i<2^{k-1}} a_{2i}\xi^{2i} + \xi \sum_{i<2^{k-1}} a_{2i+1}\xi^{2i} = \\ \mathcal{F}(p_1)(\xi^{-2}) + \xi\mathcal{F}(p_2)(\xi^{-2})$$

עבור פולינומים p_1 ו-p_2 ממעלה 2^{k-1}, ומאידך

$$\mathcal{F}(p)(-\xi^{-1}) = \sum_{i<2^k} a_i(-\xi)^i = \sum_{i<2^{k-1}} a_{2i}\xi^{2i} - \xi \sum_{i<2^{k-1}} a_{2i+1}\xi^{2i} = \\ \mathcal{F}(p_1)(\xi^{-2}) - \xi\mathcal{F}(p_2)(\xi^{-2})$$

ולכן החישוב של שני הערכים $\mathcal{F}(p_1)(\xi^{-2})$ ו-$\xi\mathcal{F}(p_2)(\xi^{-2})$ מאפשר לחשב שני ערכים של התמרת פורייה המקורית. לכן, זמן החישוב לערך אחד הוא בסדר גודל של k, וחישוב כל הערכים לוקח $k2^k = n\log(n)$ צעדים (ובאופן דומה להתמרה ההפוכה). סוף הרצאה 16, 14 בדצמ

6 ראשוניים בסדרות חשבוניות

ראינו בתרגיל 5.1.1 שיש אינסוף ראשוניים מהצורה $4n+3$, ובטענה 5.1.3 שישנם אינסוף ראשוניים מהצורה $4n+1$ (ויש מעט מאד ראשוניים משתי הצורות האחרות). באופן כללי, בהינתן מספרים טבעיים $a, b > 0$, אפשר לשאול: האם יש אינסוף ראשוניים מהצורה $an+b$? כמו

במקרה $a=4$, השאלה מעניינת רק אם a ו-b זרים. במקרה הזה, הזכרנו כבר בהקדמה (משפט ד') שהתשובה היא חיובית.

תרגיל 6.0.1. נניח שמשפט דיריכלה נכון עבור a. הוכיחו שהוא נכון גם לכל a' שמחלק את a.

שיטת ההוכחה למקרה $a=4$ התבססה בצורה די מפורשת על הבנת הפריקות בחוג גאוס, ולא ניתנת להכללה ישירה למקרה הכללי. ההוכחה שנראה משתמשת במקום זה בכלים אנליטיים. למעשה, היא מוכיחה יותר: בכל סדרה כזו יש "כמות לא זניחה" של ראשוניים. השלב הראשון הוא להגדיר במדויק מה הטענה הזו אומרת.

6.1 צפיפות ראשוניים

נניח ש-a,b כמו בהנחה של משפט דיריכלה. נסמן ב-$\mathbb{P}(a,b)$ את הראשוניים מהצורה $an+b$. קבוצה זו תלויה רק בשארית של b ביחס ל-a, וכיוון ש-b זר ל-a, הוא מייצג איבר של U_a, חבורת האיברים ההפיכים ב-$\mathbb{Z}/a$. אם אנחנו מאמינים שהראשוניים מפוזרים באופן אחיד בין השאריות האלה, אנחנו מצפים שאם נגריל בצורה אקראית ראשוני, יהיה סיכוי של $\frac{1}{\varphi(a)}=\frac{1}{|U_a|}$ שהוא יהיה מהצורה $an+b$ (כאשר φ פונקציית אוילר). כדי לומר את זה בצורה מדויקת, צריך להגדיר מהו הגודל היחסי של קבוצת ראשוניים Q מתוך כלל הראשוניים. במלים אחרות, אנחנו רוצים להצמיד לכל קבוצה כזו מספר $d(Q)\in[0,1]$, כך שהתכונות הבאות (לפחות) יתקיימו:

הגדרה 6.1.1. *פונקציית צפיפות* על ראשוניים היא פונקציה חלקית d על קבוצות של ראשוניים, עם ערכים ב-$[0,1]$, המקיימת: פונקציית צפיפות

1. $d(\mathbb{P})=1$ (כאשר $\mathbb{P}$ קבוצת כל הראשוניים)
2. $d(\{p\})=0$ עבור ראשוני בודד p
3. אם Q_1 ו-Q_2 קבוצות זרות, אז $d(Q_1\cup Q_2)=d(Q_1)+d(Q_2)$.

אם d מוגדרת על קבוצה Q של ראשוניים, נאמר שיש ל-Q צפיפות (ההנחה היא שיש צפיפות לפחות לקבוצות שמופיעות בתנאים הנ"ל)

תרגיל 6.1.2. הוכיחו שאם d מקיימת את התנאים הנ"ל, אז $d(Q_1)\geqslant d(Q_2)$ אם $Q_1\backslash Q_2$ סופית. בפרט, $d(Q_1)=d(Q_2)$ אם $Q_1\triangle Q_2$ סופית

מיד נגדיר פונקציה כזו, שנקראת *צפיפות דיריכלה*. כדי להוכיח את משפט דיריכלה, מספיק להראות ש-$d(\mathbb{P}(a,b))>0$. ההגדרה היא אנליטית.

נזכיר מההקדמה *שפונקציית זיטא* של רימן נתונה על-ידי הטור פונקציית זיטא

$$\zeta(s)=\sum_{n=1}^{\infty}n^{-s} \tag{6.1}$$

כפי שציינו שם, הטור מתכנס עבור $s>1$, ולכן בתחום זה, זוהי אכן פונקציה. באופן יותר כללי, לכל קבוצה A של טבעיים, נסמן $\zeta_A(s)=\sum_{n\in A}n^{-s}$.

טענה 6.1.3. *לכל $A \subseteq \mathbb{N}$, הטור $\zeta_A(s)$ מתכנס עבור $s > 1$. אם $A = \bigcup_i A_i$ כאשר A_i סדרה עולה של קבוצות, אז הסדרה $\zeta_{A_i}(s)$ מתכנסת ל-$\zeta_A(s)$ לכל s כזה.*

הוכחה. הטור מתכנס כי הוא מורכב מאיברים חיוביים, וחסום על-ידי $\zeta(s)$. לכל i מתקיים $\zeta_A(s) - \zeta_{A_i}(s) = \zeta_{A \setminus A_i}(s)$. אם n_i המינימום של $B_i = A \setminus A_i$, הסדרה n_i שואפת ל-∞, ולכן הסדרה $\zeta_{B_i}(s) \leqslant \zeta_{\mathbb{N}_{\geqslant n_i}}(s)$ שואפת ל-0. $\square$

בהוכחה של אוילר לאינסופיות הראשוניים ראינו שמשתלם לכתוב סכומים חלקיים של הטור כמכפלה של פונקציות שתלויות ב-p, הפונקציות $Z_p(s) = \frac{1}{1-p^{-s}}$. לכל קבוצה Q של ראשוניים, נסמן ב-$N(Q)$ את הטבעיים שכל הגורמים הראשוניים שלהם כלולים ב-Q. אם Q סופית, נסמן $Z_Q(s) = \prod_{p \in Q} Z_p(s)$.

תרגיל 6.1.4. הוכיחו שאם Q קבוצה סופית של ראשוניים, אז $\zeta_{N(Q)}(s) = Z_Q(s)$ לכל $s > 0$ (בפרט, הצדדים מתכנסים).

כדי לעבוד עם טיעונים כמו בהוכחה של אוילר, נגדיר:

הגדרה 6.1.5. עבור סדרה a_n של ממשיים חיוביים, נאמר שהמכפלה $\prod_{i=0}^{\infty} a_i$ מתכנסת אם הסדרה $p_n = \prod_{i=0}^{n} a_i$ מתכנסת לגבול L שונה מ-0. במקרה זה, נכתוב $\prod_i a_i = L$.

תרגיל 6.1.6. הוכיחו שהגבול של מכפלה מתכנסת תמיד חיובי, ושהמכפלה $\prod a_i$ מתכנסת ל-L אם ורק אם הטור $\sum \log(a_i)$ מתכנס ל-$\log(L)$.

באמצעות ההגדרה הזו אפשר להכליל את הטענה של תרגיל 6.1.4 לקבוצה כלשהי של ראשוניים (אבל עם תחום התכנסות מוקטן).

טענה 6.1.7. *לכל קבוצה Q של ראשוניים, המכפלה $\prod_{p \in Q} Z_p(s)$ מתכנסת ל-$\zeta_{N(Q)}(s)$ לכל $s > 1$*

הטענה למעשה כבר הוכחה בהקדמה, אבל נחזור על ההוכחה

הוכחה. לכל $k > 0$ נסמן ב-Q_k את קבוצת האיברים של Q שקטנים מ-k, כך שהמכפלה היא הגבול על פני k של $Z_{Q_k}(s) = \zeta_{N(Q_k)}(s)$ (לפי תרגיל 6.1.4). מאידך, לפי טענה 6.1.3, הגבול של צד ימין הוא $\zeta_{N(Q)}$. $\square$

עבור $s = 1$, הטור שמגדיר את פונקציית זיטא הוא הטור ההרמוני, ולכן מתבדר. לכן, כאשר s שואף ל-1 (מימין), הערך של $\zeta(s)$ שואף לאינסוף. ככל שהקבוצה Q של הראשוניים יותר קטנה, ההתכנסות של המכפלה "יותר חזקה", ולכן פונקציית ζ המתאימה שואפת ל-∞ יותר לאט כאשר s שואף ל-1 (למשל, אם Q סופית, היא לא שואפת ל-∞ בכלל). לכן, קצב השאיפה ל-∞ נותן איזשהו מדד לצפיפות של Q. כדי לדייק את הטיעון הזה, יש להבין ראשית את ההתנהגות של ζ עצמה בגבול.

טענה 6.1.8. $\lim_{s \to 1}(s-1)\zeta(s) = 1$.

הוכחה. עבור $s>1$ קבוע, $(t^{1-s})' = (1-s)t^{-s}$, וכיוון שהגבול של t^{1-s} כאשר $t\to\infty$ הוא 0, מקבלים

$$\frac{1}{s-1} = \int_1^\infty t^{-s}\mathbf{d}t = \sum_{i=1}^{\infty}\int_i^{i+1} t^{-s}\mathbf{d}t$$

כיוון t^{-s} פונקציה יורדת, $(i+1)^{-s} \leqslant \int_i^{i+1} t^{-s}\mathbf{d}t \leqslant i^{-s}$, ולכן הסכום כולו מקיים $\zeta(s)-1 \leqslant \frac{1}{s-1} \leqslant \zeta(s)$. לכן $(s-1)\zeta(s)-(s-1) \leqslant 1 \leqslant (s-1)\zeta(s)$, כלומר $1 \leqslant (s-1)\zeta(s) \leqslant s$, ולוקחים את הגבול. □

נסמן $f(s)\sim g(s)$ אם $\lim_{s\to 1}\frac{f}{g}=1$ (אז הוכחנו ש-$\zeta(s)\sim\frac{1}{s-1}$)

מסקנה 6.1.9. $\zeta_{\mathbb{P}} \sim \log\circ\zeta \sim -\log(s-1)$. *הסדרה* $\zeta_A(s)$ *חסומה כאשר* $s\to 1$, *כאשר* $A=\{p^k \mid p\in\mathbb{P}, k\geqslant 2\}$.

הוכחה. נוכיח ראשית את החלק השני: עבור $s>1$,

$$\zeta_A(s) = \sum_p\sum_{k>1}\frac{1}{p^{ks}} = \sum_p \frac{1}{p^{2s}}\frac{1}{1-p^{-s}} = \sum_p \frac{1}{p^s(p^s-1)} \leqslant \sum_p \frac{1}{p(p-1)} \leqslant \sum_{n>1}\frac{1}{n(n-1)} = 1 \quad (6.2)$$

בשביל החלק הראשון, נוסחת המכפלה נותנת לכל $s>1$ ש-

$$\log(\zeta(s)) = \sum_p \log(Z_p(s)) = -\sum_p \log(1-p^{-s})$$

פיתוח טיילור עבור $\log(1-t)$ הוא $-\sum_{k>0}\frac{t^k}{k}$, אז

$$\log(\zeta(s)) = \sum_p\sum_{k>0}\frac{p^{-ks}}{k} = \sum_p p^{-s} + \sum_{p,k>1}\frac{1}{kp^{ks}} = \zeta_{\mathbb{P}}(s) + \sum_{p,k>1}\frac{1}{kp^{ks}}$$

כאשר שינוי סדר הסכימה מוצדק כי הטור מתכנס בהחלט. המחובר השני בסכום חסום על-ידי ζ_A, אז כיוון ש-$\zeta(s)$ מתבדרת כאשר $s\to 1$, מקבלים את הקירוב הראשון $\zeta_{\mathbb{P}}\sim\log\circ\zeta$.

השקילות השניה נובעת מהטענה הקודמת: $\zeta(s) = \frac{1}{s-1}(1+\phi(s))$, כאשר $\phi(s)$ פונקציה שהגבול שלה ב-1 הוא 0. אז

$$\log(\zeta(s)) = -\log(s-1) + \log(1+\phi(s))$$

ולכן

$$\frac{\log(\zeta(s))}{-\log(s-1)} = 1 + r(s)$$

כאשר ב-$s=1$, הגבול של $r(s)$ הוא 0. □

נשים לב שהמסקנה בפרט נותנת הוכחה נוספת של המשפט של אוילר מההקדמה. סוף הרצאה 17, 17 בדצמ
אם $f(s)=(s-1)^r$, עבור r ממשי, אז $\log(f(s))=r\log(s-1)$. במלים אחרות, הגבול של $\frac{\log(f(s))}{\log(s-1)}$ מודד את קצב הגידול של f (ב-$s=1$). ראינו כבר שאנחנו מצפים ללמוד על צפיפות הראשוניים בקבוצה Q דרך קצב הגידול של $\zeta_{N(Q)}$ ב-$s=1$. מסיבות דומות לטענה האחרונה, אפשר להחליף את $\log(\zeta_{N(Q)})$ ב-ζ_Q. לכן, אנחנו מגיעים להגדרה הבאה:

הגדרה 6.1.10. אם Q קבוצת ראשוניים, נאמר של-Q יש *צפיפות דיריכלה* אם הגבול צפיפות דיריכלה

$$d(Q)=\lim_{s\longrightarrow 1}\frac{\zeta_Q(s)}{\zeta_{\mathbb{P}}(s)}=\lim_{s\longrightarrow 1}\frac{\zeta_Q(s)}{-\log(s-1)}$$

קיים (ואז $d(Q)$ נקרא צפיפות דיריכלה של Q).

טענה 6.1.11. *צפיפות דיריכלה מקיימת את תנאי פונקציית צפיפות (הגדרה 6.1.1).*

תרגיל 6.1.12. הוכיחו את הטענה

עכשיו אפשר לנסח במדויק את הגרסה החזקה יותר של משפט דיריכלה:

משפט 6.1.13. *אם $a>0$ ו-b זר ל-a, לקבוצה $\mathbb{P}(a,b)$ של ראשוניים מהצורה $an+b$ יש צפיפות דיריכלה* $\frac{1}{\varphi(a)}$.

התרגיל הבא, שמחזק את תרגיל 5.1.9, הוא מסקנה של המשפט:

תרגיל 6.1.14. נקבע $n>0$ טבעי אי-זוגי (לשם הפשטות. נימוק דומה קיים לכל n שלם)

1. נניח ש-n מכפלה של ראשוניים שונים, ונסמן $a=4n$. הוכיחו שקיימת העתקה של חבורות $\chi:U_a\to\mu_2$ כך ש-$\chi(\bar{p})=\left(\frac{n}{p}\right)$ לכל ראשוני p שזר ל-a, כאשר $\bar{p}$ התמונה של p ב-U_a (רמז: משפט ההדדיות)

2. הוכיחו שהגרעין H של ההעתקה χ מהסעיף הקודם הוא מאינדקס 2 ב-U_a.

3. הסיקו שאם n הוא ריבוע ב-$\mathbb{F}_p$ לכמעט כל p (כלומר, פרט למספר סופי), אז הוא ריבוע ב-$\mathbb{Z}$.

6.2 המקרה $a=4$

בתור חימום להוכחה הכללית של משפט דיריכלה, נסקור את המקרה $a=4$. נדלג בשלב זה על ההצדקות המדויקות של הצעדים, משום שהם מהווים מקרה פרטי של הצעדים שניתן בהמשך.

עלינו להוכיח שלכל אחת מהקבוצות Q_1 ו-Q_3 של ראשוניים מהצורה $4n+1$ ו-$4n+3$, בהתאמה, יש צפיפות דיריכלה $\frac{1}{2}$. הרעיון הוא להראות, בצורה כמותית, שאיברי הקבוצה הראשונה "מבטלים" את איברי הקבוצה השנייה.

על מנת לעשות זאת, נתבונן בפונקציית זטא "עם סימנים":

$$L(s)=\sum_{i=0}^{\infty}(-1)^i(2i+1)^{-s}=\sum_{n=1}^{\infty}\chi(n)n^{-s}$$

כאשר $\chi(n) \in \{1,0,-1\}$ הוא 0 עבור n זוגי, ו-$\chi(4n+a) = a$ עבור $a = \pm 1$. באופן דומה, אם נגדיר

$$W_p(s) = \frac{1}{1+p^{-s}}$$

נקבל עבור $s > 1$ באופן דומה לטענה 6.1.7

$$L(s) = \prod_{p \in Q_1} Z_p(s) \prod_{p \in Q_3} W_p(s)$$

לכן, כמו במסקנה 6.1.9, נקבל ש-

$$\log(L(s)) = \zeta_{Q_1}(s) - \zeta_{Q_3}(s) + r(s)$$

כאשר $r(s)$ פונקציה חסומה כש-$s \to 1$. מצד שני,

$$\log(\zeta(s)) = \zeta_{\mathbb{P}} + r_1(s) = \zeta_{Q_1} + \zeta_{Q_3} + r_1(s) - 2^{-s}$$

שוב עבור פונקציה חסומה $r_1(s) + 2^{-s}$. לכן:

$$2\zeta_{Q_1} \sim \log(\zeta(s)) + \log(L(s)) \tag{6.3}$$

$$2\zeta_{Q_3} \sim \log(\zeta(s)) - \log(L(s)) \tag{6.4}$$

ועל מנת להוכיח את הטענה, מספיק להראות שהמכפלה שמגדירה את $L(s)$ מתכנסת (ובכלל זה שונה מ-0) כאשר s שואף (מימין) ל-1. אבל את הטור אפשר לרשום באופן הבא:

$$L(s) = (1-3^{-s}) + (5^{-s} - 7^{-s}) + \cdots \geqslant 1 - 3^{-s} > \frac{2}{3}$$

וגם באופן הבא:

$$L(s) = 1 - (3^{-s} - 5^{-s}) - \cdots < 1$$

בסך הכל מקבלים ש-

$$2\zeta_{Q_1}(s) = \log(L(s)) + \zeta_{\mathbb{P}} + r(s)$$

כאשר $r(s)$ ו-$\log(L(s))$ חסומות בגבול ל-1, ולכן $\frac{2\zeta_{Q_1}}{\zeta_{\mathbb{P}}} \sim 1$, כלומר $d(Q_1) = \frac{1}{2}$ (באופן דומה ל-Q_3).

תרגיל 6.2.1. הוכיחו באותו אופן את משפט דיריכלה עבור $a = 3$

סוף הרצאה 18, 21 בדצמ

6.3 הוכחת משפט דיריכלה

ישנם שני רכיבים עיקריים שצריך להכליל מהמקרה הקודם על מנת להוכיח את המקרה הכללי: ההגדרה הכללית של הפונקציה L שתאפשר לבודד את הסדרות שאנחנו מעוניינים בהן, וחקר התכונות האנליטיות של פונקציה זו. את הרכיב השני נשאיר כקופסה שחורה, ונתמקד ברכיב הראשון, אותו למעשה כבר ראינו.

הצעד הראשון הוא הכללה של פונקציית זטא ל-"קבוצות ממושקלות":

טור דיריכלה

הגדרה 6.3.1. לכל פונקציה $f:\mathbb{N}\to\mathbb{C}$, *טור דיריכלה* המתאים הוא הטור:

$$L(s,f)=\sum_{n\geqslant 1} f(n)n^{-s}$$

במקרה הכללי ביותר הטור לא חייב להתכנס עבור שום s, ונתייחס אליו רק כאל טור פורמלי, אבל אנחנו נתעניין במקרה בו $|f(n)|\leqslant 1$, ובמקרה זה הטור מתכנס בהחלט (כלומר $L(s,|f|)$ מתכנס) עבור $s>1$ (למשל, על-ידי השוואה ל-$\zeta(s)$).

כפי שאמרנו, דרך אחת לחשוב על ההגדרה הזו היא כהכללה של פונקציות זיטא המשויכות לקבוצה: לכל תת-קבוצה A של הטבעיים, $\zeta_A(s)=L(s,\chi_A)$, כאשר $\chi_A:\mathbb{N}\to\mathbb{C}$ היא הפונקציה המציינת: $\chi_A(i)=1$ אם $i\in A$ ו-0 אחרת.

ראינו שלפונקציות זיטא מהצורה $\zeta_{N(Q)}$ תכונה מועילה במיוחד: הן ניתנות להצגה כמכפלה. את התכונה שמאפשרת זאת ניתן לתאר בצורה יותר מופשטת:

תרגיל 6.3.2. נניח ש-A קבוצה של טבעיים חיוביים.

1. הוכיחו ש-A מהצורה $N(Q)$ עבור קבוצת ראשוניים Q אם ורק אם היא מקיימת את התנאי: לכל $n,m>0$ טבעיים, $nm\in A$ אם ורק אם $n,m\in A$.

2. הוכיחו ש-A מקיימת את התנאי בסעיף הקודם אם ורק אם $\chi_A(nm)=\chi_A(n)\chi_A(m)$ לכל $n,m\in\mathbb{N}$.

פונקציה כפלית לחלוטין

הגדרה 6.3.3. פונקציה $\chi:\mathbb{N}\to\mathbb{C}$ נקראת *פונקציה כפלית לחלוטין* אם $\chi(nm)=\chi(n)\chi(m)$ לכל $n,m\in\mathbb{N}$.

המינוח "כפלית לחלוטין" הוא על-מנת להבדיל ממחלקה יותר כללית של "פונקציות כפליות", בהן הדרישה היא רק עבור n,m זרים (כדוגמת פונקציית אוילר), אבל אנחנו לא נתעניין בדוגמאות הכלליות יותר.

תרגיל 6.3.4. אם χ כפלית לחלוטין וחסומה, אז היא חסומה על-ידי 1: $|\chi(n)|\leqslant 1$ לכל $n\in\mathbb{N}$

מלבד הדוגמאות שמגיעות מקבוצות מהצורה $N(Q)$, ראינו עוד מחלקה של דוגמאות:

דוגמא 6.3.5. לכל $a>1$, כל הומומורפיזם $\bar{\chi}:U_a\to\mathbb{C}^\times$ מגדיר פונקציה כפלית לחלוטין χ על-ידי

$$\chi(n)=\begin{cases}\bar{\chi}(\bar{n}) & n,a \text{ זרים}\\ 0 & \text{אחרת}\end{cases}$$

כאשר $\bar{n}\in U_a$ התמונה של n ב-U_a. לפעמים לא נבדיל בסימונים בין $\bar{\chi}$ ל-χ.

נשים לב שגם בדוגמא זו, הפונקציה היא חסומה.

על מנת להכליל גם את הצד הכפלי, לכל $u\in\mathbb{C}$ נסמן $Z_p(s,u)=\frac{1}{1-up^{-s}}$.

טענה 6.3.6. *נניח ש-$\chi:\mathbb{N}\to\mathbb{C}$ פונקציה כפלית לחלוטין וחסומה. אז לכל $s>1$ מתקיים*

$$L(s,\chi)=\prod_{p\in\mathbb{P}} Z_p(s,\chi(p))$$

ההוכחה דומה מאד להוכחת טענה 6.1.7:

תרגיל 6.3.7. נניח ש-χ פונקציה כפלית לחלוטין. לכל $k>0$, נגדיר

$$\chi_k(i)=\begin{cases}\chi(i) & i\in N(Q_k)\\ 0 & \text{אחרת}\end{cases}$$

כאשר Q_k כמו בהוכחת 6.1.7

1. הוכיחו שלכל $k>0$ מתקיים $L(s,\chi_k)=\prod_{p\in Q_k}Z_p(s,\chi(p))$.
2. הוכיחו את טענה 6.3.6

תרגיל 6.3.8. נניח ש-$\chi:U_a\to\mathbb{C}^\times$ ההעתקה הטריוויאלית. הוכיחו ש-$L(s,\chi)=\frac{\zeta(s)}{\zeta_{N(Q)}(s)}$, כאשר Q קבוצה סופית של ראשוניים.

במונחים שהוגדרו, אפשר לתאר את ההוכחה בסעיף הקודם באופן הבא. בחבורה הדואלית $\breve{U_4}$ של U_4 יש שני איברים, האיבר הטריוויאלי 1, והאיבר χ שנקבע על-ידי $\chi(3)=-1$. לכן,

$$L(s)=L(s,\chi)=\prod_p Z_p(s,\chi(p))$$

ו-

$$\zeta(s)=L(s,1)Z_2(s)$$

ולכן את המשוואות שקיבלנו אפשר לרשום כ-

$$\log(L(s,\chi))=\zeta_{Q_1}-\zeta_{Q_3}+r_\chi$$

ו-

$$\log(L(s,1))=\zeta_{Q_1}+\zeta_{Q_3}+r_1$$

כאשר r_1,r_χ חסומות כש-$s\to 1$, והתוצאה התקבלה על-ידי סיכום והפרש שני השוויונים.

קושי אחד בהכללת השיטה למקרה הכללי היא העובדה שהערכים של הפונקציות L הם כבר לא ממשיים חיוביים אלא מספרים מרוכבים, ולכן פונקציית log אינה מוגדרת חד-משמעית. אנחנו ניקח בתור ההגדרה של log את הטור בו השתמשנו:

$$\log(1-z)=-\sum_{k>0}\frac{z^k}{k}$$

עבור מספרים מרוכבים z בתוך עיגול היחידה, טור זה מתכנס (משום שהוא מתכנס בהחלט), והוא הפכי (מקומית) לפונקציית האקספוננט. בפרט, log לוקחת כפל לחיבור. עכשיו, כמו במסקנה 6.1.9 מקבלים:

טענה 6.3.9. *לכל פונקציה כפלית לחלוטין וחסומה χ מתקיים עבור $s > 1$:*

$$\log(L(s,\chi)) = \sum_p \chi(p)p^{-s} + r_\chi(s)$$

כאשר r_χ חסומה כש-$s \to 1$

הוכחה. לפי טענה 6.3.6 והגדרת log, נקבל כמו בהוכחת 6.1.9 (כיוון שהטור מתכנס בהחלט)

$$\log(L(s,\chi)) = \sum_p \log(Z_p(s,\chi(p))) =$$

$$\sum_p \sum_{k>0} \frac{\chi(p)^k p^{-sk}}{k} = \sum_p \chi(p)p^{-s} + \sum_{p,k>1} \frac{\chi(p)}{kp^{ks}} \tag{6.5}$$

כאשר האיבר הכללי של הטור $r_\chi(s) = \sum_{p,k>1} \frac{\chi(p)}{kp^{ks}}$ חסום על-ידי האיבר המתאים בטור r_1 שהופיע באותה הוכחה, ולכן חסום גם הוא. $\square$

מסקנה 6.3.10. *לכל $\chi \in \breve{U_a}$ מתקיים*

$$\log(L(s,\chi)) = \sum_{b \in U_a} \chi(b)\zeta_{\mathbb{P}(a,b)}(s) + r_\chi(s)$$

הוכחה. מקבצים את הראשוניים בטענה לפי השארית שלהם ביחס ל-a. $\square$

הביטוי במסקנה נראה מוכר: לכל s, נגדיר $h_s : \breve{U_a} \to \mathbb{C}$ ו-$v_s \in \mathbb{C}[U_a]$ על-ידי:

$$h_s(\chi) = \log(L(s,\chi^{-1})) \tag{6.6}$$

$$v_s = \sum_{b \in U_a} \zeta_{\mathbb{P}(a,b)}(s) b \tag{6.7}$$

אז המסקנה האחרונה מראה ש-

$$\mathcal{F}(v_s)(\chi) = \sum_{b \in U_a} \zeta_{\mathbb{P}(a,b)}(s)\chi^{-1}(b) = h_s(\chi) - r(\chi,s) \tag{6.8}$$

כאשר $r_s(\chi) = r(\chi,s) = r_{\chi^{-1}}(s)$ פונקציה חסומה כש-$s \to 1$. מהפעלת ההתמרה ההפוכה נקבל:

$$\begin{aligned}
\phi(a)v_s &= \widetilde{\mathcal{F}}(\mathcal{F}(v_s)) && \text{טענה 5.4.2} && (6.9)\\
&= \widetilde{\mathcal{F}}(h_s - r_s) && \text{שוויון (6.8)} && (6.10)\\
&= \Big(\sum_{b \in U_a} \sum_{\chi \in \breve{U_a}} h_s(\chi)\chi(b)b\Big) - \widetilde{\mathcal{F}}(r_s) && \text{משוואה (5.2)} && (6.11)\\
&= \Big(\sum_{b \in U_a} \sum_{\chi \in \breve{U_a}} \log(L(s,\chi^{-1}))\chi(b)b\Big) - u_s && \text{הגדרת } h_s && (6.12)
\end{aligned}$$

כאשר $u_s = \widetilde{\mathcal{F}}(r_s) = \sum_b u_{s,b} b \in \mathbb{C}[U_a]$ משפחה של איברים עם מקדמים $u_{s,b}$ חסומים כאשר $s \to 1$ (כי לפי נוסחא 5.2, כל מקדם כזה הוא צירוף לינארי של הפונקציות $h_s(\chi)$ של s, עם מקדמים שאינם תלויים ב-s). לכן, מהשוואת מקדמים, לכל $b \in U_a$ מתקיים

$$\phi(a)\zeta_{\mathbb{P}(a,b)}(s) = \sum_{\chi \in \widetilde{U_a}} \log(L(s,\chi^{-1}))\chi(b) - u_{s,b}$$

דוגמא 6.3.11. כאשר $a = 4$ מקבלים עבור $b = 1$:

$$2\zeta_{\mathbb{P}(a,1)} = \log(L(s,1)) + \log(L(s,\chi))\chi(1) + u_{s,1} = \log(\zeta(s)) + \log(L(s)) + u_{s,1}$$

ועבור $b = 3$

$$2\zeta_{\mathbb{P}(a,3)} = \log(L(s,1)) + \log(L(s,\chi))\chi(3) + u_{s,3} = \log(\zeta(s)) - \log(L(s)) + u_{s,3}$$

כפי שכבר ראינו

כמו במקרה $a = 4$, כיוון שאנחנו יודעים שעבור $\chi = 1$, הפונקציה $L(s,1)$ היא בקירוב ζ (כלומר, עד כדי פונקציה חסומה), ההוכחה מסתיימת עם העובדה הבאה:

עובדה 6.3.12. *אם $\chi \in \widetilde{U_a}$ איבר לא טריוויאלי, אז הטור $L(s,\chi)$ מתכנס לפונקציה רציפה על התחום $s > 0$, ו-$L(1,\chi) \neq 0$*

מהעובדה נובע ש-$\log(L(s,\chi))$ חסומה לכל $\chi \neq 1$, ולכן משלימה את הוכחת המשפט. במקרה $a = 4$ הוכחנו את העובדה על-ידי חישוב ישיר. הוכחת העובדה במקרה הכללי דורשת כלים נוספים, ואנחנו נדלג עליה. סוף הרצאה 19, 24 בדצמ

7 תבניות ריבועיות

במסקנה 2.4.10 ראינו מיהם המספרים הטבעיים שמופיעים כסכום של שני ריבועים שלמים. במילים אחרות, תיארנו את התמונה $p(\mathbb{Z}^2)$, כאשר $p(x,y) = x^2 + y^2$. הפולינום $p(x,y)$ הוא דוגמא ל*תבנית ריבועית* מעל השלמים, במובן הבא:

הגדרה 7.0.1. נניח ש-A חוג (חילופי). פולינום בו כל המונומים הם ממעלה 2 נקרא *תבנית ריבועית* מעל A תבנית ריבועית

אנחנו נתמקד בתבניות ריבועיות בשני משתנים מעל השלמים, כלומר פולינומים מהצורה

$$p(x,y) = ax^2 + bxy + cy^2 \tag{7.1}$$

כאשר a,b,c מספרים שלמים (המקרה המעניין הוא כאשר $a,c \neq 0$, ובהמשך נטיל מגבלות נוספות). אנחנו נתקוף את הבעיה ממספר כיוונים. כמובן שאם נתונה לנו העתקה מהחוג A לחוג B, אפשר להתייחס לתבנית כתבנית מעל B. בפרט, אפשר לחשוב על התבנית כתבנית מעל $\mathbb{R}$.

7.1 תבניות מעל הממשיים

כאמור, אנחנו נתחיל מהבנה של התבניות כתבניות עם מקדמים ב-$\mathbb{R}$. זה מאפשר לחשוב על הבעיה בצורה יותר גאומטרית.

טענה 7.1.1. *פולינום $p(x,y)$ מעל $\mathbb{R}$ הוא תבנית ריבועית אם ורק אם הוא הומוגני ממעלה 2, כלומר, לכל $t,x,y\in\mathbb{R}$ מתקיים $p(tx,ty)=t^2p(x,y)$.*

הטענה נכונה גם למספר אחר של משתנים, וגם לשדות (אינסופיים) אחרים, עם הוכחה דומה.

הוכחה. נניח ש-$p(x,y)$ הומוגני, ממעלה כוללת n. כיוון ש-$\mathbb{R}$ אינסופי, קיימים $u,v\in\mathbb{R}$ עבורם הפולינום $r(t)=p(tu,tv)$ הוא ממעלה n, אבל מתקיים גם $r(t)=t^2r(u,v)=dt^2$ לכל t (כאשר $d=p(u,v)$). שוב משום ש-$\mathbb{R}$ אינסופי, $n=2$. ההוכחה תושלם בתרגיל הבא. $\square$

תרגיל 7.1.2. השלימו את ההוכחה באופן הבא:

1. הוכיחו שאם $\Bbbk$ שדה אינסופי ו-$p(x_1,\dots,x_n)$ פולינום מעל $\Bbbk$ כך ש-$p(\bar{a})=0$ לכל $\bar{a}\in\Bbbk^n$ אז p הוא פולינום האפס. הראו שזה לא בהכרח נכון אם $\Bbbk$ סופי.
2. הוכיחו שאם $p(x,y)$ פולינום הומוגני מדרגה 2, אז כל המונומים שמופיעים בו הם מדרגה זוגית (כלומר, x^iy^j כאשר $i+j$ זוגי). הניחו שהמציין של $\Bbbk$ אינו 2.

נניח עכשיו ש-$p(x,y)=ax^2+bxy+cy^2$ כאשר $a,b,c\in\mathbb{R}$ ו-$a\neq 0$. אז $p(x,1)$ פולינום ממעלה שנייה, ונקבע על-ידי שני השורשים שלו, שעשויים להיות שניהם ממשיים, או מרוכבים (שאינם ממשיים) צמודים (המקרה של שורש כפול לא מעניין מבחינתנו). שני המקרים הללו נבדלים בסימן של *הדיסקרימיננטה* $d=d(p)=b^2-4ac$: המקרה הראשון חל אם ורק אם $d>0$. אנחנו נטפל במקרה המרוכב, $d<0$, כיוון שהוא יותר פשוט. לכן, *מעכשיו נניח* $d<0$. דיסקרימיננטה

במקרה זה, כאמור, ישנם שני שורשים מרוכבים, שבדיוק אחד מהם נמצא ב*חצי המישור העליון* חצי המישור העליון

$$\mathbb{H}=\{z\in\mathbb{C}\mid\Im(z)>0\}\tag{7.2}$$

מאידך, אם $\tau\in\mathbb{H}$, ישנו פולינום מתוקן יחיד ששורשיו הם τ והצמוד שלו, והדיסקרימיננטה שלו שלילית, ולכן תבנית ריבועית p_τ, שנקבעת עד-כדי הכפלה במספר ממשי. בסך-הכל הוכחנו:

מסקנה 7.1.3. *ישנה התאמה הפיכה בין איברים $\tau\in\mathbb{H}$ ותבניות ממשיות p_τ עם דיסקרימיננטה שלילית, שנקבעת על-ידי התנאי: $p_\tau(\tau,1)=0$.*

דוגמא 7.1.4. התבנית $p(x,y)=x^2+y^2$ מתאימה ל-$i\in\mathbb{H}$, משום ש-$p(i,1)=0$.

כמובן שלא כל תבנית כזו היא עם מקדמים ב-$\mathbb{Z}$ (או כפולה של תבנית כזו). בנוסף, תבניות מסוימות יהיו שקולות מבחינת המספרים השלמים שהן מייצגות. כדי להבין את המצב, נשים לב שאם $A:\mathbb{R}^2\to\mathbb{R}^2$ העתקה לינארית הפיכה, ו-p תבנית ריבועית, אז $p\circ A^{-1}$ תבנית ריבועית אף היא (היא הומוגנית מדרגה 2). אוסף ההעתקות הלינאריות של $\mathbb{R}^2$ לעצמו מהווה חבורה $\mathrm{GL}_2(\mathbb{R})$, תחת פעולת ההרכבה. הפעולה של הרכבה עם תבניות ריבועיות מהווה דוגמא לפעולה של חבורה, במובן הבא:

הגדרה 7.1.5. אם G חבורה, *פעולה של* G על קבוצה X היא פונקציה $a : G \times X \to X$ המקיימת $a(e, x) = x$ ו-$a(g, a(h, x)) = a(gh, x)$ לכל $g, h \in G$ ו-$x \in X$ (כאשר $e \in G$ היחידה). פעולה
אם הפונקציה a ידועה, נרשום gx במקום $a(g, x)$.

נדגיש שהמידע של הפעולה של חבורה G על קבוצה X כולל לא רק את החבורה והקבוצה אלא גם את הפונקציה a. יתכנו פעולות שונות של חבורה G על אותה קבוצה X. סוף הרצאה 20, 28 בדצמ

תרגיל 7.1.6. נניח ש-G חבורה ו-X קבוצה ש-G פועלת עליה.

1. נסמן ב-$\mathrm{Sym}(X)$ את חבורת התמורות של X (העתקות הפיכות מ-X לעצמה). הוכיחו שהפונקציה מ-G ל-$\mathrm{Sym}(X)$ שנתונה על-ידי $g \mapsto f_g$, כאשר $f_g(x) = gx$, היא העתקה של חבורות. הוכיחו שכל פעולה של G על X מתאימה להעתקה יחידה כזו.

2. הוכיחו שכל חבורה G פועלת על עצמה על-ידי $(g, h) \mapsto gh$ (ההעתקה המתאימה מ-G ל-$\mathrm{Sym}(G)$ נקראת *העתקת קיילי*, ומראה שכל חבורה איזומורפית לחבורת תמורות) העתקת קיילי

   באופן יותר כללי, אם H תת-חבורה של G, הצמצום של הכפל נותן פעולה $a : H \times G \to G$.

3. נגדיר $x \sim y$ עבור $x, y \in X$ אם $gx = y$ עבור איזשהו $g \in G$. הוכיחו ש-$\sim$ יחס שקילות על X.

   כל מחלקת שקילות של היחס הזה נקראת *מסלול* תחת הפעולה של G. במקרה של הפעולה של תת-חבורה H של G על G, כבר הסתכלנו על מסלולים כאלה בהוכחת משפט לגרנז' (טענה 4.1.5). קבוצת המסלולים (כלומר, קבוצת המנה של יחס השקילות) מסומנת ב-X/G. הפעולה נקראת *פעולה טרנזיטיבית* אם יש לה לכל היותר מסלול אחד. פעולה טרנזיטיבית

4. הוכיחו שלכל איבר $x \in X$, הקבוצה $G_x = \{g \in G \mid gx = x\}$ היא תת-חבורה של G. תת-חבורה זו נקראת *המייצב* של x. המייצב

5. נניח ש-Y קבוצה נוספת, ו-Y^X קבוצת כל הפונקציות מ-X ל-Y. הוכיחו ש-$a : G \times Y^X \to Y^X$ הנתונה על-ידי $a(g, p)(x) = p(g^{-1}x)$ היא פעולה של G על Y^X.

החבורה $G = GL_2(\mathbb{R})$ פועלת מעצם הגדרתה על המישור $\mathbb{R}^2$. הזכרנו שאם p תבנית ריבועית מעל $\mathbb{R}$ אז כך גם $p \circ A^{-1}$ לכל $A \in GL_2(\mathbb{R})$, ולכן אם נסמן ב-X את קבוצת התבניות הריבועיות מעל $\mathbb{R}$, אז כמו בתרגיל נקבל:

מסקנה 7.1.7. *הפונקציה* $a : GL_2(\mathbb{R}) \times X \to X$*, הנתונה על-ידי* $a(A, p) = p \circ A^{-1}$ *היא פעולה של החבורה. לכל* $A \in GL_2(\mathbb{R})$*, אם* $d(p) < 0$ *אז גם* $d(p \circ A) < 0$*, ואם* p *כפולה של* q*, אז גם* $p \circ A$ *כפולה של* $q \circ A$.

הוכחה. נותר להוכיח רק את הטענה על הדיסקרימיננטה. כיוון שהפעולה בבירור לוקחת תבניות עם שורש כפול לתבניות עם שורש כפול, שני המקרים נבדלים בשאלה האם שורש אחד צמוד של השני. תנאי זה נשמר על-ידי הרכבה עם מטריצה ממשית. □

ראינו שלתבניות ממשיות עם דיסקרימיננטה שלילית ניתן להתאים איבר יחיד τ בחצי המישור העליון. בהינתן תבנית כזו p ו-$A \in \mathrm{GL}_2(\mathbb{R})$, טבעי לשאול לאיזה איבר מתאימה התבנית $p \circ A^{-1}$. לכל מטריצה ממשית $A = \left[\begin{smallmatrix} r & s \\ u & v \end{smallmatrix}\right]$, נגדיר $\mu_A(\tau) = \frac{r\tau+s}{u\tau+v}$. כיוון ש-$u, v$ ממשיים ולא שניהם 0, נוסחה זו מגדיר העתקה מ-$\mathbb{C}\backslash\mathbb{R}$ לעצמה.

טענה 7.1.8. *תהי $A = \left[\begin{smallmatrix} r & s \\ u & v \end{smallmatrix}\right] \in \mathrm{GL}_2(\mathbb{R})$, ונסמן $k = \det(A)$ (הדטרמיננטה של A). נניח ש-p תבנית עם דיסקרימיננטה שלילית, ונסמן $q = p \circ A^{-1}$.*

1. *לכל $\tau \in \mathbb{C}\backslash\mathbb{R}$ מתקיים $\Im(\mu_A(\tau)) = \frac{k\Im(\tau)}{|u\tau+v|^2}$. בפרט, לכל $\tau \in \mathbb{H}$, גם $k\mu_A(\tau) \in \mathbb{H}$*
2. *μ_A היא הזהות אם ורק אם A סקלרית (מהצורה tI כאשר I הזהות). לכל $t \in \mathbb{R}$ הפיך, $\mu_{tA} = \mu_A$.*
3. *אם $k > 0$ ו-$\tau \in \mathbb{H}$ מתאים ל-p, אז $\mu_A(\tau)$ מתאים ל-q. בפרט, ההעתקה $(A, \tau) \mapsto \mu_A(\tau)$ מגדירה פעולה של החבורה G של מטריצות מדטרמיננטה חיובית, על $\mathbb{H}$.*
4. *הפעולה בסעיף הקודם היא טרנזיטיבית: לכל $\tau \in \mathbb{H}$ יש $B \in G$ כך ש-$\mu_B(\tau) = i$.*
5. *אם $\mu_A(\tau) = \tau$ אז $kq = p$.*

הוכחה.
1. תרגיל
2. תרגיל
3. נסמן ב-q את התבנית הריבועית $p \circ A^{-1}$. לפי הומוגניות,

$$q(\mu_A(\tau), 1) = q(\frac{r\tau+s}{u\tau+v}, 1) = (u\tau+v)^{-2}q(r\tau+s, u\tau+v) = \\ (u\tau+v)^{-2}q(A \cdot \langle\tau, 1\rangle) = (u\tau+v)^{-2}p(\tau, 1) = 0 \quad (7.3)$$

לכן $\mu_A(\tau)$ מתאים ל-q (לפי הסעיף הראשון, איבר זה אכן נמצא ב-$\mathbb{H}$).

נוכיח עכשיו ש-G פועלת על $\mathbb{H}$. עלינו להוכיח שאם $A, B \in G$ אז $\mu_{AB}(\tau) = \mu_A(\mu_B(\tau))$, לכל $\tau \in \mathbb{H}$. נבחר תבנית p ש-τ מתאים לה. אז $\mu_{AB}(\tau)$ מתאים ל-$p \circ (AB)^{-1}$ ו-$\mu_B(\tau)$ מתאים ל-$p \circ B^{-1}$, ולכן $\mu_A(\mu_B(\tau))$ מתאים ל-$(p \circ B^{-1}) \circ A^{-1}$. אז שתי התבניות שוות, אז גם האיברים ב-$\mathbb{H}$ שווים.

4. תרגיל
5. נניח ש-$\mu_A(\tau) = \tau$. כיוון ש-p ו-q מתאימות לאותו איבר של $\mathbb{H}$, יש קבוע ממשי t עבורו $p = tq$. אם $l^2 = k$ (ממשי, כי $k > 0$), אז $A = lA'$ כאשר $\det(A') = 1$, ו-$kq = p \circ A'^{-1}$, אז אפשר להניח ש-$k = 1$, ועלינו להוכיח ש-$t = 1$.

נבחר $B\in G$ כך ש-$\mu_B(\tau)=i$ (כמובטח בסעיף הקודם), ונגדיר $p'=p\circ B^{-1}$ ו-$q'=q\circ B^{-1}$. כדי להוכיח ש-$p=q$ מספיק להוכיח ש-$p'(1,0)=q'(1,0)$. אבל p' (ו-q') תבנית שמתאימה ל-i, כלומר (כפולה של) x^2+y^2, ו-

$$q'=q\circ B^{-1}=p\circ A^{-1}\circ B^{-1}=p'\circ(BA^{-1}B^{-1})$$

המטריצה $A'=BAB^{-1}$ מקיימת $\mu_{A'}(i)=i$ ומדטרמיננטה 1, אז היא מהצורה $\left[\begin{smallmatrix} r & s\\ -s & r\end{smallmatrix}\right]$ ולכן

$$p'(1,0)=1=\det(A')=r^2+s^2=p'(r,s)=q'(1,0)$$

וסיימנו $\square$

תרגיל 7.1.9. השלימו את הסעיפים החסרים בהוכחה. הוכיחו גם שלכל תבנית ריבועית p עם דיסקרימיננטה שלילית יש מטריצה A מעל $\mathbb{R}$ עם דטרמיננטה 1, כך ש-$p\circ A$ היא התבנית $c(x^2+y^2)$ עבור קבוע c.

כיוון שאנחנו נתעניין בתבניות רק עד-כדי הכפלה בקבוע, אפשר להצטמצם לפעולה של החבורה $\mathrm{SL}_2(\mathbb{R})$ של העתקות מדטרמיננטה 1.

אם הדטרמיננטה של העתקה A היא שלילית, אז $A(\tau)$ יהיה בחצי המישור התחתון, אבל אותו חישוב מקרה שהוא יהיה שורש של המשוואה הריבועית המתאימה, ולכן האיבר המתאים ל-$p\circ A^{-1}$ הוא $\overline{A(\tau)}$.

תרגיל 7.1.10. חשבו את העתקת מביוס המתאימה להעתקה $p(x,y)\mapsto p(y,x)$. הוכיחו שהמקדמים של x^2 ושל y^2 ב-p שווים אם ורק אם האיבר $\tau\in\mathbb{H}$ שמתאים ל-p נמצא על מעגל היחידה

סוף הרצאה 21, 31 בדצמ

על-מנת לקשור את הדיסקרימיננטה של p ושל $p\circ A$, נוח לתאר בצורה נוספת את התבניות הריבועיות. נזכיר שמטריצה C היא *מטריצה סימטרית* אם $C^T=C$, כאשר C^T היא המטריצה המשוחלפת. מטריצה סימטרית

טענה 7.1.11. *1. לכל מטריצה ריבועית C בגודל 2, הפונקציה $p_C(x,y)=\langle x,y\rangle\cdot C\cdot\langle x,y\rangle^T$ היא תבנית ריבועית.*

2. כל תבנית ריבועית היא מהצורה p_C עבור C סימטרית יחידה.

3. הדיסקרימיננטה של p_C היא $-4\det(C)$

4. לכל מטריצה A ומטריצה סימטרית C מתקיים $p_C\circ A=p_{A^TCA}$ (שימו לב ש-A^TCA אכן סימטרית!)

5. לכל מטריצה A מתקיים $d(p\circ A)=\det(A)^2d(p)$. בפרט, אם $\det(A)=1$ אז ל-p ול-$p\circ A$ אותה דיסקרימיננטה.

נשים לב שהסעיף האחרון נותן הוכחה נוספת של הסעיף האחרון בטענה 7.1.8.

הוכחה. 1. הפונקציה הומוגנית מדרגה 2

2. אם $p(x,y)=ax^2+bxy+cy^2$, אז $p=p_C$ אם ורק אם $C=\begin{bmatrix} a & b_1 \\ b_2 & c \end{bmatrix}$, כאשר $b_1+b_2=b$. זוהי מטריצה סימטרית אם ורק אם $b_1=b_2=\frac{b}{2}$

3. נובע מיידית מהסעיף הקודם

4. נובע ישירות מהגדרת p_C

5. נובע ישירות משני הסעיפים האחרונים, כי $\det(A^T)=\det(A)$. □

7.2 תבניות מעל השלמים

נחזור עכשיו לבעיה שהתחלנו איתה, ונניח שהמקדמים של התבנית הם מספרים שלמים. אנחנו ממשיכים להניח שהדיסקרימיננטה $d=b^2-4ac$ שלילית, ובמצב הזה

$$4ap(x,y)=4a^2x^2+4abxy+4acy^2= \\ 4a^2x^2+4abxy+(b^2-d)y^2=(2ax+by)^2-dy^2>0 \quad (7.4)$$

לכל x,y ממשיים. לכן, לכל האיברים בתמונה של p אותו סימן, שהוא הסימן של a. נניח מעכשיו ש-a חיובי.

כזכור, התמקדנו בתבניות עד כדי כפל בממשי (הפיך). כל תבנית שלמה שקולה במובן הזה לתבנית שלמה *יחידה* p בה המקדמים זרים. אם q תבנית שלמה שמתקבלת מ-p על-ידי הכפלה בקבוע, הקבוע חייב להיות טבעי m, וקבוצת המספרים המיוצגים על-ידי q מתקבלת מ-$p(\mathbb{Z}^2)$ על-ידי הכפלה ב-m. תבנית כמו p נקראת *תבנית פרימיטיבית*, **אנחנו נתמקד בתבניות פרימיטיביות בהמשך**. תבנית פרימיטיבית

ראינו שלכל שתי תבניות p,q כאלה ישנה מטריצה הפיכה A מעל $\mathbb{R}$ (לא יחידה) עבורה $p=q\circ A$. אם A שייכת לתת-החבורה $\mathrm{SL}_2(\mathbb{Z})$ של מטריצות עם מקדמים שלמים (ודטרמיננטה 1), התבניות בבירור מייצגות אותם טבעיים. אם $p=q\circ A$ עבור מטריצה כזו A, נאמר ש-p ו-q *תבניות שקולות* (זה אכן יחס שקילות לפי תרגיל 7.1.6). לפי טענה 7.1.11, יש לתבניות כאלה אותה דיסקרימיננטה, ותבנית ששקולה לתבנית פרימיטיבית היא פרימיטיבית. תבניות שקולות

תרגיל 7.2.1. נניח ש-$n,m\in\mathbb{Z}$. הוכיחו:

1. n,m מופיעים בתור שורה באיבר של $\mathrm{SL}_2(\mathbb{Z})$ אם ורק אם הם זרים.

2. אם n,m זרים ו-$A\in\mathrm{SL}_2(\mathbb{Z})$ אז גם הרכיבים של $A\cdot\langle n,m\rangle^T$ זרים

מצד שני, אם $u=p(n,m)$ כאשר n,m זרים, נגיד ש-p *מייצגת בהחלט* את u. נשים לב ש-p תמיד מייצגת בהחלט את המקדמים a,c, ושהתנאי נשמר תחת שקילות (לפי התרגיל האחרון). כתוצאה, הכיוון ההפוך גם נכון: מייצגת בהחלט

טענה 7.2.2. *אם $p(x,y)$ מייצגת בהחלט את u, אז p שקולה לתבנית בה המקדם של x^2 הוא u*

הוכחה. עלינו למצוא העתקה לינארית $A\in\mathrm{SL}_2(\mathbb{Z})$ כך ש-$u=p\circ A(1,0)$. לפי ההנחה יש n,m זרים עבורם $p(n,m)=u$, אז מספיק להראות שיש A כזו שהעמודה הראשונה שלה היא $\langle n,m\rangle$, אבל זה בדיוק מה שאומר התרגיל. □

מסקנה 7.2.3. *נניח ש-u זר ל-d. אז u מיוצג בהחלט על-ידי תבנית (פרימיטיבית) מדיסקרימיננטה $d<0$ אם ורק אם d היא ריבוע ב-$\mathbb{Z}/4u$.*

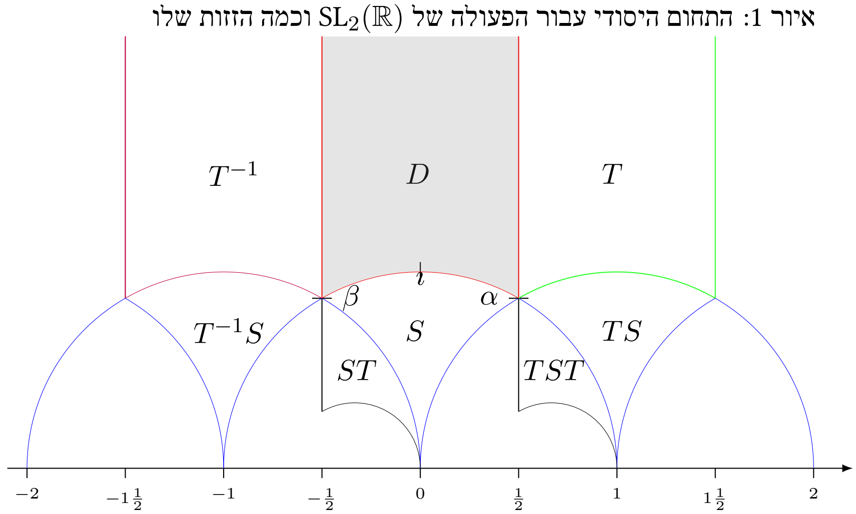
נשים לב שאם u אי-זוגי, התנאי על d שקול ל: ריבוע ב-$\mathbb{Z}/u$ ו-0 או 1 ביחס ל-4.

הוכחה. נניח ש-u מיוצג בהחלט על-ידי p. לפי טענה 7.2.2, אפשר להניח ש-$p(x,y)=ux^2+bxy+cy^2$, אז $d=b^2-4uc=b^2$ ב-$\mathbb{Z}/4u$. מאידך, נניח ש-d ריבוע ב-$\mathbb{Z}/4u$. אז $d=b^2+4um$ עבור b,m שלמים כלשהם, ו-u מיוצג בהחלט על-ידי התבנית $ux^2+bxy+my^2$. כיוון ש-u זר ל-d, זוהי תבנית פרימיטיבית. $\square$

דוגמא 7.2.4. נניח ש-u ראשוני אי-זוגי. אז u מיוצג על-ידי תבנית אם ורק אם הוא מיוצג בהחלט על-ידה. נניח שהתבנית היא מהצורה $p(x,y)=x^2+cy^2$ (כאשר $c>0$). אז הדיסקרימיננטה היא $-4c$, ולכן אם u מיוצג על-ידי p, אז $-c$ ריבוע ב-$\mathbb{Z}/4u$, כלומר $\left(\frac{-c}{u}\right)=1$. עבור $c=1$, ראינו את זה כבר מספר פעמים.

ראינו שכל תבנית פרימיטיבית עם דיסקרימיננטה שלילית מתאימה לאיבר יחיד בחצי המישור העליון. לכן, ניתן לראות את השקילות בין תבניות כיחס שקילות על נקודות ב-$\mathbb{H}$. בפרט, אפשר לשאול האם יש קבוצה שניתן לתאר בקלות בחצי המישור, שכוללת נציג אחד מכל מחלקה. על מנת לעשות זאת, נוח לענות במקביל על השאלה: איך נראית החבורה $\mathrm{SL}_2(\mathbb{Z})$ מבחינת יוצרים ויחסים?

נסמן $T=\begin{bmatrix}1&1\\0&1\end{bmatrix}$ ו-$S=\begin{bmatrix}0&1\\-1&0\end{bmatrix}$. במונחים של הפעולה על חצי המישור העליון, $T(\tau)=\tau+1$ ו-$S(\tau)=-\frac{1}{\tau}$, כלומר, T היא הזזה ימינה ב-1, ו-S מחליפה את פנים חצי המעגל העליון עם החוץ. נסמן ב-D התחום ב-$\mathbb{H}$ שנתון על-ידי $|z|\geqslant 1$ ו-$1/2 \geqslant |\Re(z)|$.



איור 1: התחום היסודי עבור הפעולה של $\mathrm{SL}_2(\mathbb{R})$ וכמה הזזות שלו

תחום יסודי

בגלל המשפט הבא, D נקרא *תחום יסודי* לפעולה של $\mathrm{SL}_2(\mathbb{Z})$ על $\mathbb{H}$.

משפט 7.2.5. *נסמן ב-D התחום ב-$\mathbb{H}$ שנתון על-ידי $|z| \geqslant 1$ ו-$|\Re(z)| \leqslant 1/2$, ונסמן $T = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$ ו-$S = \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$.*

1. *כל איבר ב-$\mathbb{H}$ שקול תחת $\mathrm{SL}_2(\mathbb{Z})$ לאיבר של D*
2. *אם שני איברים $x, y \in D$ הם שקולים, אז הם נמצאים על השפה, ו-$x - y = \pm 1$ או $x = -\frac{1}{y}$*
3. *המייצב של i הוא $\{I, S\}$, המייצב של $\alpha = e^{\pi i/3}$ הוא $\{I, TS, TSTS\}$ ושל $\beta = \alpha^2$ הוא $\{I, ST, STST\}$. המייצב של יתר הנקודות טריוויאלי.*
4. *$\mathrm{SL}_2(\mathbb{Z})$ נוצרת על-ידי S ו-T, שמקיימים את היחסים $S^2 = 1$ ו-$(ST)^3 = 1$*

סוף הרצאה 22, 4 בינו 2021

הוכחה. נסמן ב-G את תת-החבורה של $\mathrm{SL}_2(\mathbb{Z})$ שנוצרת על-ידי S ו-T.

1. מספיק להוכיח שכל איבר שקול לאיבר של D תחת G. נבחר $\tau \in \mathbb{H}$. לפי הסעיף הראשון של טענה 7.1.8, לחלק הדמיוני של $\mu_A(\tau)$, עבור איברים שונים $A = \left[\begin{smallmatrix} r & s \\ u & v \end{smallmatrix}\right] \in G$, יש מקסימום. אפשר להניח ש-τ הוא כבר כזה בו המקסימום מתקבל, ושהחלק הממשי שלו בין $-1/2$ ל-$1/2$. עלינו להוכיח ש-$|\tau| \geqslant 1$, אבל אם זה אינו המצב אז $\Im(\mu_S(\tau)) = \frac{\Im(\tau)}{|\tau|^2} > \Im(\tau)$, בניגוד לבחירת τ.
2. נניח ש-$\mu_A(\tau) = \tau'$ עבור $\tau \in D$ ו-$A = \left[\begin{smallmatrix} r & s \\ u & v \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$. אפשר להניח ש-$\Im(\tau') = \frac{\Im(\tau)}{|u\tau+v|^2} \geqslant \Im(\tau)$, כלומר, ש-$|u\tau + v| \leqslant 1$.

   כיוון ש-$\tau \in D$, החלק המדומה של τ הוא לפחות $\Im(\alpha) = \frac{\sqrt{3}}{2}$, ולכן אם $|u| > 1$ אז החלק הדמיוני גדול מ-1 (בערכו המוחלט), וזה סותר את ההנחה ש-$|u\tau + v| \leqslant 1$. לכן האפשרויות עבור u הן $-1, 0, 1$. אם $u = 0$ בהכרח $v = 1$ (משום ש-$A \in \mathrm{SL}_2(\mathbb{Z})$), ולכן A חזקה של T. זה נותן את האפשרויות $|\Re(\tau)| = 1/2$.

   נניח ש-$u = 1$. שוב משום ש-$|\tau + v| \leqslant 1$, בהכרח $v = 0$ אלא אם $\tau = \beta$ (אחרת החלק הממשי גדול מ-$1/2$ בערכו המוחלט). אם $v = 0$ אז לפי ההנחה $|\tau| \leqslant 1$ אבל כיוון ש-$\tau \in D$ גם $|\tau| \geqslant 1$ וביחד $|\tau| = 1$. לכן $\Im\tau' = \Im\tau$, ומחילופי תפקידים נובע ש-$|\tau'| = 1$. האפשרויות היחידות הן $\tau = \tau'$ או $\tau' = -\frac{1}{\tau}$.
3. הניתוח דומה לסעיף הקודם (תרגיל)
4. עלינו להראות שכל איבר $A \in \mathrm{SL}_2(\mathbb{Z})$ שייך ל-G. לפי הסעיף הראשון, יש $B \in G$ כך ש-$\mu_A(2i) = \mu_B(2i)$. כיוון שהמייצב של $2i$ טריוויאלי (ב-$\mathrm{SL}_2(\mathbb{Z})$), בהכרח $A = B$. $\square$

תרגיל 7.2.6. השלימו את ההוכחה

תבנית מצומצמת

במונחים של תבניות, תבנית נקראת *תבנית מצומצמת* אם האיבר המתאים לה בחצי המישור העליון בתחום היסודי, ולא בחלק $\Re(\tau) = 1/2$ או $\Re(\tau) > 0$ אם $|\tau| = 1$. כיוון ש-$p(x, y) = ax^2 + bxy + cy^2 = a(x - \tau)(x - \bar{\tau})$, מקבלים $b = -2a\Re(\tau)$ ו-$c = a|\tau|^2$, כלומר:

מסקנה 7.2.7. *תבנית שלמה חיובית פרימיטיבית* $p(x,y)=ax^2+bxy+cy^2$ *היא מצומצמת אם ורק אם* $c \geqslant a$ *ו-* $|b| \leqslant a$*, ואם* $a=c$ *או* $|b|=a$ *אז* $b \geqslant 0$.

נעיר שהתנאים במסקנה *לא מבטיחים* שהתבנית היא פרימיטיבית.

תרגיל 7.2.8. הוכיחו שראשוני אי-זוגי q הוא מהצורה $10k^2+14km+5m^2$ (עבור k,m שלמים) אם ורק אם השארית שלו ביחס ל-4 הוא 1.

סוף הרצאה 7, 23 בינו

מה אפשר לומר על תבניות מדיסקרימיננטה נתונה d? נזכיר שלתבניות שקולות אותה דיסקרימיננטה, ולכן אפשר להצטמצם לתבניות מצומצמות. עבור תבניות כאלה, המסקנה נותנת: $d=b^2-4ac \leqslant a^2-4a^2=-3a^2$, כלומר $a^2 \leqslant \frac{-d}{3}$. כיוון ש-$a$ טבעי, יש מספר סופי של אפשרויות ל-a ולכן גם ל-$|b| \leqslant a$ ול-c. הוכחנו

מסקנה 7.2.9. *לכל* $d<0$ *יש מספר סופי* $h(d)$ *של תבניות מצומצמות* p *מעל* $\mathbb{Z}$ *עם* $d(p)=d$. *המספר* $h(d)$ *נקרא* מספר המחלקה *של* d. מספר המחלקה

המסקנה הזו מאפשרת לנו לתת הוכחה נוספת של מסקנה 2.4.8, כלומר, שראשוני אי-זוגי q הוא סכום של שני ריבועים אם ורק אם הוא מהצורה $4k+1$. עלינו להראות שתנאי זה שקול לכך שהראשוני מיוצג על-ידי x^2+y^2, תבנית מדיסקרימיננטה -4. התנאים לעיל מראים שזוהי התבנית המצומצמת היחידה מדיסקרימיננטה זו (כלומר, $h(-4)=1$), ולכן שניתן להחליף אותה בכל תבנית מדיסקרימיננטה זו, ולכן התוצאה נובעת מדוגמא 7.2.4.

תרגיל 7.2.10.

1. מיצאו את כל התבניות המצומצמות עם הדיסקרימיננטות $-8,-28,-32,-124$

2. הוכיחו ש-$h(-4n) \geqslant e$, כאשר e מספר הדרכים לרשום את n כמכפלה של מספרים זרים $a<c$.

תרגיל 7.2.11. הוכיחו שראשוני הוא מהצורה k^2+3m^2 אם ורק אם הוא 3 או מהצורה $3l+1$, בשתי שיטות (בדומה למה שראינו עבור k^2+m^2):

1. באמצעות מסקנות 7.2.3, 7.2.7 ו-7.2.9

2. נסמן $\xi_3=\frac{\sqrt{-3}-1}{2}$. הוכיחו שהחוג $A_3=\{k+m\xi_3 \mid k,m \in \mathbb{Z}\}$ הוא תחום פריקות יחידה (רמז: שימו לב ש-ξ_3 הוא שורש יחידה. החליפו את הריבוע בטענה 2.4.3 במשולש מתאים)

3. הוכיחו שאם $p=3l+1$ אז הוא מחלק מספר מהצורה k^2+3m^2 (רמז: משפט ההדדיות)

4. הסיקו את הטענה משני הסעיפים האחרונים

7.3 ראשוניים מהצורה k^2+nm^2

נתמקד עכשיו בתבניות מהצורה $p(x,y)=x^2+ny^2$, כאשר $n>0$. השיקולים מהצורה שכבר ראינו עבור $n=1$ (ו-$n=3$) מראים:

טענה 7.3.1. *נניח ש-q ראשוני אי-זוגי שזר ל-n. אז q מחלק מספר שמיוצג בהחלט על-ידי p אם ורק אם* $\left(\frac{-n}{q}\right) = 1$

הוכחה. אם q מחלק את $u^2 + nv^2$ אז $u^2 + nv^2 = 0$ ב-$\mathbb{F}_q$. כיוון שהנחנו ש-u, v זרים, וש-q זר ל-n, כל הרכיבים במשוואה הזו שונים מ-0 ב-$\mathbb{F}_q$, ולכן $-n = \frac{u^2}{v^2}$ הוא ריבוע שונה מ-0 שם.

מאידך, אם $-n = s^2$ עבור $s \neq 0$ ב-$\mathbb{F}_q$, ו-u מספר שלם שהשארית שלו ביחס ל-q היא s, אז $u^2 + n = 0$ ב-$\mathbb{F}_q$, כלומר $u^2 + n \cdot 1^2$ מתחלק ב-q. □

עבור $n = 1$ ו-$n = 3$ התנאי שמופיע בטענה האחרונה שקול גם לתשובה לגבי הייצוג, וההוכחה הראשונה שראינו לעובדה הזו (עבור $n = 1$) השתמשה בטענה, ובעובדה שאם q מחלק מספר שמיוצג בהחלט, אז הוא עצמו מיוצג (בהחלט). נזכיר את ההוכחה של החלק האחרון: אם q מחלק את $k^2 + m^2$, אז בחוג גאוס הוא מחלק את $(k - im)(k + im)$ ולכן לא יכול להיות ראשוני שם. בנקודה הזו יש שימוש בעובדה בסיסית שהוכחנו: חוג גאוס הוא תחום פריקות יחידה. בפרט, הנימוק הזה נכשל כאשר החוג המתאים A_n אינו תחום כזה. למשל, הוא נכשל עבור $n = 5$ (תרגיל 2.4.17).

ראינו גישה נוספת לאותה בעיה, באמצעות שקילות של תבניות: מסקנה 7.2.3 מראה שהתנאי $\left(\frac{-n}{q}\right) = 1$ שקול לכך ש-q מיוצג על-ידי *איזושהי* תבנית מדיסקרימיננטה $d(p) = -4n$. אם היינו יודעים ש-p היא (עד כדי שקילות) התבנית היחידה מהדיסקרימיננטה הזו, היינו פותרים את הבעיה. התיאור של תבניות מצומצמות מדיסקרימיננטה נתונה מופיע במסקנות 7.2.7 ו-7.2.9. עבור $n = 5$, הדיסקרימיננטה היא -20, ולכן תבנית מצומצמת מדיסקרימיננטה כזו חייבת לקיים $a^2 \leqslant 6$, כלומר a עשוי להיות 1 או 2. אם $a = 2$ אז $b^2 - 8c = -20$ ו-$b = 2, c = 3$ פותרים את הבעיה (וגם מקיימים את התנאים האחרים של מסקנה 7.2.7). לכן, גם השיטה הזו לא עובדת במקרה זה.

למעשה, אין שיטה שתעבוד: כל אחד מהראשוניים 3 ו-7 (לדוגמא) מקיימים את התנאי $\left(\frac{-5}{q}\right) = 1$, אבל בבירור אינם מהצורה $k^2 + 5m^2$ (ושניהם מחלקים את $21 = 1^2 + 5 \cdot 2^2$).

במונחים של מספר המחלקה, השיטה שתיארנו עובדת למקרה ש-$h(-4n) = h(d) = 1$. מהם המספרים הללו? מסתבר שיש רק מספר קטן של כאלה (זוהי השערה של גאוס שהוכחה על-ידי לנדאו):

משפט 7.3.2. *המספרים היחידים n עבורם $h(-4n) = 1$ הם* $1, 2, 3, 4, 7$.

הוכחה. כבר ראינו שהדיסקרימיננטות שמופיעות בתרגיל הן ממספר מחלקה 1. בכיוון ההפוך, עלינו למצוא תבנית מצומצמת מדיסקרימיננטה $d = -4n$ שאינה $x^2 + ny^2$. המקרה של-n יותר ממחלק ראשוני אחד טופל בתרגיל 7.2.10.

נניח ש-$n = q^r$ עבור ראשוני q. אם $q = 2$ ו-$r \geqslant 4$ אז $4x^2 + 4xy + (\frac{n}{4} + 1)y^2$ מקיימת את התנאים. המקרה $r = 3$ טופל בתרגיל 7.2.10.

נניח ש-q אי-זוגי. אם $n + 1 = ac$ פירוק לא טריוויאלי כאשר $a < c$ זרים, אז $ax^2 + 2xy + cy^2$ פותר את הבעיה. אחרת, $n + 1$ חזקה של ראשוני, שחייב להיות 2, כלומר $n + 1 = 2^s$. אם $s \geqslant 6$ אז $8x^2 + 6xy + (\frac{n+1}{8} + 1)y^2$ פותרת את הבעיה. אחרת, המקרים האפשריים הם רק $n = 1, 3, 7, 15, 31$. כיוון ש-15 אינו חזקה של ראשוני, ו-$1, 3, 7$ ברשימה, נותר המקרה $n = 31$, שגם טופל בתרגיל 7.2.10. □

הכישלון הכפול במקרה $n=5$ בסעיף הקודם מרמז שעשוי להיות קשר בין שני הגורמים: ריבוי תבניות מצומצמות מדיסקרימיננטה $-4n$ מצד אחד, וכישלון של פריקות יחידה בחוג המתאים A_n מצד שני. על-מנת לתאר את הקשר הזה, נגדיר ראשית במדויק את החוג A_n:
עבור המקרה $n=3$ השתמשנו בחוג A_3 שהרחיב ממש את החוג ה"נאיבי" $B=\mathbb{Z}[\sqrt{-3}]$.
החוג B אינו תחום ראשי: האידיאל $I=(2,1+\sqrt{-3})$ הוא החיתוך של B עם האידיאל שנוצר על-ידי ה"איבר החסר" $a=\frac{1+\sqrt{-3}}{2}$ ב-A_3 (אכן, B אפילו אינו תחום פריקות יחידה, $(4=2^2=(1+\sqrt{-3})(1-\sqrt{-3})$. כפי שמיד נסביר, המקור לבעיה הוא ש-a פותר משוואה פולינומית מתוקנת $r(x)=0$, עבור $r(x)=x^2-x+1$, אבל אינו נמצא ב-B.

נניח ש-K שדה, ו-$B\subseteq K$ תת-חוג. ראינו בתרגיל 2.3.22 שבמצב הזה B הוא תחום שלמות. אם כל איבר ב-K אפשר לרשום כמנה של שני איברים ב-B, אז K נקרא *שדה השברים* של B (שדה כזה K הוא אכן יחיד, עד כדי איזומורפיזם יחיד מעל B, וקיים לכל תחום שלמות. הבנייה של שדה כזה דומה מאד לבנייה של $\mathbb{Q}$ מתוך $\mathbb{Z}$). במצב הזה, החבורה הכפלית $K^\times$ מכילה את החבורה הכפלית $B^\times$, ואם B תחום פריקות יחידה אז המנה $K^\times/B^\times$ היא חבורה חילופית חופשית על (התמונות של) האיברים הראשוניים ב-B.

שדה השברים

דוגמא 7.4.1. החבורה $\mathbb{Q}^\times/\{1,-1\}$ נוצרת באופן חופשי על-ידי התמונות של הראשוניים: כל שבר ניתן לרשום בצורה יחידה כמכפלה סופית של חזקות (אולי שליליות) של ראשוניים, עד-כדי סימן

כפי שעשינו עבור שברים, אפשר לסמן, לכל ראשוני $p\in B$, ב-$v_p(a)$ את החזקה של p בפירוק של $a\in K^\times$. זה מגדיר העתקה $v_p:K^\times\to\mathbb{Z}$ שמקיימת את כל התכונות שהראינו בתרגיל 2.1.13 (העתקה כזו נקראת *הערכה דיסקרטית*), וברור שאיבר $a\in K^\times$ נמצא ב-B אם ורק אם $v_p(a)\geqslant 0$ לכל ראשוני $p\in B$. שימוש פשוט בתכונות הללו מראה ש-B הוא חוג נורמלי, במובן של ההגדרה הבאה:

הערכה דיסקרטית

הגדרה 7.4.2. נניח ש-B תחום שמוכל בחוג K.

1. איבר $a\in K$ נקרא *איבר אינטגרלי* מעל B אם $p(a)=0$ עבור פולינום מתוקן p מעל B. איבר אינטגרלי
2. ההרחבה $B\subseteq K$ נקראת *הרחבה אינטגרלית* אם כל איבר של K הוא אינטגרלי מעל B. הרחבה אינטגרלית
3. החוג B *סגור אינטגרלית* ב-K אם כל איבר אינטגרלי מעל B של K נמצא ב-B. סגור אינטגרלית
4. התחום B נקרא *תחום נורמלי* אם הוא סגור אינטגרלית בשדה השברים שלו. תחום נורמלי

הדיון לפני ההגדרה מראה שכל תחום פריקות יחידה הוא נורמלי. בפרט, הוא מסביר את התופעה הכללית שמונעת מהתחום $\mathbb{Z}[\sqrt{-3}]$ להיות תחום פריקות יחידה. התיקון שמצאנו גם הוא כללי:

טענה 7.4.3. *אם K חוג שמכיל תחום B, אז קבוצת האיברים האינטגרליים מעל B ב-K היא תת-חוג של K (שמכיל את B)*

הטענה לא קלה להוכחה ישירה. אנחנו נוכיח את המקרה הפרטי שאנחנו זקוקים לו באמצעות האפיון הבא. ההוכחה הכללית משתמשת באפיון דומה, שנובע מיידית ממשפט קיילי–המילטון (שתקף לחוגים חילופיים כלליים).

טענה 7.4.4. *נניח ש-B חוג שמכיל את $\mathbb{Z}$*

1. *אם B נוצר על-ידי איבר b, אז b אינטגרלי מעל $\mathbb{Z}$ אם ורק אם החבורה החיבורית של B נוצרת סופית.*

2. *B נוצר על-ידי מספר סופי של איברים אינטגרליים אם ורק אם החבורה החיבורית של B נוצרת סופית.*

הוכחה. 1. אם החבורה החיבורית של B נוצרת סופית, ונגדיר B_i תת-החבורה שנוצרת על-ידי החזקות b^j עבור $j < i$. כיוון ש-B נוצרת סופית, עבור n מספיק גבוה, $b^n \in B_n$, ולכן $B = B_n$ תת-החוג שנוצר על-ידי b, ו-b^n צירוף לינארי של החזקות הנמוכות יותר.

הכיוון ההפוך הוא מקרה פרטי של הסעיף השני

2. אם B נוצר כחוג על-ידי $b_1, \dots, b_k$, וכל b_i הוא שורש של פולינום מתוקן p_i ממעלה n_i מעל $\mathbb{Z}$, אז $b_i^{n_i}$ הוא צירוף לינארי (מעל $\mathbb{Z}$) של חזקות נמוכות יותר של b_i. אז החבורה החיבורית נוצרת על-ידי המונומים $b_1^{l_1} \cdots {}_k^{l_k}$ כאשר $l_i < n_i$ לכל i.

בכיוון ההפוך, החבורה החיבורית של תת-החוג שנוצר על-ידי איבר אחד b היא נוצרת סופית לפי הסעיף הקודם. אחרי הוספת מספר סופי של איברים, מגיעים לכל החוג. □

הוכחת טענה 7.4.3 עבור $B = \mathbb{Z}$. אם $a, b \in K$ אינטגרליים מעל $\mathbb{Z}$ ו-B תת-החוג שנוצר על-ידם, אז לפי הטענה האחרונה, החבורה החיבורית של B נוצרת סופית. תת-החוג של B שנוצר על-ידי $a + b$ (או ab) לכן גם בעל חבורה חיבורית נוצרת סופית, אז שוב לפי הטענה האחרונה $a + b$ (או ab) אינטרגליים. □

הסגור האינטרלי
נורמליזציה

הגדרה 7.4.5. החוג בטענה 7.4.3 נקרא *הסגור האינטרלי* של B ב-K. במקרה ש-K הוא שדה השברים של B, הוא נקרא *הנורמליזציה* של B.

שדה מספרים סופי
חוג השלמים

הגדרה 7.4.6. *שדה מספרים סופי* הוא שדה K ממציין 0 שהמימד שלו מעל $\mathbb{Q}$ (כמרחב וקטורי) הוא סופי. *חוג השלמים* $\mathcal{O}_K$ של K הוא הסגור האינטגרלי של $\mathbb{Z}$ בתוך K.

סוף הרצאה 24, 11 בינו

טענה 7.4.7. *נניח ש-K שדה מספרים סופי. אז חוג השלמים של K הוא חוג נורמלי ששדה השברים שלו הוא K, והחבורה החיבורית שלו נוצרת סופית.*

עם עוד קצת אלגברה, לא קשה להראות את הטענה באופן כללי. אנחנו נתמקד במקרה שמעניין אותנו: $K = \mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$, כאשר $d < 0$ (והגורמים הראשוניים של d שונים). במקרה זה $\mathcal{O}_K$ מכיל את החוג $B_d = \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$, ובפרט, הטענה לגבי שדה השברים ברורה. נוכיח את יתר החלקים בטענה על-ידי תיאור מפורש של $\mathcal{O}_K$:

טענה 7.4.8. *חוג השלמים A_d של $K_d = \mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ הוא $\mathbb{Z}[\sqrt{d}]$ אם $d - 1$ אינו מתחלק ב-4, והוא $\mathbb{Z}[\frac{\sqrt{d}-1}{2}]$ אחרת.*

הוכחה. נניח ש-u ב-A_d, ונתבונן בהעתקה הלינארית l_u על A_d. משפט קיילי–המילטון אומר ש-l_u (ולכן u) מאפסת את הפולינום האפייני שלה, שהוא פולינום מעל $\mathbb{Z}$, והעקבה t והדטרמיננטה s של l_u הם מקדמים בו. לכן הם מספרים שלמים, וחישוב ישיר מראה שאם $u = a + b\sqrt{d}$ (כאשר $a, b \in \mathbb{Q}$), אז $t = 2a$ ו-$s = a^2 - db^2$. אז $a \in 1/2\mathbb{Z}$, וכיוון ש-s, d שלמים, גם $b \in 1/2\mathbb{Z}$, ו-$a \in \mathbb{Z}$ אם ורק אם $b \in \mathbb{Z}$.

אם $a, b \notin \mathbb{Z}$ אז $4s = (2a)^2 - d(2b)^2$ כאשר $2a, 2b$ שלמים אי-זוגיים, אז ב-$\mathbb{Z}/4$ מקבלים $(2a)^2 = (2b)^2 = 1$ ולכן $d = 1$.

בכיוון ההפוך, לכל איבר בחוג הנתון העקבה והנורמה שלמים, אז כל איבר כזה הוא שורש של $p(x) = x^2 + tx + s$. □

7.5 תחומי דדקינד

במקרה $n = 3$, קיומו של האידיאל הלא-ראשי $I = (2, \sqrt{-3})$ ב-$\mathbb{Z}[\sqrt{-3}]$ "הוסבר" על-ידי "האיבר החסר" $\frac{\sqrt{-3}-1}{2}$, וכשזה הוסף, האידיאל שנוצר על-ידי I ב-$\mathbb{Z}[\xi_3]$ נוצר על-ידי ξ_3. עבור $n = 5$ הבעיה לא נפתרת באותו אופן משום שלפי הטענה האחרונה, חוג השלמים הוא $A_5 = \mathbb{Z}[\sqrt{-5}]$. לא ברור, לכן, שניתן "להפוך" אידיאלים לאידיאלים ראשיים על-ידי הוספת איברים. הרעיון של דדקינד היה לעבוד עם האידיאלים עצמם, במקום עם האיברים (זהו מקור השם "אידיאל", אלה "מספרים אידיאליים").

האנאלוגיה עובדת על-ידי זיהוי של איבר $a \in A$ עם האידיאל הראשי (a) שהוא יוצר (כאשר איברים מתאימים לאותו אידיאל אם ורק אם אחד כפולה של השני באיבר הפיך של A). המטרה היא לקבל תורת פריקות דומה לזו שבתחומי פריקות יחידה, אבל עבור אידיאלים. השלב הראשון הוא להבין מה האנאלוג של איבר ראשוני. האפיון נתון על-ידי התוצאה שקיבלנו בתרגיל 3.2.7:

הגדרה 7.5.1. אידיאל I בחוג A הוא *אידיאל ראשוני* אם A/I תחום שלמות. אידיאל ראשוני

מעכשיו עד סוף הסעיף, כל האידיאלים שונים מ-0

אם I, J אידיאלים בחוג A, נסמן ב-IJ את האידיאל שנוצר על-ידי מכפלות ab כאשר $a \in I$ ו-$b \in J$ (ככלל, לא כל איבר ב-IJ הוא מכפלה כזו). זה ברור שהמכפלה הזו היא קיבוצית וחילופית.

תרגיל 7.5.2. הוכיחו שאם I אידיאל ראשוני ו-J, K אידיאלים כך ש-$JK \subseteq I$ אז $J \subseteq I$ או $K \subseteq I$

המושג המקביל לתחום פריקות יחידה נקרא *תחום דדקינד*. ישנן מספר הגדרות שקולות, עבורנו הכי נוח להתחיל מהתנאי הבא: תחום דדקינד

הגדרה 7.5.3. תחום A נקרא *תחום דדקינד* אם לכל אידיאל I ב-A ישנו אידיאל J כך ש-IJ אידיאל ראשי תחום דדקינד

כמובן שכל תחום ראשי הוא תחום דדקינד, אבל בקרוב נראה שזו הכללה *ממש*. היתרון של ההגדרה הזו הוא שהיא מאפשרת להסיק בקלות כמה תכונות יותר מוכרות. את הראשונה ניתן לראות כאנאלוג של מושג התחום:

מסקנה 7.5.4. *אם I, J, K אידיאלים בתחום דדקינד A כך ש-$IJ = IK$ אז $J = K$.*

הוכחה. לפי ההנחה יש אידיאל P כך ש-$PI=(a)$ אידיאל ראשי. אז $aJ=PIJ=PIK=aK$. כיוון ש-A תחום אפשר לצמצם את a. $\square$

עבור איברים $a,b\in A$, את יחס החלוקה אפשר לתאר באמצעות אידיאלים כך: a מחלק את b אם ורק אם $(b)\subseteq(a)$. בתחומי דדקינד, תיאור דומה תקף לאידיאלים כלליים:

מסקנה 7.5.5. *אם $I\subseteq J$ אידיאלים בתחום דדקינד, אז יש אידיאל K כך ש-$I=JK$*

הוכחה. נניח ראשית ש-$J=(b)$ אידיאל ראשי, ונסמן $K=\{a\in A\,|\,ab\in I\}$. קל לבדוק ש-K אידיאל ו-$KJ\subseteq I$. אם $c\in I$ אז לפי ההנחה $c\in J$, ולכן $c=db$ עבור $d\in A$. לפי ההגדרה, $d\in K$ ולכן $c\in JK$.

במקרה הכללי, נבחר אידיאל P כך ש-JP ראשי. אז $IP\subseteq JP$, ולפי המקרה הראשון, יש K כך ש-$IP=JPK$. לפי הטענה הקודמת, אפשר לצמצם את P. $\square$

אם I אידיאל בחוג A *שמירבי להכלה בין האידיאלים ממש*, אז הוא ראשוני: אכן, תנאי זה שקול לכך ש-A/I שדה. אידיאל כזה נקרא *אידיאל מירבי* (מקסימלי). מהלמה של צורן נובע בקלות שכל אידיאל ממש מוכל באידיאל מירבי. בתחומי דדקינד גם ההיפך נכון:

מסקנה 7.5.6. *כל אידיאל ראשוני (שונה מאפס) בתחום דדקינד הוא מירבי*

הוכחה. אם אידיאל ראשוני I מוכל ממש באידיאל J, קיים לי המסקנה האחרונה אידיאל K כך ש-$I=KJ$. כיוון I ראשוני, $K\subseteq I$, ולכן $I=KJ\subseteq IJ$. לפי צמצום, J הוא כל החוג. $\square$

עכשיו אפשר להוכיח את התכונה שהכי קרובה לפריקות יחידה:

טענה 7.5.7. *כל אידיאל (שונה מאפס) בתחום דדקינד הוא באופן יחיד מכפלה של אידיאלים ראשוניים*

הוכחה. נתחיל מהקיום. נניח ש-I אידיאל ממש. אם I מירבי אז הוא עצמו ראשוני ואין מה להוכיח. אחרת, ישנו אידיאל מירבי J_1 שמכיל אותו ממש, ולפי מסקנה 7.5.5, ישנו אידיאל I_1 כך ש-$I=J_1I_1$. עכשיו ממשיכים עם I_1 וכן הלאה. אם התהליך נעצר אחרי מספר סופי של צעדים סיימנו, אחרת קיבלנו שרשרת אינסופית עולה ממש של אידיאלים $I=I_0\subset I_1\subset\dots$. נסמן $I=\bigcup_j I_j$. לפי ההנחה, קיים אידיאל P כך ש-$IP=(a)$ ראשי, ואיחוד של שרשרת עולה ממש של אידיאלים I_jP (זו עדיין שרשרת עולה ממש בגלל תכונת הצמצום). כיוון ש-$a\in I_jP$ לאיזשהו j, מקבלים $I_jP=IP$, וזו סתירה (השוו להוכחת טענה 2.3.24).

הוכחת היחידות דומה גם היא להוכחת טענה 2.3.19: אם $I=p_1\dots p_k=q_1\dots q_l$ עבור ראשוניים p_i,q_j, אז $I\subseteq q_1$ ולכן $p_j\subseteq q_1$ עבור איזשהו j. לפי מקסימליות $p_j=q_1$, וניתן לצמצם אותם ולהמשיך. $\square$

ראינו שלתחומי דדקינד תכונות דומות לשל תחומי פריקות יחידה, אבל לא ראינו עד דוגמאות לא טריוויאליות. נדגיש שבאופן כללי תחומי דדקינד *אינם* הכללה של תחומי פריקות יחידה: למשל, ישנם תחומי פריקות יחידה רבים בהם יש אידיאלים ראשוניים שאינם מירביים. למעשה, מסתבר שתחומי פריקות יחידה היחידים שהם תחומי דדקינד הם תחומים ראשיים. גם המסקנות האחרות אינן תופסות באופן כללי:

דוגמא 7.5.8. נניח $A=\mathbb{C}[x,y]$. זהו תחום פריקות יחידה. האידיאל $I=(x)$ הוא אידיאל ראשוני שאינו מירבי. הוא מוכל באידיאל $J=(x,y)$, וברור שלא קיים אידיאל K עבורו $I=JK$. כמו כן, אם $K=(x^2,y^2)$, אז אפשר לבדוק בקלות ש-$JK=J^3$ (שני הצדדים נוצרים מהמונומים מדרגה 3) אבל $K\neq J^2=(x^2,xy,y^2)$. אותה דוגמא מראה שאין פירוק יחיד כמכפלה של ראשוניים.

הסיבה שהדוגמאות הללו עובדות היא ש-A הוא חוג שמתאים גאומטרית למרחב ממימד 2 (המישור), ואידיאלים שונים מאד מאיברים במימדים יותר גבוהים. דוגמאות כאלה לא מופיעות בהקשר שלנו. דוגמא יותר רלוונטית היא:

דוגמא 7.5.9. בחוג $A=\mathbb{Z}[\sqrt{-3}]$, האידיאלים $I=(2),J=(1-\sqrt{-3})$ ו-$K=I+J$ מקיימים, $IK=I^2+IJ=(4)+IJ$ ו-$JK=JI+J^2=IJ+(4)$, אבל $I\neq J$.

הדוגמא הזו עובדת מאותה סיבה שנתקלנו בבעיות לגבי החוג הזה בעבר. מסתבר שהתיקון שביצענו עובד לכל חוגי המספרים. כדי להוכיח זאת, אנחנו זקוקים לעובדה הבאה:

עובדה 7.5.10. *תחום A הוא תחום דדקינד אם ורק אם הוא נתרי, נורמלי וכל אידיאל ראשוני שונה מ-0 הוא מירבי*

נתריות היא תנאי סופיות: כל שרשרת עולה ממש של אידיאלים (ביחס להכלה) היא סופית. נתריות
במהלך ההוכחה של יחידות הפירוק לאידיאלים הוכחנו למעשה שכל תחום דדקינד הוא נתרי. ראינו גם שכל אידיאל ראשוני הוא מירבי.

בשלב זה, אנחנו מתעניינים בכיוון השני של הטענה. לפי ההגדרה, כל חוג מספרים הוא נורמלי. כל חוג נוצר סופית מעל $\mathbb{Z}$ הוא נתרי (זה מקרה פרטי של משפט הבסיס של הילברט), אבל הנתריות וגם התנאי על האידיאלים נובע עבור חוגי מספרים מהטענה הבאה:

טענה 7.5.11. *אם I אידיאל שונה מ-0 בחוג מספרים $A=\mathcal{O}_K$, אז $\mathcal{O}_K/I$ חוג סופי.*

הוכחה. האידיאל $I\cap\mathbb{Z}$ ב-$\mathbb{Z}$ שונה מ-0, כי אם $a\in I$ שונה מ-0, אז $p(a)=0$ עבור פולינום מעל $\mathbb{Z}$ עם מקדם חופשי שונה מ-0, ואז המקדם הזה ב-I.

אז אפשר להניח ש-I נוצר על-ידי שלם m. אם $a_1,\dots,a_k$ יוצרים את A כחבורה, אז כל איבר של A/m אפשר לרשום כצירוף לינארי של התמונות של a_i עם מקדמים ב-$\mathbb{Z}/m$, ויש רק מספר סופי של צירופים כאלה. $\square$

מסקנה 7.5.12. *כל חוג מספרים הוא תחום דדקינד*

הוכחה. אם I אידיאל ראשוני שונה מ-0 ב-A אז A/I תחום שלמות סופי, ולכן לפי תרגיל 3.2.7 שדה. לכן I מירבי. אם $I_0\subset I_1\subset\dots$ שרשרת עולה, היא נותנת שרשרת עולה ב-A/I_0, שחייבת להיות סופית אם החוג סופי. לכן התוצאה נובעת מהעובדה. $\square$

7.6 חבורת המחלקות

נניח ש-A תחום דדקינד, עם שדה שברים K.

הגדרה 7.6.1. *אידיאל שיברי* של A הוא תת-חבורה נוצרת סופית $0 \neq I$ של K (החבורה החיבורית), כך ש-$aI \subseteq I$ לכל $a \in A$. אידיאל שיברי

אפשר להכפיל אידיאלים שבריים באותו אופן כמו אידיאלים רגילים. אם אידיאלים רגילים הם "שלמים אידיאליים", אז אידיאלים שבריים הם "שברים אידיאליים". בפרט:

טענה 7.6.2 *1. $I \subseteq A$ היא אידיאל שברי אם ורק אם יש $a \in K$ עבורו aI אידיאל ב-A (בפרט, כל אידיאל הוא אידיאל שברי)*

2. כל אידיאל שברי I הוא הפיך: קיים אידיאל שברי $J = I^{-1}$ כך ש-$IJ = A$.

3. כל אידיאל שברי ניתן לרשום באופן יחיד כ-$p_1^{n_1} \dots p_k^{n_k}$, כאשר p_i אידיאלים ראשוניים ב-A ו-$n_i \in \mathbb{Z}$.

הוכחה. תרגיל $\square$

בטענה זו כבר השתמשנו במובלע בכך שההפכי I^{-1} הוא יחיד. זה נובע מתכונת הצמצום. במלים אחרות, אפשר לנסח את הטענה כך:

מסקנה 7.6.3. *אוסף האידיאלים השבריים מהווה חבורה חילופית תחת כפל. זוהי החבורה החילופית החפשית שנוצרת על-ידי האידיאלים הראשוניים (השונים מ-0) ב-A.*

לכל איבר שונה מאפס $a \in A$ התאמנו את האידיאל הראשונים שנוצר על-ידו. התאמה זו ניתן להרחיב לשדה השברים, כאשר להפכיים מתאימים את האידיאל השברי המתאים. זוהי העתקה של חבורות מהחבורה הכפלית של K (עם גרעין $A^\times$). העתקה זו היא על בדיוק אם כל אידיאל ראשי. לכן, אפשר "למדוד" המרחק של A מלהיות תחום ראשי באמצעות המנה:

הגדרה 7.6.4. *חבורת המחלקות* $C(A)$ של תחום דדקינד A היא המנה של חבורת האידיאלים השבריים בתת-חבורה שנוצרת על-ידי האידיאלים הראשיים. אם K שדה מספרים, נסמן לעתים $C(K)$ במקום $C(\mathcal{O}_K)$. חבורת המחלקות

7.7 מספר המחלקה

כשהכשלון של $\mathbb{Z}[\sqrt{-5}]$ להיות תחום ראשי הוביל לכשלוננו לתאר את הראשוניים מהצורה $n^2 + 5m^2$, נכשלנו בזה בדרך נוספת: היו שתי תבניות מצומצמות שונות מדיסקרימיננטה -20. עכשיו יש באפשרותינו לתאר את הקשר בין שני הכשלונות.

יותר ספציפית, אנחנו נתאר התאמה הפיכה (של קבוצות) בין איברי חבורת המחלקות עבור השדה $K = \mathbb{Q}(\sqrt{d})$, כאשר $d < 0$ (חסר ריבועים), לתבניות מצומצמות מדיסקרימיננטה d. לשם הפשטות, נתמקד במקרה ש-d אינו מהצורה $4n+1$. על מנת להתחיל, נשים לב:

טענה 7.7.1. *כל אידיאל שברי של K איזומורפי כחבורה ל-$\mathbb{Z}^2$*

הוכחה. נניח ש-I אידיאל שברי. כיוון ש-K ממציין 0, אין ב-I (כחבורה) איברים מסדר סופי, ולכן היא איזומורפית ל-$\mathbb{Z}^n$ עבור איזשהו n. אם $a_1, \dots, a_n \in I$ בלתי-תלויים מעל $\mathbb{Z}$, אז הם בלתי תלויים גם מעל $\mathbb{Q}$. כיוון ש-K ממימד 2 מעל $\mathbb{Q}$, קיבלנו ש-$n \leqslant 2$. מאידך, ההעתקה $x \mapsto a_1 x$ היא העתקה חד-חד-ערכית (כי $\mathcal{O}_K$ תחום!) מ-$\mathcal{O}_K$ ל-I, וכיוון ש-$\mathcal{O}_K$ עצמו נוצר על-ידי שני איברים $1, \sqrt{d}$, סיימנו. □

אם A חבורה חילופית חופשית על שני יוצרים, נאמר שפונקציה $p : A \to \mathbb{Z}$ היא תבנית ריבועית אם קיים איזומורפיזם $T : \mathbb{Z}^2 \to A$ כך ש-$p \circ T$ תבנית ריבועית במובן הרגיל. במצב הזה, אם $S : \mathbb{Z}^2 \to A$ איזומורפיזם נוסף, אז $T^{-1} \circ S$ אוטומורפיזם של $\mathbb{Z}^2$, ולכן $p \circ S = (p \circ T) \circ (T^{-1} \circ S)$ גם היא תבנית ריבועית *ששקולה* ל-$p \circ T$. כיוון ששקילות שומרת על מושגים כמו פרימיטיביות ועל הדיסקרימיננטה, אפשר לשייך תכונות אלה ל-p. לכן, תבנית ריבועית על A קובעת מחלקת שקילות של תבניות במובן הרגיל, או, במקרה של תבנית פרימיטיבית מדיסקרימיננטה שלילית, תבנית מצומצמת יחידה (אנחנו מזניחים לשם הפשטות את ההבדל בין שקילות תחת $\mathrm{SL}_2(\mathbb{Z})$ ו-$\mathrm{GL}_2(\mathbb{Z})$, בפועל צריך מידע נוסף של *אוריינטציה* על A).

הדוגמא הבסיסית לתבנית על $\mathcal{O}_K$ היא הנורמה. בבסיס $1, \sqrt{d}$ זוהי התבנית הסטנדרטית $p(x, y) = x^2 - dy^2$. אנחנו רוצים לייצר תבניות נוספות על-ידי שימוש באידיאלים שבריים בתור החבורה. לשם כך, עלינו להכליל את מושג הנורמה של איבר לאידיאלים. אם n מספר טבעי, אז $\mathcal{O}_K/n$ הוא חוג עם n^2 איברים (נוצר באופן חופשי על-ידי התמונות של 1 ו-$\sqrt{d}$, איברים מסדר n). זוהי גם הנורמה של n כאיבר של $\mathcal{O}_K$. התרגיל הבא מראה שזה נכון לכל איבר:

תרגיל 7.7.2. נניח ש-A מטריצה 2×2 מעל $\mathbb{Z}$, עם דטרמיננטה $d = \det(A) \neq 0$. הוכיחו שהתמונה של A על $\mathbb{Z}^2$ היא מאינדקס $|d|$ ב-$\mathbb{Z}^2$. הסיקו שלכל $a \in \mathcal{O}_K$ מספר האיברים ב-$\mathcal{O}_K/a$ הוא $N(a)$.

התרגיל מצדיק את ההגדרה הבאה:

הנורמה של אידיאל

הגדרה 7.7.3. *הנורמה של אידיאל* I ב-$\mathcal{O}_K$ היא מספר האיברים ב-$\mathcal{O}_K/I$.

העובדה הבסיסית שהנורמה היא כפלית נכונה גם עבור אידיאלים:

עובדה 7.7.4. *אם I ו-J אידיאלים ב-$\mathcal{O}_K$, אז* $N(IJ) = N(I)N(J)$

נעיר שאם I, J הם אידיאלים, אז $IJ \subseteq I \cap J$. אם מתקיים שוויון, אז העובדה האחרונה נובעת ממשפט השאריות הסיני, אבל ככלל ההוכחה יותר קשה ואנחנו נדלג עליה.

עכשיו, נניח ש-I אידיאל ב-$\mathcal{O}_K$. אם $a \in I$, אז $(a) \subseteq I$, ולכן קיים אידיאל J כך ש-$(a) = IJ$. לכן, $N(a) = N((a)) = N(IJ) = N(I)N(J)$. במלים אחרות, $N(I)$ מחלק את $N(a)$, ולכן יש לנו פונקציה $p : I \to \mathbb{Z}$ שנתונה על-ידי $p(a) = \frac{N(a)}{N(I)}$, וברור שהיא תבנית ריבועית על I. כיוון שהנורמה חיובית על $\mathcal{O}_K$, כך גם p, ולכן זוהי תבנית עם דיסקרימיננטה שלילית, וניתן לבדוק שהיא פרימיטיבית. לכן, שייכנו לכל אידיאל ב-$\mathcal{O}_K$ תבנית p_I.

טענה 7.7.5. *הדיסקרימיננטה של p_I היא d.*

הוכחה. זה נובע ישירות מהטענה הכללית הבאה: אם p תבנית ריבועית על $\mathbb{Z}^2$ מדיסקרימיננטה d, ו-$A \subseteq \mathbb{Z}^2$ תת-חבורה מאינדקס n (אז בהכרח איזומורפית ל-$\mathbb{Z}^2$), אז הדיסקרימיננטה של הצמצום של p ל-A היא $n^2 d$. נשאיר את ההוכחה כתרגיל □

לבסוף, נשים לב:

טענה 7.7.6. *התבנית q_I תלויה (עד כדי שקילות) רק בתמונה של I ב-$C(K)$ (כלומר, אם $I = aJ$ אז ל-q_I ו-q_J מתאימה אותה מחלקת שקילות של תבניות)*

הוכחה. תרגיל $\square$

כיוון שכל איבר ב-$C(K)$ ניתן לייצג על-ידי אידיאל (לא שברי), אנחנו מקבלים:

מסקנה 7.7.7. *קיימת העתקה מוגדרת היטב מחבורת המחלקות $C(K)$ לקבוצת התבניות המצומצמות מדיסקרימיננטה d, שנקבעת על-ידי הדרישה שאידיאל $I \subseteq \mathcal{O}_K$ מתאים לתבנית q_I שהוגדרה לעיל.*

לא נוכיח את זה, אבל מסתבר שההתאמה הזו היא חד-חד-ערכית ועל. בפרט, המספר $h(d)$ שהגדרנו הוא הגודל של חבורת המחלקות. נובע מכך גם שעל קבוצת התבניות המצומצמות קיים מבנה של חבורה. המבנה הזה התגלה על-ידי גאוס, ונקרא *הרכבת גאוס*, אבל התיאור הישיר שלו מסובך

הרכבת גאוס

סוף הרצאה 25, 14 בינו

מקורות

[1] Alan Baker. *A comprehensive course in number theory*. Cambridge University Press, Cambridge, ,2012 pp. xvi+251. ISBN: .978-1-107-60379-0 DOI: 10.1017/CBO9781139093835.

[2] David A. Cox. *Primes of the form $x^2 + ny^2$*. 2nd ed. Pure and Applied Mathematics (Hoboken). Fermat, class field theory, and complex multiplication. John Wiley & Sons, Inc., Hoboken, NJ, ,2013 pp. xviii+356. ISBN: -978-1-118 .39018-4 DOI: 10.1002/9781118400722.

[3] Graham Everest and Thomas Ward. *An introduction to number theory*. Vol. .232 Graduate Texts in Mathematics. Springer-Verlag London, Ltd., London, ,2005 pp. x+294. ISBN: ;978-1-85233-917-3 .1-85233-917-9

[4] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*. 2nd ed. Vol. .84 Graduate Texts in Mathematics. Springer-Verlag, New York, ,1990 pp. xiv+389. ISBN: 0-387-97329-X. DOI: 10.1007/978-1-4757-2103-4.

[5] Daniel A. Marcus. *Number fields*. 2nd ed. Universitext. Springer, ,2018 pp. xviii+203. ISBN: ;978-3-319-90232-6 .978-3-319-90233-3 DOI: 10.1007/978-3-319-90233-3.

[6] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery. *An introduction to the theory of numbers*. 5th ed. John Wiley & Sons, Inc., New York, ,1991 pp. xiv+529. ISBN: .0-471-62546-9

[7] J.-P. Serre. *A course in arithmetic*. Translated from the French, Graduate Texts in Mathematics, No. .7 Springer-Verlag, New York-Heidelberg, ,1973 pp. viii+115.

[8] John Stillwell. *Elements of number theory*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, ,2003 pp. xii+254. ISBN: .0-387-95587-9 DOI: 10.1007/978-0-387-21735-2.

[9] Ramin Takloo-Bighash. *A Pythagorean introduction to number theory*. Undergraduate Texts in Mathematics. Right triangles, sums of squares, and arithmetic. Springer, Cham, ,2018 pp. xviii+279. ISBN: ;978-3-030-02603-5 .978-3-030-02604-2 DOI: 10.1007/978-3-030-02604-2.

[10] Audrey Terras. *Fourier analysis on finite groups and applications*. Vol. .43 London Mathematical Society Student Texts. Cambridge University Press, Cambridge, ,1999 pp. x+442. ISBN: .0-521-45718-1 DOI: 10 . 1017 / CBO9780511626265.