<u>אלגברה מופשטת 2 – תרגיל בית 9</u>

מתרגלים: ד"ר אפי כהן ואדם צ'פמן.

1. מספר מרוכב α נקרא שלם אלגברי אם קיים פולינום מתוקן $p \in \mathbb{Z}[x]$ כך ש $p(\alpha)=0$. הם מהווים תת-חוג של שדה המספרים המרוכבים. נסמנו B.
   a. הוכיחו כי אם $b \in B$ אזי $\sqrt{b} \in B$.
   b. הסיקו כי B איננו אטומי.

פיתרון:

אם b שלם אלגברי אז הוא שורש של איזשהו פולינום מתוקן $p(x)$. נסמן $q(x)=p(x^2)$. זהו גם כן פולינום מתוקן עם מקדים שלמים, רק שהפעם $\sqrt{b}$ שורש שלו, ולכן $\sqrt{b}$ הוא שלם אלגברי.

ניקח את 2. הוא לא הפיך משום שחצי איננו שלם אלגברי, משום שבכל פולינום מתוקן כשמציבים חצי אז המקדם העליון הופך להיות חצי בחזקה שגבוהה מדי מכדי שהסכום עם שאר המונומים יוכל להתאפס.

נניח בשלילה כי 2 מתפרק למכפלת אי-פריקים $p_1 p_2 \ldots p_r$.

כעת, $p_1=\sqrt{p_1}\cdot\sqrt{p_1}$. אם $\sqrt{p_1}$ הפיך אזי p_1 הפיך וזו סתירה, ולכן $\sqrt{p_1}$ לא הפיך.

אולם, זה אומר ש p_1 פריק, וזו גם כן סתירה.

לכן B איננו אטומי.

2. יהי $D \in \mathbb{Z}$ חופשי מריבועים. הוכיחו כי $\mathbb{Z}[\sqrt{D}] \cong \left\{ \begin{pmatrix} a & bD \\ b & a \end{pmatrix} : a,b \in \mathbb{Z} \right\}$.

פיתרון:

מגדירים את הפונקצייה

$\varphi:\mathbb{Z}[\sqrt{D}]\to\left\{\begin{pmatrix} a & bD \\ b & a \end{pmatrix} : a,b\in\mathbb{Z}\right\}$ המקיימת $\varphi(a+b\sqrt{D})=\begin{pmatrix} a & bD \\ b & a \end{pmatrix}$.

צריך להראות שהיא מקיימת את התכונות של הומומורפיזם חוגים וגם שהיא חח"ע ועל.

3. הציגו את $x^3-9\in\mathbb{Z}_{11}[x]$ כמכפלת פולינומים אי-פריקים.

פיתרון:

מחפשים שורש לפולינום ב $\mathbb{Z}_{11}$ [כי אחרת הוא אי-פריק. זה נכון בגלל שהמעלה שלו 3] שורש כזה הוא 4. כלומר, $x-4\,|\,x^3-9$. ע"י חלוקת פולינום ניתן לקבל ש $x^3-9=(x-4)(x^2+4x+5)$. ע"י הצבות ניתן לראות של x^2+4x+5 אין שורשים ב $\mathbb{Z}_{11}$ ולכן אי-פריק. כמובן שגם $x-4$ אי-פריק [פולינומים ממעלה 1 מעל שדה תמיד פריקים, משום שכל פירוק שלהם מכיל פולינום אחד ממעלה 1 ועוד אולי איברים ממעלה 0 שהם בהכרח הפיכים]

4. פרקו את $130i$ למכפלת ראשוניים ב $\mathbb{Z}[i]$.

פיתרון:

$130i=2\cdot 5\cdot 13\cdot i$. i הוא הפיך, ולכן הוא לא משחק תפקיד חשוב. ידוע שהראשוניים הטבעיים היחידים שנשארים ראשוניים בשלמים של גאוס הם אלה ששארית החלוקה שלהם ב4 היא 3. המספרים 2, 5 ו13 אינם כאלה, ולכן הם מתפרקים למכפלת שני ראשוניים שצמודים זה לזה. $2=(1+i)(1-i)$, $5=(2+i)(2-i)$ ו $13=(3+2i)(3-2i)$.

הפירוק לראשוניים אם כך הוא

$$130i=(1+i)(1-i)\cdot(2+i)(2-i)\cdot(3+2i)(3-2i)\cdot i.$$

5. מצאו את המחלק המשותף המקסימלי של x^4+3x^3+4x+2 ו x^3+2x+2 ב $\mathbb{Z}_5[x]$. בטאו אותו כצירוף ליניארי של שני הפולינומים.

פיתרון:

כשמחלקים את הפולינומים זה בזה עם שארית מקבלים

$$x^4+3x^3+4x+2=(x+3)(x^3+2x+2)+3x^2+x+1$$

$$x^3+2x+2=(2x+1)(3x^2+x+1)-x+1$$

הפולינום $-x+1$ מחלק את $3x^2+x+1$ ולכן התהליך מסתיים איתו והוא המחלק המשותף המקסימלי של שני הפולינומים המקוריים.

כעת,

$$\begin{aligned}&-x+1=x^3+2x+2-(2x+1)(3x^2+x+1)=\\&x^3+2x+2-(2x+1)(x^4+3x^3+4x+2-(x+3)(x^3+2x+2))=\\&(2x^2+2x+4)(x^3+2x+2)-(2x+1)(x^4+3x^3+4x+2)\end{aligned}$$

6. יהי R תחום שלמות. לקבוצה $S\subseteq R$ נגדיר $S^*=\{s\in S:\exists_{a\in S}a+<s>\subseteq S\}$. נסמן $R_0=R\setminus\{0\}$ ו $R_{i+1}=R_i^*$. הראו ש R_1 היא קבוצת האיברים הלא הפיכים השונים מאפס ב R. הראו שאם R אוקלידי אז $\bigcap_{i=0}^{\infty}R_i=\phi$. [רמז: הראו באינדוקציה ש $d(s)\geq n$ לכל $s\in R_n$]

פיתרון:

יהי איבר הפיך $r\in R_0$. $<r>=R$, ולכן לא קיים $a\in R_0$ כך ש $a+<r>\subseteq R_0$.

מאידך, לכל $s\in R_0$ לא הפיך, $r\notin<s>$, ולכן $0\notin r+<s>$, משמע $r+<s>\subseteq R_0$. מכאן ש R_1 היא קבוצת האיברים הלא הפיכים ב R_0 [שזה כל הלא הפיכים ב R פרט לאיבר האפס].

נוכיח באינדוקציה כי $d(s)\geq n$ לכל $s\in R_n$.

נבדוק עבור $n=1$. ב R_1 כל האיברים אינם הפיכים, ולכן הדרגה של כולם גדולה מאפס (איברים שדרגתם 0 הם רק ההפיכים. זאת הראינו בתרגול)

נניח נכונות עבור $n=k$ ונוכיח עבור $n=k+1$.

נניח בשלילה כי קיים איבר $s \in R_{k+1}$ שעבורו $d(s) \le k$. מכיוון ש $s \in R_k$ גם כן, אז לפי הנחת האינדוקציה $d(s)=k$.

לפי הגדרת R_{k+1}, קיים איבר $a \in R_k$, כך ש $a+<s> \subseteq R_k$. נחלק את a ב s עם שארית ונקבל $a=qs+r$. אם $r=0$ אזי $0=a-qs \in a+<s> \subseteq R_k \subseteq R_0$ ולכן סתירה.

אחרת, $d(r)<d(s)=k$. אולם, $r \in R_k$ וזה בסתירה להנחת האינדוקציה.

משמע, לכל $s \in R_{k+1}$, $d(s) \ge k+1$.