אלגברה מופשטת 2 – תרגול 10

הגדרה:
תחום שלמות R נקרא "אטומי" או "תחום פריקות" אם כל איבר $a \in R$ מתפרק למכפלה $up_1 \dots p_n$ כאשר $u \in U(R)$ (משמע הפיך) ו $p_1, \dots, p_n$ אי-פריקים.

דוגמאות:
1. החוגים $\mathbb{Z}$, $\mathbb{Z}[x]$ ו $F[x]$ (כאשר F שדה) הם אטומיים.
2. החוג $F[x^r : r \in \mathbb{Q}]$ איננו אטומי.

הגדרה:
תחום אטומי R נקרא "תחום פריקות יחידה" אם לכל שני פירוקים של אותו איבר $up_1 \dots p_n$ ו $vq_1 \dots q_m$ מתקיים $m = n$ וגם ישנה תמורה $\sigma \in S_n$ כך ש $q_{\sigma(k)} \sim p_k$.

דוגמאות:
1. $\mathbb{Z}$ הוא תחום פריקות יחידה.
2. $\mathbb{Z}[\sqrt{10}]$ איננו תחום פריקות יחידה משום ש $6 = 2 \cdot 3 = (4 - \sqrt{10}) \cdot (4 + \sqrt{10})$ הם שני פירוקים שלא מקיימים את התנאי הנ"ל.

משפט: כל תחום ראשי הוא תחום פריקות יחידה.

מסקנה: $\mathbb{Z}[\sqrt{10}]$ איננו תחום ראשי.

משפט: בתחום ראשי R, a אי פריק $\Leftrightarrow$ $< a >$ מקסימלי.

הוכחה: ($\Leftarrow$) אם $< a > \subset I \subset R$ אזי מכיוון שR ראשי קיים $b \in R$ כך ש $< b >= I$ ולכן קיים $c \in R \setminus U(R)$ כך ש$a = bc$, משמע a פריק.

($\Rightarrow$) אם $< a >$ מקסימלי וגם $a = bc$ כך ש$b \notin U(R)$ אזי $b \mid a$ ולכן $< a > \subseteq < b > \subset R$. בגלל המקסימליות של $< a >$, $< a >=< b >$, משמע $a \sim b$, כלומר a אי-פריק.

[שימו לב כי בכוון ההפוך אין צורך להשתמש בהנחה כי התחום R הוא דווקא ראשי]

משפט: בתחום ראשי, $p \in R$ אי-פריק אם ורק אם הוא ראשוני.

הוכחה: ידוע כבר כי בכל תחום ראשי, ראשוני גורר אי-פריק. נראה כי במקרה זה אי-פריק גורר ראשוני. אם p אי-פריק אזי $< p >$ מקסימלי, ולכן $< p >$ ראשוני, משמע p ראשוני.

תרגיל: יהי p שלם ראשוני גדול מ2, ו$d \in \mathbb{Z}$ כך ש$p \nmid d$. אם $x^2 \equiv d \pmod{p}$ פתירה אז בחוג $\mathbb{Z}[\sqrt{d}]$ מתקיים $< p >= P_1 \cdot P_2$ כך ש $P_1 \neq P_2$.

פיתרון: נקרא לפיתרון לקונגרואנציה a. איבר כללי הנמצא במכפלת האידיאלים ב$\mathbb{Z}[\sqrt{d}]$ $< p, a+\sqrt{d} > \cdot < p, a-\sqrt{d} >$ הוא מהצורה $c_1 p^2 + c_2 p(a-\sqrt{d}) + c_3 p(a+\sqrt{d}) + c_4 (a-\sqrt{d})(a+\sqrt{d})$, ולכן

$$< p, a+\sqrt{d} > \cdot < p, a-\sqrt{d} >=< p > \cdot < p, a+\sqrt{d}, a-\sqrt{d}, \frac{a^2-d}{p} > .$$

כעת $2a = (a-\sqrt{d}) + (a+\sqrt{d})$. אם $p \mid a$ אזי $p \mid a^2$ ולכן $p \mid d$ וזו סתירה.

לכן $p \nmid a$, משמע $\gcd(2a, p) = 1$ ולכן $1 \in < p, a+\sqrt{d}, a-\sqrt{d}, \frac{a^2-d}{p} >$

משמע $< p, a+\sqrt{d}, a-\sqrt{d}, \frac{a^2-d}{p} >= \mathbb{Z}[\sqrt{d}]$. כלומר

$$< p, a+\sqrt{d} > \cdot < p, a-\sqrt{d} >=< p >.$$

אם הם היו שווים אז $< p, a+\sqrt{d} >$ היה מכיל את p ואת $2a$ ולכן מאותם שיקולים $< p, a+\sqrt{d} >= \mathbb{Z}[\sqrt{d}]$ ולכן גם $< p >= \mathbb{Z}[\sqrt{d}]$ וזו סתירה.

הכללה של מושג הנורמה:

תרגיל: יהי R תח"ש. הראו ש $\widehat{N}: R \to \mathbb{N} \cup \{\infty\}$ המוגדרת ע"י $\widehat{N}(a) = \left|R/Ra\right|$ היא כפלית.

פתרון: $\widehat{N}(ab) = \left|R/Rab\right|$

נרצה להשתמש באיזו' 3:

בוודאי שמתקיים $Rab \subseteq Ra$ ולכן $R/Ra \cong \left(R/Rab\right) \Big/ \left(Ra/Rab\right)$.

כיוון שחוג הוא גם חבורה חיבורית ותת-חוג הוא תת-חבורה, ניתן להשתמש בלגרנג' ולקבל $\left|R/Ra\right| = \left|\left(R/Rab\right) \Big/ \left(Ra/Rab\right)\right| = \frac{\left|R/Rab\right|}{\left|Ra/Rab\right|}$. מכאן נקבל $\left|R/Ra\right|\left|Ra/Rab\right| = \left|R/Rab\right|$. כעת נשאר להראות ש $\left|Ra/Rab\right| = \left|R/Rb\right|$.

קל לראות שהפונקציה $f: R/Rb \to Ra/Rab$ המוגדרת ע"י $f(x+Rb) = ax+Rab$ היא מוגדרת היטב וחח"ע ועל (למעשה היא איזו' חבורות).

הערה: ראינו בתרגול הקודם שכל אידאל שונה מ {0} של $\mathbb{Z}[\sqrt{D}]$ מכיל איבר של $\mathbb{Z}$. בצורה דומה מוכיחים שבכל אידאל שונה מ {0} של $\mathcal{O}_D$ יש איבר של $\mathbb{Z}$. לכן חוג המנה עבור כל אידאל שונה מ {0} הוא סופי.

תרגיל: הראו שב- $R = \mathcal{O}_D$ מתקיים $|N(x)| = \widehat{N}(x) = \left|R/Rx\right|$ (כאשר $N(x)$ היא הנורמה הרגילה ב $\mathcal{O}_D$).

פתרון: נראה רק עבור המקרה $D \not\equiv 1 (\mathrm{mod}\, 4)$ (החלק השני תרגיל בית).

יהי $x = a + b\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$. אזי ניתן להניח ש a, b זרים, כיוון ששתי הנורמות כפליות (בדקו מדוע).

כעת $N := |N(x)| = |a^2 - Db^2| \in \mathbb{Z} \cap < x >$, ולכן ב $\mathbb{Z}[\sqrt{D}]/< x >$ יש לכל היותר N^2 איברים (כי ניתן לעשות מודול N לכל אחד מהרכיבים). כעת לפי בחירת N מתקיים b זר ל N, ולכן הפיך מודולו N. כלומר קיים b' כך ש $bb' = 1 (\mathrm{mod}\, N)$ כאשר נעשה מודולו $< x >$ השיוויון יישמר, ולכן b הפיך מודולו $< x >$.
כעת $a + b\sqrt{D} \equiv 0 \pmod{< x >} \Rightarrow \sqrt{D} = -ab' \pmod{< x >}$. מכאן ניתן להסיק שניתן לבחור נציג מתוך $0,..., N-1$ לכל איבר ב $\mathbb{Z}[\sqrt{D}]/< x >$.
כעת צריך להראות שכל הנציגים האלה שונים, אבל זה נכון אם ורק אם $\alpha \not\equiv 0 (\mathrm{mod} < x >)$ לכל $0 \le \alpha \le N-1$.
אם $\alpha \equiv 0 (\mathrm{mod} < x >)$ אזי $a + b\sqrt{D} \mid \alpha$ ולכן $a - b\sqrt{D} = \overline{a + b\sqrt{D}} \mid \overline{\alpha} = \alpha$, לכן $N \mid \alpha$, סתירה.

הגדרה: יהי R תחום שלמות. פונקצייה $d: R \to \mathbb{N} \cup \{0, -\infty\}$ המקיימת $-\infty = d(x) \Leftrightarrow x = 0$ נקראת אוקלידית אם

1. $d(a) \le d(ab)$ לכל $a, b \in R$.
2. לכל $b \neq 0$ ולכל a קיימים $q, r \in R$ כך ש $a = qb + r$ וגם $d(r) < d(b)$ או $r = 0$.

אם קיימת פונקצייה כזאת עבור R אזי הוא נקרא "תחום אוקלידי".

דוגמאות:

1. $\mathbb{Z}[i]$ הוא תחום אוקלידי, עם הפונקצייה $d(a+bi) = a^2 + b^2$.
2. $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ איננו תחום אוקלידי [לא ניתן לזה הוכחה בשלב זה].

משפט: אם R חוג קומוטטיבי עם יחידה ו $f, g \in R[x]$ כך ש $g(x)$ פולינום מתוקן, אזי קיימים $r, q \in R[x]$ כך ש $f = gq + r$ וגם $\deg(r) < \deg(g)$ או $r = 0$.

משפט: תחום אוקלידי הוא תחום ראשי.

הוכחה: אם $R \lhd I \neq 0$ אזי ניקח $0 \neq b \in I$ כך ש $d(b) = \min\{d(c) : 0 \neq c \in I\}$. אזי בגלל האוקלידיות, כל איבר אחר ב I חייב להתחלק ב b (כי אחרת יש סתירה למינימליות) ולכן $I = < b >$.

תרגיל: הראו ש $\mathbb{Z}[x]$ אינו תחום אוקלידי.

פתרון: $\mathbb{Z}[x]$ אינו תחום ראשי, כיוון ש $< 2, x >$ אינו אידאל ראשי (הראינו זאת בתרגול קודם).

שאלה: מדוע פונקצית הדרגה של פולינומים אינה d מתאימה?

תשובה: לא תמיד קיימת חלוקה עם שארית כאשר המחלק אינו מתוקן (לדוגמה x לא מתחלק טוב ב 2x בחוג $\mathbb{Z}[x]$)

תרגיל: אם F שדה אזי $F[[x]]$ אוקלידי עם $d(\sum_{n=0}^{\infty} a_n x^n) = \min\{i : a_i \neq 0\}$.

פיתרון: קל לראות ש $d(fg) = d(f) + d(g) > d(f)$ לכל $f, g \in F[[x]]$ השונים מאפס.

נניח $g \neq 0$. צריך להוכיח כי קיימים $r, q \in F[[x]]$ שעבורם $f = gq + r$ וגם $d(r) < d(g)$ או $r = 0$. אם מלכתחילה $d(f) < d(g)$ אז ניקח $r = f$ ו $q = 0$. נניח ש $m = d(f) \geq d(g) = n$. אזי $f = x^m f_0$ ו $g = x^n g_0$ כאשר $d(f_0) = d(g_0) = 0$ [כלומר יש להם מקדם חופשי שונה מאפס]. לכן g_0 הפיך. ניקח $q = x^{m-n} g_0^{-1} f_0$ ו $r = 0$ וסיימנו.

תרגיל: הראה כי בתחום אוקלידי, a הפיך אם ורק אם $d(a) = d(1)$.

הוכחה: אם a הפיך אזי $d(a) \leq d(a \cdot a^{-1}) = d(1)$ וגם $d(1) \leq d(1 \cdot a) = d(a)$, ולכן $d(a) = d(1)$. אם $d(a) = d(1)$ אז נרשום $1 = qa + r$. במקרה זה $r = 0$ או ש $d(r) < d(1)$ אך האופצייה השנייה לא אפשרית, ולכן $1 = qa$, כלומר a הפיך.

תרגיל בית:

ב $\mathbb{Z}[\sqrt{3}]$, $N(-5 + \sqrt{3}) = 25 - 3 = 22$. הוכיחו כי

$|\mathbb{Z}[\sqrt{3}] / < -5 + \sqrt{3} >| = 22$.