אלגברה מופשטת 2 – תרגיל כיתה 8

מתרגלים: ד"ר אפי כהן ואדם צ'פמן.

הגדרה:

תחום שלמות R נקרא "אטומי" או "תחום פריקות" אם כל איבר $a \in R$ מתפרק למכפלה $up_1 \ldots p_n$ כאשר $u \in U(R)$ (משמע הפיך) ו $p_1, \ldots, p_n$ 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 $up_1 \ldots p_n$ ו $vq_1 \ldots q_m$ מתקיים $m = n$ וגם ישנה תמורה $\sigma \in S_n$ כך ש $p_k \sim q_{\sigma(k)}$.

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 $R \subset I \subset <a>$ אזי מכיוון שR ראשי קיים $b \in R$ כך ש$I=<b>$ 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 $R \subset <b> \subseteq <a>$. בגלל המקסימליות של $<a>$, $<a>=<b>$, משמע $a \sim b$, כלמור a אי-פריק.

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

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

פיתרון: 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$d \nmid p$. 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 $(a+\sqrt{d})+(a-\sqrt{d})=2a$. אם $p\,|\,a$ אזי $p\,|\,a^2$ ולכן $p\,|\,d$ וזו סתירה. לכן

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

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

$\mathbb{Z}[\sqrt{d}]=<p,a+\sqrt{d}>$ ולכן גם $\mathbb{Z}[\sqrt{d}]=<p>$ וזו סתירה.

הגדרה: יהי R תחום שלמות. פונקצייה $d:R\to\mathbb{N}\cup\{-\infty\}$ המקיימת

$x=0 \Leftrightarrow d(x)=-\infty$ 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 $d(r)<d(b)$.

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. $\mathbb{Z}\left[\dfrac{1+\sqrt{-19}}{2}\right]$ איננו תחום אוקלידי [לא ניתן לזה הוכחה בשלב זה].

טענה (לבית): הראה כי 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 $r=0$.

טענה: תחום אוקלידי הוא תחום ראשי.

הוכחה: אם $0 \neq I \lhd R$ 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: 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 $f, g \in F[[x]]$.

נניח $g \neq 0$. צריך להוכיח כי קיימים $r, q \in F[[x]]$ שעבורם $f = gq + r$ וגם

$d(r) < d(g)$. 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 חופיש 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

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