פתרון תרגיל בית 6 מבוא לחוגים ומודולים
88-212 סמסטר ב' תשפ"א

שאלה 1 (חזרה). יהיו R, S חוגים. נניח שקיים הומומורפיזם $\varphi : R \to S$. הראו כי
$R[x]/(\ker\varphi)[x] \cong (\operatorname{Im}\varphi)[x]$.
(בהרצאה ראיתם את זה במקרה של ההטלה הטבעית $R \to R/I$.)

הוכחה. נגדיר העתקה $\psi : R[x] \to S[x]$ לפי

$$\psi\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} \varphi(a_i) x^i.$$

נטען כי ψ הומומורפיזם של חוגים. אכן, יהיו $\sum_{i=0}^{n} a_i x^i, \sum_{j=0}^{m} b_j x^j \in R[x]$. אפשר להניח כי $m = n$ (אם לא, נוסיף עוד מעלות עם מקדמי 0 לפולינום מהמעלה הנמוכה יותר).

$$\psi\left(\left(\sum_{i=0}^{n} a_i x^i\right) + \left(\sum_{j=0}^{n} b_j x^j\right)\right) = \psi\left(\sum_{i=0}^{n} (a_i + b_i) x^i\right) = \sum_{i=0}^{n} \varphi(a_i + b_i) x^i =$$

$$= \sum_{i=0}^{n} \varphi(a_i) x^i + \sum_{i=0}^{n} \varphi(b_i) x^i = \psi\left(\sum_{i=0}^{n} a_i x^i\right) + \psi\left(\sum_{j=0}^{m} b_j x^j\right)$$

עבור הכפליות:

$$\psi\left(\left(\sum_{i=0}^{n} a_i x^i\right) \cdot \left(\sum_{j=0}^{m} b_j x^j\right)\right) = \psi\left(\sum_{k=0}^{m+n}\left(\sum_{i=0}^{k} a_i b_{k-i}\right) x^k\right) = \sum_{k=0}^{m+n} \varphi\left(\sum_{i=0}^{k} a_i b_{k-i}\right) x^k =$$

$$= \sum_{k=0}^{m+n}\sum_{i=0}^{k} \varphi(a_i)\varphi(b_{k-i}) x^k =$$

$$= \left(\sum_{i=0}^{n} \varphi(a_i) x^i\right)\left(\sum_{j=0}^{m} \varphi(b_j) x^j\right) = \psi\left(\sum_{i=0}^{n} a_i x^i\right) \cdot \psi\left(\sum_{j=0}^{m} b_j x^j\right)$$

וכמו כן $\psi(1) = 1$.

מה הגרעין של ψ?

$$\ker\psi = \left\{\sum_{i=0}^{n} a_i x^i \in R[x] \mid \psi\left(\sum_{i=0}^{n} a_i x^i\right) = 0\right\} = \left\{\sum_{i=0}^{n} a_i x^i \in R[x] \mid \sum_{i=0}^{n} \varphi(a_i) x^i = 0\right\} =$$

$$= \left\{\sum_{i=0}^{n} a_i x^i \in R[x] \mid \forall 0 \le i \le n : \varphi(a_i) = 0\right\} = \left\{\sum_{i=0}^{n} a_i x^i \in R[x] \mid \forall 0 \le i \le n : a_i \in \ker\varphi\right\} =$$

$$= (\ker\varphi)[x]$$

מה התמונה של ψ? ברור כי $\operatorname{Im}\psi \subseteq (\operatorname{Im}\varphi)[x]$. ומצד שני, גם ההכלה בכיוון השני נכונה: אם $\sum_{i=0}^{n} b_i x^i \in (\operatorname{Im}\varphi)[x]$, אז קיימים $a_i \in R$ כך ש-$\varphi(a_i) = b_i$, ואז $\psi\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} b_i x^i$.

בסך הכל, לפי משפט האיזומורפיזם הראשון נקבל את הדרוש. □

שאלה 2. יהי $D \in \mathbb{Z}$. הוכיחו ששדה השברים של $\mathbb{Z}[\sqrt{D}]$ הוא $\mathbb{Q}[\sqrt{D}]$.

פתרון. קודם כל, אפשר להניח ש-D איננו ריבוע ב-$\mathbb{Z}$. אחרת $\mathbb{Z}\left[\sqrt{D}\right] = \mathbb{Z}$ ושדה השברים הוא $\mathbb{Q}\left[\sqrt{D}\right] = \mathbb{Q}$.

נטען כי $\mathbb{Q}\left[\sqrt{D}\right]$ הוא שדה. אכן, קל לראות כי הוא תת-חוג של $\mathbb{C}$ (ודאו שאתם יודעים להוכיח את זה), לכן הוא תחום שלמות. כדי להוכיח שכל איבר שונה מאפס בו הוא הפיך, יהי $0 \neq x = a + b\sqrt{D} \in \mathbb{Q}\left[\sqrt{D}\right]$. נתבונן בנורמה שלו $N\left(a + b\sqrt{D}\right) = \left(a + b\sqrt{D}\right)\left(a - b\sqrt{D}\right) = a^2 - Db^2$. הנורמה שונה מאפס, כי D אינו ריבוע ב-$\mathbb{Z}$. לכן

$$\left(a + b\sqrt{D}\right)^{-1} = \frac{a - b\sqrt{D}}{N\left(a + b\sqrt{D}\right)} \in \mathbb{Q}\left[\sqrt{D}\right].$$

כדי להוכיח שהוא שדה השברים, ניעזר באפיון הבא: שדה השברים של תחום שלמות R הוא השדה המינימלי המכיל את R. כיוון ש-$\mathbb{Z}\left[\sqrt{D}\right] \subseteq \mathbb{C}$, אפשר יהיה למצוא שם גם עותק של שדה השברים של $\mathbb{Z}\left[\sqrt{D}\right]$ (כלומר, תת-שדה של $\mathbb{C}$ שאיזומורפי להגדרה הפורמלית של שדה השברים של $\mathbb{Z}\left[\sqrt{D}\right]$). נסמן את העותק הזה F. כיוון ש-$\mathbb{Z} \subseteq F$, גם $\mathbb{Q} \subseteq F$. אבל גם $\sqrt{D} \in F$, לכן $\mathbb{Q}\left[\sqrt{D}\right] \subseteq F$. כיוון ש-$\mathbb{Q}\left[\sqrt{D}\right]$ הוא שדה בעצמו, נקבל שוויון $F = \mathbb{Q}\left[\sqrt{D}\right]$.

שאלה 3.

א. הוכיחו כי $\langle x^2 - 2\rangle$ הוא אידאל ראשוני ב-$\mathbb{Z}[x]$.

ב. מהו האידאל המקסימלי M במיקום $\mathbb{Z}[x]_{\langle x^2-2\rangle}$? מצאו יוצר שלו.

ג. לאיזה שדה איזומורפי $M/^{\mathbb{Z}[x]_{\langle x^2-2\rangle}}$?

הוכחה.

א. אפשר להראות ש-$\mathbb{Z}\left[\sqrt{2}\right] \cong \mathbb{Z}[x]/\langle x^2-2\rangle$ כמו שראינו פעמים רבות. כיוון שהמנה היא תחום שלמות, האידאל $\langle x^2 - 2\rangle$ ראשוני.
אפשר גם להוכיח ש-$x^2 - 2$ אי-פריק ב-$\mathbb{Z}[x]$, וכיוון ש-$\mathbb{Z}[x]$ תחום פריקות יחידה נקבל ש-$x^2 - 2$ ראשוני ב-$\mathbb{Z}[x]$.

ב. נכתוב קודם את המיקום:

$$\mathbb{Z}[x]_{\langle x^2-2\rangle} = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in \mathbb{Z}[x],\ \left(x^2 - 2\right) \nmid g(x) \right\}.$$

ראינו בתרגול שהאידאל המקסימלי במיקום R_P הוא PR_P. לכן האידאל המקסימלי פה הוא

$$M = \langle x^2 - 2\rangle \mathbb{Z}[x]_{\langle x^2-2\rangle} = \left\{ \frac{f(x)\left(x^2 - 2\right)}{g(x)} \mid f(x), g(x) \in \mathbb{Z}[x],\ \left(x^2 - 2\right) \nmid g(x) \right\}.$$

היוצר הוא $\frac{x^2-2}{1}$.

ג. נסמן $R=\mathbb{Z}[x]$, $P=\langle x^2-2\rangle$. אנחנו יודעים שחוג המנה R_P/PR_P אמור לצאת שדה, כי PR_P הוא אידאל מקסימלי. השדה הזה מכיל את כל הפונקציות הרציונאליות $\frac{f(x)}{g(x)}$ כאשר $g(x)\nmid\left(x^2-2\right)$, אבל $\frac{x^2-2}{1}+M=0+M$. לכן x משחק את התפקיד של $\sqrt{2}$, ואפשר באמת להגדיר הומומורפיזם

$$\varphi:\mathbb{Z}[x]_{\langle x^2-2\rangle}\to\mathbb{Q}\left[\sqrt{2}\right]$$

לפי

$$\varphi\left(\frac{f(x)}{g(x)}\right)=\frac{f\left(\sqrt{2}\right)}{g\left(\sqrt{2}\right)}.$$

שימו לב שזה מוגדר היטב כי $g(x)\nmid\left(x^2-2\right)$, ומכאן ניתן להסיק $g\left(\sqrt{2}\right)\neq 0$. ודאו שזהו הומומורפיזם על ושהגרעין שלו הוא M, והמסקנה תנבע ממשפט האיזומורפיזם הראשון.

□

שאלה 4. לכל $n\in\mathbb{N}$ נסמן $\mathbb{Z}\left[\frac{1}{n}\right]=S^{-1}\mathbb{Z}$ כאשר $S=\left\{n^k\;\middle|\;k\in\mathbb{N}\cup\{0\}\right\}$ בדומה למה שעשינו בכיתה. יהי p מספר ראשוני.

א. הוכיחו שלא קיים חוג R המוכל ממש בין החוגים $\mathbb{Z}\subsetneq R\subsetneq\mathbb{Z}\left[\frac{1}{p}\right]$.

ב. הוכיחו שאם $m|n$, אז $\mathbb{Z}\left[\frac{1}{n}\right]\subseteq\mathbb{Z}\left[\frac{1}{m}\right]$. הוכיחו שאם $n\nmid m^k$ לכל $k\in\mathbb{N}$, אז זו הכלה ממש.

ג. מצאו סדרת מספרים $n_1,n_2,n_3,\ldots$ כך שתהיה הכלה ממש בשרשרת החוגים

$$\mathbb{Z}\left[\frac{1}{n_1}\right]\subsetneq\mathbb{Z}\left[\frac{1}{n_2}\right]\subsetneq\mathbb{Z}\left[\frac{1}{n_3}\right]\subsetneq\cdots\subsetneq\mathbb{Q}$$

פתרון. א. יהי $\mathbb{Z}\subsetneq R\subseteq\mathbb{Z}\left[\frac{1}{p}\right]$. כל איבר של $\mathbb{Z}\left[\frac{1}{p}\right]$ הוא מהצורה $\frac{n}{p^k}$ לאיזשהו $n\in\mathbb{Z}$ ו-$k\geq 0$. כיוון ש-$\mathbb{Z}\subsetneq R$, נקבל שקיימים $k,n>0$ שעבורם $\frac{n}{p^k}\in R$ ו-$p\nmid n$. על ידי כפל ב-$p^{k-1}\in R$ נקבל $\frac{n}{p}\in R$. $p\nmid n$, לכן $\gcd(p,n)=1$, כלומר קיימים $a,b\in\mathbb{Z}$ שעבורם $ap+bn=1$. זה מראה שמתקיים

$$R\ni\frac{bn}{p}=\frac{1-ap}{p}=\frac{1}{p}-a$$

אך $a\in\mathbb{Z}$ ולכן $\frac{1}{p}\in R$. מכאן נקבל $\mathbb{Z}\left[\frac{1}{p}\right]\subseteq R$, כלומר $R=\mathbb{Z}\left[\frac{1}{p}\right]$.

ב. אם $m\mid n$ אז $n=mk$ לאיזשהו $k\in\mathbb{Z}$, ולכן $\frac{1}{m}=k\cdot\frac{1}{n}\in\mathbb{Z}\left[\frac{1}{n}\right]$.
מצד שני, אם נניח בנוסף $\mathbb{Z}\left[\frac{1}{n}\right]=\mathbb{Z}\left[\frac{1}{m}\right]$ נקבל $\frac{1}{n}\in\mathbb{Z}\left[\frac{1}{m}\right]$, כלומר $\frac{1}{n}=\frac{t}{m^k}$, ולכן $n\mid m^k$, בסתירה.

ג. צריך לקחת סדרת מספרים שמחלקים אחד את השני: למשל,

$$\mathbb{Z}\subsetneq\mathbb{Z}\left[\frac{1}{2}\right]\subsetneq\mathbb{Z}\left[\frac{1}{4}\right]\subsetneq\cdots\subsetneq\mathbb{Q}.$$

אף אחד מהם לא שווה ל-$\mathbb{Q}$ כי בכולם 3 לא הפיך.

שאלה 5. תנו דוגמה לתחום אוקלידי R עם פונקציה אוקלידית d ואיברים a,b המקיימים $d(a)=d(b)$, אבל $\langle a\rangle\neq\langle b\rangle$.

פתרון. אפשר לבחור $R = \mathbb{Q}[x]$ שהוא אוקלידי עם הפונקציה של הדרגה. נבחר $a = x$ ו-$b = x + 1$ שהם בודאי מאותה דרגה, אבל $\langle a \rangle \neq \langle b \rangle$ כי הם לא חברים.

שאלה 6. חשבו בעזרת אלגוריתם אוקלידס את מחלק משותף מקסימלי $(f(x), g(x))$ של זוגות האיברים הבאים. אפשר לבחור שהוא יהיה פולינום מתוקן.

א. $f(x) = x^2 + x + 1$, $g(x) = x^3 - 2x^2 + x + 4$ בחוג $\mathbb{Q}[x]$.

ב. $f(x) = x^3 + 2x^2 + 3x - 3$, $g(x) = x^2 - 1$ בחוג $\mathbb{F}_5[x]$.

פתרון.

א. נבצע שלושה שלבים באלגוריתם אוקלידס, ושימו לב שהשלב האחרון מייד מראה שמדובר בשארית 0:

$$\begin{aligned} x^3 - 2x^2 + x + 4 &= \left(x^2 + x + 1\right) \cdot (x - 3) + (3x + 7) \\ x^2 + x + 1 &= (3x + 7) \cdot \left(\frac{1}{3}x - \frac{4}{9}\right) + \frac{37}{9} \\ 3x + 7 &= \frac{37}{9} \cdot \left(\frac{27}{37}x + \frac{63}{37}\right) + 0 \end{aligned}$$

ולכן הפולינומים זרים, כלומר $(f(x), g(x)) = 1$.

ב. הפעם נדרשים רק שני שלבים:

$$\begin{aligned} x^3 + 2x^2 + 3x - 3 &= \left(x^2 - 1\right) \cdot (x + 2) + (4x - 1) \\ x^2 - 1 &= (4x - 1) \cdot (4x + 1) + 0 \end{aligned}$$

ולכן בחוג $\mathbb{F}_5[x]$ מתקיים כי הפולינום המתוקן שאנו מחפשים הוא

$$(f(x), g(x)) = 4^{-1} \cdot (4x + 1) = 4 \cdot (4x + 1) = x - 4 = x + 1$$

שאלה 7. יהי R תחום שלמות, ותהי פונקציה $d : R \to \mathbb{N} \cup \{0, -\infty\}$ המקיימת $d(0) < d(x)$ לכל $x \neq 0$.

נניח שהיא מקיימת את התנאי הראשון שראינו בכיתה לאוקלדיות: לכל $b \neq 0$ ולכל a קיימים $q, r \in R$ כך ש-$a = qb + r$ וגם $d(r) < d(b)$.

הפונקציה לא בהכרח מקיימת את התנאי השני: אם $a|b$, אז $d(a) \leq d(b)$. הוכיחו שבמקרה זה R הוא עדין תחום אוקלידי. הדרכה: הראו שהפונקציה

$$\delta(a) = \min\{d(ax) \mid 0 \neq x \in R\}$$

היא פונקציה אוקלידית. במילים: $\delta(a)$ שווה לערך המינימלי של d מבין האיברים שאינם אפס באידאל $\langle a \rangle$.

פתרון. אנחנו צריכים להוכיח שלוש דרישות:

- $\delta(0) < \delta(x)$ לכל $x \neq 0$: ברור מההגדרה.
- חילוק עם שארית: יהיו $a, b \in R$ כך ש-$b \neq 0$. ניקח $0 \neq x \in R$ כך ש-$d(bx)$ מינימלי (כלומר $\delta(b) = d(bx)$). אפשר לחלק עם שארית את a ב-bx ביחס ל-d המקורית ולקבל

$$a = q(bx) + r$$

כאשר $d(r) \leq d(bx) = \delta(b)$. אבל $\delta(r) \leq d(r)$, לכן נקבל $\delta(r) \leq \delta(b)$, כנדרש.

- אם $a \mid b$, אז $\delta(a) \leq \delta(b)$: אם $a \mid b$ אז $\langle b \rangle \subseteq \langle a \rangle$. לכן המינימום בחישוב של $\delta(b)$ נלקח על פחות איברים מאשר בחישוב של $\delta(a)$, כלומר $\delta(a) \leq \delta(b)$.

שאלה 8. העשרה: קראו את המאמר "חוגי שברים בדרך הקשה" מאת ז'וזה פליפה ולוש ובדקו שזה למעשה יותר קל.

בהצלחה!