פתרון תרגיל 7

יאיר אוגש ועידןריין

7 במאי 2018

שאלה 2.

נוכיח כי R הוא חוג מקומי בכך שנוכיח ש $R \setminus R^\times$ הוא אידיאל.
R הוא תת חוג של חוג המטריצות עם איברים מהשדה, לכן איבר בחוג R הפיך אם ורק אם הדטרמיננטה שלו היא אפס. לכן לכל איבר בחוג R, הדטרמיננטה היא a^3. מכיוון שF הוא שדה, $a^3 = 0$ אם ורק אם $a = 0$. לכן:

$$R \setminus R^\times = \{r \in R \big| det(r) = 0\} = \left\{ \begin{pmatrix} 0 & B & C \\ 0 & 0 & D \\ 0 & 0 & 0 \end{pmatrix} \Bigg| b, c, d \in F \right\}$$

מההצגה לעיל ברור ש־ $R \setminus R^\times$ הוא תת חבורה חיבורית של R. כדי לסיים, עלינו להוכיח שלכל $r \in R$, $a \in R \setminus R^\times$, מתקיים ש־ $ar, ra \in R \setminus R^\times$. אבל, ידוע שהדטרמיננטה של מטריצות היא כפלית לכן $det(ar) = det(ra) = det(r) * det(a) = det(r) * 0 = 0$. $det(ar) = det(ra) = 0$ ולפיכך מתקיים ש־ $ar, ra \in R \setminus R^\times$. לכן, $R \setminus R^\times$ הוא אידיאל ולכן R הוא חוג מקומי.

שאלה 3.

צריך להראות ששדה השברים של $Z[\sqrt{D}]$ הוא $Q[\sqrt{D}]$
אם D לא חופשי מריבועים אז $\sqrt{D} = m * \sqrt{D_2}$ כאשר D_2 חפשי מריבועים או 1 ומתקיים $q(Z[\sqrt{D}]) = q(Z[\sqrt{D_2}])$ כי $1/m \in q(Z[\sqrt{D}])$
אם D_2 הוא 1 אז $Z[\sqrt{D}] = Z[\sqrt{D_2}] = Z, Q[\sqrt{D}] = Q[\sqrt{D_2}] = Q$ וידוע ששדה השברים של Z הוא Q ולכן במקרה זה שדה השברים של $Z[\sqrt{D}]$ הוא $Q[\sqrt{D}]$
כעת בה"כ D חפשי מריבועים ולכל $a + b\sqrt{D} \in Z[\sqrt{D}]$ יש הפיך שהוא $\frac{1}{a^b - b^2 D} * a - b\sqrt{D}$ שהוא ב $Q[\sqrt{D}]$ ולכל $x \in Q[\sqrt{D}]$ מתקיים $x = \frac{a}{b} + \frac{c}{d} * \sqrt{D} = \frac{ad + bc\sqrt{D}}{bd}$ שנמצא בשדה השברים של $Z[\sqrt{D}]$
ומהכלות אלה קיבלנו ששדה השברים של $Z[\sqrt{D}]$ הוא $Q[\sqrt{D}]$

שאלה 4.

א.

יהי $x \in R$, R תחום הערכה. כדי להוכיח R חוג מקומי, נוכיח ש־ x או $1 - x$ חייבים להיות הפיכים. אם $x = 0, 1$ אז אחד מהם הוא היחידה 1 ולכן בפרט הפיך כדרוש. אחרת, נניח $x, 1 - x \neq 0$.לפי הגדרת F כשדה שברים, $x * (1 - x)^{-1} \in F^\times$. בגלל ש־ R תחום הערכה, $x * (1 - x)^{-1} \in R$ או $x^{-1} * (1 - x) \in R$. נקרא לערך הזה $r \in R$. אזי $x = r * (1 - x)$ או $1 - x = r * x$. אם $x = r * (1 - x)$, אז $1 - (1 - x) = r * (1 - x)$ ואז $1 = (r + 1) * (1 - x)$, לכן $1 - x$ הוא הפיך . אם $1 - x = r * x$ אז $1 = (r + 1) * x$ ולכן x הפיך.
לסיכום, הראנו שלכל $x \in R$, $x \in R^\times$ או $1 - x \in R^\times$, לכן R חוג מקומי.

ב.

יהיו $R \triangleleft I, J$ אידיאלים בתחום הערכה. נניח בלי הגבלת הכלליות שקיים $r \in I \setminus J$ וכעת נוכיח ש־ $J \subset I$. יהי $j \in J$. $0 \in I, J$ לפי הגדרת האידיאל כתת חבורה חיבורית ולכן $r \neq 0$.
אם $j = 0$, אז ראינו כבר ש־ $j \in I$. אם $j \neq 0$, אז לפי הגדרת F כשדה שברים, $\frac{r}{j} \in F^\times$.
לכן, בגלל ש־ R תחום הערכה, $\frac{r}{j} \in R$ או $\frac{j}{r} \in R$. נקרא לערך הזה $a \in R$. אם $\frac{r}{j} = a$, אז $r = j * a$. אבל, מכיוון ש־ J הוא אידיאל ב־ R, $r = ja \in J$ אבל הנחנו ש־ $r \notin J$.
לכן, האפשרות השנייה חייבת לקרות: $\frac{j}{r} = a$. אבל אז, $j = ra$ ובגלל ש־ I אידיאל ב־ R, $j = ra \in I$.
לסיכום, הוכחנו שאם קיים $r \in I \setminus J$, אז $J \subset I$ ומכאן נובע הדרוש.
בכיוון ההפוך, נניח שהאידיאלים של R מסודרים בשרשרת, כלומר שלכל $I, J \triangleleft R$, $I \subseteq J$ או $J \subseteq I$. לפי הגדרת שדה השברים F שקיים כי לכל תחום שלמות מובטח שקיים שדה שברים, לכל $x \in F^\times$ קיימים $a, b \in R \setminus \{0\}$ כך ש־ $x = a * b^{-1}$. נתבונן ב־ $\langle a \rangle, \langle b \rangle \subset R$. אלו שני אידיאלים ב־ R ולכן לפי ההנחה, $\langle a \rangle \subseteq \langle b \rangle$ או $\langle a \rangle \supseteq \langle b \rangle$. אם $\langle a \rangle \subseteq \langle b \rangle$, אז $a \in \langle b \rangle$, לכן קיים $r \in R$ כך ש־ $a = r * b$. לכן, $x = a * b^{-1} = (rb)b^{-1} = r \in R$, כלומר $x \in R$.
מצד שני, אם $\langle a \rangle \supseteq \langle b \rangle$, אז $b \in \langle a \rangle$, לכן קיים $r \in R$ כך ש־ $b = r * a$. נשים לב ש־ $x^{-1} = b * a^{-1} = r * a * a^{-1} = r \in R$, כלומר $x^{-1} \in R$.
לסיכום, הראינו שלכל $x \in F^\times$, $x \in R$ או $x^{-1} \in R$. לכן, R הוא תחום הערכה והוכחנו הדרוש.

שאלה 5.

א.

נניח R חוג כך ש $Z \subset R \subseteq Z[\frac{1}{p}]$ ונראה $R = Z[\frac{1}{p}]$
קיים $x \in R$ כך ש $x \in Z[1/p] \setminus Z$
לכן $x = \frac{a}{b}$ כאשר $p \mid b$ ו $p \nmid a$ ונכתוב $b = pk$
מסגירות R לכפל נקבל $kx = \frac{ka}{b} = \frac{a}{p} \in R$
p, a זרים כי p ראשוני שאינו מחלק את a ולכן קיימים q, r כך ש $qp + ra = 1$
ומסגירות R לכפל ולחיבור נקבל ש $\frac{1}{p} = \frac{ra+qp}{p} = \frac{ra}{p} + q = rx + q \in R$
סך הכל $R \subseteq Z[\frac{1}{p}]$ ולכן מהכלה דו כיוונית הם שווים

ב.

נניח $n \mid m$ ונראה $\frac{1}{m} \in Z[\frac{1}{n}]$
קיים $s \in Z$ כך ש $n = ms$
לכן מהגדרת שברים $\frac{1}{m} = \frac{s}{n} = s\frac{1}{n} \in Z[\frac{1}{n}]$ ומתקבל $Z[\frac{1}{m}] \subseteq Z[\frac{1}{n}]$
נניח כעת $\forall k : n \nmid m^k$ נראה ש $\frac{1}{n} \notin Z[\frac{1}{m}]$ ולכן $Z[\frac{1}{n}] \neq Z[\frac{1}{m}]$
נניח בשלילה ש $\frac{1}{n} \in Z[\frac{1}{m}]$ ולכן $\frac{1}{n} = \frac{a}{m^k}$ וקיבלנו ש $na = m^k$ בסתירה לכך ש $n \nmid m^k$

ג.

נבחר n_i להיות מכפלת i האיברים הראשוניים ומסעיף קודם נובע ש $Z[\frac{1}{n_i}] \subset Z[\frac{1}{n_{i+1}}]$
וכל אחד מאלה שונה מQ כי אין הפכי למספר הראשוני הבא

שאלה 6

א.

ניזכר ש־ N כפלי, כלומר שמתקיים $N(\alpha * \beta) = N(\alpha) * N(\beta)$ לכל $\alpha, \beta \in \mathcal{O}_D$. יהי $s \in \mathcal{O}_D^\times$, לכן קיים s^{-1} כך ש־ $s * s^{-1} = 1$ ולכן הנורמה שלו מקיימת $N(s) * N(s^{-1}) = N(s * s^{-1}) = N(1) = 1$ ומכיוון שהנורמה היא מספר שלם נקבל ש־ $N(s)$ הפיך ב־ $\mathbb{Z}$ ולכן $N(s) = \pm 1$.
לכן, אם $x \sim y$ אז לפי ההגדרה קיים $s \in \mathcal{O}_D^\times$ כך ש־ $x = s * y$ ולכן מכפליות הנורמה נקבל את הדרוש: $N(x) = N(s * y) = N(s) * N(y) = \pm N(y)$

ב.

נפריד אם ניקח $D = 3, x = 1 + \sqrt{3}, y = 2$. מתקיים $N(x) = N(y) = 4$, אבל הם לא חברים כי אם נניח בשלילה שכן אז קיים $s \in \mathcal{O}_3$ כך ש־ $s * 2 = 1 + \sqrt{3}$ אבל מהגדרת $\mathcal{O}_3$ זה אומר שקיימים $a, b \in \mathbb{Z}$ כך ש־ $(a + b\sqrt{3}) * 2 = 1 + \sqrt{3}$ ואז נקבל: $a * 2 = 1, b * 2 = 1$ ואין למשוואות האלו פתרון ב־ $\mathbb{Z}$ ולכן הם לא חברים, ומצאנו הפרכה כדרוש