פתרון תרגיל בית 5 מבוא לחוגים ומודולים 88-212
סמסטר ב׳ תשע״ח

23 באפריל 2018

שאלה 1. יהי R חוג ויהי $P \lhd R$ אידאל.

(א ⇐ ב) P ראשוני. יהיו $a,b \in R$ כך ש $\langle a\rangle\langle b\rangle \subseteq P$. מראשוניות P נקבל ש: $\langle a\rangle \subseteq P$ או $\langle b\rangle \subseteq P$ ולכן $a \in P$ או $b \in P$.

(ב ⇐ ג) יהיו $A,B \leq_\ell R$ אידאלים שמאליים כך ש $AB \subseteq P$. נניח בשלילה ש $A,B \nsubseteq P$, אז קיימים $a \in A, b \in B$ כך ש $a,b \notin P$. Ra ו Rb הם האידאלים השמאליים הנוצרים על ידי a ו b. נשים לב שאיבר כללי מהאידאל השמאלי $RbRa$ הוא מהצורה: $\alpha_1 a\beta_1 b + \cdots + \alpha_k a\beta_k b$. לכן איבר כללי מהאידאל $\langle RbRa\rangle$ יהיה מהצורה $\alpha_1 a\beta_1 b\gamma_1 + \cdots + \alpha_k a\beta_k b\gamma_k$. אבל זה בדיוק איבר כללי מהאידאל $\langle a\rangle\langle b\rangle$. כלומר קיבלנו: $\langle a\rangle\langle b\rangle = \langle RbRa\rangle$. עכשיו בגלל ש $Ra \subseteq A$ וגם $Rb \subseteq B$ אז $RbRa \subseteq AB$ אך $AB \subseteq P$ ו P הוא אידאל לכן $\langle a\rangle\langle b\rangle = \langle RbRa\rangle \subseteq P$. מסעיף (ב): $a \in P$ או $b \in P$, בסתירה.

(ג ⇐ ד) מאוד דומה לשלב הקודם. יהיו $A,B \leq_r R$ אידאלים ימניים כך ש $AB \subseteq P$. נניח בשלילה ש $A,B \nsubseteq P$, אז קיימים $a \in A, b \in B$ כך ש $a,b \notin P$. ע״י הסתכלות על האיבר הכללי נקבל: $\langle a\rangle\langle b\rangle = \langle bRaR\rangle$ ונסיק: $\langle a\rangle\langle b\rangle = \langle bRaR\rangle \subseteq P$. $\langle a\rangle, \langle b\rangle$ הם אידאלים ובפרט אידאלים שמאליים לכן מסעיף (ג) $\langle a\rangle \subseteq P$ או $\langle b\rangle \subseteq P$ ולכן $a \in P$ או $b \in P$, בסתירה.

(ד ⇐ א) (ד) הוא בעצם תנאי יותר חזק מ (א) כי כל אידאל הוא בפרט אידאל ימני, לכן ברור וסיימנו.

שאלה 2. א. ברור שזאת תת חבורה. נראה שזה אידאל: יהיו $(a,b) \in R \times R$, $(x,0) \in R \times \{0\}$. אז $(x,0)(a,b) = (xa,0) \in R \times \{0\}$ וגם $(a,b)(x,0) = (ax,0) \in R \times \{0\}$. נראה שהוא ראשוני. יהיו אידאלים $A,B \lhd R \times R$ כך ש $AB \subseteq R \times \{0\}$ נניח שקיימים $a \in A$, $b \in B$ כך ש $a,b \notin R \times \{0\}$ אבל $a \cdot b \in R \times \{0\}$. נסמן $a = (a_1,a_2)$, $b = (b_1,b_2)$. אז: $a_2b_2 = 0 \Leftarrow ab = (a_1b_1, a_2b_2) \in R \times \{0\}$ אבל R תחום שלמות לכן אין מחלקי אפס ולכן $a_2 = 0$ או $b_2 = 0$. כלומר $a \in R \times \{0\}$ או $b \in R \times \{0\}$, בסתירה.

ב. שתי דוגמאות: יהי $n \in \mathbb{N}$, נשים לב שהאידאלים הראשוניים היחידים של $(\mathbb{Z}_2)^n$ הם תתי קבוצות שבכל רכיב יש את כל $\mathbb{Z}_2$ פרט לרכיב אחד שם יש $\{0\}$. סך הכל יש n אידאליים ראשוניים. אפשרות אחרת היא לקחת את $\mathbb{Z}_{2^n}$. כל תתי החבורות איזומורפיים ל $\mathbb{Z}_{2^k}$ עבור $1 \leq k \leq n$ או לחבורה הטריוויאלית. קל לבדוק שכל תתי החבורות הם גם אידאלים ראשוניים אז אם לא מחשיבים את האידאל שהוא כל החוג נקבל בדיוק n אידאלים ראשוניים.

שאלה 3. $I \lhd S$ ראשוני. יהיו $I \lhd S$ הומ'. f כי $f^{-1}(I)$ אידאל לכן גם $A, B \lhd R$ אידאלים. נראה ש $f(AB) = f(A)f(B)$. איבר כללי של $f(A)f(B)$ נראה מהצורה

$$f(a_1)f(b_1) + \cdots + f(a_n)f(b_n)$$

כאשר $a_i \in A,\ b_i \in B$. מצד שני איבר כללי של $f(AB)$ הוא הפעלה של f על איבר כללי של AB כלומר

$$f(a_1b_1 + \cdots + a_nb_n) = f(a_1)f(b_1) + \cdots + f(a_n)f(b_n)$$

עבור $a_i \in A, b_i \in B$ כלליים. לכן יש שוויון. עכשיו, אם $AB \subseteq f^{-1}(I)$ אז $f(A)f(B) \subseteq I$ אבל $f(A), f(B) \lhd S$ לכן מראשוניות I מתקיים $f(A) \subseteq I$ או $f(B) \subseteq I$. מכאן ש $A \subseteq f^{-1}(I)$ או $B \subseteq f^{-1}(I)$ וסיימנו.

במקרה הפרטי ש R הוא תת חוג של S יחד עם $id : R \hookrightarrow S$ הומ' ההכלה הטבעי, נקבל שאם $I \lhd S$ הוא אידאל ראשוני, אז $R \cap I = i^{-1}(I) \lhd R$.

שאלה 4. יהי R חוג. יהיו $I, J \lhd R$ אידאלים נאותים, מקסימליים ושונים. מתקיים $IJ \subseteq I \cap J$. לא ייתכן $J \subseteq I$ או $I \subseteq J$ כי I, J מקסימליים. לכן $I \cap J \not\subseteq I$ וגם $I \cap J \not\subseteq J$ ולכן $I \cap J$ לא ראשוני.

שאלה 5. יהי R חוג חילופי. יהיה I אידאל ראשוני של R. יהי $a \in R$. נראה באינדוקציה שאם קיים $n \in \mathbb{N}$ כך ש $\langle a \rangle^n \subseteq I$ אז $a \in I$. עבור $n = 1$, $\langle a \rangle \subseteq I$ גורר $a \in I$. נניח שזה נכון עבור $n - 1$. $\langle a \rangle^n = \langle a \rangle^{n-1} \langle a \rangle \subseteq I$ לכן $\langle a \rangle \subseteq I$ או $\langle a \rangle^{n-1} \subseteq I$ אבל שני המקרים גוררים $a \in I$, אז סיימנו. עכשיו אם $a \in I$ נילפוטנטית, אז קיים $n \in \mathbb{N}$ כך ש $a^n = 0$. נשים לב שבגלל ש R חוג קומוטטיבי אז בכל איבר של $\langle a \rangle^n$ אפשר להוציא את $a^n = 0$ בתור גורם כפלי ולכן $\langle a \rangle^n = \{0\}$. ברור ש $\langle a \rangle^n = \{0\} \subseteq I$ ולכן $a \in I$.

שאלה 6. א. תהי $\{M_i\}_{i \in I}$ משפחה של מונואידים. נראה:

$$U(\prod_i M_i) = \prod_i U(M_i)$$

יהי $a \in \prod_i M_i$ איבר הפיך. a מורכב מרכיבים a_i. a הפיך משמעותו שכל a_i הפיך ב M_i. לכן $a \in \prod_i U(M_i)$. מצד שני, יהי $a \in \prod_i U(M_i)$. a מורכב מרכיבים a_i כך שקיימים a_i^{-1} ב M_i. הכפל של $\prod_i M_i$ הוא רכיב רכיב לכן a^{-1}המורכב מכל ה a_i^{-1} הוא בדיוק איבר הופכי של a. לכן $a \in U(\prod_i M_i)$.

ב. ניזכר ש $U(\mathbb{Z}_n) = u_n$ כאשר $\mathbb{Z}_n$ הוא מונואיד עבור כפל נציגים רגיל. לכן מסעיף (א):

$$U(\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}) = u_{m_1} \times \cdots \times u_{m_k}$$

$\{m_1, \ldots, m_k\}$ קו מקסימליים בזוגות. לכן ממשפא השאריות הסיני קיים הומ' של חוגים על:

$$f : \mathbb{Z} \twoheadrightarrow \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$$

כך שהגרעין של f הוא $\mathbb{Z}_{m_1\cdots m_k}\mathbb{Z}$ כלומר $\mathbb{Z}_{(m_1\cdots m_k)}$. ממשפט איזו' 1:

$$\frac{\mathbb{Z}}{_{(m_1\cdots m_k)}\mathbb{Z}} \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$$

לכן

$$u_n = U(\mathbb{Z}_n) = U(\frac{\mathbb{Z}}{_n\mathbb{Z}}) = U(\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k})$$

ומכאן

$$u_n = u_{m_1} \times \cdots \times u_{m_k}$$

ג. מסעיף (ב) ישר נקבל:

$$\varphi(n) = |u_n| = |u_{m_1} \times \cdots \times u_{m_2}| = \varphi(m_1)\cdots\varphi(m_k)$$

כאשר $m_i = p_i^{s_i}$. ואז

$$\varphi(m_i) = p_i^{s_i-1}(p_i - 1)$$

לכן:

$$\varphi(n) = p_1^{s_1-1}(p_1 - 1)\cdots p_t^{s_t-1}(p_t - 1)$$