פתרון תרגיל בית 2 אלגברה מופשטת 2

1. האם קיים הומומורפיזם (לאו דוקא אוניטרי) $\varphi:\mathbb{Z}_n\to\mathbb{Z}_m$ כאשר:

(א) $m|n$

כן. הפונקציה $a\mapsto a \pmod m$ מוגדרת היטב במקרה זה והיא הומומורפיזם. היא מוגדרת היטב כי $a+n\mapsto (a+n) \pmod m = a \pmod n$ שכן $n\equiv 0 \pmod m$.

(ב) $n|m$ ו $n\neq m$.

נשים לב שבשביל שיהיה הומומורפיזם כזה, הפונקציה צריכה לקיים $n\varphi(1)\equiv 0$ וש$\varphi(1)^2=\varphi(1)$. (זה יקבע את כל הפונקציה, וגם יוודא שהיא הומומורפיזם- למה?).
נשאר לנו לברר מתי יש איבר כזה ב$\mathbb{Z}_m$:
נתחיל מהדרישה ש$\varphi(1)^2=\varphi(1)$ כלומר צריך אידמפוטנט ב$\mathbb{Z}_m$:
נניח שהפירוק לראשוניים של m הוא $p_1^{d_1}p_2^{d_2}\cdots p_k^{d_k}$
ונשים לב שאם $x^2-x\equiv 0 \pmod m$ אז $x^2-x\equiv 0 \mod p_i^{d_i}$ לכל i.
אבל ל x ו $x-1$ יש גורמים ראשוניים שונים ולכן או ש $x\equiv 0 \mod p_i^{d_i}$ או ש $x\equiv 1 \mod p_i^{d_i}$. ולכן עבור כל p_i צריך או להתחלק ב $p_i^{d_i}$ או להיות זר לו.

עכשיו נוסיף את הדרישה ש$n\varphi(1)\equiv 0 \pmod m$:
נניח שאיזשהו $p_i^{d_i}|n$. נסמן $m'=\frac{m}{p_i^{d_i}}$ ונשים לב ש $m'\equiv 1 \mod p_i^{d_i}$ כי הם זרים. נקבע ש$\varphi(1)=m'$. מתקיים ש$n\varphi(1)=nm'\equiv 0$ כי $m|nm'$. וכמו כן $m'^2-m'\equiv 0 \pmod m$ כי $\varphi(1)^2-\varphi(1)=m'^2-m'$ וגם $m'|(m'^2-m')$ ולכן ביחד $p_i^{d_i}|m'^2-m'$ מה שאומר ש $m'^2-m'\equiv 1^2-1=0 \mod p_i^{d_i}$ נקבל ש $m|m'^2-m'$.

נניח כעת שאין גורם כזה. אזי במקרה כזה הדרישה $m|n\varphi(1)$ מכריחה אותנו ש $p_i|\varphi(1)$ לכל i, אבל אז $\varphi(1)\not\equiv 1 \mod p_i^{d_i}$ (כי הם לא זרים) ולכן בהכרח

$\varphi(1) \equiv 0 \mod p_i^{d_i}$ לכל i אבל אז יוצא ש $\varphi(1) \equiv 0 \pmod m$. כלומר קיבלנו שההומומורפיזם היחידי במקרה כזה זה הומומורפיזם האפס.

2. רשמו את ההומומורפיזם (עם יחידה) היחיד $\mathbb{Z} \to M_2(\mathbb{Z}_n)$. כמה הומומורפיזמים (עם יחידה) יש $\varphi: \mathbb{Z}\left[\sqrt{2}\right] \to M_2(\mathbb{Z}_2)$?

יחידה חייבת לעבור ליחידה ולכן $1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

מפה מוכרח ש $k \mapsto \begin{pmatrix} k \pmod n & \\ & k \pmod n \end{pmatrix}$ (למה?).

השיקול הנ"ל נכון גם ל $\varphi: \mathbb{Z}\left[\sqrt{2}\right] \to M_2(\mathbb{Z}_2)$

נשאר לקבוע רק מהו התמונה של $\varphi\left(\sqrt{2}\right)$, כלומר צריך איבר ב$M_2(\mathbb{Z}_2)$ שהריבוע שלו הוא $\begin{pmatrix} 2 & \\ & 2 \end{pmatrix} = 0$.

חישוב פשוט נותן שאלו הן המטריצות $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

ולכן יש 4 הומומורפיזמים.

3. הבאים הם כולם תת-חוגים של $\mathbb{Z} \times \mathbb{Z}$, מי מהם אידיאל?

(א) $\Delta = \{(a,a) \mid a \in \mathbb{Z}\}$

לא אידיאל. כי למשל למרות ש $(1,1) \in \Delta$, $(1,2)(1,1) = (1,2) \notin \Delta$.

(ב) $\{(2a,3b) \mid a,b \in \mathbb{Z}\}$

אידיאל. קל להשתכנע שזו תת-חבורה חיבורית. ולכל $(m,n) \in \mathbb{Z}\times\mathbb{Z}$ מתקיים $(m,n)(2a,3b) = (2ma,3nb)$ שייך לאידיאל.

למעשה, זהו האידיאל $2\mathbb{Z} \times 3\mathbb{Z}$.

(ג) $\{(2a,0) \mid a \in \mathbb{Z}\}$

זהו אידיאל. באופן דומה לסעיף הקודם. למעשה זהו האידיאל $2\mathbb{Z} \times \{0\}$ (ראו את השאלה הבאה).

(ד) $\{(a,-a) \mid a \in \mathbb{Z}\}$

לא אידיאל. למשל $(1,-1)$ נמצא שם, אבל $(1,0)(1,-1) = (1,0)$ לא נמצא שם.

4. יהיו R_1, R_2 חוגים, $I_i \lhd R_i$ אידיאלים.

(א) הוכיחו כי $I_1 \times I_2 \lhd R_1 \times R_2$.

אנחנו יודעים ממופשטת 1 שזו תת-חבורה חיבורית.

נראה בליעה: $(r_1,r_2)(i_1,i_2)=(r_1i_1,r_2i_2)$. ומכיוון ש $r_ii_i\in$ אידיאלים I_i ולכן המכפלה שייכת ל $I_1\times I_1$.

(ב) $I=R_1\times\{0\}$ ו $J=\{0\}\times R_2$ הם אידיאלים המקיימים $I+J=R_1\times R_2$, $IJ=JI$ ו $IJ=I\cap J=\{0\}$.
ברור ש $I_1+I_2\subseteq R_1\times R_2$, עבור $(r_1,r_2)\in R_1\times R_2$
מתקיים $(r_1,r_2)=(r_1,0)+(0,r_2)\in I_1+I_2$ ולכן זהו שיוויון.
כמו כן, $(r_1,0)(0,r_2)=(0,r_2)(r_1,0)=(0,0)$ ולכן $IJ=IJ=0$.
וגם ברור שהחיתוך הוא אפס.

5. הוכיחו כי אם $\{A_i\}_{i\in I}$ שרשרת של אידיאלים, אזי $\cup A_i$ הוא אידיאל.
פתרון:
יהיו $a,b\in\cup A_i$ אזי יש $i,j\in I$ כך ש $a\in A_i$ ו $b\in A_j$. מכיוון ש $\{A_i\}_{i\in I}$ זה שרשרת, יש $k\in I$ כך ש $A_i,A_j\subseteq A_k$ ונקבל ש $a,b\in A_k$ ואז $a\pm b\in A_k\subseteq\cup A_i$.
כעת נראה בליעה: יהי $r\in R$ ו $a\in\cup A_i$, אזי $a\in A_i$ לאיזשהו $i\in I$. A_i אידיאל ולכן $ra\in A_i\subseteq\cup A_i$.

6. יהיו I,J,K אידיאלים של חוג מסוים.

(א) הוכיחו: $I(J+K)=IJ+IK$
$\supseteq$: $J,\ K\subseteq J+K$ ולכן $IJ,\ IK\subseteq I(J+K)$ ולכן $IJ+IK\subseteq I(J+K)$
(כי סכום אידיאלים הוא האידיאל המינימלי שמכיל אותם).
$\subseteq$: מספיק להראות שכל איבר מהצורה $i(j+k)$ נמצא ב $IJ+IK$ (למרות שזה לא האיבר הכללי שם, ודאו שאתם מבינים זאת.) מחוק הפילוג ברור ש $i(j+k)=ij+ik\in IJ+IK$.

(ב) אם $I\subseteq J$ הוכיחו $J\cap(I+K)=I+(J\cap K)$.
$\supseteq$: $I\subseteq J\cap(I+K)$ וגם $J\cap K\subseteq J\cap(I+K)$ ולכן $I+(J\cap K)\subseteq J\cap(I+K)$.
$\subseteq$: איבר כללי הוא מהצורה $i+j$ כאשר $i\in I$ ו $j\in J\cap K$. אז מצד אחד, מכיוון ש $j\in K$ אז $i+j\in I+K$. ומצד שני, מכיוון ש $I\subseteq J$ אז $i\in J$. $i+j\in J$ ולכן $i+j\in J\cap(I+K)$.

7. יהי חוג R. $A\subseteq R$ תת-קבוצה.

(א) המאפס השמאלי של A בחוג הוא הקבוצה
$Ann_l(A)=\{x\in R\,|\,xa=0\ \forall a\in A\}$ הוכיחו שזהו אידיאל שמאלי.
הקבוצה לא ריקה כי $0\in Ann_l(A)$.
סגירות לחיבור היא ברורה.
יהי $r\in R$ ו $x\in Ann_l(A)$, אזי לכל $a\in A$ $rxa=r(xa)=r0=0$ ולכן $rx\in Ann_l(A)$.

(ב) נניח A הוא אידיאל שמאלי של R, הוכיחו כי $Ann_l(A)$ הוא אידיאל (דו"צ).
יהי $r \in R$ ו $x \in Ann_l(A)$, אזי לכל $a \in A$ $xra = x(\underbrace{ra}_{\in A}) = 0$ ולכן $xr \in Ann_l(A)$.

(ג) הוכיחו כי עבור תת-קבוצות $A, B \subseteq R$ המכילות את 0 מתקיים $Ann_l(A+B) = Ann_l(A) \cap Ann_l(B)$.
מכיוון ש$A, B \subseteq A+B$ (זה נכון כי הן מכילות את אפס)
אז ברור ש $Ann_l(A+B) \subseteq Ann_l(A) \cap Ann_l(B)$.
מצד שני, אם $x \in Ann_l(A) \cap Ann_l(B)$ אז עבור $a+b \in A+B$ מתקיים $x(a+b) = xa + xa = 0$ ולכן $x \in Ann_l(A+B)$.

8. יהי R חוג קומוטטיבי. נאמר שאיבר $x \in R$ הוא נילפוטנטי אם $x^n = 0$ לאיזשהו $n \in \mathbb{N}$.

(א) הוכיחו שקבוצת כל האיברים הנילפוטנטים היא אידאל שנסמנו ב$\mathcal{N}$.
זה לא קבוצה ריקה כי 0 נילפוטנטי.
עבור $x, y \in \mathcal{N}$ כאשר $x^n = y^m = 0$,
מכיוון שהחוג קומוטטיבי $(x+y)^{n+m} = \sum \binom{n+m}{k} x^k y^{n+m-k}$
בכל מחובר או ש$k \geq n$ או ש $n+m-k \geq m$ ובכל מקרה זה יוצא אפס. ולכן $x+y \in \mathcal{N}$.
יהי $r \in R$, אזי מכיוון שהחוג קומוטטיבי $(rx)^n = r^n x^n = 0$ ולכן $rx \in N$.

(ב) תנו דוגמא לחוג לא קומוטטיבי שבו קבוצת האיברים הנילפוטנטים הוא לא אידיאל.
למשל ב $M_2(\mathbb{R})$ המטריצות $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ ו $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ הן נילפוטנטיות, אך סכומן לא (ולכן אין סגירות לחיבור).

9. יהי R תחום ויהיו $a, b \in R$. הוכיחו כי $Ra = Rb$ אם"ם $a = ub$ כאשר $u \in R$ איבר הפיך.
$\Leftarrow$ לפי הנתון $a \in Rb$ כלומר ש$a = rb$. מצד שני $b \in Ra$ ולכן $b = r'a$. אם כן, $a = rr'a$ אבל R הוא תחום ולכן $rr' = 1$.
$\Rightarrow$ אם $a = ub$ אז ברור ש $Ra \subseteq Rb$, ומכיוון שu הפיך אפשר לרשום $b = u^{-1}a$ מה שאומר ש$Rb \subseteq Ra$.