אלגברה מופשטת 2 – תרגיל כיתה 5

מתרגלים: ד"ר אפי כהן ואדם צ'פמן.

הגדרה

יהי R חוג קומוטטיבי, $I \lhd R$. הרדיקל של I הוא: $\sqrt{I} = \left\{ x \in R \middle| \exists n \in \mathbb{N} : x^n \in I \right\}$

מההגדרה נובע באופן מיידי ש $I \subseteq \sqrt{I}$. אם $I = \sqrt{I}$ אז I נקרא אידיאל רדיקלי.

טענה

יהי $I \lhd R$ אידיאל ראשוני בחוג קומוטטיבי R אז I אידיאל רדיקלי.

פתרון

צ"ל $I = \sqrt{I}$, מכיוון ש $I \subseteq \sqrt{I}$ מספיק להוכיח ש $\sqrt{I} \subseteq I$. יהי $x \in \sqrt{I}$ ז"א קיים $n \in \mathbb{N}$ כך ש $x^n \in I$. צ"ל $x \in I$.

נוכיח באינדוקציה: עבור $n = 1$ $x^1 = x \in I$. נניח נכונות עבור n ז"א אם $x^n \in I$ אז $x \in I$. ונוכיח נכונות עבור $n+1$, נניח ש $x^{n+1} \in I$ ז"א $x^{n+1} = x \cdot x^n \in I$, מכיוון ש I אידיאל ראשוני אז או ש $x \in I$ או ש $x^n \in I$. אם $x \in I$ סיימנו, אם $x^n \in I$ אז על פי הנחת האינדוקציה $x \in I$.

תרגיל

מצאו אידיאל רדיקלי שאינו ראשוני.

פתרון

$\left\langle x^2 - 1 \right\rangle \lhd \mathbb{C}[x]$ זהו אידיאל שאינו ראשוני. נוכיח ש $\left\langle x^2 - 1 \right\rangle$ אידיאל רדיקל ז"א צ"ל ש $\left\langle x^2 - 1 \right\rangle = \sqrt{\left\langle x^2 - 1 \right\rangle}$. יהי $f(x) \in \sqrt{\left\langle x^2 - 1 \right\rangle}$, ז"א קיים $n \in \mathbb{N}$ כך ש $\left(f(x) \right)^n = \left(x^2 - 1 \right) \cdot g(x)$ נניח ש $\deg f = d$ אזי מעל $\mathbb{C}$ ניתן לכתוב $f(x) = (x - \alpha_1)(x - \alpha_2)...(x - \alpha_d)$. ז"א

$$\left(f(x) \right)^n = (x - \alpha_1)^n (x - \alpha_2)^n ... (x - \alpha_d)^n = (x+1)(x-1) \cdot g(x)$$

ולכן קיימים i, j כך ש $\alpha_i = 1, \alpha_j = -1$ ז"א

$\left(f(x)\right)^n = (x-1)^n (x+1)^n \cdot g_0(x) = \left(x^2-1\right)^n \cdot g_0(x)$ לכן $f(x) = \left(x^2-1\right) \cdot g_0(x)$ ז"א

$\left\langle x^2-1 \right\rangle = \sqrt{\left\langle x^2-1 \right\rangle}$ נקבל ש $I \lhd \mathbb{C}[x]$ לכל $I \subseteq \sqrt{I}$ מכיוון ש $f \in \left\langle x^2-1 \right\rangle$

<u>טענה</u>

יהי R חוג קומוטטיבי, $S \subset R$ קבוצה סגורה לכפל ויהי $I \lhd R$ כך שהוא מקסימאלי ביחס לתכונה $I \cap S = \{\ \}$, אז I אידיאל ראשוני.

<u>הוכחה</u>

יהי $f, g \in R$ כך ש $f, g \notin I$ נוכיח ש $f \cdot g \notin I$. על פי המקסימאליות של I, לאידיאלים $I + \left\langle f \right\rangle, I + \left\langle g \right\rangle$ יש חיתוך לא ריק עם S. ז"א קיימים איברים $i, j \in I$ כך ש $af + i \in S, bg + j \in S$. נשים לב ש $a \in R \setminus I$ מכיוון שאם $a \in I$ אז $af + i \in I$ בסתירה לכך ש $I \cap S = \{\ \}$, באותו אופן נקבל ש $b \in R \setminus I$.

מכיוון ש S סגורה לכפל נקבל ש $\left(bg + j\right) \cdot \left(af + i\right) \in S$, מצד שני $\left(bg + j\right) \cdot \left(af + i\right) = abfg + big + ajf$ ולכן אם $f \cdot g \in I$ נקבל ש $\left(bg + j\right) \cdot \left(af + i\right) \in I$ בסתירה לכך ש $I \cap S = \{\ \}$ ולכן $f \cdot g \notin I$ לכן I אידיאל ראשוני.

<u>הערה</u>

בהינתן קבוצה סגורה לכפל S נוכל להשתמש בלמה של צורן כדי להוכיח קיום של אידיאל מקסימאלי I ביחס לתכונה $I \cap S = \{\ \}$.

<u>תרגיל</u>

הוכיחו ש $\sqrt{I} = \cap \{P \lhd R : I \subseteq P,\ P$ ראשוני$\}$.

<u>פתרון</u>

יהיו $a \in \sqrt{I}$, P אידיאל ראשוני כך ש $I \subseteq P$. אז קיים $n \in \mathbb{N}$ כך ש $a^n \in I \subseteq P$ מכיוון ש P אידיאל ראשוני נקבל מהתרגיל הקודם ש $a \in P$, ולכן

$a \in \cap \{P \lhd R : I \subseteq P,\ P$ ראשוני$\}$.

יהי $a \notin \sqrt{I}$ ולכן לכל n טבעי $a^n \notin I$. נבנה אידיאל ראשוני P כך ש $a \notin P$. נתבונן ב קבוצה סגורה כיפלית $S = \{a^n\}_{n \geq 1}$, אז קיים אידיאל מקסימאלי P ביחס לתכונה $P \cap S = \{\ \}$, ולפי הטענה הקודמת Pראשוני ו $P \cap S = \{\ \}$ ולכן $a \notin P$.

<u>הגדרה</u>

יהי $N = \{a \in R : \exists n \in \mathbb{N}, a^n = 0\}$ אוסף האיברים הנילפוטנטים. N הוא אידיאל ונקרא הנילרדיקל.

<u>תרגיל</u>

הוכיחו ש $N = \cap \{P \lhd R :\ P$ ראשוני$\}$.

<u>פתרון</u>

נובע ישירות מהתרגיל הקודם עבור $I = \{0\}$, כי $N = \sqrt{\{0\}}$.

<u>תרגיל</u>

נתון הומומורפיזם $f : R \to S$. האם תמונה של איבר מקסימאלי\ראשוני הוא בהכרח איבר מקסימאלי\ראשוני?

<u>פתרון</u>

לא. ראינו כבר שתמונה של אידיאל איננה בהכרח אידיאל וגם אם התמונה היא אידיאל, אזי היא איננה בהכרח אידיאל מקסימאלי\ראשוני.

למשל: $f : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ כך ש $f(a) = (a,0)$. $p\mathbb{Z} \lhd \mathbb{Z}$ כאשר p ראשוני הוא אידיאל מקסימאלי וראשוני ו $f[p\mathbb{Z}] = p\mathbb{Z} \times \{0\} \lhd \mathbb{Z} \times \mathbb{Z}$. אבל $\mathbb{Z} \times \mathbb{Z} \Big/ p\mathbb{Z} \times \{0\} \cong \mathbb{Z}_p \times \mathbb{Z}$ לא שדה ולא תחום שלמות, מכיוון ש $(1,0) \cdot (0,1) = (0,0)$.

<u>משפט ההתאמה</u>

יהי R חוג, $I \lhd R$. אז האידיאלים ב $R \Big/ I$ הם מהצורה $J \Big/ I$ כש $J \lhd R$.

<u>טענה</u>

יהי $\varphi: R \to S$ אפימורפיזם. אם $\ker\varphi \subseteq M \lhd R$ אידיאל מקסימאלי אז $\varphi[M] \lhd S$ מקסימאלי.

<u>הוכחה</u>

נוכיח ראשית ש $\varphi[M] \lhd S$. ניתן להשאיר את ההוכחה ש $\varphi[M]$ תת חבורה חיבורית כתרגיל בית (קל יחסית כי אם $a,b \in \varphi[M]$ אז קיימים $a_0,b_0 \in M$ כך ש $\varphi(a_0)=a, \varphi(b_0)=b, a_0-b_0 \in M$ ואז $(\varphi(a_0-b_0)=a-b \in \varphi[M]$). יהיו $s \in S$, $a \in \varphi[M]$, צ"ל $as \in \varphi[M], sa \in \varphi[M]$. מכיוון ש $s \in S$ ונתון ש φ על אז קיים $s' \in R$ כך ש $\varphi(s')=s$ מכיוון ש $a \in \varphi[M]$ קיים $a' \in M$ כך ש $\varphi(a')=a$. $as=\varphi(a')\cdot\varphi(s')=\varphi(a's') \in \varphi[M]$. באותו אופן ניתן להוכיח ש $sa \in \varphi[M]$.

נניח בשלילה ש $\varphi[M] \lhd S$ אינו אידיאל מקסימאלי, ז"א קיים $J \lhd S$ כך ש $\varphi[M] \subset J \subset S$. מכיוון ש φ על נקבל ש $R/\ker\varphi \cong \mathrm{Im}\,\varphi = S$ לכן, $\varphi: R \to S$ הוא הומומורפיזם המנה $\varphi: R \to R/\ker\varphi \cong S$ כך ש $\varphi(a)=a+\ker\varphi$.

נובע ש: 1. $\varphi[M]=M/\ker\varphi$. 2. על פי משפט ההתאמה $J=J'/\ker\varphi$ כש $J' \lhd R$. לכן $M/\ker\varphi \subset J'/\ker\varphi \subset R/\ker\varphi$ ולכן $M \subset J' \subset R$ ז"א ש M אינו מקסימאלי.

<u>טענה</u>

יהי $\varphi: R \to S$ אפימורפיזם. אם $\ker\varphi \subseteq I \lhd R$ אידיאל ראשוני אז $\varphi[I] \lhd S$ ראשוני.

<u>הוכחה</u>

תרגיל בית

<u>הערה</u>

בטענה האחרונה חשוב ש $\ker\varphi \subseteq I$. למשל, $R=\mathbb{Z}$, $I=\mathbb{Z}_n$ כש I אינו ראשוני $\varphi:\mathbb{Z}\to\mathbb{Z}_n$. $\{0\}\lhd\mathbb{Z}$ הוא אידיאל ראשוני אבל $\varphi\left[\{0\}\right]=\{0\}$ אינו ראשוני ב $\mathbb{Z}_n$ מכיוון ש $\mathbb{Z}_n$ אינו תחום שלמות.

<u>תרגיל</u>

יהיו $I_1,I_2,...,I_k\lhd R$ אז ההעתקה $\varphi:R\to R/I_1\times R/I_2\times...\times R/I_k$ המוגדרת ע"י $\varphi(a)=(a+I_1,a+I_2,...,a+I_k)$ היא הומומורפיזם של חוגים.

מהו $ker\varphi$?

<u>פתרון</u>

$$\ker\varphi=\left\{a\in R:a+I_1=0_{R/I_1},a+I_2=0_{R/I_2},...,a+I_k=0_{R/I_k}\right\}=$$
$$=\{a\in R:a\in I_1\wedge...a\in I_k\}=I_1\cap I_2\cap...\cap I_k$$

<u>הערה</u>

על פי משפט האיזומורפיזים הראשון $R/\ker\varphi\cong\mathrm{Im}\,\varphi$ ולכן קיים שיכון (הומומורפיזם חח"ע)

$$\varphi:R/I_1\cap I_2\cap...I_k\to R/I_1\times R/I_2\times...\times R/I_k.$$

<u>הגדרה</u>

אידיאלים $I_1,I_2,...,I_k\lhd R$ יקראו קומקסימאלים אם לכל $i\neq j$ $I_i+I_j=R$.

<u>הערה</u>

ראינו שבחוג קומוטטיבי אם I,J קומקסימאלים אז $I\cap J=IJ$.

<u>משפט השאריות הסיני</u>

$\varphi:R\to R/I_1\times R/I_2\times...\times R/I_k$ הוא על אם האידיאלים $I_1,I_2,...,I_k\lhd R$ קומקסימאלים, לכן במקרה זה $R/I_1\cap I_2\cap...I_k\cong R/I_1\times R/I_2\times...\times R/I_k$.

<u>הוכחה עבור k=2</u>

אם $I_1, I_2 \lhd R$ אידיאלים קומקסימאלים. צריך להוכיח שהומומורפיזים החח"ע $\varphi : R \to R/I_1 \times R/I_2$ הוא על, ז"א $a_1 + I_1 \in R/I_1, a_2 + I_2 \in R/I_2$, יש למצוא $a \in R$ כך ש $a = a_1 \pmod{I_1}, a = a_2 \pmod{I_2}$. כיוון ש $I_1 + I_2 = R$ קיימים $b_1 \in I_1, b_2 \in I_2$ כך ש $b_1 + b_2 = 1_R$. נסמן $a = a_1 b_1 + a_2 b_2 \in I_2 + I_1$. מכיוון ש $b_1 + b_2 = b_1 \pmod{I_1} = 1 \pmod{I_1}$ ומכיוון ש $b_2 \in I_1$ מתקיים $a = a_1 b_1 + a_2 b_2 = a_1 b_1 \pmod{I_1} = a_1 \pmod{I_1}$ ובאופן דומה אפשר להראות ש $a = a_2 \pmod{I_2}$.

<u>הערה</u>

משפט השאריות הסיני אומר למעשה שלכל $a_1, ..., a_k \in R$ קיים $x \in R$ כך ש $x = a_j \pmod{I_j}$ לכל $1 \le j \le k$. ה x הנ"ל אינו יחיד, אלא רק מודולו $I_1 \cap I_2 \cap ... \cap I_k$.

<u>דוגמא</u>

אם $m\mathbb{Z}, n\mathbb{Z} \lhd \mathbb{Z}$ כש $(m,n) = 1$ אז על פי תכונת ה gcd קיימים $a, b \in \mathbb{Z}$ כך ש $am + bn = 1$ ז"א $1 \in m\mathbb{Z} + n\mathbb{Z} \to m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$ ולכן $m\mathbb{Z}, n\mathbb{Z}$ קו מקסימאלים.

נובע מכך ש $\mathbb{Z}_{mn} \cong \mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \cap n\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.

<u>תרגיל</u>

מצא $a \in \mathbb{Z}$ כך ש $a = 1 \pmod{3}, a = 2 \pmod{5}, a = 3 \pmod{7}$.

<u>פתרון</u>

a כזה קיים על פי משפט השאריות הסיני כש $R = \mathbb{Z}$ האידיאלים $I_1 = 3\mathbb{Z}, I_2 = 5\mathbb{Z}, I_3 = 7\mathbb{Z}$ קומקסימאלים מכיוון ש 3,5,7 זרים בזוגות.

נשים לב ש $1 = 15 - 14 \in 5\mathbb{Z} - 7\mathbb{Z}$. נסמן $a_1 = 1, a_2 = 2, a_3 = 3$, $b' = 15 \in 5\mathbb{Z}, b'' = -14 \in 7\mathbb{Z}$ על פי הוכחת משפט השאריות הסיני, נסמן $c = b'' \cdot a_2 + b' \cdot a_3 = -14 \cdot 2 + 15 \cdot 3 = 17$ כך נקבל ש $c \pmod{5} = 2, c \pmod{7} = 3$. האידיאלים $I_1 = 3\mathbb{Z}, I_2 \cap I_3 = 35\mathbb{Z}$ גם קומקסימאלים, ולכן

$1 = 36 - 35 \in 3\mathbb{Z} + 35\mathbb{Z}$ נסמן $b_1 = -35 \in I_2 \cap I_3, b_2 = 36 \in I_1$ אז

$$a = b_1 \cdot a_1 + b_2 \cdot c = -35 \cdot 1 + 36 \cdot c = 577 \pmod{105} = 52$$

<u>תרגיל</u>

הוכיחו ש $\mathbb{R}[x] \Big/ \langle x^2 - 5x + 6 \rangle \cong \mathbb{R} \times \mathbb{R}$

<u>פתרון</u>

נשים לב ש $x^2 - 5x + 6 = (x-2)(x-3)$ לכן $\langle x^2 - 5x + 6 \rangle = \langle x-2 \rangle \langle x-3 \rangle$. מכיוון שבחוגים קומוטטיבים $\langle ab \rangle = \langle a \rangle \langle b \rangle$. נוכיח ש $\langle x-2 \rangle + \langle x-3 \rangle = \mathbb{R}[x]$ ז"א נוכיח שהאיברים קומקסימאלים: $\langle x-2 \rangle + \langle x-3 \rangle = \langle x-2 \rangle \cap \langle x-3 \rangle \leftarrow (x-2) - (x-3) = 1 \in \langle x-2 \rangle + \langle x-3 \rangle$

ממשפט השאריות הסיני נקבל ש

$$\mathbb{R}[x] \Big/ \langle x-2 \rangle \langle x-3 \rangle \cong \mathbb{R}[x] \Big/ \langle x-2 \rangle \cap \langle x-3 \rangle \cong \mathbb{R}[x] \Big/ \langle x-2 \rangle \times \mathbb{R}[x] \Big/ \langle x-3 \rangle .$$

מהאפימורפיזים $\mathbb{R}[x] \to \mathbb{R}, x \to a$ נקבל שהגרעין הוא $\langle x-a \rangle$ ולכן לכל $a \in \mathbb{R}$

$$\mathbb{R}[x] \Big/ \langle x-a \rangle \cong \mathbb{R} .$$

<u>תרגיל</u>

יהי R חוג $I, J \lhd R$ קומקסימאלי. אז לכל $e, f \in \mathbb{N}$ I^e, J^f קומקסימאלים.

<u>פתרון</u>

מספיק להוכיח שלכל $f \in \mathbb{N}$ I, J^f קומקסימאלים, מכיוון שאז נסמן $I = J^f, J = I$ ונקבל שוב $I, J \lhd R$ אידיאלים קומקסימאלים ואז לכל $e \in \mathbb{N}$ I, J^e יהיו קומקסימאלים כדרוש.

נוכיח באינדוקציה שלכל $f \in \mathbb{N}$ $(I+J)^f \subseteq I + J^f$. עבור $f = 1$ זה ברור. נניח נכונות ל f ונוכיח ל $f+1$

$$(I+J)^{f+1} = (I+J) \cdot (I+J)^f \subseteq (I+J)\left(I + J^f\right) = II + IJ^f + JI + J^{f+1} \subseteq I + J^{f+1} .$$

לכן $R = R^f = (I+J)^f \subseteq I + J^f \subseteq R$ קיבלנו ש $I + J^f = R$ כדרוש.

<u>דוגמא</u>

נסתכל על $\mathbb{Q}[x]$ אז $\left\langle x^4-4x^3\right\rangle=\left\langle x^3\right\rangle\left\langle x-4\right\rangle=\left\langle x\right\rangle^3\left\langle x-4\right\rangle \lhd \mathbb{Q}[x]$ האידיאלים $\left\langle x\right\rangle,\left\langle x-4\right\rangle$ הם קומקסימאלים מכיוון ש $x-(x-4)=4\in\left\langle x\right\rangle+\left\langle x-4\right\rangle$. ולכן מהתרגיל הקודם האידיאלים $\left\langle x\right\rangle^3,\left\langle x-4\right\rangle$ הם קומקסימאלים.

$$\mathbb{Q}[x]\Big/\left\langle x^4-4x^3\right\rangle=\mathbb{Q}[x]\Big/\left\langle x^3\right\rangle\left\langle x-4\right\rangle=\mathbb{Q}[x]\Big/\left\langle x^3\right\rangle\cap\left\langle x-4\right\rangle\cong\mathbb{Q}[x]\Big/\left\langle x^3\right\rangle\times\mathbb{Q}[x]$$

<u>תרגיל</u>

ידוע שאוסף הפונקציות ההפיכות $R=\{f:\mathbb{R}\to\mathbb{R}\}$ הוא חוג.

א. הראו שלכל $a\in\mathbb{R}$ הקבוצה $I_a=\{f\in\mathbb{R}:f(a)=0\}$ היא אידיאל של R.

ב. הראו שכל שני אידיאלים שונים כאלה הם קומקסימאלים.

ג. הראו שלכל $a_1,...,a_t\in\mathbb{R}$ שונים ולכל $b_1,...,b_t\in\mathbb{R}$ שונים קיימת פונקציה הפיכה $f:\mathbb{R}\to\mathbb{R}$ כך ש $f(a_i)=b_i$.

<u>פתרון</u>

א. $I_a\lhd\mathbb{R}$ כי זהו הגרעין של הומומורפיזים ההצבה $\varphi:R\to\mathbb{R}$ $\varphi(f)=f(a)$.

ב. יהיו $a,b\in\mathbb{R}$ כך ש $a\neq b$. נוכיח ש $I_a+I_b=R$. נמצא $f\in I_a,g\in I_b$ כך ש $f+g=1$ נסתכל על $f(x)=\frac{1}{b-a}(x-a),g(x)=\frac{1}{a-b}(x-b)$ ואכן מתקיים ש $f+g=1$.

ג. ממשפט השאריות הסיני נקבל שההעתקה $R\to R/I_{a_1}\times...\times R/I_{a_t}$ היא על. נסתכל על הפונקציות הקבועות $g_i(x)=b_i$. כאיברים ב R/I_{a_i}. $(g_1,g_2,...,g_t)\in R/I_{a_1}\times R/I_{a_2}...\times R/I_{a_t}$.

ולכן קיימת פונקציה $f\in R$ כך ש $f(x)=g_i(x)\left(\mathrm{mod}\, I_{a_i}\right)$ ובפרט $f(a_i)=g_i(a_i)=b_i$

<u>הערה</u>

משפט השאריות הסיני אינו נכון עבור מספר אינסופי של אידיאלים. למשל, ניקח התרגיל הנ"ל במקום את R את $\mathbb{R}[x]$. אם $\{a_i\}_{i\in I}$ סדרה אינסופית של מספרים השונים זה מזה, לא קיימת פונקציה $f(x)\in\mathbb{R}[x]$ כך ש $f-a_j\in I_{a_j}$ כי אז היו ל f אינסוף שורשים.