מועד ב תשס"ו

חלק א:

1. הפרך: "אם a ו b מחלקי אפס בחוג לא קומוטטיבי R אז ab=0"

פתרון

נתבונן בחוג $M_2[\mathbb{R}]$. $a=\begin{pmatrix}1&0\\0&0\end{pmatrix}, b=\begin{pmatrix}0&1\\0&0\end{pmatrix}$ החוג $M_2[\mathbb{R}]$ לא קומוטטיבי ו $ab\neq 0$.

2. הפרך: "הנורמה $N\left(a+b\sqrt{-2}\right)=a^2+2b^2$ של כל איבר ראשוני ב $\mathbb{Z}\left[\sqrt{-2}\right]$ היא מספר ראשוני".

פתרון

נוכיח ש 5 איבר אי פריק ב $\mathbb{Z}\left[\sqrt{-2}\right]$ ומכיוון ש $\mathbb{Z}\left[\sqrt{-2}\right]$ תחום פריקות יחידה נקבל ש 5 איבר ראשוני ב $\mathbb{Z}\left[\sqrt{-2}\right]$. $N(5)=25$ נניח ש 5 פריק ז"א קיימים x,y כך ש $N(x)\cdot N(y)=25$ ולכן $N(x)=5$ אבל למשוואה $a^2+2b^2=5$ אין פתרון ולכן 5 ראשוני אבל הנורמה לא מספר ראשוני.

3. הפרך: "אם R תחום ראשי אז גם $R[x]$ תחום ראשי".

פתרון

$\mathbb{Z}$ תחום ראשי אבל $\mathbb{Z}[x]$ לא תחום ראשי.

4. הפרך: "אם $A,B,C,D\in M_n(\mathbb{Z})$ מטריצות כך ש $A\sim B\wedge C\sim D$, אז $AC\sim BD$.

פתרון

נסמן $A=\begin{pmatrix}2&0\\0&3\end{pmatrix}, B=\begin{pmatrix}1&0\\0&6\end{pmatrix}$ מכיוון ש

$$\begin{pmatrix}2&0\\0&3\end{pmatrix}\overset{R_1+R_2\to R_1}{\sim}\begin{pmatrix}2&3\\0&3\end{pmatrix}\overset{C_2-C_1\to C_2}{\sim}\begin{pmatrix}2&1\\0&3\end{pmatrix}\overset{C_1-C_2\to C_1}{\sim}\begin{pmatrix}1&1\\-3&3\end{pmatrix}\overset{C_2-C_1\to C_2}{\sim}\begin{pmatrix}1&0\\-3&6\end{pmatrix}\overset{3R_1+R_2\to R_2}{\sim}\begin{pmatrix}1&0\\0&6\end{pmatrix}$$

אז $A\sim B$

באותו אופן $C\sim D$ כאשר $C=\begin{pmatrix}3&0\\0&5\end{pmatrix}, D=\begin{pmatrix}1&0\\0&15\end{pmatrix}$

$AC=\begin{pmatrix}6&0\\0&15\end{pmatrix}$, $BD=\begin{pmatrix}1&0\\0&90\end{pmatrix}$. נמצא את הצורה הקנונית של AC.

$$\begin{pmatrix}6&0\\0&15\end{pmatrix}\overset{2C_1+C_2\to C_2}{\sim}\begin{pmatrix}6&12\\0&15\end{pmatrix}\overset{R_2-R_1\to R_1}{\sim}\begin{pmatrix}-6&3\\0&15\end{pmatrix}\overset{C_1+C_2\to C_1}{\sim}\begin{pmatrix}-3&3\\15&15\end{pmatrix}\overset{5R_1+R_2\to R_2}{\sim}\begin{pmatrix}-3&3\\0&30\end{pmatrix}\overset{C_1+C_2\to C_2}{\sim}\begin{pmatrix}-3&0\\0&30\end{pmatrix}$$

בגלל יחידות הצורה הקנונית נקבל שהמטריצות לא שקולות.

בדרך נוספת: להראות ש M_{AC} לא איזומורפי ל M_{BD}.

5. נתבונן ב $R=\mathbb{Z}$ ובפונקציה $f(x)=x^4-16$. $f(0)=-16\neq 0$, $I=\langle -16\rangle$.
$f(x)\equiv x^4 \pmod I$ ו $f(x)=x^4-16$ פריק מכיוון ש $f(x)=x^4-16=(x^2-4)(x^2+4)$.

חלק ב

6.

א. יהי $\phi: R\to S$ הומומורפיזם של חוגים, ו $I\lhd S$ אידיאל. הוכח ש $\phi^{-1}(I)$ אידיאל של R.

ב. אם I ראשוני, אז $\phi^{-1}(I)$ ראשוני.

ג. מצא הומומורפיזם $\phi:\mathbb{Z}[x]\to\mathbb{Q}[x]$ ואידיאל מקסימאלי I של $\mathbb{Q}[x]$, כך ש $\phi^{-1}(I)$ אינו מקסימאלי.

פתרון

א. נניח ש $x,y\in\phi^{-1}(I)$ אז $\phi(x),\phi(y)\in I$ מכיוון ש I אידיאל ומכיוון ש ϕ הומומורפיזים $\phi(x-y)=\phi(x)-\phi(y)\in I$ ולכן $x-y\in\phi^{-1}(I)$.

יהי $x\in\phi^{-1}(I)$ ויהי $r\in R$. מכיוון ש $x\in\phi^{-1}(I)$ נקבל ש $\phi(x)\in I$ ומכיוון ש I אידיאל ו ϕ הומומורפיזם נקבל ש $\phi(r\cdot x)=\phi(r)\cdot\phi(x)\in I$ ולכן $r\cdot x\in\phi^{-1}(I)$ באותו אופן ניתן להוכיח ש $x\cdot r\in\phi^{-1}(I)$.

נניח בשלילה ש $\phi^{-1}(I)$ לא ראשוני, ז"א קיימים $A,B\lhd R$ כך ש $AB\subseteq\phi^{-1}(I)$, A לא מוכל ב $\phi^{-1}(I)$ ו B לא מוכל ב $\phi^{-1}(I)$ נניח ש $a\in A\setminus\phi^{-1}(I),b\in B\setminus\phi^{-1}(I)$ ולכן $\phi(a)\notin I\wedge\phi(b)\notin I$ מכיוון ש I ראשוני $\langle\phi(a)\rangle\cdot\langle\phi(b)\rangle$ לא מוכל ב I ולכן קיים $x\in\langle\phi(a)\rangle\cdot\langle\phi(b)\rangle\setminus I$ מכיוון ש $x\in\langle\phi(a)\rangle\cdot\langle\phi(b)\rangle$ נקבל ש $x=\left(\sum_{i=1}^{n}\alpha_i\phi(a)\beta_i\right)\left(\sum_{i=1}^{m}\gamma_i\phi(b)\delta_i\right)$. (אני חושב שהכוונה לחוגים קומוטטיבים או לאפימורפיזים כמו בתרגיל 2.4.19 בחוברת. אם החוגים קומוטטיבים הייה בתרגיל בית)

אם החוגים לא קומוטטיבים אבל מדובר באפימופיזים אז: קיימים $\alpha_i',\beta_i',\gamma_i',\delta_i'$ כך ש $\phi(\alpha_i')=\alpha_i,\phi(\beta_i')=\beta_i,\phi(\gamma_i')=\gamma_i,\phi(\delta_i')=\delta_i$

$$x=\left(\sum_{i=1}^{n}\alpha_i\phi(a)\beta_i\right)\left(\sum_{i=1}^{m}\gamma_i\phi(b)\delta_i\right)=\left(\sum_{i=1}^{n}\phi(\alpha_i')\phi(a)\phi(\beta_i')\right)\left(\sum_{i=1}^{m}\phi(\gamma_i')\phi(b)\phi(\delta_i')\right)=$$

$$\left(\sum_{i=1}^{n}\phi(\alpha_i' a\beta_i')\right)\left(\sum_{i=1}^{m}\phi(\gamma_i' b\delta_i')\right)=\phi\left(\left(\sum_{i=1}^{n}(\alpha_i' a\beta_i')\right)\left(\sum_{i=1}^{m}(\gamma_i' b\delta_i')\right)\right)\notin I\to$$

$$\left(\sum_{i=1}^{n}(\alpha_i' a\beta_i')\right)\left(\sum_{i=1}^{m}(\gamma_i' b\delta_i')\right)\notin\phi^{-1}(I).$$

$$\left(\sum_{i=1}^{n}(\alpha_i' a\beta_i')\right)\in A,\left(\sum_{i=1}^{m}(\gamma_i' b\delta_i')\right)\in B\wedge AB\subseteq\phi^{-1}(I)\to\left(\sum_{i=1}^{n}(\alpha_i' a\beta_i')\right)\left(\sum_{i=1}^{m}(\gamma_i' b\delta_i')\right)\in\phi^{-1}(I)$$

וקיבלנו סתירה.

אפשר גם להוכיח בדרך נוספת: להשתמש בעובדה שבאפימורפיזים אם $A\lhd R$ אז $\phi(A)\lhd S$.

ב. ההומורפיזים $\phi(a)=a$ לכל $a\in\mathbb{Z}[x]$ והאידיאל $\langle x\rangle$. $\langle x\rangle$ מקסימאלי ב $\mathbb{Q}[x]$ מכיוון ש $\mathbb{Q}[x]/\langle x\rangle\cong\mathbb{Q}$ שדה. $\phi^{-1}(\langle x\rangle)$ אינו מקסימאלי מכיוון ש $\phi^{-1}(\langle x\rangle)=\langle x\rangle$ אבל $\mathbb{Z}[x]/\langle x\rangle\cong\mathbb{Z}$ לא שדה.

7. יהי $D\in\mathbb{Z}$ ללא גורמים ריבועיים, ויהי p גורם ראשוני שלו. נסמן $R=\mathbb{Z}[\sqrt{D}]$.

א. הוכח

a. אם $D<0$ ו$|D|$ איננו ראשוני אזי לא קיים איבר מנורמה p בR.

b. אם $-\dfrac{D}{p}$ איננו שארית ריבועית מודולו p אז אין איברים מנורמה p בR.

ב. אם מתקיים אחד התנאים בסאיף א אזי p אי-פריק בR.

ג. הוכח כי המקרה זה R אינו תחום פריקות יחידה.

פיתרון:

נניח בשלילה כי $D<0$ ו$|D|$ איננו ראשוני וכי קיים איבר $a+b\sqrt{D}\in R$ מנורמה p. אזי $|D|\,p=a^2+b^2$. אולם, $|D|$ איננו ראשוני ולכן $p<|D|$, משמע $b^2=0$, אך אז $p=a^2$ וזו סתירה.

נניח בשלילה כי $-\dfrac{D}{p}$ איננו שארית ריבועית מודולו p וכי קיים איבר $a+b\sqrt{D}\in R$ מנורמה p. אזי $p=a^2-b^2D$. כעת, $p\,|\,D,p$ ולכן $p\,|\,a^2$ ולכן $p\,|\,a$. נסמן $a=cp$. כעת, $p\nmid b$ בגלל שאחרת $p^2\,|\,a^2-b^2D=p$ וזו סתירה, ולכן b הפיך מודולו p.

אנו מקבלים ש $1=c^2p-b^2\dfrac{D}{p}$, ולכן $1\equiv -b^2\dfrac{D}{p}\pmod p$. משמע $(b^{-1})^2\equiv -\dfrac{D}{p}\pmod p$ וזו סתירה להנחה.

אם מתקיים התנאי הראשון בסעיף א (לגבי השני זו טעות) אזי אין איבר מנורמה p, ולכן לו p היה פריק אז היו קיימים $a,b\in R$ כך ש $ab=p$ שאינם הפיכים, כלומר הנורמה של שניהם היא p וזה בלתי אפשרי.

במקרה זה, לו R היה תחום פריקות יחידה, אזי מכיוון ש $D=p\cdot\dfrac{D}{p}=\sqrt{D}\cdot\sqrt{D}$ ו p אי-פריק, היינו מקבלים ש $p\mid\sqrt{D}$, אבל אז $p^2\mid D$ וזו סתירה לכך ש D חופשי מריבועים.

.8

א. הגדר תכולה של פולינום מעל תחום פריקות יחידה.

ב. מצא את התכולה של הפולינום $x^2(y^2-y)+2xy(y+1)+y^2$ כפולינום ב x מעל $\mathbb{Q}[y]$ וכפולינום ב y מעל $\mathbb{Q}[x]$.

ג. הוכח כי אם $c(f)=c(g)=1$ אזי $c(fg)=1$.

פיתרון:

תכולה היא המחלק המשותף המקסימלי של המקדמים של הפולינום.

כפולינום ב x התושבה היא y. נרשום אותו כפולינום ב y:

$x^2(y^2-y)+2xy(y+1)+y^2=(x^2+2x+1)y^2+(-x^2+2x)y$ ולכן התשובה היא 1.

נניח כי $c(fg)=a>1$. נסמן $f=f_nx^n+\ldots+f_0$ ו $g=g_mx^m+\ldots+g_0$.

נניח כי $a\nmid f_n$. המקדם העליון של fg הוא f_ng_m, ובגלל שהוא מתחלק ב a ו $a\nmid f_n$, אנו מקבלים ש $a\mid g_m$. נביט במקדם של x^{m+n-1} ב fg, $f_ng_{m-1}+f_{n-1}g_m$. איבר זה מתחלק ב a וגם המחובר $f_{n-1}g_m$ מתחלק ב a, ולכן המחובר f_ng_{m-1} מתחלק ב a, ומכיוון ש $a\nmid f_n$, אנו מקבלים $a\mid g_{m-1}$. באופן דומה ניתן להראות שכל המקדמים ב g מתחלקים ב a, ולכן $c(g)\neq 1$.

9. נתונה המטריצה $A=\begin{pmatrix}0&0&60\\2&5&t\\-5&-5&60\end{pmatrix}$ כאשר t הוא מספר שלם. חשבו את הפירוק לחבורות ציקליות של $G=\mathbb{Z}^3/A\mathbb{Z}^3$. מצא את $|G/3G|$ כאשר $t=8,9,10$.

פיתרון:

$$\begin{pmatrix}0&0&60\\2&5&t\\-5&-5&60\end{pmatrix}\xrightarrow{C_2\leftarrow C_2-2C_1}\begin{pmatrix}0&0&60\\2&1&t\\-5&5&60\end{pmatrix}\xrightarrow{C_1\leftarrow C_1-2C_2}$$

$$\begin{pmatrix}0&0&60\\0&1&t\\-15&5&60\end{pmatrix}\xrightarrow{R_3\leftarrow R_3-5R_2}\begin{pmatrix}0&0&60\\0&1&t\\-15&0&60-5t\end{pmatrix}\xrightarrow{C_3\leftarrow C_3-tC_2}$$

$$\begin{pmatrix}0&0&60\\0&1&0\\-15&0&60-5t\end{pmatrix}\xrightarrow{R_3\leftarrow -R_3+R_1}\begin{pmatrix}0&0&60\\0&1&0\\15&0&5t\end{pmatrix}$$

אם $3\,|\,t$ אז $15\,|\,5t$ ואז הצורה הקנונית היא $\begin{pmatrix}1&0&0\\0&15&0\\0&0&60\end{pmatrix}$.

במקרה זה $G=\mathbb{Z}_{15}\oplus\mathbb{Z}_{60}$ ואז $|G/3G|=\mathbb{Z}_3\oplus\mathbb{Z}_3$

אחרת, אפשר לקבל מיד את הצורה $\begin{pmatrix}0&0&60\\0&1&0\\15&0&5\end{pmatrix}$ או $\begin{pmatrix}0&0&60\\0&1&0\\15&0&-5\end{pmatrix}$ ומשם הצורה הקנונית תהייה $\begin{pmatrix}1&0&0\\0&5&0\\0&0&180\end{pmatrix}$.

אי-לכך, $G=\mathbb{Z}_5\oplus\mathbb{Z}_{180}$, ואז $|G/3G|=\mathbb{Z}_3$