~~תורת החבורות~~

חוגים ומודולים

<u>מרצה</u>: ד"ר קליין

<u>הגדרה</u>: חוג הוא קבוצה שעליה מוגדרות שתי פעולות + ו· . עבור + החוג הוא חבורה קומוטטיבית וביחס לכפל זהו מונואיד (אסוציאטיבית ויש יחידה) כמו כן מתקיימים חוקי הדיסטריבוטיביות.

<u>ספרים</u>: Basic algebra 1, Jackobson.

<u>הגדרה</u> מודול: מרחב וקטורי מעל חוג.

<u>הגדרה</u> $S\subseteq R$ יקרא חוג חלקי אם הוא סגור על חיבור וכפל, ומכיל את 1, 0, ועבור $x\in S$ $-x\in S$.

<u>טענה</u> חיתוך של חוגים חלקיים הוא חוג חלקי

<u>הגדרה</u> החוג הנוצר ע"י A הוא החוג החלקי הקטן ביותר המכיל את A.

<u>טענה</u> החוג הנוצר ע"י קבוצה A הוא חיתוך כל החוגים המכילים את A.

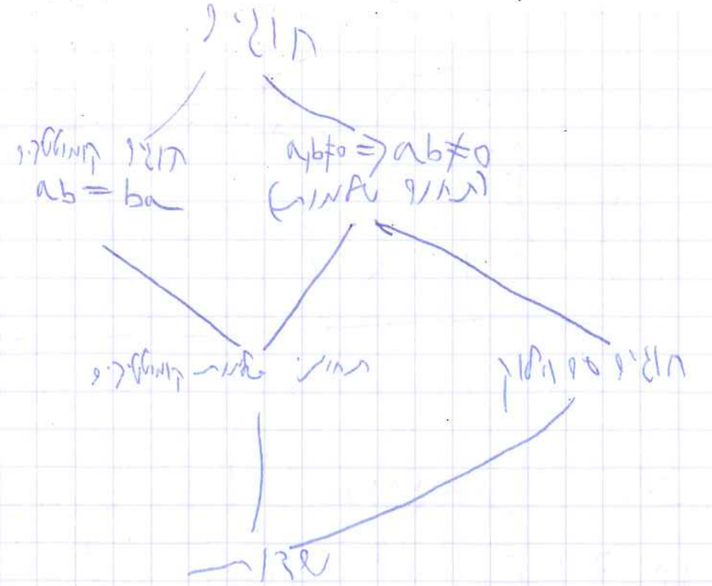
<u>הגדרה</u> החוג $\mathbb{Z}[\sqrt{-1}]=\{a+b\sqrt{-1} \mid a,b\in\mathbb{Z}\}$ נקרא חוג המספרים השלמים של גאוס

<u>הגדרה</u> חוג השאריות מודולו n הוא החוג $\{0,\dots,n-1\}$ שבו החיבור והכפל הם הרגילים מודולו n.

<u>טענה</u> $(-a)(-b)=-(ab)$

<u>טענה</u> אם $ab=ba$ (בחוג קומוטטיבי) אז:

$$(a+b)^n=\sum_{i=0}^{n}\binom{n}{i}a^i b^{n-i}$$



<u>הגדרה</u> $a\in R$ נקרא מחלק אפס שמאלי אם קיים $0\neq b$ כך ש $ab=0$. כנ"ל מחלק אפס ימני.

<u>הערה</u> R תחום שלמות אמ"מ אין מחלקי אפס שמאליים

<u>טענה</u> אם a אינו מחלק 0 שמאלי אזי

$ab=ac \Rightarrow b=c$ (כי $ab=ac \Rightarrow a(b-c)=0$)

<u>הערה</u> R תחום שלמות אמ"מ $ab=ac \Rightarrow b=c$

<u>הגדרה</u> $U(R)$ קבוצת כל ההפיכים בחוג.

<u>טענה</u> $U(R)$ חבורה.

<u>הגדרה</u> יהי $a\in R$ אם קיים k כך ש $a^k=0$ אזי a נ
נילפוטנטי.

<u>הגדרה</u> $e^2=e$ נקרא אידמפוטנט.

<u>טענה</u> בתחום שלמות 0,1 הם היחידים שהם אידמפוטנטים

<u>הוכחה</u> $e^2=e \Rightarrow e(e-1)=0 \Rightarrow e\in\{0,1\}$

<u>הגדרה</u> יהי R,S חוגים, $f:R\to S$. f יקרא
איזומורפיזם אם f חח"ע ועל וכן

$$f(a+b)=f(a)+f(b)$$
$$f(ab)=f(a)f(b)$$

<u>הגדרה</u> שני חוגים נקראים איזומורפיים אמ"מ קיים ביניהם
איזומורפיזם.

<u>הגדרה</u>

$$e_{ij}=\begin{pmatrix}0&\cdots&0\\ \vdots&1&\vdots\\ 0&\cdots&0\end{pmatrix}$$

תרגיל

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} = \sum_{1\le i,j\le n} a_{ij} b_{ij}$$

הגדרה $M_n(R)$ חוג המטריצות מסדר n על החוג R

הגדרה $U(M_n(R))$ החבורה הלינארית הכללית מעל R

הגדרה R חוג קומוטטיבי, $A\in M_n(R)$ אזי נגדיר

אזי $|A|=\det A$ כרגיל.

הגדרה $\operatorname{Adj} A$ ~~Adj~~ כרגיל

משפט $A(\operatorname{Adj}A)=I\det A$ ~~A adj~~

משפט $\det(AB)=\det A\cdot\det B$

הגדרה המינורים — כמו ~~a~~ כרגיל.

משפט $A\in U(M_n(R))$ אמ"מ $\det A\in U(R)$

משפט $A\in M_n(R)$, R קומוטטיבי, $AB=1$ ~~AB~~ $\Rightarrow BA=1$

הוכחה עפ"י הטענה הקודמת, וכפל מינורים.

משפט 14 R חוג קומוטטיבי, $A\in M_n(R)$ כך ש $\det A=0$

אזי קיים $v=\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}\neq 0$ כך ש $Av=0$

הוכחה: נניח r כך שיש תת־מטריצה מסדר r שאינה 0, וכל גדול יותר גדלה
היא 0. ע"י החלפות שורות ועמודות
נקבל ש

$$A=\begin{pmatrix} B_r & C_{r+1} \\ & \end{pmatrix} \qquad 0\neq\det B_r$$

אבל $0=\det C_{r+1}$ נפתח את $\det C_{r+1}$ לפי
השורה האחרונה:

$$0=a_{r+1,1}|B_{r+1,1}|\cdots a_{r+1,r+1}|B_{r+1,r+1}|$$

$0\neq|B_r|=|B_{r+1,r+1}|$ נקבל פתרון לא טריוויאלי.

Av המשוואה ה $r+1$ (הן).

$x_1=|B_{r+1,1}|,\ x_2=\dots\ x_{r+1}=|B_{r+1,r+1}|,\ x_{r+2}=0\dots x_n=0.$

אותו פתרון הוא פתרון של כל מערכת המשוואות - כי:

אם המשוואה שיבחר היא הראשונה נקבל כך את הפתרון שלנו, וזה כאילו פתחנו את הדטרמיננטה של $|C(A)|$ לפי שתי שורות שוות. ולכן המשוואה מתקיימת.

ואם המשוואה שיבחר אחת מ-$n-r$ האחרונות אז נציב את הפתרון קיבלנו דטרמיננטה של מטריצה מסדר $r+1$ ולכן 0.

מ.ש.ל.

משפט: $A_{(n\times n)}$ א"מ מחלק-0 $(\det A)|0$

הוכחה: אם $A|0$ אזי קיים B כך ש $AB=0$ נכפול את השוויון משמאל:

$$(\text{Adj}A)AB=0$$
$$\Downarrow$$
$$(\det A)B=0$$

ולכן $\det A$ מאפס כל איבר של $B\neq0$ ולכן הוא מחלק 0.

אם $(\det A)|0$ אזי קיים $c\neq0$ כך ש $(\det A)c=0$ נוכיח קיום פתרון V לא טריוויאלי של $AV=0$ מאחר ו c מאפס את כל איברי A נסמן אותם קיים r כך שיש דטרמיננטה חלקית B_r גדולה ביותר כך ש $|B_r|c\neq0$ נעשה את אותו תהליך ונקח:

$$x_1=|B_{r+1,1}|c, \; \dots, \; x_{r+1}=|B_{r+1,r+1}|c, \; x_{r+2}=0, \; \dots, \; x_n=0$$

והשאר לפי אותה הוכחה גמרנו.

דוגמה: $\left\{\begin{pmatrix} a & b\\ -b & a\end{pmatrix} \middle| \, a,b\in\mathbb{R}\right\}$ איזומורפי ל C

הגדרה $\mathbb{H}=\left\{\begin{pmatrix} a & b \\ -\bar b & \bar a\end{pmatrix} \middle| a,b\in\mathbb{C}\right\}$

טענה $\mathbb{H}$ חוג חילוק.

הוכחה סגירות לחיבור טריוויאלית

סגירות לכפל ע"י חישוב.

$$\begin{vmatrix} a & b\\ -\bar b & \bar a\end{vmatrix} = a\bar a-b\bar b=|a|^2+|b|^2$$

אם $0=\det\begin{pmatrix} a & b\\ -\bar b & \bar b\end{pmatrix}$ אז"א $b=a=0$ ולכן

יש לכל איבר שונה מ-0 ב-$\mathbb{H}$ יש הפיך

ב-$M_n(\mathbb{C})$ ע"י חישוב הוא יהיה ב-$\mathbb{H}$

טענה $\mathbb{H}$ איזומורפי ל

$$\alpha+\beta\underbrace{\begin{pmatrix} i & 0\\ 0 & -i\end{pmatrix}}_{=i}+\gamma\underbrace{\begin{pmatrix} 0 & 1\\ -1 & 0\end{pmatrix}}_{=j}+\delta\underbrace{\begin{pmatrix} 0 & i\\ i & 0\end{pmatrix}}_{=k}$$

ול- $\alpha+\beta i+\gamma j+\delta k$

הגדרה $\{\pm 1,\pm i,\pm j,\pm k\}$ חבורת הקווטרניונים

הגדרה צמוד:

$$\mathrm{adj}(\alpha+\beta i+\gamma j+\delta k)=\alpha-\beta i-\gamma j-\delta k$$

טענה יהי z קווטרניון ו-A צורתו המטריציונית

אז:

$$\mathrm{Adj}\, z\sim \mathrm{Adj}\, A$$

טענה $X,Y\in\mathbb{H}$ אז $\overline{X+Y}=\bar X+\bar Y$ וכן $\overline{XY}=\bar Y\bar X$

הגדרה יהי $X\in\mathbb{H}$ אז הנורמה

$$N(X)=X\bar X=\alpha^2+\beta^2+\gamma^2+\delta^2$$

טענה $N(XY)=N(X)N(Y)$

הוכחה

$$N(XY)=XY\overline{XY}=XY\bar Y\bar X=X\bar X Y\bar Y=N(X)N(Y)$$

הגדרה העקבה:

$$T(X)=2\alpha=X+\bar X$$

טענה $\forall X\in\mathbb{H}\quad X^2-T(X)X+N(X)=0$

הגדרה יהי R חוג ו $\equiv$ יחס שקילות. נאמר כי $\equiv$ יחס שקילות חוגית אם $a\equiv a'$ וכן $b\equiv b'$ אזי $a+b\equiv a'+b'$ וגם $ab\equiv a'b'$

הגדרה $\bar{a}=\{b\in R \mid b\equiv a\}$

הגדרה $\bar{R}=\{\bar{a}\mid a\in R\}$

הגדרה $\bar{0}=\{a\in R\mid a\equiv 0\}=I$

טענה עבור ההגדרה הקודמת $\bar{R}=R/I$

טענה $a\in I,\ b\in R \Rightarrow ab\in I$

הוכחה $a\equiv 0,\ b\equiv b \Rightarrow ab\equiv 0b \Rightarrow ab\equiv 0 \Rightarrow ab\in I$

טענה I תת חוג של R וכן היא סגורה תחת כפל מאיברי R

הגדרה ~~I שמקיים~~ I תת חוג חלקי של R שסגור תחת כפל ב-R יקרא אידיאל.

טענה יהי I אידיאל ב-R אזי R/I חוג.

הוכחה עבור חיבור סגירות. לכן עבור כפל אם $a\equiv a'$ וכן $b\equiv b'$ אזי

$$ab-a'b'=(a-a')b+a'(b-b')\in I$$

ולכן $ab\equiv a'b'$

טענה $\bar{a}=a+I$

טענה $(a+I)(b+I)=ab+I$

טענה $(a+I)+(b+I)=(a+b)+I$

טענה $\bar{1}=1+I$

טענה חיתוך של אידיאלים הוא אידיאל.

הגדרה יהי $S\subseteq R$ נסמן

$$(S)=\bigcap_{S\subseteq I\lhd R} I$$

האידיאל הנוצר ע"י S.

טענה יהי $a\in R$ אזי

$$(a)=\{\sum x_i a y_i \mid x_i\in R,\ y_i\in R\}$$

__טענה__ $(a_1,\dots a_n)=(a_1)+\dots+(a_n)$

__טענה__ יהיו I,J אידיאלים אז $I+J=(I\cup J)$

__הגדרה__ יהיו I,J אידיאלים אז

$$IJ=\{\sum a_ib_i \mid a_i\in I, b_i\in J\}$$

__טענה__ $(IJ)K=I(JK)$

__טענה__ $(I+J)K=IK+JK$

__טענה__ יהי R קומוטטיבי ו־$a\in R$ אז

$$(a)=\{xa \mid x\in R\}=Ra$$

__טענה__ עבור R קומוטטיבי

$$(a_1\dots a_n)=Ra_1+\dots+Ra_n$$

__הגדרה__ $I\subseteq R$ אידיאל ימני אם (1) $I\leq R$

(2) $a\in I$ $b\in R$

$\Downarrow$

$ab\in I$

__הגדרה__ אידיאל שמאלי כנ"ל

__טענה__ $R\neq 0$ חוג עם חילוק אמ"מ אין לו אידיאלים ימניים פרט לטריוויאליים $(0,R)$

__הוכחה__ כ"נ: R חוג עם חילוק יהי $I\neq 0$ אידיאל ימני. יהי $0\neq a\in I$ קיים $b\in R$ כך ש $ab=1$ ולכן $1\in I$ ולכן $\forall x\in R$ $x\in I$ ולכן $I=R$

כ"נ: נניח שאין ל־R אידיאלים ימניים. יהי $R\ni a\neq 0$ אז aR אידיאל ימני ולכן $aR=R$ ולכן $1\in aR$ ולכן קיים $b\in R$ כך ש $ab=1$

__טענה__ $I\subset\mathbb{Z}$ הוא אידיאל אמ"מ $I=n\mathbb{Z}$

__טענה__ $(k)\supset(l) \iff k\mid l$

__טענה__ $a\mathbb{Z}+b\mathbb{Z}=d\mathbb{Z}$ אמ"מ $d=\gcd(a,b)$

__טענה__ $(a)\cap(b)=([a,b])$

טענה p ראשוני $\Leftarrow$ $\mathbb{Z}/(p)$ שדה.

טענה $U(\mathbb{Z}/(k)) = \{\bar{a} \mid (a,k)=1\}$

טענה $\phi(k) = |U(\mathbb{Z}/(k))| = k\cdot(1-\frac{1}{p_1})\cdots(1-\frac{1}{p_r})$

כאשר $\{p_i\}$ הראשוניים (השונים) המחלקים את k.

הגדרה יהיו R,R' חוגים, $f:R\to R'$ תקרא הומומורפיזם אם היא הומומורפיזם של החיבור ושל הכפל ולכן $f(1)=1'$

טענה $f:R\to R/I$ המוגדרת ע"י $a\longmapsto a+I$ היא הומומורפיזם

הגדרה ν הומומורפיזם הטבעי.

הגדרה אפימורפיזם: הומומורפיזם על

הגדרה מונומורפיזם: הומומורפיזם חח"ע

הגדרה איזומורפיזם: מונומורפיזם שהוא אפימורפיזם

הגדרה יהי $f:R\to R'$ הומומורפיזם. הגרעין שלו:

$$\ker f = f^{-1}(0')$$

טענה $\ker f$ אידיאל.

טענה f חח"ע אמ"מ $\ker f=\{0\}$

משפט יהי $\eta:R\to R'$ הומומורפיזם, η כך ש- $I<\ker\eta$ אידיאל. אזי קיים $\bar{\eta}:R/I\to R'$ הומומורפיזם יחיד כך שהדיאגרמה הבאה תתחלף:

$$\begin{tikzcd} R \arrow[rr, "\eta"] \arrow[dr, "\nu"'] & & R' \\ & R/I \arrow[ur, "\bar{\eta}"'] & \end{tikzcd}$$

הוכחה יחידות: אם קיים הוא חייב:

$$\bar{\eta}(a+I)=\eta(a)$$

נבדוק אם $\bar{\eta}$ מוגדר היטב

$$a+I=b+I \Rightarrow a-b\in I<k \Rightarrow \eta(a-b)=0 \Rightarrow \eta(a)-\eta(b)=0 \Rightarrow$$
$$\eta(b)=\eta(a)$$

__טענה__ משפט ההומומורפיזם הראשון: יהי $f: R \to R'$ הומומורפיזם אזי קיים מונומורפיזם מ $R/\ker f$ ל R'.

__הגדרה__ אם קיים אפימורפיזם מ R ל R' יקרא R' תמונה הומומורפית של R.

__טענה__ אם $f: R \to R'$ אפימורפיזם אזי $R/\ker f \cong R'$

__טענה__ יהי $\eta: R \xrightarrow{\text{אפי}} R'$, K הגרעין. אזי קיימת התאמה חח"ע בין תת"ח $(+)$ של R' לבין התת"ח $(+)$ של R המכילות את K.

__טענה__ יהי $\eta: R \to R'$ ההומומורפיזם אזי

$\eta(H)$ תת"ח של R' $\Longleftarrow$ H תת חוג של R

$\eta(H)$ אידיאל של R' $\Longleftarrow$ H אידיאל כך

__טענה__ יהי $\eta: R \xrightarrow{\text{אפי}} R'$ הומומורפיזם, $I \supseteq \ker\eta$ אידיאל, אזי

$$R/I \cong R'/I'$$

כאשר $I' = \eta(I)$

__טענה__ יהי R חוג, $I \subset R$ אידיאל, $S \subset R$ תת חוג. אזי $S+I$ תת"ח של R, $S \cap I$ אידיאל של S,

$$S/S\cap I \cong S+I/I$$

__הוכחה__ $S+I$ תת"ח:

$$(s_1+a_1)(s_2+a_2) = s_1s_2 + (s_1a_2 + a_1s_2 + a_1a_2) = s + a$$

$$1 = 1 + 0 \in S+I$$

$S \cap I$ אידיאל ב S: $S\cap I$ תת חבורה, טריויאלי, סגירות לכפל טריויאלית.

[illegible] משקול להתאמות

$$\phi: S \to S+I \to \frac{S+I}{I}$$

$$s \longmapsto s \longmapsto s+I$$

φ הוא על, ולפי המשפט היסודי

$$S/\ker\phi \cong S+I/I$$

כל שנותר ש $S\cap I=\ker\phi$

<u>טענה</u> החוג הקטן ביותר החלק לחוג R, הוא התמונה של הומומורפיזם $\theta:\mathbb{Z}\to R$ שמקיים $\theta(1)=1$

<u>טענה</u> החוג הקטן ביותר $\cong \mathbb{Z}/(k)$

<u>הגדרה</u> הk שנוצר לעיל, נקרא הקרקטריסטיקה של החוג R.

<u>טענה</u> אם $k=ord(1)$ בחבורה החיבורית

כלומר $ord(1)=\infty \Leftarrow k=0$

<u>טענה</u> הקרקטריסטיקה של תחום שלמות היא 0 או p ראשוני.

<u>טענה</u> אם k הקרקטריסטיקה של חוג R אזי $ka=0\ \forall a\in R$

<u>הגדרה</u> יהי R קומוטטיבי בעל קרק' p ראשוני. נגדיר

$$\eta: R\to R$$

בצורה $a\mapsto a^p$

<u>טענה</u> η היא אנדומורפיזם (הומומורפיזם מהחוג לעצמו)

<u>הוכחה</u> $\eta(a+b)=(a+b)^p=\sum\binom{p}{i}a^{p-i}b^{i}=$

ולכן $p\mid\binom{p}{i}\ \forall 0<i<p$

$=a^p+b^p=\eta(a)+\eta(b)$

כפל זה טריוויאלי, $\eta(1)=1$ טריוויאלי

<u>טענה</u> אם R שדה סופי, η אוטומורפיזם (של פרובניוס)

<u>הוכחה</u> $\ker(\eta)$ אידיאל בR וR שדה סופי ולכן $\ker(\eta)\in\{\{0\},R\}$ R לא כולו אפסים כי $\eta(1)=1$

ולכן $\ker\eta=0$

הגדרה סכום ישר של חוגים. $R_1 \oplus R_2$

טענה אם $R=\bigoplus_{i=1}^{k} R_i$ אזי $U(R)=\bigoplus_{i=1}^{k} U(R_i)$

הגדרה יהיו $\{I_i\}_{1}^{k}$ אידיאלים דו״צ R. נגדיר

$$\varphi: R \to R/I_1 \oplus \cdots \oplus R/I_k$$

כך: $x \mapsto (x+I_1, \dots, x+I_k)$

טענה $\ker\varphi=\bigcap_{i=1}^{k} I_i$

טענה φ על $\Longleftarrow \forall_{i\neq j}\ R=I_i+I_j$

הוכחה נוכיח עבור $i=1$, $j=2$. ψ על $\Longleftarrow \psi: R\to R/I_1\oplus R/I_2$

היא על אפימורפיזם יש x,y כך ש

$$\psi(x)=(0,1)$$
$$\psi(y)=(1,0)$$

לכן מתקיים, $x\in I_1$, $y\in I_2$, $\psi(x+y)=(1,1)$, $\psi(1)=(1,1)$

ולכן $1-(x+y)\in \ker\psi=I_1\cap I_2\subseteq I_1+I_2$

וכמו כן $x+y\in I_1+I_2$, ולכן $1\in I_1+I_2$, I_1+I_2 הוא

אידיאל המכיל את 1 ולכן $I_1+I_2=R$

מ.ש.ל.

הגדרה שני אידיאלים I,J המקיימים $I+J=R$ נקראים קו-מקסימליים.

הגדרה $\{I_i\}_{1}^{k}$ יקראו קו-מקסימליים אם לכל $1\le i,j\le k$

$$R=A_i+A_j$$

טענה אם $\{I_i\}$ קו-מקסימליים אז $\left\{\bigcap_{i=1}^{k-1} I_i ; I_k\right\}$ קו-מקסימליים.

הוכחה

$$(I_1+I_k)(I_2+I_k)\cdots(I_{k-1}+I_k)=R$$

כל גורם שווה ל-R, ול-R יש יחידה

נפתח את הסוגריים, ונקבל ש

מכפלה $\underset{I_k\ \text{אידאל}}{\subseteq} I_1\cdots I_{k-1}+I_k\subseteq I_1\cap I_2\cap\cdots\cap I_{k-1}+I_k$

ולכן זה שווה ל-R.

מ.ש.ל.

משפט השאריות הסיני:

טענה: יהיו $\{I_i\}_1^k$ אידיאלים. $\varphi: R\to\bigoplus_{i=1}^k R/I_i$ על אמ"מ $\{I_i\}$ קומקסימליים.

הוכחה: כיוון אחד הוכח.

נניח $\{I_i\}$ קומקסימליים. ההוכחה באינדוקציה:

$k=2$: $\varphi: R\to R/I_1\oplus R/I_2$, $R=I_1+I_2$ ולכן קיימים $b_1\in I_1$, $b_2\in I_2$ כך ש $1=b_1+b_2$. יהיו $a_1,a_2\in R$, נגדיר

$$a=a_1b_2+a_2b_1$$

$$\bar a=\bar a_1\bar b_2+\bar a_2\bar b_1=\bar a_1\bar b_2 \quad \mod I_1$$

$$\bar 1=\bar b_1+\bar b_2=\bar b_2 \quad \mod I_1$$

$$\bar a=\bar a_1\bar b_2=\bar a_1\bar 1=\bar a_1 \quad \mod I_1$$

באותו אופן $\bar a=\bar a_2 \mod I_2$

לכן

$$\varphi(a)=(\bar a_1,\bar a_2)$$

לכן φ על.

כעת נניח $\varphi: R\to\bigoplus_{i=1}^{k} R/I_i$ על עבור $k-1$

מהנחת האינדוקציה, יהיו $\{a_i\}_1^k\subset R$. קיים c כך ש

$$c\equiv a_j \pmod{I_j} \quad 1\le j\le k-1$$

$\bigcap_1^{k-1} I_i, I_k$ הם קומקסימליים, ולכן לפי $k=2$ קיים a כך ש

$$a\equiv c \pmod{\bigcap_1^{k-1} I_i}$$

$$(1)\quad a\equiv a_k \pmod{I_k}$$

כעת $a-c\in I_j$, ולכן $a\equiv c \pmod{I_j}$, ולכן

$$a\equiv a_j \pmod{I_j} \quad 1\le j\le k-1$$ יחד עם (1)

מש"ל.

מסקנה

$$R/\bigcap_{i=1}^k I_i \cong \bigoplus_{i=1}^k R/I_i$$

מסקנה אם $\{n_i\}\subset\mathbb{N}$ זרים בזוגות – אז

$$\mathbb{Z}/(\prod m_i) \overset{?}{\cong} \bigoplus \mathbb{Z}/(m_i)$$

מסקנה לחבורות כפל

$$U(\mathbb{Z}/\prod m_i) \cong \bigoplus U(\mathbb{Z}/(m_i))$$

מסקנה $\phi(\prod m_i) = \prod \phi(m_i)$

מסקנה $\phi(n) = \prod \phi(p_i^{r_i})$

מסקנה $\phi(p^r) = p^r(1-\frac{1}{p})$

מסקנה $\phi(n) = n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_r})$

הגדרה אם R תחום ולכל b,c קיימים $e,f\neq 0$ כך ש $be=cf$ אז נאמר כי התחום מקיים את תנאי הכפולה המשותפת הימנית.

טענה יהי D תחום המקיים את תנאי הכפולה המשותפת הימנית. אזי קיים חוג עם חילוק המכיל את D שאיבריו מנות "ימניות" של איברי D.

הוכחה נתבונן ב $\{(a,b) \mid a,b\in D, b\neq 0\}$. נגדיר $(a,b)\equiv(c,d)$ אם קיימים u,v שונים מאפס כך ש $0\neq bu=dv$ ו $au=cv$.

זה יחס שקילות: $\equiv$ רפלקסיבי וסימטרי, כעת נניח ש $(a,b)\equiv(c,d),(c,d)\equiv(e,f)$ ~~...~~ u,w כך ש $0\neq bu=fw$. לפי התנאי קיימים $x,y\neq 0$ כך ש $bux=dy$

$(a,b)\equiv(c,d)$ ולכן $aux=cy$, ולכן $bu=fw$ ולכן $dy=fwx$

$(c,d)\equiv(e,f)$ ולכן $ewx=cy$, ולכן $aux=ewx$. D תחום ולכן $au=ew$. ולכן $(a,b)\equiv(e,f)$ ולכן $\equiv$ טרנזיטיבי.

נגדיר את מחלקת השקילות של (a,b) להיות a/b. ~~...~~ יהיו a/b, c/d. קיימים u,v כך ש $bu=dv\neq 0$ ונגדיר $\frac{a}{b}+\frac{c}{d}=\frac{au+cv}{bu}$

נוכיח שזה חד-ערכי: יהיו $\frac{a'}{b'}=\frac{a}{b}$, $\frac{c'}{d'}=\frac{c}{d}$, $b'u'=d'v'\neq 0$. $\frac{a'}{b'}+\frac{c'}{d'}=\frac{a'u'+c'v'}{b'u'}$. ~~...~~ קיימים x,y כך ש $bux=b'u'y$

אם $a/b=a'/b'$ אזי ① $aux=a'u'y$. $vd=bu$, $b'u'=d'v'$ ולכן

$y'v'd'x=vd$, $dvx=d'v'y$ ולכן $c/d=c'/d'$ גורר $y'c'x=cv$, $cvx=c'v'y$. נחזור אל

זה לפי ① ונקבל שהחיבור מוגדר היטב. אסוציאטיביות

קומוטטיביות, ⓪, איבר הופכי ~~...~~ מיידי.

כפל: יהיו a/b, c/d קיימים $u,v\neq 0$ כך ש $bu=cv$

ונגדיר $(a/b)(c/d)=au/dv$ ~~(a/b)~~ אם נניח $a'/b'=a/b$,

$c/d=c'/d'$, $b'u'=c'v'$, $v'\neq 0$. מהגדרה קיימים x,y כך ש $y'd'x=vd$, $dvx=d'v'y$, $c/d=c'/d'$ ולכן

$y'c'x=cv$, $cvx=c'v'y$, $cv=bu$ ו $c'b=b'a'$ ולכן $y'b'x=bu$, $bux=b'u'y$. $a/b=a'/b'$ ולכן

$y'a'x=au$, $aux=a'u'y$ ולכן הכפל מוגדר היטב. אסוציאטיביות

כפל, וכו' היחידה מיידי. לכן הדיסטריבוטיביות מיידית (לבדוק)

לכן $\bar{R}=\{a/b \mid a,b\in R, b\neq 0\}$ הוא שדה. נגדיר $\varphi: R\to\bar{R}$

בצורה $a\to a/1$. מיידי ש φ ~~...~~ מונומורפיזם

<u>הגדרה</u> חוג R מקיים את תנאי השרשרת

העולה לאידיאלים אם לכל סדרה

של אידיאלים $I_1\subset I_2\subset\dots\subset\dots$

קיים k כך שלכל $m,n\geq k$ $I_m=I_n$

אזי R יקרא חוג נותריאני.

<u>טענה</u> יהי R תחום נותריאני אז לכל $0\neq a,b\in R$ קיימים

$x,y\in R$ כך ש $0\neq ax=by$

<u>הוכחה</u> נגדיר את האידיאלים הבאים ע"י

~~$I_1=(ba), b^2a, b^3a$~~ $I_1=(ba)$

$I_2=(ba,b^2a)$ $I_3=(ba,b^2a,b^3a)$ ... $I_n=(\{b^ia\}_{i=1}^n)$

זוהי סדרה של אידיאלים עולה ע"פ תנאי השרשרת העולה

קיים k כך ש $I_k=I_{k+1}$. כלומר

$$(ba,\dots,b^ka)=(ba,\dots,b^ka,b^{k+1}a)$$

כלומר

$$b^{k+1}a=bax_1+b^2ax_2+\dots+b^kax_k$$

נצמצם את b משני הצדדים (בתחום) ~~...~~

אם $x_1=0$, נעצור. אחרת ...

$$b^{k+1-i}a=ax_i+b\,ax_{i+1}+b^2ax_{i+2}+\dots+b^{k-i}ax_k$$

נקבל $(\dots,b x_{i+1},\dots)\in R[x]$

$b(\dots)=ax_i$

$x_i\neq 0$, ולכן סתירה.

<u>הגדרה</u>: חוג קומוטטיבי נקרא נתרי אם כל שרשרת עולה של אידאלים מתייצבת.

<u>משפט</u>: חוג ראשי הוא נתרי.

<u>הוכחה</u>: ניקח $I_1\subseteq I_2\subseteq\dots$ נתבונן ב

$$I=\bigcup I_j$$

זהו גם אידאל, ולכן נוצר ע"י איבר אחד a, ולכן קיים k כך ש $a\in I_k$, אז k הוא המקום שבו נעצרים.

<u>הגדרה</u>: יהי $R\subset R'$ חוגים קומוטטיביים. אז $R[u]$ מסמן את החוג הקטן ביותר המכיל את R ואת u.

<u>טענה</u>:

$$R[u\cup v]=(R[u])[v]$$

<u>טענה</u>: יהי $R\subset R'$ קומוטטיביים, $\{u_i\}_{i=1}^{n}\subset R'$ אז

$$R[u]=R[u_1][u_2]\dots[u_n]$$

<u>טענה</u>: יהי $R\subset R'$ קומוטטיביים, $u\in R'$ אז

$$R[u]=\left\{\sum_{i=0}^{n}a_iu^i \,\middle|\, n\in\mathbb{N},\ a_i\in R\right\}$$

<u>הגדרה</u>: אם לכל איבר של $R[u]$ יש הצגה יחידה בצורה $a_0+a_1u^1+\dots a_nu^n$ עם מקדמים מ-R, אומרים ש-u טרנסצנדנטי מעל R.

<u>טענה</u>: u טרנסצנדנטי אמ"מ

$$\sum_{i=0}^{n}c_iu^i=0\Rightarrow\forall i\ c_i=0$$

הגדרה יהי R קומוטטיבי. נגדיר

$$R[X]=\{(a_0,a_1,\dots,a_n,0,0\dots)\}$$

הגדרה חיבור $a,b\in R[X]$ נגדיר

$$a+b=(a_0+b_0,a_1+b_1,\dots)\in R[X]$$

הגדרה כפל $a,b\in R[x]$ נגדיר

$$ab=(a_0b_0,a_0b_1+a_1b_1,\dots,\sum_{i=0}^{k}a_ib_{k-i},\dots)$$

טענה $R[X]$ עם הפעולות הנ"ל הוא חוג קומוטטיבי.

טענה $\varphi:R\to R[x]$ המוגדרת $a\mapsto(a,0,0\dots)$ מונומורפיזם!

טענה אם $R\subset R'$ קומוטטיביים, $u\in R'$ נעלם מעל R, אז

$$R[X]\cong R[u]$$

טענה (התכונה האוניברסלית של חוג הפולינומים) יהי $\eta:R\to S$ הומומורפיזם, $u\in S$. אז קיים הומומורפיזם יחיד $\eta_u:R[X]\to S$
כך ש $a\mapsto\eta(a)$, $X\mapsto u$ (כאשר $X=(0,1,0,\dots)$)
וכך ש $\eta_u\circ\varphi=\eta$

הגדרה נאמר ש T מקיימת את התכונה האוניברסלית ביחס ל R אם לכל חוג S, $\eta:R\to S$ הומומורפיזם, $u\in S$, קיים הומומורפיזם יחיד ...

טענה אם T מקיימת את ... ביחס ל R אז $T\cong R[X]$

טענה יהי $\varphi:R[x]\to R[u]$ הומומורפיזם, $R\subset R'$, $u\in R'$ אלגברי. אז $\ker\varphi$ הוא אידיאל I, כך ש $R\cap I=\{0\}$

טענה יהי R חוג, $I\lhd R[x]$ אידיאל $\neq 0$, $I\cap R=\{0\}$, אז $R[X]/I$ איזומורפי לחוג מהצורה $R[u]$, כאשר u אלגברי מעל R.

טענה (התכונה האוניברסלית)

הגדרה $R\subset R'$, $\{a_i\}\subset R'$, אזי אם $R[\{u_i\}]\cong R[\{x_i\}]$ יקראו בלתי-תלויים אלגברית מעל R.

טענה יהי E חוג עם חילוק. אזי ניתן להרחיב את $E[X]$ לחוג מנות

הוכחה ב $E[X]$ כל אידיאל הוא ראשי; לכן הוא נותרי; לכן ניתן להפוך אותו לחוג מנות.

טענה יהי R חוג x משתנה סמלי, ונניח

$$ax = xa^\sigma + a^\delta$$

כאשר σ, δ מתפלגות [illegible] הומומ׳

$$(a+b)^\sigma = a^\sigma + b^\sigma$$

$$(ab)^\sigma = a^\sigma b^\sigma$$

$$(a+b)^\delta = a^\delta + b^\delta$$

$$(ab)^\delta = a^\delta b^\sigma + a b^\delta$$

אזי נקבל $R[x]$ חוג פולינומים לא-קומוטטיבי.

מסקנה R תחום $\Leftarrow$ $R[x]$ תחום

תרגיל $x-a \mid f(x) \iff f(a)=0$

טענה יהי F שדה אינסופי, $0 \neq f \in F(x_1, \dots, x_r)$ אזי קיימים $a_1 \dots a_r$ בשדה ש-$f(a_1 \dots a_r) \neq 0$.

הוכחה באינדוקציה. המקרה $r=1$ ברור. כי [illegible] מעל שפולינום ממעלה n יש לכל היותר n שורשים ובשדה אינסופי נכתוב f כפולינום במשתנה אחד שמקדמיו פולינומים בשאר $r-1$ המשתנים וכו׳ וממשיך

טענה יהי F שדה בן q איברים, יהי $0 \neq f \in F[x_1 \dots x_r]$ אשר מעלתו בכל אחד מהמשתנים קטנה מ-q אזי קיימים $a_1 \dots a_r$ כך ש-$f(a_1 \dots a_r) \neq 0$

הגדרה נגדיר העתקה מ-$F[x]$ לקבוצת הפונקציות הפולינומיאליות (על F) ההעתקה הקנונית.

טענה בשדה סופי F מסדר q ~~[illegible]~~ הגרעין של ההעתקה הקנונית הוא האידיאל $(x^q - x)$.

הגדרה כמו ההגדרה הקודמת, עבור הרבה משתנים
$$\varphi: F[\{x_i\}_1^r] \to \{f: F^r \to F\}$$

טענה $\ker \varphi = (x_1^q - x_1, x_2^q - x_2, \dots, x_r^q - x_r)$

<u>טענה</u>: לשדה סופי כל פונקציה היא פולינומיאלית

<u>הגדרה</u>: יהי M מונואיד קומוטטיבי. $U=U(M)$
ההפיכים ב-M. $a,b\in M$ יקראו חברים
אם $a=ub$, $\exists u\in U$ ויסומן $a\sim b$

<u>הגדרה</u>: $m\in M$ יקרא אי-פריק אם אינו הפיך
ואינו מכפלה של שני איברים לא הפיכים.

<u>הגדרה</u>: ל-M יש פריקות אם כל $b\in M-U(M)$ הוא
מכפלה של אי-פריקים.

<u>הגדרה</u>: ל-M פריקות יחידה אם: (א) ל-M יש פריקות
(ב) אם $a=b_1\ldots b_s=c_1\ldots c_t$ b_i, c_j אי-פריקים
אז: $s=t$ וגם

$$\exists\sigma\in S_t \quad \forall 1\le i\le t \quad b_i\sim c_{\sigma(i)}$$

<u>דוגמא</u>: יהי $M=\{a+b\sqrt{-5}\,|\,a,b\in\mathbb{Z}\}$ אז: ל-M יש פריקות
אך היא אינה יחידה.

<u>הוכחה</u>: נגדיר $N(a+b\sqrt{-5})=a^2+5b^2$. אז: $N(rs)=N(r)N(s)$
מכאן נובע בקלות ש

$$U(M)=\{\pm1\}$$

וגם שקיימת פריקות. אבל

$$9=3\cdot3=(2+\sqrt{-5})(2-\sqrt{-5})$$

וכן $3\nsim 2+\sqrt{-5}$
וכן $3, 2+\sqrt{-5}, 2-\sqrt{-5}$ הם אי-פריקים ע"י חשבון
נורמות.

<u>הגדרה</u>: חוג ראשי: הוא חוג שבו כל אידאל
נוצר ע"י איבר אחד.

<u>הגדרה</u>: נאמר שמונואיד M מקיים את תנאי
השרשרת לחלוקה אם לשרשרת שלה

$$\ldots a_4|a_3|a_2|a_1|a_0$$

והחל ממקום מסוים כל הגורמים חוזרים.

<u>טענה</u>: פריקות יחידה ⇐ תנאי השרשרת:

יהי M תחום פריקות יחידה, $a\in M$ אזי מספר

המחלקים של a מודולו חברות הוא סופי:

כי נפרק את a ל $a=b_1\dots b_s$

בנוסף, אם $c|a$ אזי קיים d כך ש $a=cd$

נפרק את c, d ונקבל מיידית שמספר

המחלקים של $a \leq 2^s$

מ.ש.ל.

<u>הגדרה</u> $a\in M$ יקרא ראשוני אם ~~אינו~~ הוא לא הפיך

ומתקיים $a|bc$ גורר $a|b$ או $a|c$

<u>טענה</u>: a ראשוני ⇐ a אי-פריק. למונואידים שמתבטל

קיים גם.

<u>דוגמה</u>: הדוגמה הקודמת $3|3\cdot 3=(2+\sqrt{-5})(2-\sqrt{-5})$ ולכן

3 אי-פריק אך לא ראשוני.

<u>הגדרה</u> תנאי הראשוניות: כל אי-פריק הוא ראשוני.

<u>טענה</u>: פריקות יחידה ⇐ תנאי הראשוניות

<u>הוכחה</u>: יהי a אי-פריק, $a|bc$ כלומר: $ad=bc$

עבור d כלשהו! נפרק:

$$b_1\cdots b_r c_1\cdots c_s=a d_1\dots d_t$$

מיחידות הפירוק נובע ש-a חבר של

אחד הגורמים משמאל. וגמרנו

מ.ש.ל. M הומוטפי אם צמצום

<u>טענה</u>: פריקות יחידה ⇔ תנאי השרשרת ותנאי הראשוניות

<u>הוכחה</u> ⇐ כבר הוכחנו

⇒ (1) תנאי השרשרת ⇐ פריקות:

יהי $a\in M$ אם a אי-פריק גמרנו. אם לא

אזי: $a=a_1b_1$ כאשר $a_1|a$ וכן $a_1\nmid a$ a_1 הוא

או אי-פריק וגם יש אי-פריק שמחלק את a

או $a_1=a_2b_2$ ... נקבל סדרה

$$\dots|a_2|a_1|a$$

תנאי השרשרת מתקיים וכך ש... חס
אינו-פריק. ולכן לכל $a\in M$ קיים אי-פריק שמחלק
~~אותו.~~

הוכחה: יהי $a\in M$ אזי: $a=c_1a'$ c_1 אי-פריק
$a'=c_2a''$ c_2 אי-פריק
לפי תנאי השרשרת $(\ldots a'''|a''|a')$ ולכן התהליך מסתיים
מתישהו, $a^{(n+1)}\sim a^{(n)}$ כלומר, עבור אותו n

$$a=c_1c_2c_3\ldots c_{n+1}a^{(n+1)}$$

כאשר $a^{(n+1)}$ הוא בהכרח הפיך. ולכן יש פריקות.

(2) ראשוניות + פריקות ⇒ פריקות יחידה.
הוכחה: $a=b_1\ldots b_s=c_1\ldots c_t$ כך ש b_i,c_j
אי-פריקים. לפי תנאי הראשוניות לכל
b_s ראשוני. ולכן קיים j כך ש $b_s|c_j$
אבל c_j אי-פריק ולכן $b_s\sim c_j$ נניח $j=t$
נצמצם את b_s ו c_t. לפי האינדוקציה
$s-1=t-1$ ולכן $s=t$, וגם הגורמים חברים.
מ.ש.ל.

<u>הגדרה</u> יהיו $a,b\in M$ $d\in M$ הוא ממג"מ של a,b אמ"מ
(1) $d|a$, $d|b$
(2) $c|a$, $c|b$ ⇒ $c|d$

<u>הגדרה</u> תנאי הממג"מ = לכל שני איברים קיים ממג"מ
<u>טענה</u> פריקות יחידה ⇒ תנאי הממג"מ.
<u>טענה</u> תנאי הממג"מ ⇒ תנאי הראשוניות.
<u>הערה</u> יהי M מונואיד שקיים בו תנאי הממג"מ. (1) אזי: יהיו $a_1,a_2,a_3\in M$ אזי קיים d
כך ש $i=1,2,3$; $d|a_i$ וכן $c|a_i$ ⇒ $c|d$.
$\boxed{d=(a_1,(a_2,a_3))}$. מתקיים: $d\sim((a_1,a_2),a_3)$
(2) $(ca,cb)=c(a,b)$: נסמן $d=(a,b)$, $e=(ca,cb)$
כמובן $cd|ca,cb$ ⇒ $cd|e$ ⇒ $e=cdu$

אזי $ca=ex$. ולכן $\Leftarrow ca=cdux \Leftarrow a=dux$

$\Leftarrow du|a$ ובאותו אופן $du|b$. ולכן $du|d$ ולכן

u הפיך ולכן $d\sim du \Leftarrow e=cdu\sim cd$

(3) $(a,b)\sim 1$, וכן $(a,c)\sim 1$ $\Leftarrow$ $(a,bc)\sim 1$:

יהיו a,b,c כנדרש. אזי: $(ca,cb)\sim c$ ולכן

מ.ש. $(a,cb) = ((a,ca),cb) \sim (a,(ca,cb)) \sim (a,c)\sim 1$

כעת הוכחת הטענה: יהי $a\in M$ אי-פריק. $a|bc$.

כעת a אי-פריק ולכן $(a,b)\sim 1$ או $(a,b)\sim a$.

במקרה השני סיימנו. ולכן נניח $(a,b)\sim 1$

כעת אם $(a,c)\not\sim 1$ היה $(a,bc)\not\sim 1$

בסתירה לכך ש $a|bc$. ולכן $(a,c)=a$

ולכן $a|c$.

מ.ש.

<u>טענה</u> כל ~~...~~ תחום ראשי מקיים

את תנאי השרשרת

<u>הוכחה</u> הוכחנו את תנאי השרשרת לאידיאלים. כלומר

כל שרשרת ~~...~~ היא מהצורה:

$$(a_1)\subset(a_2)\subset\ldots\subset(a_n)=(a_{n+1})\ldots$$

כעת יהיו $a_4|a_3|a_2|a_1$. $\Rightarrow$ זה שקול ל

$$(a_1)\subset(a_2)\subset(a_3)\subset(a_4)\ldots$$

ולכן קיים n כך ש $(a_n)=(a_{n+1})$ וזה יתכן רק

אם $a_n\sim a_{n+1}$

מ.ש.

<u>טענה</u> כל תחום אוקלידי ראשי מקיים את תנאי הממג"ל:

<u>הוכחה</u>: יהיו $a,b\in R$ נתבונן באידיאל הנוצר ע"י a,b.

התחום הוא ראשי ולכן האידיאל $(a,b)=(d)$

$a\in(d) \Leftarrow d|a$, $b\in(d) \Leftarrow d|b$

$d\in(a,b) \Leftarrow d=ax_0+by_0$ כעת נניח $c|a,b$ אז:

$c|d$ (מ.ש.ת). ולכן d הוא הממג"ל.

משפט: תחום ראשי הוא תחום פריקות יחידה.

הוכחה: בהרצאות הקודמות.

אוקלידי

$\Downarrow$

ראשי

$\Downarrow$

פריקות יחידה

מערכת $\Rightarrow$ ראשוניות $\Leftrightarrow$ פריקות $\Leftarrow$ ממצה

הגדרה: תחום שלמות D נקרא תחום אוקלידי (אוקלידס) אם קיימת $\delta: D\setminus\{0\} \to \mathbb{N}\cup\{0\}$ כך ש:

(א) $\delta(ab) \geq \delta(a)$

(ב) אם $a,b\in D^*$ אז קיימים $q,r\in D$ כך ש $a=bq+r$ ו $r=0$ או $\delta(r)<\delta(b)$

משפט: כל תחום אוקלידי הוא ראשי.

הוכחה: נקח אידיאל $I\neq 0$. יהי $0\neq b\in I$ כך שלכל $x\in I$: $\delta(b)\leq\delta(x)$. נראה כי: $(b)\subset I$. יהי $a\in I$ לפי תנאי (ב) $a=bq+r$. אם $r=0$ סיימנו.

$r\neq 0 \Rightarrow \delta(r)<\delta(b)$ בסתירה למינימליות.

$r=a-bq\in I$ סתירה. ולכן $I=(b)$

מ.ש.ל.

הגדרה: (D תחום) $f\in D[x]$ התוכן של f (הגורם המשותף המקסימלי):

$$c(f)=(a_0,\dots,a_n)$$

כאשר $f=a_0+a_1x+\dots$

הגדרה: $f\in D[x]$ כך ש $c(f)\sim 1$ נקרא פרימיטיבי.

טענה: (למה של גאוס): מכפלה של שני פולינומים פרימיטיביים היא פרימיטיבית. (בתחום פריקות יחידה)

הוכחה: יהיו $f=\sum_{i=0}^{n} b_ix^i$, $g=\sum_{i=0}^{m} a_ix^i$

כך ש $(\{b_i\})\sim 1\sim(\{a_i\})$

משמע ⇐ fg לא פרימיטיבי אז קיים p-ראשוני המחלק
המחלק אותו. כה אודה המקדם הגדול $p \nmid f$
$p \nmid g$ קיים ⇐ r, s מינימליים כך ש
$p \nmid a_r$ $p \nmid b_s$ אזי נסמן c מקדם
של x^{r+s} ב fg. אזי $p|c$. אולם

$$c = \underbrace{\cdots}_{0-\bmod p} + a_r b_s + \underbrace{\cdots}_{0-\bmod p}$$

ולכן $p | a_r b_s$ ולכן $p|a_r$ או $p|b_s$ סתירה.
ולכן fg פרימיטיבי.
מ.ש.ל.

<u>טענה</u> יהי D תחום ממשל״י, F שדה המנות של D $\varphi \in F[x]$
אזי $\varphi = qf$ כך ש $f \in D[x]$ פרימיטיבי
ו $q \in F$, וכן רישום זה יחיד עד כדי חברות
ב D.

<u>טענה</u> אם D מקיים תכונות הממשל״י אז גם $D[x]$ כנ״ל.
<u>הוכחה</u> יהיו $f, g \in D[x]$ נרשום $f = af_1$, $g = bg_1$ כך ש
f_1, g_1 פרימיטיביים. יהי $d = (a,b)$. יהי F שדה המנות
של D. נתבונן ב f_1, g_1 מעל F. בשדה אין בעיה
(קיים ממשל״י). ואז: יהי $h \overset{F}{=} (g_1, f_1)$ נרשום אותו
$h = \varphi h_1$ כך ש $h_1 \in D[x]$ פרימיטיבי ו φ הפיך ולכן
h_1 הוא גם ממשל״י של f_1, g_1 ב F.
כעת $h_1 |_F f_1$ ולכן $h_1 q = f_1$ כאשר $q \in F[x]$
נרשום $q = \beta q_1$ ו q_1 פרימיטיבי ב $D[x]$ אז
$f_1 = \beta h_1 q_1$ h_1, q_1 פרימיטיביים ב D ⇐ $h_1 q_1$
f_1 פרימיטיבי ב D ⇐ β הפיך ב D.
ולכן $q = \beta q_1$ ב D. ולכן $h_1 |_D f_1, g_1$:
כעת יהי $k \in D[x]$ כאשר $k |_D f_1, g_1$ ב F מידן
ש $k |_F h_1$ וכן פרימיטיביות של k פרימיטיבי וכמו
קודם נקבל $k |_D h_1$. ולכן $h_1 = (f_1, g_1)$
כעת $(a,b) h_1 = (f, g)$.
מ.ש.ל.

מסקנה: D מקיים תנאי השרשרת לראשיים $\Leftarrow$ $D[x]$ מקיים תנאי השרשרת לראשיים
הוכחה: מיידית.

טענה: D בעל פריקות יחידה $\Leftarrow$ $D[x]$ בעל פריקות יחידה

למה (גאוס): יהי D תחום בעל פריקות יחידה. $f,g\in D[x]$ פרימיטיביים אזי fg פרימיטיבי.

הוכחה: יהי $f=\sum a_i x^i$, $g=\sum b_i x^i$, $fg=\sum_{i=0}^{m+n} c_i x^i$ נסמן $(c_0,\dots,c_{m+n})=d$

נניח בשלילה ש-d אינו הפיך.

יהי $r\geq 0$ כך ש-$(a_0,\dots,a_{r-1},d)\notin U(D)$ אך $(a_0,\dots,a_r,d)\in U(D)$ נסמן $d_1=(a_0,\dots,a_{r-1},d)$

כעת עם d_1 אפשר לעשות את אותו התרגיל עם המקדמים של g: קיים s כך ש-$(b_0,\dots,b_{s-1},d_1)\notin U(D)$ אבל $(b_0,\dots,b_s,d_1)\in U(D)$

נסמן $c=(b_0,\dots,b_{s-1},d_1)$ $c|d_1$ $c\notin U(D)$ כמו כן

$$\underbrace{c_{r+s}}_{c|d}=\underbrace{a_0b_{r+s}+\dots+a_{r-1}b_{s+1}}+a_rb_s+\underbrace{a_{r+1}b_{s-1}+\dots+a_{r+s}b_0}_{c|d_1|d|b_i\quad i\leq s-1}$$

כולם מתחלקים ב-c ולכן $c|c_{r+s}$

מסקנה: $c|a_rb_s$ אבל (c,b_s) הפיך מהגדרת s. וכן (d_1,a_r) הפיך ולכן (c,a_r) הפיך כי $c|d_1$. גורל מצד $\Leftarrow$ ראשוניות

ולכן c זר ל-b_s ול-a_r גורר ש-c זר ל-a_rb_s. סתירה, ולכן d הפיך.

מש"ל.

טענה חוג הפולינומים מעל שדה הוא חוג פריקות יחידה.

הערה $D[x_1]$ חוג ראשי: לכן חוג פריקות יחידה, ולכן $D[x_1,x_2]$ חוג פריקות יחידה וכו'..

טענה יהי D תחום ממשל. יהי $f\in D[x]$ ממעלה ≥ 1 ואי פריק, ויהי F שדה המנות של D. אזי f אי-פריק ב $F[x]$

הוכחה f פרימיטיבי מידית. נניח $f(x)=\varphi_1\varphi_2$, $\varphi_i\in F[x]$ אזי $\varphi_i=\alpha_i f_i$ כאשר f_i ב D פרימיטיבי. אזי $f=\alpha_1\alpha_2 f_1 f_2$ f פרימיטיבי ולכן $\alpha_1\alpha_2\in D$ והפך. ואז $f=(\alpha_1\alpha_2 f_1)f_2$ פירוק של f ב $D[x]$ סתירה. לכן f אי-פריק ב $F[x]$ מש"ל.

טענה (קריטריון אייזנשטיין). יהי D חוג תכונת הממשל. ויהי $f=a_0+a_1x+\dots+a_nx^n$ וקיים $p\in D$ אי-פריק כך ש $p|a_i$ $\forall 0\leq i<n$, $p^2\nmid a_0$, $p\nmid a_n$ אזי f אי-פריק ב $D[x]$ (ומכאן ב $F[x]$ כש F שדה המנות של D).

הגדרה תהי M חבורה קומוטטיבית. נסמן $End\, M$ קבוצת כל ההומומורפיזמים $\varphi:M\to M$

הגדרה יהיו $\alpha,\beta\in End\, M$ אז נגדיר

$$(\alpha+\beta)(x)=\alpha(x)+\beta(x)$$

הגדרה יהי $\alpha,\beta\in End\, M$ נסמן $\alpha\beta(x)=\alpha(\beta(x))$

טענה $(End\, M,+,\cdot)$ חוג עם יחידה.

טענה $\mathbb{Z}\underset{\text{כחוג}}{\cong} End\,\mathbb{Z}$

טענה $M_n(\mathbb{Z})\ \cancel{\quad}\ \underset{\text{כחוג}}{\cong} End\,\mathbb{Z}^n$

טענה $\mathbb{Z}/(n)\underset{\text{כחוג}}{\cong} End\,\mathbb{Z}/n\mathbb{Z}$

הגדרה חוג R נקרא חוג של אנדומורפיזמים אם קיימת חבורה קומוטטיבית M כך ש $R\subset End\, M$

טענה כל חוג איזומורפי לחוג של אנדומורפיזמים.

הוכחה: לוקחים כפול מ מאשר החלפה ההדדית

לכל R נגדיר עבור $a\in R$ $a_L: R\to R$

כדוגמה $x\mapsto ax$. a_L אנדומורפיזם של R

מיד נקבל ש $R\cong\{a_L | a\in R\}\subseteq End R$

מש"ל

הערה: באותו אופן היינו יכולים להגדיר $a_R: R\to R$

כדוגמה $x\mapsto xa$

אבל אז לא היה מתקיים ש... כי $(ab)_R=b_R a_R$

($a\mapsto xa$ הוא יהיה כלל הפוך אנטי-אנדומורפיזם)

הגדרה: יהי R חוג. נגדיר R^o החוג ההפכי:

יש לו אותו R אבל אנטי-איזומורפי ל-R!

$a+b$ כמו הרגיל

$a*b$ נגדיר להיות ba

כלומר $R^o=(R,+,*)$

טענה: $R^o\cong\{a_R | a\in R\}$

הגדרה: $R_L=\{a_L | a\in R\}$, $R_R=\{a_R | a\in R\}$

טענה: $R_L=C(R_R)$, $R_R=C(R_L)$

הוכחה: נוכיח למשל $R_R=C(R_L)$. יהי $a_R\in R_R$ אזי

לכל $b_L\in R_L$ מתקיים $a_R b_L=b_L a_R$ כי:

$(a_R b_L)(x)=bxa$

$(b_L a_R)(x)=bxa$

ולכן $a_R\in C(R_L)$

כעת יהי $\eta\in C(R_L)$ אזי לכל $b\in R$

$\eta b_L=b_L\eta$ נגדיר $a=\eta(1)$ אזי

$a_R(x)=xa$, $\eta(x)=\eta(x\cdot 1)=\eta(x_L(1))=$

$=(\eta x_L)(1)=(x_L\eta)(1)=x_L(a)=xa$

ולכן $a_R=\eta$. ולכן $C(R_L)=R_R$

מש"ל

הגדרה: מודול הוא שלישיה $(R,M,\cdot)$ כאשר R חוג

M חבורה אבלית ו-$\cdot$ פעולה $\cdot: R\times M\to M$

המקיימת: $a(m_1+m_2)=am_1+am_2$ לכל $a\in R$

וכן מתקיים (בפונקציה זה אנדומורפיזם.) $m \mapsto a_m$)

$1m=m$, $(ab)m=a(bm)$, $(a+b)m=am+bm$

הגדרה יהי $a\in End\,R$ נגדיר $a_L: M\to M$ כדלהלן

$a_L(m)=am$

$\{a_L \mid a\in R\} < End\,M$

טענה $\varphi: R\to \{a_L\}$ המוגדרת $a\mapsto a_L$ היא הומומורפיזם

טענה יהי M חבורה אבלית, R חוג, $\eta: R\to End\,M$ הומומורפיזם

אזי ניתן להפוך את M למודול מעל R.

הוכחה נגדיר $am=[\eta(a)](m)$ קל לבדוק שמתקיימות התכונות.

דוגמאות ① $\mathbb{R}^n$

② כל חבורה אבלית - מעל $\mathbb{Z}$ (כפעולת חזקה)

הגדרה מודול חלקי - כמו שאפשר לצפות

הגדרה יהי (R,M) מודול $S\subset M$ נגדיר $\langle S\rangle$ המודול החלקי הקטן ביותר המכיל את S.

הגדרה יהי $N\subset M$ מודול חלקי מעל R. נגדיר M/N מודול המנה

הגדרה $\eta: M\to M'$ תקרא הומומורפיזם של מודולים אם

$\eta(ax)=a\eta(x)$ $a\in R,\ x\in M$

$\eta(x+y)=\eta(x)+\eta(y)$ $\forall x,y\in R$

טענה M/N ו- ההעתקה הקנונית היא הומומורפיזם

טענה התמונה והגרעין של הומומורפיזם הם מודולים חלקיים

משפט משפטי האיזומורפיזם תקפים

//

משפט

$$\frac{N+P}{P} \cong \frac{N}{P\cap N}$$

<u>הגדרה</u> מודול M יקרא ציקלי אם

$$\exists x\in M \quad Rx=\{ax\mid a\in R\}=M$$

<u>הגדרה</u> יהי M מודול מעל R, ויהי $x\in M$ אז
נגדיר $M_x:R\to Rx$ בצורה $a\mapsto ax$. זהו
הומומורפיזם מודולים, נקרא ל-$\ker M_x$ הסדר
של x. אם $\ker M_x\neq 0$ נאמר כי
ל-x סדר סופי, ואחרת אינסופי.

<u>הגדרה</u> יהיו M,N שני מודולים מעל R. נסמן
$Hom(M,N)$ את קבוצת כל ההומומורפיזמים
$M\to N$ בפעולות הרגילות.

<u>הערה</u> $Hom(M,M)$ עם כפל הרכבה הוא חוג.

<u>הגדרה</u> החוג $Hom(M,M)$ יסומן $End_R M$

<u>הערה</u>

$$End_R M=\{\eta\in End M\mid a_L\eta=\eta a_L\ \forall a_L\}=C(R_L)$$

כלומר $End_R M$ הוא המרכז של R_L ב-$End\, M$

<u>הגדרה</u>: מודול אי-פריק - מודול חסר מודולים חלקיים לא טריוויאליים
(כלומר $M\neq 0$, וגם $N\le M \Rightarrow (N=M)\vee(N=0)$)

<u>טענה</u> M אי-פריק $\Leftrightarrow$ $M\neq 0$ ולכל $0\neq x\in M$ $M=Rx$

<u>טענה</u> M אי-פריק $\Leftrightarrow$ $M\cong R/I$ כאשר I אידיאל
שמאלי מקסימלי ב-R, ולכן R/I מתאר כל
המודולים.

<u>הוכחה</u> M אי-פריק $\Rightarrow$ $M=Rx$ $\Rightarrow$ $M\cong R/\ker(a\mapsto ax)$

$M\cong R/I$ אם I מקסימלי $\Leftarrow$ $N\le M$ איזומורפי ל-I'/I $\Leftarrow$
$N\cong I'/I\cong 0$ או $N\cong R/I\cong M$

<u>טענה</u> (הלמה של שור) יהיו M_1,M_2 מודולים אי-פריקים.
$\eta:M_1\to M_2$ הומומורפיזם. אז $\eta=0$ או η איזומורפיזם.

<u>טענה</u> M אי-פריק $\Rightarrow$ $End_R M$ חוג עם חילוק.

הערה המודול R^n, R חוג, כפי שהיינו מצפים.

הגדרה יהי M מודול. $\{b_i\}$ תיקרא בסיס של M אם היא פורשת את M, וגם היא בת"ל.

הגדרה אם למודול M יש בסיס, נקרא לM מודול חופשי. למספר איברי הבסיס נקרא הדרגה של M. (הדרגה של M אינה מוגדרת תמיד באופן יחיד).

טענה R קומוטטיבי $\Leftarrow$ $\boxed{R^n\cong R^m \Rightarrow m=n}$

הוכחה נניח בשלילה. ניקח ל R^n בסיס $\{e_i\}_1^n$, ונניח $\{f_i\}_1^m$ בסיס של R^m אזי:

$$\begin{pmatrix} f_1\\ \vdots \\ f_m\end{pmatrix} = A_{m\times n}\begin{pmatrix} e_1\\ \vdots \\ e_n\end{pmatrix},\quad \begin{pmatrix} e_1\\ \vdots \\ e_n\end{pmatrix} = B_{n\times m}\begin{pmatrix} f_1\\ \vdots \\ f_m\end{pmatrix}$$

ולכן $\begin{pmatrix} e_1\\ e_n\end{pmatrix} = BA\begin{pmatrix} e_1\\ e_n\end{pmatrix}$ $\{e_i\}$ בת"ל, ולכן $BA=I_{n\times n}$ וכן $AB=I_{m\times m}$

נסמן $A'=\begin{pmatrix} A & \vdots \end{pmatrix}_{n\times n}$, $B'=\begin{pmatrix} B \\ \vdots \end{pmatrix}_{n\times n}$. כעת: $B'A'=I_n$. אבל $A'B'=diag(I_m,0)$ וזה לא יתכן כי R חוג קומוטטיבי, ומשפט ... לאחת ההנחות הראשונות בקורס.

טענה יהי M מודול מעל חוג קומוטטיבי, ויהיו $\{b_i\},\{c_i\}$ בסיסים של M. אזי: $(b_i)=A(c_i)$ $A\in U(M_n(R))$

טענה $Hom(R^m,R^n) \overset{התאמה}{=\!=} M_{m\times n}(R)$ (כתוצאה מטל' התרגיל)

טענה $End_R R^n$ אנטי-איזומורפי ל $M_n(R)$

הערה אם R קומוטטיבי, יש $\eta: M_n(R)\to M_n(R)$ אנטי-איזומורפיזם, $A\mapsto A^T$, ולכן $End_R M$ איזומורפי ל $M_n(R)$ ע"י הרכבת η לאנטי-איזומורפיזם של הטענה הקודמת.

הגדרה סכום ישר של מודולים $\{M_i\}_1^n$ $\quad M_1\oplus M_2\oplus\cdots\oplus M_n=\bigoplus_{i=1}^n M_i$

הגדרה סכום ישר של הומומורפיזמים?

טענה

$$\bigoplus_{i=1}^n Hom(M_i,N)\cong Hom\left(\bigoplus_{i=1}^n M_i,N\right)$$

הגדרה סכום ישר פנימי: מודול M, $M_i\subset M$ מודולים המקיימים: $M_i\cap\left(\sum_{j\neq i}M_j\right)=\{0\}$, $M=\sum_{i=1}^n M_i$

M יקרא הסכום הישר של $\{M_i\}$

טענה: אם M סכום ישר פנימי של $\{M_i\}$ אז $M \cong \bigoplus_{i=1}^{n} M_i$

הגדרה: מודול נקרא נוצר סופית אם קיימת לו תת-קבוצה סופית היוצרת אותו.

משפט יסודי: D תחום ראשי קומוטטיבי, K מודול חלקי של D^n אזי K חופשי, ודרגתו $\leq n$. 133

הוכחה: באינדוקציה על n: $n=1$: $K \subset D^1 \cong D$ מודול חלקי, כלומר אידיאל. $K=0$, מודול חופשי מדרגה 0. אחרת $K=DF$ כאשר $F\in D$. אזי $\{F\}$ קס"ס של DF. (כי F יוצר את D, וכן הוא בת"ל כי D תחום)

כעת נניח שהמשפט נכון עבור $n-1$. יהי $K \subset D^n$ מודול חלקי. תהי

$\mu : D^n \to D^n/D^{n-1}$ ההעתקה הקנונית. נסמן $\bar{K}=\mu(K)$

$D^n/D^{n-1} \cong D$ ולכן אם $\bar{K}=0$ אזי $K\subset D^{n-1}$, ואז מהנחת האינדוקציה גמרנו. ולכן נניח $\bar{K}\neq 0$. אזי לפי $n=1$ $\bar{K}=D\bar{F}$ כאשר $\bar{F}=F_1+D^{n-1}$, $F_1\in K$. כעת לפי משפט האיזומורפיזם: $\bar{K}=\frac{K+D^{n-1}}{D^{n-1}} \cong K/K\cap D^{n-1}$. כעת $K\cap D^{n-1}\subset D^{n-1}$ ולכן מהאינדוקציה $K\cap D^{n-1}$ חופשי מדרגה $\leq n-1$.

נבחר לו קס"ס $F_2,\dots,F_m \in K$ $(n-1\geq m-1)$. נראה ש $\{F_i\}_1^m$ בסיס של K. נניח ש $\sum b_iF_i=0$ אזי $\sum b_j\bar{F}_j=0$ אבל $\bar{F}_j=0$, $j\geq 2$ ולכן $b_1\bar{F}_1=0$ ולכן $b_1=0$ ולכן $\sum_{j=2} b_jF_j=0$ ו $\{F_j\}_2^m$ קס"ס ולכן $b_j=0$ $\forall j$. ולכן $\{F_i\}_1^m$ קס"ס של K. מש"ל.

[illegible] חושב: $M \cong D^{(n)}/K$ K חופשי מדרגה $\leq n$.

יהי $e_1,\dots,e_n$ קס"ס של $D^{(n)}$ ו $F_1,\dots,F_m$ יוצרים של K. $\begin{pmatrix}F_1\\ \vdots\\ F_m\end{pmatrix}=M\begin{pmatrix}e_1\\ \vdots\\ e_n\end{pmatrix}$ ננסה לפשט את A.

נבחר בסיס $\begin{pmatrix}e'_1\\ \vdots\\ e'_n\end{pmatrix}=P\begin{pmatrix}e_1\\ \vdots\\ e_n\end{pmatrix}$ P הפיכה

$\begin{pmatrix}F'_1\\ \vdots\\ F'_m\end{pmatrix}=Q\begin{pmatrix}F_1\\ \vdots\\ F_m\end{pmatrix}$ ואז $\begin{pmatrix}F'\end{pmatrix}=QAP^{-1}\begin{pmatrix}e'_1\\ \vdots\\ e'_n\end{pmatrix}$

<u>תזכורת</u>: $A,B\in M_{m\times n}(D)$ יקראו שקולות אם קיימות $P,Q\in \mathcal{U}(M_n(D))$ כך ש $PAQ=B$

<u>משפט</u>: יהי D תחום ראשי, $A\in M_{m\times n}(D)$ אז קיימת מטריצה שקולה ל-A שצורתה

$$\begin{pmatrix} d_1 & & & 0 \\ & \ddots & & \\ & & d_r & \\ 0 & & & 0 \end{pmatrix}$$

כך ש- $d_1|d_2|\dots|d_r$ ול d_i יקראו הגורמים האינווריאנטים של A

<u>הוכחה</u>: נבנה את המשפט הזה עבור תחום אוקלידי:

תזכורת: המטריצות האלמנטריות: (הפיכות)

(טרנספוזיציות) $\begin{pmatrix} 1 & \cdots & b \\ & \ddots & \\ & & 1 \end{pmatrix}$; $\begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & u & \\ & & & 1 \end{pmatrix}$ כפל שורה ב-u הפיך ; $\begin{pmatrix} 1 & & & \\ & 0 & 1 & \\ & 1 & 0 & \\ & & & 1 \end{pmatrix}$ (מחליף שתי שורות)

נרצה את ההגדרה לשפרת פעולות אלמנטריות כמו ~~...~~ שעושים במציאת בזות-סמית כאשר את deg מחליף $\delta(a,b)$.

מ.נ.ל

מעל הוכחה עבור D ראשי: נוסיף כמטריצה אלמנטרית נוספת את:

$$\begin{pmatrix} x & s & & \\ y & t & & 0 \\ & & 1 & \\ 0 & & & \ddots & 1 \end{pmatrix}$$

כאשר $\begin{pmatrix} x & s \\ y & t \end{pmatrix}$ הפיכה.

כעת יהי $0\neq a\in D$ אז $a=p_1\cdots p_r$, p_i ראשוניים. אז נגדיר $r=l(a)$. כעת אם l של מטריצה $\begin{pmatrix} a_{11} & a_{12} & \cdots \\ 0 & 0 & \end{pmatrix}$ אז נסמן $a=a_{11}, b=a_{12}$ וכעת אם $a|b$.

אם $a\nmid b$ אז $(a,b)=\delta$, $l(\delta)<l(a)$ כי D ראשי ולכן $d=ax+by$. נחלק ב-δ: $1=\frac{a}{\delta}x+\frac{b}{\delta}y$

נסמן $s=b/\delta$, $t=-a/\delta$ ואז $1=-tx+sy$ כעת

$$\begin{pmatrix} -t & s \\ y & -x \end{pmatrix}\begin{pmatrix} x & s \\ y & t \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

ולכן $\begin{pmatrix} x & s & & \\ y & t & & 0 \\ & & 1 & \\ 0 & & & \ddots & 1 \end{pmatrix}$ אלמנטרית.

נכפיל אותה עם המטריצה שלנו:

$$\begin{pmatrix} a_{11} & a_{12} & 0 \\ & 0 & \end{pmatrix}\begin{pmatrix} x & s & & 0 \\ y & t & & \\ & & 1 & \\ 0 & & & \ddots & 1 \end{pmatrix}=\begin{pmatrix} d & 0 & \\ & \ddots & \\ & & \end{pmatrix}$$

והצלחנו להוריד

אז $l(a_{11})$ וכן אפשר לקחת את l כמו δ של ההוכחה הקודמת ולהמשיך

$ann\, z=\{a\in D \mid az=0\}$

<u>הגדרה</u>: המטריצה $\begin{pmatrix} d_1 & & & \\ & d_n & & \\ & & 0 & \\ & & & 0 \end{pmatrix}$ תקרא הצורה הנורמלית של המטריצה A.

<u>טענה</u> <u>הוכחה</u>: הצורה הנורמלית של מטריצה היא יחידה.

נניח $A=\begin{pmatrix} d_1 & & \\ & \ddots & \\ & & \end{pmatrix}\cong\begin{pmatrix} d_1' & & \\ & \ddots & \\ & & \end{pmatrix}=B$ אזי d_1 מחלק את כל איברי A ולכן את כל איברי כל המטריצות השקולות לA, ובפרט $d_1|d_1'$ ובאותו אופן נקבל ש $d_1\sim d_1'$ ונמשיך באינדוקציה על המינורים בגודל 2×2, 3×3, ...

(כמו בהוכחה לשורה) נקבל ש לכל n: $\prod_1^n d_i \sim \prod_1^n d_i'$ ומכאן מיידית לכל i, $d_i\sim d_i'$

מש"ל.

<u>הגדרה</u>: (d_i) יקראו הגורמים האינווריאנטים.

<u>טענה</u>: יהי D תחום ראשי, $(a_i)_1^n\in D$, d הממ"מ של (a_i) אזי קיימת $Q\in GL(M_n(D))$ כך ש

$$(a_1\ldots a_n)Q=(d,0,\ldots,0)$$

<u>הוכחה</u>: באינדוקציה. עיקר הרעיון בהוכחה, אפשר

$$(a_1\ldots a_n)\xrightarrow{Q_1}((a_1,a_2),0,a_3,\ldots,a_n)\xrightarrow{Q_2}((a_1,a_2,a_3),0,0,a_4,\ldots,a_n)\xrightarrow{Q_3}\ldots\xrightarrow{Q_{n-1}}(d,0,0,0)$$

נגדיר $Q=\prod_{i=1}^{n-1}Q_i$.

מש"ל.

<u>משפט</u> (משפט המבנה של מודול נוצר סופית מעל תחום ראשי) יהי M מודול נוצר סופית מעל תחום ראשי D אזי קיימים $z_1\ldots z_s\in M$ כך ש $M=Dz_1\oplus\ldots\oplus Dz_s$ וכן $ann\, z_1\supseteq ann\, z_2\supseteq\ldots\supseteq ann\, z_s$

<u>הוכחה</u>: יהי $(X_i)_1^n \subset M$ קבוצה יוצרת את M, ויהי
$e_1 \dots e_n$ בסיס של D^n. נגדיר הומומורפיזם
$\eta: D^n \to M$ ע"י ההעתקה של
$e_i \mapsto X_i$. נסמן $K = \ker \eta$ ניקח
$F_1 \dots F_m$ אשר פורשים את K, ידוע ש

$$\begin{pmatrix} F_1 \\ \vdots \\ F_m \end{pmatrix} = A \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}$$

$A \in M_{m \times n}(D)$. אז קיימות Q, P הפיכות
מעל D כך ש $QAP^{-1} = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix}$
נגדיר

$$(*) \quad \begin{pmatrix} e_1' \\ \vdots \\ e_n' \end{pmatrix} = P \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}, \quad \begin{pmatrix} F_1' \\ \vdots \\ F_m' \end{pmatrix} = Q \begin{pmatrix} F_1 \\ \vdots \\ F_m \end{pmatrix}$$

אז $(F_i')_1^m$ פורשת את K כי Q הפיכה
וכן $(e_i')_1^n$ בסיס של D^n. כמו כן יתקיים

$$\begin{pmatrix} F_1' \\ \vdots \\ F_m' \end{pmatrix} = \begin{pmatrix} d_1 & & & 0 \\ & \ddots & & \\ & & d_r & \\ 0 & & & 0 \end{pmatrix} \begin{pmatrix} e_1' \\ \vdots \\ e_n' \end{pmatrix}$$

כי $(F') = QAP^{-1}(e')$

ולכן יתקיים $F_i' = d_i e_i'$ עבור $i \le r$, $F_{i>r}' = 0$,
$d_1 | d_2 | \dots | d_r$. נפעיל את η על $*$ ונקבל:

$$\begin{pmatrix} \eta(e_1') \\ \vdots \\ \eta(e_n') \end{pmatrix} = P \begin{pmatrix} \eta(e_1) \\ \vdots \\ \eta(e_n) \end{pmatrix} = P \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}$$

נסמן $\eta(e_i') = Y_i$, מהבנייה לעיל, (Y_i) פורשים
את M, כלומר $M = DY_1 + \dots + DY_n$. כמו כן
$0 = \eta(F_i') = \eta(d_i e_i') = d_i Y_i$, כי $F_i' \in \ker \eta$. יהיו $(b_i)_1^n \subset D$, ונניח
ש $0 = \sum_{i=1}^n b_i Y_i$ נקבל:

$$0 = \sum b_i Y_i = \sum b_i \eta(e_i') = \eta\left(\sum b_i e_i'\right)$$

ולכן $\sum b_i e_i' \in K$ ולכן הוא צ"ל של ה- F_i.

כלומר

$$\sum_{1}^{n} b_i e_i = \sum_{i=1}^{r} c_i f_i = \sum_{i=1}^{r} c_i d_i e_i$$

אבל (e_i) בסיס של D^n, ולכן ~~$c_i d_i = 0$~~

לכל $1 \le i \le r$, $b_i = c_i d_i$, ו- $b_i = 0$ לכל $i > r$.

ולכן עבור $i \le r$ נקבל

$$b_i y_i = c_i d_i y_i = c_i \cdot 0 = 0$$

ועבור $i > r$

$$b_i y_i = 0 \cdot y_i = 0$$

ולכן לכל i $b_i y_i = 0$. קיבלנו:

$$\sum b_i y_i = 0 \Longrightarrow b_i y_i = 0 \quad \forall i$$

ולכן $M = Dy_1 \oplus \dots \oplus Dy_n$, כעת יהי $r \ge i \ge 1$ אז:

נניח $b_i y_i = 0$. מאותו תחשיב ~~$\mathrm{ann}\, y_i = \{x \mid y_i x \ne 0\}$~~

קודם נקבל $b_i = c_i d_i$. ועבור $d_i y_i = 0$, ולכן $\mathrm{ann}\, y_i = (d_i)$

ועבור $i > r$ קיבלנו שאם $b_i y_i = 0$ אז $b_i = 0$

כלומר $\mathrm{ann}\, y_i = \{0\}$ מאחר ש $d_1 | d_2 | d_3 \dots | d_r | 0 \dots 0$

נקבל

$$\mathrm{ann}\, y_1 \supseteq \mathrm{ann}\, y_2 \supseteq \dots \supseteq \mathrm{ann}\, y_n$$

דרשנו בנוסף $D \ne \mathrm{ann}\, y_1$. אבל אם $D = \mathrm{ann}\, y_1$

אז $Dy_1 = 0$, ולכן אפשר לוותר עליו

בנוסחה $M = Dy_1 \oplus \dots \oplus Dy_n$ ולכן קיבלנו

$$D \ne \mathrm{ann}\, y_1$$

מש"ל.

הערה: יהי M מודול מעל D, תחום קומוטטיבי, אז:

$\{x \in M \mid \exists a \in D, a \ne 0, ax = 0\}$ מודול חלקי.

ונקרא המודול הפיתולי של M, $\mathrm{tor}\, M$

מודול חסר פיתול.

הערה: בהוכחה הקודמת קיבלנו $M = Dy_1 \oplus \dots \oplus Dy_r \oplus Dy_{r+1} \oplus \dots \oplus Dy_n$

אז $\mathrm{tor}\, M = Dy_1 \oplus \dots \oplus Dy_r$

הערה: בנוסף $Dy_{r+1} \oplus \dots \oplus Dy_n$ מודול חופשי.

משפט המבנה:

$$\begin{tikzcd}
M \arrow[d, equal] & D^n \arrow[l, "\eta"'] \arrow[r, equal] \arrow[d, equal] & D^n \arrow[r, "\eta"] \arrow[d, equal] & M \arrow[d, equal] \\
(y_i)_1^n & \langle (e_i')_1^n \rangle \arrow[l] \arrow[d, dash] & \langle (e_i)_1^n \rangle \arrow[l, "P(e_i)_1^n"'] \arrow[r, "e_i \mapsto x_i"] \arrow[d, dash] & \langle (x_i)_1^n \rangle \arrow[d, dash] \\
& K = \ker\eta \arrow[r, equal] \arrow[d, equal] & K \arrow[r, "\eta"] \arrow[d, equal] & 0 \\
& \langle (f_i')_1^m \rangle & \langle (f_i)_1^m \rangle \arrow[l, "Q(f_i)_1^m"'] &
\end{tikzcd}$$

$f_i' = d_i e_i'$ עבור $1\le i \le r$

$f_i' = 0$ עבור $r < i \le m$

$(f_i)_1^m = A(e_i)_1^n$

נכתוב $D = QAP^{-1}$

יהי M מודול נוצר סופית מעל תחום ראשי קומוטטיבי D, ותהי $(x_i)_1^n$ קבוצת יוצרים שלו. יהי $(e_i)_1^n$ בסיס של D^n. נגדיר $\eta: D^n \to M$ ע"י $\sum a_i e_i \xmapsto{\eta} \sum a_i x_i$ ונסמן $K = \ker\eta$. K מודול חלקי של D^n ולכן הוא חפשי ודרגתו $m \le n$. תהי $(f_i)_1^m$ בסיס של K. אזי $(f_i)_1^m = A(e_i)_1^n$. קיימות מטריצות P, Q הפיכות כך ש $D = QAP^{-1}$ ו D היא $D = \mathrm{diag}(\mathrm{diag}_{i=1}^{r} d_i, 0_{m-r,n-r})$ נסמן $(e_i')_1^n = P(e_i)_1^n$ וכן $(f_i')_1^m = Q(f_i)_1^m$ אזי $(e_i')_1^n$ בסיס אחר של D^n וכן $(f_i')_1^m$ בסיס של K. כמו כן מתקיים עבור $1 \le i \le r$ $f_i' = d_i e_i'$ וכן עבור $r < i$ מתקיים $f_i' = 0$. נסמן כעת $(y_i)_1^n = \eta((e_i')_1^n)$.

<u>טענה:</u> $M = \bigoplus_{i=1}^n D y_i$

<u>הוכחה:</u> $(y_i)_1^n$ יוצרת את M: טריוויאלי. צריך להוכיח שהסכום ישר. נניח כי $0 = \sum_{i=1}^n b_i y_i$ אזי: $0 = \sum_{i=1}^n b_i \eta(e_i') = \eta(\sum b_i e_i')$

ולכן $\sum_{i=1}^n b_i e_i' \in \ker\eta$ ולכן

$$\sum_{i=1}^n b_i e_i' = \sum_{i=1}^m c_i f_i' = \sum_{i=1}^r c_i d_i e_i' + 0$$

ולכן עבור אחד $b_i=0$ ולכן $b_iy_i=0$, ועבור אחר מתקיים

$b_i=c_id_i$ כאשר עבור אחר

$$b_iy_i=c_id_iy_i=c_id_i\eta(e_i)=c_i\eta(d_ie_i)=c_i\eta(f_i)=c_i0=0$$

ולכן לכל i $b_iy_i=0$ ולכן הכיוון שני.

טענה: $\forall i \quad \operatorname{ann} y_i \supset \operatorname{ann} y_{i+1}$

הוכחה: נניח $by_{i}=0$ אזי $\eta(be_{i})=0$ ולכן $be_{i}\in K$ ולכן ~~ולכן $be_i \neq \sum$~~

$$be_i=\sum_{j=1}^{m}c_if_i=\sum_{j=1}^{m}c_id_ie_i$$

ולכן מאחר ו-$(e_i)_1^n$ בסיס נקבל ש $b=cd_i$ ולכן

ולכן $\operatorname{ann} y_i=(d_i)$

מ.ש.ל.

טענה כל מודול נוצר סופית מעל תחום ראשי הוא סכום ישר של מודול פיתול ושל מודול חופשי [$M=torM\oplus N$ כאשר N חופשי]

טענה: N בטענה הקודמת יחיד עד כדי איזומורפיזם

הוכחה קל לראות

$$N\cong M/torM$$

הגדרה יהי M מודול מעל D ראשי. יהי $p\in D$ ראשוני. נגדיר

$$M_p=\{y\in M \mid \exists k\ \ p^k y=0\}$$

טענה: M_p מודול

הגדרה מודולים $M_1,\dots,M_n\subset M$ יקראו בלתי תלויים

$$\{0\}=M_i\cap(M_1+\dots+M_{i-1}+M_{i+1}+\dots+M_n)\ \forall i$$

טענה 145 יהיו ראשוניים $p_1\dots p_k$ לא חברים אזי $M_{p_1}\dots M_{p_k}$ בלתי-תלויים.

הוכחה יהי $y\in M_{p_1}\cap(M_{p_2}+\dots+M_{p_k})$ אזי $p_1^n y=0$ וגם $(p_2 p_3\cdots p_k)^m y=0$ ולכן כי $1=\gcd(p_1^n,(p_2\cdots p_k)^m)$ מאפס את y, כלומר $y=0$

מש"ל

טענה 146 M מודול פיתול נוצר סופית $\Leftarrow$ יש מספר סופי של ראשוניים p כך ש $M_p\neq 0$. אזי הם $p_1\dots p_h$ אזי

$$M=M_{p_1}\oplus\dots\oplus M_{p_h}$$

הוכחה M נוצר סופית ולכן $M=Dx_1+\dots+Dx_n$

נניח $\operatorname{ann} x_i=(d_i)$ יש מספר סופי של ראשוניים $p_1\dots p_h$ כך ש p_i מחלק את אחד מה-d_j-ים. נשים לב כי אם $d_1=p_1^{k_1}\cdots p_h^{k_h}$ אז

$$Dx_1\subset M_{p_1}+\dots+M_{p_h}$$

מש"ל

הגדרה הפירוק הנ"ל: פירוק פרימרי.

משפט כל מודול פיתול נוצר סופית מעל ת"ר הוא סכום ישר של מודולים ציקליים שמאפסיהם מהצורה (p^e), p ראשוני.

הערה נפרק פירוק פרימרי את התוצאה מהמשפט הקודם.

משפט יהי M מודול נוצר סופית מעל תחום ראשי, וכן

$$M = Dz_1 \oplus \dots \oplus Dz_r$$
$$M = Dw_1 \oplus \dots \oplus Dw_s$$

כך ש

$$D \neq \operatorname{ann} z_1 \supseteq \dots \supseteq \operatorname{ann} z_r$$
$$D \neq \operatorname{ann} w_1 \supseteq \dots \supseteq \operatorname{ann} w_s$$

צ"ל: $s=r$ וכן $\operatorname{ann} z_i = \operatorname{ann} w_i$

הוכחה: מתוך מה שעשינו עד עכשיו, נניח M מודול פיתול. כלומר, $0 \neq \operatorname{ann} z_r$, $\operatorname{ann} w_s \neq 0$
כרגע $M = M_{p_1} \oplus \dots \oplus M_{p_n}$ ולכן
להוכיח שהכל $M = M_p$ עבור $p \in D$ כלשהו.
צ"ל
$$\operatorname{ann} Dz_i = (p^{e_i}) \quad 1 \dots r$$
$$\operatorname{ann} Dw_i = (p^{f_i}) \quad 1 \dots s$$
כאשר $e_1 \leq \dots \leq e_r$ וכן $f_1 \leq \dots \leq f_s$
וכן $s=r$ וכן $e_i = f_i$ לכל i.
נשתמש בסדרה
$$M \supseteq pM \supseteq p^2M \supseteq \dots$$
יהי k טבעי, נתבונן ב- $p^kM \supseteq p^{k+1}M$
$p^kM/p^{k+1}M$. זהו מודול מעל D שמתאפס ע"י p, ולכן נוכל לחשוב עליו כמודול מעל $D/(p)$. p ראשוני, ולכן $D/(p) = \bar{D}$ שדה.

ולכן $p^kM/p^{k+1}M$ מרחב וקטורי, ולכן יש לו מימד יחיד.

נסמן כעת t המספר כך ש

$$l_1\le l_2\le\dots\le l_t\le k<l_{t+1}\le\dots\le l_r$$

מספר המחוברים הציקליים של M שמסדר גדול מ-k הוא $r-t$. נראה כי זה שווה ל

$$\dim_{\mathbb{F}_p} p^kM/p^{k+1}M$$

וזה די קל. נזכור את המפורשת, מיחידות המימד.

הלכו כל הראשונים מתאפסים ולכן

$$p^kM=D(p^kz_{t+1})+\dots+D(p^kz_r)$$

ולכן $p^kz_{t+1}+p^{k+1}M,\dots,p^kz_r+p^{k+1}M$ פורשים את $p^kM/p^{k+1}M$

כעת נניח (רוצים להראות שהקבוצה הפורשת היא בסיס)

$$\Omega=\sum_{i=t+1}^{r}a_ip^kz_i\in p^{k+1}M$$

אזי קיימים [illegible] $\{b_i\}$

$$\Omega=\sum_{i=t+1}^{r}b_ip^{k+1}z_i$$

ולכן

$$0=\sum(a_ip^k-b_ip^{k+1})z_i$$

סכום ישר, ולכן

$$(a_ip^k-b_ip^{k+1})z_i=0$$

ולכן

$$p^{l_i}\mid a_ip^k-b_ip^{k+1}$$

$k<l_i$ ולכן אפשר לצמצם בק ואז

$$p^{l_i-k}\mid a_i-b_ip$$

ולכן בפרט

$$p\mid a_i-b_ip$$

ולכן $p\mid a_i$ ולכן $a_ip^k\in p^{k+1}M$ ולכן הקבוצה בת"ל

הגדרה: יהי V מ"ו ממימד סופי מעל F.
נהפוך את V למודול מעל $D=F[x]$
בעזרת אופ' $T:V\to V$ העתקה לינארית

$$g\in F[x],\ x\in V$$

אז:

$$gx=g(T)x$$

יהי $\{v_i\}_1^n$ ב.ס. של V מעל F אז:

$$T\begin{pmatrix}v_1\\ \vdots\\ v_n\end{pmatrix}=A\begin{pmatrix}v_1\\ \vdots\\ v_n\end{pmatrix}$$

אם $\{w_i\}_1^n$ ב.ס. אחר של V כך ש-

$$\begin{pmatrix}w_1\\ \vdots\\ w_n\end{pmatrix}=P\begin{pmatrix}v_1\\ \vdots\\ v_n\end{pmatrix}$$

אז

$$T\begin{pmatrix}w_1\\ \vdots\\ w_n\end{pmatrix}=PAP^{-1}\begin{pmatrix}w_1\\ \vdots\\ w_n\end{pmatrix}$$

טענה: כזה מודול פ"נ

הוכחה: V מ"ו ממימד סופי, ולכן לכל $x\in V$
$x,\lambda x,\lambda^2x,\lambda^3x\dots\lambda^nx$ תלויים לינארית מעל

נניח:

$$V=Dv_1+\dots+Dv_n$$

נגדיר $\eta:D^n\longrightarrow V$ העתקה $\eta(e_i)=v_i$
כאשר $(e_i)_1^n$ ב.ס. של D^n. נגדיר:

$$K=\ker\eta$$

נסמן $f_i=xe_i-\sum_{j=1}^n a_{ij}e_j\in D^n$. נראה ש- $f_i\in K$:

$$\eta(f_i)=Tv_i-\sum_{j=1}^n a_{ij}v_j=Tv_i-Av_i=0$$

נראה:

$$xe_i=f_i+\sum_j a_{ij}e_j$$

ניקח איבר כללי:

$$\sum g_i(\lambda)e_i=\sum h_i(\lambda)f_i+\sum b_ie_i$$

נראה אם $\sum g_i(\lambda)e_i \in K$ אזי הוא שווה ~~[illegible]~~ לאפס [illegible] ולכן

כי ($\sum b_i e_i$)$=0$ ~~[illegible]~~ ולכן $\sum b_i v_i = 0$ ולכן $b_i = 0$ ולכן

$$\sum g_i(\lambda)e_i = \sum h_i(\lambda)f_i$$

ולכן $\{f_i\}$ פורש את הגרעין

נוכיח שהם בסיס: בת"ל

$$\sum h_i(\lambda)f_i = 0$$

אזי:

$$\sum_i h_i(\lambda)\lambda e_i = \sum_{i,j} h_i(\lambda)a_{ij}e_j$$

$\{e_i\}$ בסיס ולכן לכל r

$$\sum h_r(\lambda)\lambda = \sum h_i(\lambda)a_{ir}$$

נבחר r כך ש $\deg h_r$ מקסימלי. בצד ימין נקבל פולינום ממעלה נמוכה יותר מאשר ~~[illegible]~~ שמאל

ולכן לכל i $h_i=0$.

כנדרש

$$\begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} = \begin{pmatrix} \lambda-a_{11} & -a_{12} & \cdots & -a_{1n} \\ \vdots & & & \vdots \\ -a_{n1} & \cdots & & \lambda-a_{nn} \end{pmatrix} \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}$$

כלומר $(f_i) = (\lambda I - A)(e_i)$, נעבור אל ~~[illegible]~~

$\lambda I - A$ לצורתה הקנונית

$$Q(\lambda I - A)P^{-1} = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & d_1(\lambda) & \\ & & & & \ddots \\ & & & & & d_s(\lambda) \end{pmatrix}$$

$$\begin{pmatrix} e'_1 \\ \vdots \\ e'_n \end{pmatrix} = P\begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}$$

כאשר $d_1 | \dots | d_s$ כנדרש

נגדיר את m ונקבל

$$\begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = P\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$$

$\{u_i\}$ בסיס של V ~~[illegible]~~ כמודול מעל $F[\lambda]$

נניח מודול מעל $D=F[\lambda]$

$$V = Du_1 \oplus Du_2 \oplus \dots \oplus Du_n$$

נניח הראשונים הם ה-0, אזי

$$V = Du_{n-s+1} \oplus \dots + Du_n$$

* נסמן ע"י

$$V = Dz_1 \oplus \dots \oplus Dz_s$$

אזי $\operatorname{ann} z_i = (d_i(\lambda))$

נניח $s=1$ אזי $V=Dz_1$, $d_1(\lambda)=f(\lambda)$

אז $\operatorname{ann} z_1 = \operatorname{ann} z = (f(\lambda))$ אזי $\deg f = n$

ולכן $z, \lambda z, \dots, \lambda^{n-1} z$ בסיס של V מעל F

נכתוב את f:

$$f(\lambda) = \lambda^n - a_1\lambda^{n-1} + a_2\lambda^{n-2} - \dots + (-1)^n a_n$$

כעת, מהגדרת λ

$$\cancel{f(z)=0} \quad Tz = \lambda z$$

$$T(\lambda z) = \lambda^2 z$$

$$T\lambda^{n-2}z = \lambda^{n-1}z$$

$$T\lambda^{n-1}z = \lambda^n z = f(\lambda)z + a_1\lambda^{n-1}z - \dots + (-1)^{n-1}a_n z =$$

$$= a_1\lambda^{n-1}z - \dots + (-1)^{n-1}a_n z$$

ולכן המטריצה המייצגת לפי הבסיס T היא:

$$\begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & 0 & 1 \\ (-1)^{n-1}a_n & \dots & & -a_2 & a_1 \end{pmatrix}$$

נקראת המטריצה המלווה של f

(companion matrix)

נזכיר למקרה הכללי: $s\neq 1$ $d_1(\lambda)\ldots d_s(\lambda)$

הם הגורמים האינווריאנטים של $\lambda I-A$

נסמן $\deg d_i(\lambda)=n_i$ אז: $f(\lambda)=\prod d_i(\lambda)$

כאשר $f(\lambda)=\det I\lambda-A$ הפולינום האופייני. לכן $n_1+\ldots+n_s=n=\deg f$ ונוכל לבחור בסיס

של V כמו מעל F יהיה למשל

$$\bigcup_{i=1}^{s}\bigcup_{j=0}^{n_i-1}\{\lambda^j z_i\}$$

ואז T יוצר את המטריצה (הנקראת הצורה הקנונית הרציונלית של T ביחס לבסיס הנ"ל):

$$B=\operatorname{diag}_{i=1}^{s} B_i$$

כאשר B_i המטריצה המלווה של $d_i(\lambda)$

$A,B\in M_n[F]$ דומות אמ"מ אותם גורמים אינווריאנטים

אמ"מ $\lambda I-A$, $\lambda I-B$ שקולות מעל

$U(M_n(F[x]))$ אמ"מ אותה צורה קנונית

רציונלית אמ"מ אותם מחלקים אלמנטריים

אמ"מ אותה צורת ז'ורדן (כאשר היא קיימת)

~~הגדרה~~ $d_s(\lambda)=m(\lambda)$ הפולינום המינימלי

טענה $m(T)x=0$ לכל $x\in V$

הוכחה $V=Dz_1\oplus\ldots\oplus Dz_s$, $d_i(T)z_i=0$, $d_i|d_s$, ולכן

$d_s(T)z_i=0$ $\forall i$, ו-$\{z_i\}_{i=1}^{s}$ יוצרים את V.

טענה לא קיים פולינום ממעלה קטנה מ-m שמאפס את V.

יהי M נוצר סופית מעל תחום ראשי D

ונתון $\eta\in\mathrm{Hom}(M,M)$. נפרק אותו:

$$M=Dz_1\oplus\ldots\oplus Dz_s$$

כאשר $\mathrm{ann}(z_1)\supseteq\ldots\supseteq\mathrm{ann}\, z_s$

נגדיר $w_i=\eta(z_i)$ אז ברור ש $\{w_i\}$ יוצרים

נבדוק ש- η מוגדר היטב. ברור ש $az_i=0 \Rightarrow aw_i=0$.

ולכן $\mathrm{ann}\, z_i \subset \mathrm{ann}\, w_i$ $\forall i$.

כיוון נניח ש $\{w_i\}$ קב' ש. $\mathrm{ann}\, z_i \subset \mathrm{ann}\, w_i$ $\forall i$,

נגדיר $\eta(\sum a_i z_i)=\sum a_i w_i$ זה מוגדר היטב. כי אם

$$\sum a_i z_i=\sum b_i z_i$$

אז $\sum(a_i-b_i)z_i=0$, ולכן לכל i $(a_i-b_i)z_i=0$, ולכן

$(a_i-b_i)w_i=0$, ולכן $\sum a_i w_i=\sum b_i w_i$.

נניח כעת את w_i בצורה:

$$w_i=\sum_j b_{ij} z_j$$

כעת $d_i z_i=0 \Rightarrow d_i w_i=0 \Rightarrow \sum_j d_i b_{ij} z_j=0 \Rightarrow d_i b_{ij} z_j=0$

ולכן b_{ij} מקיימים $d_j \mid d_i b_{ij}$ כאשר

$$(d_i)=\mathrm{ann}\, z_i$$

כלומר $d_i b_{ij}=c_{ij} d_j$ עבור c_{ij} כלשהו. כלומר:

$$\begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_s \end{pmatrix} B = C \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_s \end{pmatrix}$$

נסמן $\Delta=\mathrm{diag}_{i=1}^{s}\, d_i$ כלומר, המטריצה B המייצגת את הטרנספורמציה היא כזאת שקיימת C כך ש $\Delta B=C\Delta$. נסמן $R=\{B\in M_s(D) \mid \exists C\in M_s(D)\ \Delta B=C\Delta\}$

<u>טענה</u> R הוא חוג חלקי של $M_s(D)$

<u>הוכחה</u> אם $\Delta B_1=C_1\Delta$, $\Delta B_2=C_2\Delta$ אז $\Delta(B_1+B_2)=(C_1+C_2)\Delta$

וגם $\Delta B_1 B_2=C_1\Delta B_2=C_1C_2\Delta$

<u>טענה</u> $\eta \longrightarrow (b_{ij})$ אפי' הומומורפיזם.

<u>טענה</u> יש איזומורפיזם ל R/K כאשר

$$K=M_s(D)\Delta$$

<u>הוכחה</u> (1) $K\subset R$ אי'

1) נניח $\eta=0$ אזי $W_i=\sum b_{ij}z_j=0$ ולכן $b_{ij}z_j=0$ ולכן

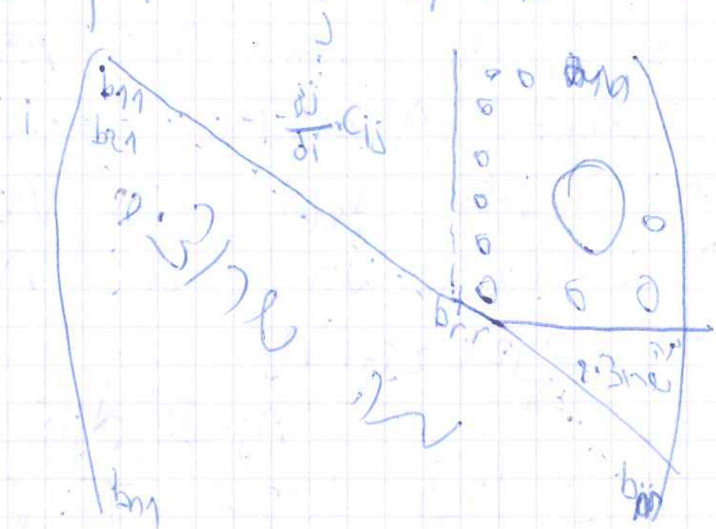
$d_j | b_{ij}$ ולכן $b_{ij}=c_{ij}d_j$ ולכן (A_{ij})

$$(b_{ij})=(c_{ij})\Delta\in K$$

הערה: נעבור למקרה לא-אומורפיזם $B\mapsto B^T\mapsto \eta''$

נניח שיש $\{d_i\}$ כך ש $d_1 \dots d_r\neq 0$, ולכן $d_{r+1}=\dots=d_s=0$

נניח שיש $d_j | d_i b_{ij}$ נתון ... (b_{ij})



במקרה הכללית לפי הרצף

דוגמה: $M=\mathbb{Z}_{a_1}\oplus\mathbb{Z}_{a_2}\oplus\mathbb{Z}_{a_3}$ כך ש $n_1=4, n_2=12, n_3=24$ המינימום

של $a_{1,2,3}$ של ההגדרה הכללית היא:

$$R=\left\{\begin{pmatrix} b_{11} & 3c_{12} & 6c_{13} \\ b_{21} & b_{22} & 2c_{23} \\ b_{31} & b_{32} & b_{33}\end{pmatrix}\right\}$$

$$K=M_3(\mathbb{Z})\begin{pmatrix} 4 & 0 & 0 \\ 0 & 12 & 0 \\ 0 & 0 & 24\end{pmatrix}=\dots$$

ולכן $D\underset{ab}{\cong}R/K$ כאשר R מודולו K. אזי

$$R/K\cong\begin{pmatrix} 0,1,2,3 & 0,3,6,9 & 0,6,12,18 \\ 0,1,2,3 & 0-11 & 0,2,4,\dots,22 \\ 0,1,2,3 & 0-11 & 0-23\end{pmatrix}$$

אזי $|R/K|=4^5 12^3\cdot 24$ כלומר $|R/K|=2^{19}\cdot 3^2$

דוגמה: $T:V\to V$ ו-V מימדי סופי, $D=F[\lambda]$

$$V=Dz_1\oplus\dots\oplus Dz_s$$

כשהמשפט היא $d_1(\lambda)|\dots|d_s(\lambda)$ אזי

$$R=\left\{\begin{pmatrix} b_{11} & & \\ & \frac{d_j(\lambda)}{d_i(\lambda)}c_{ij} & \\ b_{ij} & & b_{ss}\end{pmatrix}\right\} \quad \text{ו} \quad K=\left\{\begin{pmatrix} \cdots & \cdots \end{pmatrix}\right\}$$

לכן קל לראות מה R/K

$R/K \cong$

משפט 1

תהי $A\in M_n(F)$. מה המימד של S: כל המטריצות המתחלפות עם A

משפט (Frobenius) תהי $A\in M_n(F)$, $S\subset M_n(F)$ המטריצות המתחלפות עם A

~~אזי~~ אם $d_1(\lambda)\dots d_s(\lambda)$ הם הגורמים האינווריאנטים של A אז המימד של S הוא

$$\sum_{j=1}^{s}(2s-2j+1)n_j$$

כאשר $n_j=\deg d_j(\lambda)$

הגדרה $T:V\to V$ נקרא ציקלי אם $V=D_z$ כאשר $D=F[\lambda]$

משפט T ציקלי $\iff C(T)=F[T]$

הוכחה T ציקלי $\Leftarrow n_1=n_s=\dim S \Leftarrow \dim S=\dim F[T] \Leftarrow S=F[T]$

כי $C(T)=S\supseteq F[T]$

T לא ציקלי $\Leftarrow \dim S > n_s \Leftarrow \dim S>\dim F[T] \Leftarrow$ ...

הכלה $S \supset F[T]$ ממש

מ.ש.ל.

למה לכל $T:V\to V$ מעל F $F[T]\subset C(C(T))$

משפט $C(C(T))=F[T]$

הוכחה $U\in C(T) \Leftarrow U\in \mathrm{Hom}(V,V)$ כש-V מודול מעל $D=F[T]$ אזי

מתחלף את המרכב של $D'=\mathrm{Hom}(V,V)$.

קל לראות ש- $(x\mapsto ax)\in C(D')$ $\forall a\in D$ עבור קבוע

כמו כן $F[T]\subset C(D')$ לכן נשאר להוכיח ש

המרכב הוא מוכפלה הכל: יהי $\gamma\in C(D')$ נפרק את V

$V=D_{z_1}\oplus\dots\oplus D_{z_s}$ נגדיר $E_{is}:V\to V$ כך ש

$E_{is}\in D'$ ... כל מקדם $\sum_{j=1}^{s}a_j z_j \longmapsto a_s z_i$

ולכן $\gamma\epsilon_{is}=\epsilon_{is}\gamma$ לכל i; ולכן $\gamma z_s=\gamma\epsilon_{ss}z_s=\epsilon_{ss}(\gamma z_s)=\epsilon_{ss}(\sum a_i z_i)=a_s z_s$

כלומר $\gamma z_s=a_s z_s$. כמו כן

$$\gamma z_i=\gamma\epsilon_{is}z_s=\epsilon_{is}\gamma z_s=\epsilon_{is}a_s z_s=a_s\epsilon_{is}z_s=a_s z_i$$

ולכן לכל i: $\gamma(z_i)=a_s z_i$ ולכן לכל $z\in V$: $\gamma(z)=a_s z$

מ.ש.ל

דוגמה: $A=\begin{pmatrix}1&0&0\\0&0&1\\0&-1&2\end{pmatrix}$ פולינומים אלמנטריים: $(\lambda-1)^2, \lambda-1$ ולכן

$V=Dz_1\oplus Dz_2$ כאשר המאפס של z_1 הוא $\lambda-1$

ושל z_2 הוא $(\lambda-1)^2$ הבסיס של V: $z_1, z_2, \lambda z_2$

איבר של $\mathrm{Hom}(V,V)$ הוא $\begin{pmatrix}b_{11}&b_{12}(\lambda-1)\\b_{21}&b_{22}+b'_{22}\lambda\end{pmatrix}$. נקרא לו U ובנוסף

$\lambda^2 z_2-2\lambda z_2+z_2=0$

אז:

$$Uz_1=b_{11}z_1+b_{12}(\lambda-1)z_2$$

$$Uz_2=b_{21}z_1+(b_{22}+b'_{22}\lambda)z_2$$

$$U\lambda z_2=b_{21}\lambda z_1+b_{22}\lambda z_2+b'_{22}\lambda^2 z_2=$$

$$=b_{21}z_1+b_{22}\lambda z_2+b'_{22}(2\lambda z_2-z_2)$$

אז U הוא בבסיס

$$U\Longleftrightarrow\begin{pmatrix}b_{11}&-b_{12}&b_{12}\\b_{21}&b_{22}&b'_{22}\\b_{21}&-b'_{22}&b_{22}+2b'_{22}\end{pmatrix}$$

ולכן המטריצות המתחלפות עם A הן מהצורה

קיום המיון:

$$\begin{tikzcd}
M & A^n \arrow[l, "m"'] \arrow[r, equal] \arrow[d, equal] & A^n \arrow[r, "m"] \arrow[d, equal] & M \arrow[d, dash] \\
(y_i)_1^n \arrow[u, equal] & (e'_i)_1^n \arrow[l, "m"'] \arrow[dd, dash] & (e_i)_1^n \arrow[l, "P(e_i)_1^n"'] \arrow[r, "e_i \mapsto x_i"] \arrow[d, dash] & (x_i)_1^n \arrow[d, dash] \\
& & \ker m = K \arrow[r, "m"] \arrow[d, equal] & 0 \\
0 & (f'_i)_1^m \arrow[l, "m"'] & (f_i)_1^m = A(e_i)_1^n \arrow[l, "Q(f_i)_1^m"'] &
\end{tikzcd}$$

$1 \le i \le r \quad f'_i = d_i e'_i$

$m \geq i > r \quad f'_i = 0$

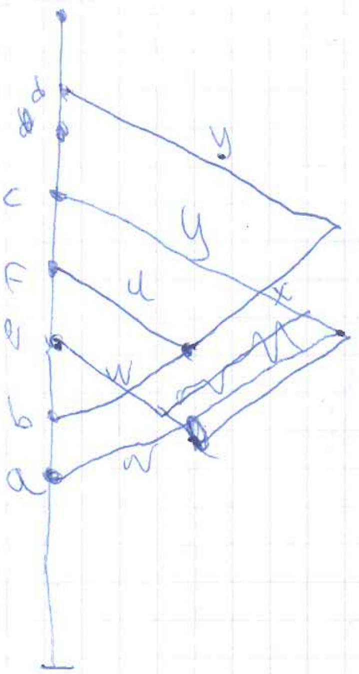
יחידות המיון:

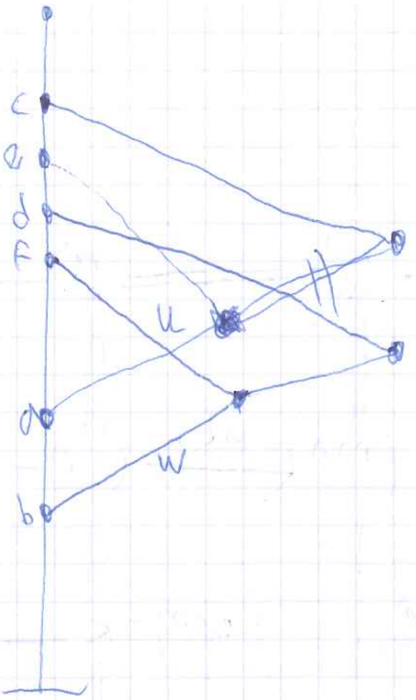
$$\operatorname{ann} D_{z_i} = (p^{l_i}) \qquad \bigoplus D_{z_i} = M_p = \bigoplus D_{w_i} \qquad \operatorname{ann} D_{w_i} = (p^{f_i})$$

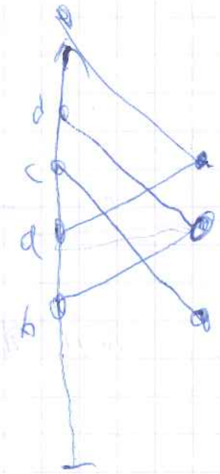
$$\begin{tikzcd}
M_p \arrow[d, dash] \\
pM \arrow[d, dash] \\
p^2M \arrow[d, dash] \\
\vdots \arrow[d, dash] \\
p^kM \arrow[r] \arrow[d, dash] & p^kM/p^{k+1}M \arrow[d, equal] \\
p^{k+1}M & \langle p^k z_{t+1} + p^{k+1}M, \ldots, p^k z_r + p^{k+1}M \rangle
\end{tikzcd}$$

$l_1 \le \ldots \le l_t \le k < l_{t+1} \le \ldots \le l_r$

מ"ו מעל $D/(p) = \bar{D}$







ראשוני

נניח a פריק אז $a=bc$,

$a|bc$

ולכן $a|b$ או $a|c$

נניח $a|b$ אז קיים d כך ש

אז $ad=b$

$adc=bc$

$dc=1$

ולכן c הפיך סתירה

~~V מ"ו מעל~~

V מודול מעל $D=F(\lambda)$

$$V \xrightarrow{T} V$$

V מ"ו מעל F

V מ"ו מעל F

$$V \xrightarrow{T} V$$

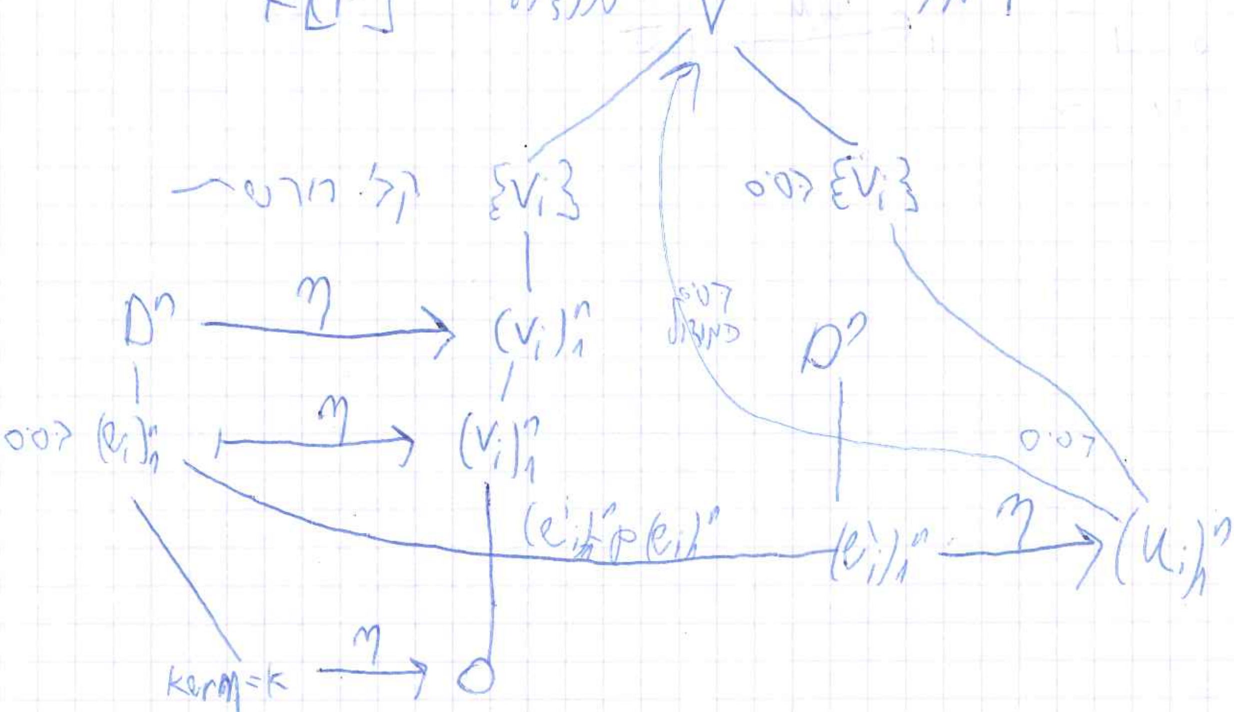
V מודול מעל $D=F(\lambda)$

$V \overset{T}{\circlearrowright}$ מ"ו מעל F

$D=F[T]$ מעל מודול

$T=A=(a_{ij})_{a_{i,j}}$

$F[T]$ מודול V מ"ו F



$$\left\{ \varepsilon_i = \lambda e_i - \sum_{j=1}^{n} a_{ij} v_j \right\} = (\lambda I - A)(e_i)_1^n$$

טענה: יהי O תחום ראשי קומוטטיבי, $O^n \supseteq K$ מודול חלקי.
אזי K חופשי ודרגתו $\leq n$.
הוכחה באינדוקציה:

$$\begin{tikzcd}
& O^n \arrow[dl, dash] \arrow[d, dash] \\
O^{n-1} & K
\end{tikzcd}$$

$$\begin{tikzcd}
& O^n \arrow[dl, dash] \arrow[d, dash] \arrow[rr, "M", "\text{ההעתקה הקנונית}"'] & & O^n/O^{n-1} \arrow[d, dash] \arrow[r, "\cong"] & O \\
O^{n-1} \arrow[d, dash] & K \arrow[dl, dash] \arrow[rr, "M"] & & \bar{K} \arrow[r, "\cong"] \arrow[d, equal, "n=1"] & F/K \cap O^{n-1} \\
K \cap O^{n-1} & F_1 & & O\bar{F} \arrow[ll, "M^{-1}"'] &
\end{tikzcd}$$

נ.ס.ע
$F_2, \dots, F_m$

~~$12 = 6+4+3+2+1 = 16 = 15 = 5+3+1 = 8 = 3+1 = 4 = 3 = 1 = 1$~~

~~$1260 = 360 + 200 + 155 + 72 + 100 + 6 + 5 + 4 + 3 + 2 + 1 + 108 =$~~

~~$= 1 + 2 + 3 + 4 + 6 + 9 + 12 + 18 + 27 + 36 + 54 = 1000$~~

$S = 1$

$$0 = f(\lambda) \qquad Dz_1 = V \xrightarrow[n]{\text{מ' לינארית}} F$$

$$\operatorname{ann} z_1 = (f(\lambda))$$

בסיס

$$\langle z, \lambda z, \ldots, \lambda^{n-1} z \rangle$$

$$\deg f = n$$

$$f = \lambda^n - a_1\lambda^{n-1} + \ldots + (-1)^n a_n$$

$$Tz = \lambda z$$

$$T(\lambda z) = \lambda^2 z$$

$$\vdots$$

$$T\lambda^{n-2} z = \lambda^{n-1} z$$

$$T\lambda^{n-1} z = \lambda^n z = f(\lambda) z + a_1\lambda^{n-1} z - \ldots + (-1)^{n-1} a_n z =$$

$$= a_1\lambda^{n-1} z - \ldots + (-1)^{n-1} a_n z$$

אז מטריצה ל T היא

$$\begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & & 1 \\ & & & 0 & 1 \\ (-1)^{n-1} a_n & \ldots & \ldots & -a_2 & a_1 \end{pmatrix}$$

מט' מלווה ל F

המקרה הכללי $(s \geq 1)$:

$D = F(\lambda)$

$V = \bigoplus D z_i$ מ"ו ממי' n מעל F

ב"ס: $\left\langle \bigcup_{i=1}^{s} \bigcup_{j=0}^{n_i-1} \{\lambda^j z_i\} \right\rangle$

$\operatorname{ann} z_1 = (F_1(\lambda))$, $\deg = n_1$

$\vdots$

$\operatorname{ann} z_s = (F_s(\lambda))$, $\deg = n_s$

$\sum_{i=1}^{s} n_i = n$

המטריצה

$[T] = B = \operatorname{diag}_{i=1}^{s} B_i$

כאשר B_i המלווה ל $\cancel{\ }$ $d_i(x)$

~~End~~

$$\eta : R^n \circlearrowleft \in \mathrm{End}_R R^n$$

יהי R^n ל בסיס $(x_i)_1^n$

$$(y_i) = \eta((x_i))$$

$\exists !$

$$(y_i) = M(x_i) \qquad M \in M_n(R)$$

$$\eta(z) = \eta\left(\sum a_i x_i\right) = \sum M(a_i x_i)$$

$$\eta \circ \varphi(z) = \eta(M(a_i)) = NM(a_i) \qquad \begin{matrix} \varphi = M \\ \eta = N \end{matrix}$$

$D' = Hom(M, M)$

M נוצר סופית, D ראשי $\quad M \xrightarrow[\in D']{\eta} M$

$(d_1) = \operatorname{ann} z_1 = \operatorname{ann} w_1$

$\vdots$

$(d_s) = \operatorname{ann} z_s = \operatorname{ann} w_s$

$\Delta = \operatorname{diag}_{i=1}^{s} d_i$

$$M = \bigoplus_{1}^{s} D z_i$$

$$(w_i)_1^s \xleftarrow[B \in M_s(D)]{\eta} (z_i)$$

$$(w_i)_1^s = B(z_i)_1^s \longleftarrow (z_i)$$

$d_j \mid d_i b_{ij}$

אם B מקיימת שקיימת C כך ש $\Delta B = C\Delta$

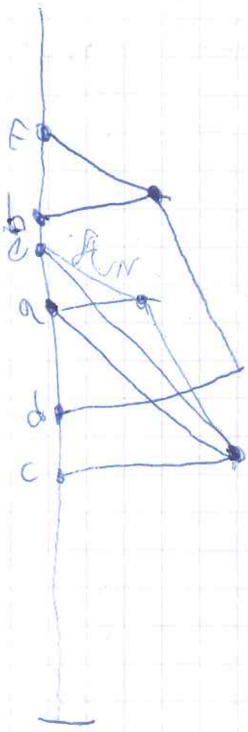
$$M_s(D) \xrightarrow[\text{יחיד}]{\text{חוג}} R = \{B \in M_s(D) \mid \exists C \in M_s(D)\ \Delta B = C\Delta\}$$

$\cup^{-1}$

$D' = Hom(M, M)$

$$D' \cong^{-1} R \big/ M_s(D)\Delta$$

רק שלמות:

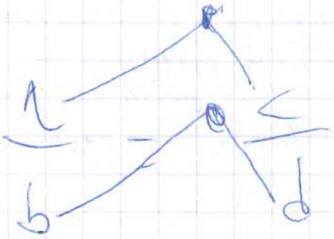


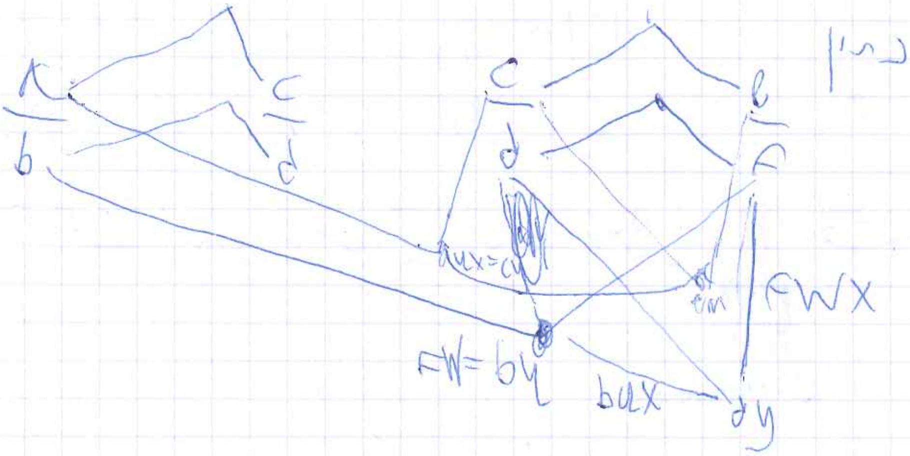
$(a,b)\equiv(c,d)$

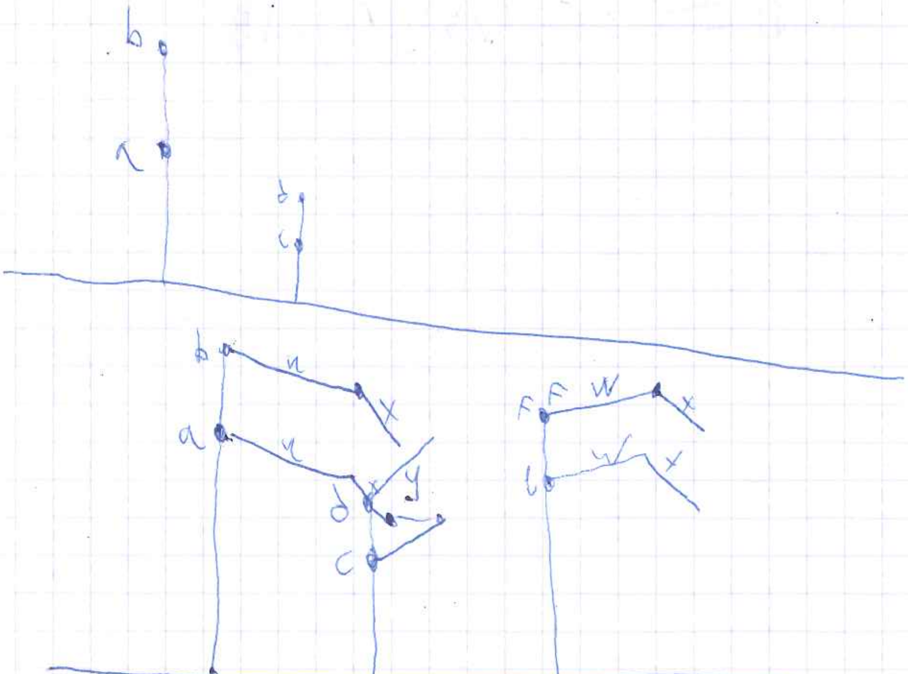
$0\neq bu=dv$

$\Downarrow$

$au=cv$







עוד תרגילים ב"חוגים ומודולים"

1. הראה שאם בהגדרת המושג "חוג" אין מניחים שהחבור קומוטטיבי אז זה נובע ממילא מתוך הדרישות האחרות.

2. הקבוצה $\{ m+n\sqrt{-3}$ | m,n שניהם שלמים או שניהם חצאי שלמים אי-זוגיים $\}$ היא חוג חלקי של $\mathbb{C}$.

3. בחוג R יהיו a,b שני איברים. נסמן $a' = ab-ba = [a,b]$ ואז $a^{(k)} = [a^{(k-1)}, b]$ עבור $k=2,3,\ldots$ (נסמן גם: $a^{(0)}=a$).
הוכח כי:

$$\sum_{i=0}^{k} b^{i} a b^{k-i} = \sum_{j=0}^{k} \binom{k+1}{j+1} b^{k-j} a^{(j)}$$

4. כל תחום סופי הוא חוג עם חילוק.

5. יהיו a,b שני איברים בחוג R. הוכח שאם $1-ab$ הפיך אז $1-ba$ הפיך.

6. אם לאיבר u בחוג R יש הפוך ימני v ואין לו הפוך ימני נוסף אזי v הוא גם הפוך שמאלי.

7. אם לאיבר u בחוג R יש יותר מהפוך ימני אחד אז יש אינסוף הפוכים ימניים לאיבר זה.
(אם $uv=1$ אז $vu\neq 1$. בדוק שהאיברים $(1-vu)u^{i}$ $i=0,1,2,\ldots$ שונים ביניהם ואז $v+(1-vu)u^{i}$ הפוכים ימניים של u)

8. יהיו a,b איברים בחוג R ויהיו $a,b,ab-1$ הפיכים. הראה כי $a-b^{-1}$ הפיך ואז $(a-b^{-1})^{-1}-a^{-1}$ הפיך ומתקיים $((a-b^{-1})^{-1}-a^{-1})^{-1} = aba-a$.

ברוך דרבמן

תרגיל בחוגים ושדות

①

$$(a+b)+(-1)(b+a)=a+b+(-1)b+(-1)a=a+1b+(-1)b+(-1)a=$$
$$a+(1+(-1))b+(-1)a=a+0b+(-1)a=1\cdot a+(-1)a=(1+(-1))a=0\cdot a=0$$

נחבר לשני האגפים $(b+a)$ ונקבל

$$(a+b)+(-1)(b+a)+1(b+a)=(a+b)+(1+(-1))(b+a)=a+b+0(b+a)=(a+b)=(b+a)=0+(b+a)$$

כלומר $a+b=b+a$

מש"ל.

② סגירות לגבי חיבור

$$(m+n\sqrt{-3})+(k+l\sqrt{-3})=(m+k)+(n+l)\sqrt{-3}$$

ולכן אם m ו-n הם מאותו הסוג (שניהם שלמים, או שניהם חצאי אי-זוגיים) וכן k,l הם מאותו הסוג אז $m+k$ וכן $n+l$ הם מאותו הסוג. ולכן תוצאת החיבור שייכת לקבוצה.

סגירות לגבי כפל:

$$(m+n\sqrt{-3})(k+l\sqrt{-3})=(mk-3nl)+(ml+nk)\sqrt{-3}$$

אם m,n,k,l שלמים אז $mk-3nl$, $ml+nk$ שלמים

ואין צ"ל. אם m,n,k,l חצאים של מספרים אי-זוגיים אז אם נסמן $m=\frac{2m'+1}{2}$ וכו'.. נקבל: (כאשר m',n',k',l' שלמים)

$$mk-3nl=\frac{2m'+1}{2}\cdot\frac{2k'+1}{2}-3\frac{2n'+1}{2}\frac{2l'+1}{2}=\frac{4m'k'+2m'+2k'+1-12n'l'-6n'-6l'-3}{4}=$$

$$=\frac{2m'k'+m'+k'-6n'l'-3n'-3l'-1}{2}$$

וזהו חצי של מספר אי-זוגי. באותו אופן גם $ml+nk$ הוא חצי של מספר אי-זוגי. ולמרנו. כעת אם m,n שלמים וכן k,l חצאים של מספרים אי-זוגיים אז אם m,n שניהם זוגיים או שניהם אי-זוגיים נקבל ש $ml+nk$, $mk-3nl$ שניהם שלמים/לחילופין שניהם חצאים

עם אינטגרלים ושוב גמרנו. אם מה תצאי] a,b
שלמים נתבונן במקרה הקודם דרך הקומוטטיביות של
והחיבור.

קיום המשלים לכל איבר בקבוצה הוא טריויאלי, וכן $1+0\sqrt{3}$
הוא איבר יחידה לכפל והוא בקבוצה ולכן הקבוצה
הינה חוג חלקי של $\mathbb{C}$
מ.ש.ל.

③ ההוכחה באינדוקציה:

ⓐ עבור $k=0$ נקבל $a=a$ וגמרנו!

ⓑ נניח שמתקיים $\sum_{i=0}^{k-1} b^i a b^{k-i-1} = \sum_{i=0}^{k-1} \binom{k}{i+1} b^{k-i-1} a^{(i)}$

אזי:

$$\sum_{i=0}^{k} b^i a b^{k-i} = b\left(\sum_{i=0}^{k-1} b^i a b^{k-i-1}\right) + ab^k = b\sum_{i=0}^{k-1}\binom{k}{i+1} b^{k-i-1} a^{(i)} + ab^k =$$

$$= \sum_{i=0}^{k-1}\binom{k}{i+1} b^{k-i} a^{(i)} + ab^k =$$

9. יהיו S קבוצה חלקית לחוג R. נגדיר את המרכז (centralizer) של S בחוג R על ידי:

$$C(S)=\{a\in R \mid as=sa,\ \forall s\in S\}$$

(א) הוכח ש-$C(S)$ חוג חלקי.

(ב) $C(R)$ נקרא המרכז (center) של R והוא חוג חלקי קומוטטיבי.

(ג) מהו $C(S)$ ב-$M_n(R)$ כאשר $S=\{e_{ij} \mid 1\le i,j\le n\}$?

(ד) מהו $C(S)$ ב-$M_n(R)$ כאשר S מכיל מטריצה אחת בלבד והיא $N=e_{12}+e_{23}+\dots+e_{n-1,n}$?

(ה) מהו $C(S)$ ב-$M_n(R)$ כאשר R קומוטטיבי ו-S היא קבוצת המטריצות האלכסוניות.

10. יהיו S חוג ובו קבוצה איברים $\{e_{ij} \mid 1\le i,j\le n\}$ המקיימים $e_{ij}e_{kl}=\delta_{jk}e_{il}$ וכן $\sum_{i=1}^{n}e_{ii}=1$. עבור $a\in S$ ולכל זוג i,j בין 1 ל-n נגדיר $a_{ij}=\sum_{k=1}^{n}e_{ki}\,a\,e_{jk}$.

ויהי $R=C(\{e_{kl} \mid 1\le k,l\le n\})$.

(א) הוכח כי $a_{ij}\in R$ וכן $a=\sum_{i,j}a_{ij}e_{ij}$

(ב) הוכח שאם $r_{ij}\in R$ לכל i,j ומתקיים $\sum_{i,j}r_{ij}e_{ij}=0$ אז $r_{ij}=0$ לכל i,j.

(ג) הסק שהחוג S איזומורפי לחוג $M_n(R)$

11. R חוג, R' קבוצה ויש $\eta:R'\to R$ העתקה חד חד ערכית ועל. הוכח שניתן להפוך את R' לחוג על ידי ההגדרות:

$$a'+b'=\eta^{-1}(\eta(a)+\eta(b))\ ;\quad 0'=\eta^{-1}(0)$$

$$a'b'=\eta^{-1}(\eta(a)\eta(b))\ ;\quad 1'=\eta^{-1}(1)$$

ו-η איזומורפיזם בין R' ל-R.

12. (א) אם u הפיך בחוג R ומגדירים $\eta:R\to R$ על ידי $\eta(a)=ua$ מהו החוג שמתקבל בהתאם לתרגיל הקודם? מהו איזומורפיזם?

(ב) בחוג R נגדיר פעולות חבור וכפל חדשות על ידי:

$$a\oplus b=a+b-1$$

$$a\cdot b=a+b-ab$$

הוכח שמתקבל חוג איזומורפי ל-R (נצל הרעיון η).

13. הוכח כי $\mathbb{H}_0$ קבוצת הקווטרניונים $\alpha+\beta i+\gamma j+\delta k$ עם $\alpha,\beta,\gamma,\delta$ רציונליים הוא חוג עם חילוק חלקי ל-$\mathbb{H}$. הכלל על חוגים עם חילוק חלקיים נוספים.

14. הוכח כי החוג החלקי ל-$M_2(\mathbb{C})$ הנוצר על ידי $\mathbb{C}\cup\mathbb{H}$ הוא $M_2(\mathbb{C})$.

15. הוכח כי קבוצת המטריצות ב-$M_4(\mathbb{R})$ בעלות המבנה

$$\begin{pmatrix}\alpha & \beta & \gamma & \delta\\ -\beta & \alpha & -\delta & \gamma\\ -\gamma & \delta & \alpha & -\beta\\ -\delta & -\gamma & \beta & \alpha\end{pmatrix}$$

הינה חוג חלקי איזומורפי ל-$\mathbb{H}$.

16. מהו המרכז של $\mathbb{H}$ ומהו $C(i)$?

17. יהי D חוג עם חילוק, C מרכזו ו-S חוג עם חילוק חלקי של D. אם S^* חבורה חלקית נורמלית של D^* אז $S=D$ או $S\subseteq C$ (זהו משפט של Cartan-Brauer-Hua).
ראה הוכחה בספר של Cohn Algebra Vol. 2, עמוד 251.

18. יהי I אידיאל בחוג R. נגדיר:

$U_1 = \{ a \in U(R) \mid a \equiv 1 \pmod I \}$.

הוכח כי U_1 חבורה חלקית נורמלית של U.

19. אם I אידיאל ב-R נסמן ב-$M_n(I)$ את כל המטריצות ב-$M_n(R)$ שכל אבריהן לקוחים מ-I. הוכח כי $M_n(I)$ אידיאל ב-$M_n(R)$ וכי כל אידיאל ב-$M_n(R)$ הוא בעל הצורה הנ"ל. הסק: אם R חוג-עם-חילוק אז ב-$M_n(R)$ אין אידיאלים לא טריויאליים (חוג בעל התכונה המתוארת קרוי "פשוט").

20. אם I אידיאל ב-R הוכח:

$$M_n(R)/M_n(I) \simeq M_n(R/I).$$

21. תהי A מטריצה 2×2 מעל $\mathbb{Z}/(p)$, p ראשוני. הוכח כי אם $q=(p^2-1)(p^2-p)$ אזי $A^{q+2}=A^2$ (רמז: הוכח קודם שאם A הפיכה אזי $A^q=1$).

22. הקבוצה של המטריצות $R=\left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \mid a,b,c \in \mathbb{Z} \right\}$ היא חוג חלקי של $M_2(\mathbb{Z})$. מצא את כל האידיאלים של R.

23. אם R חוג פשוט (הגדרה בתרגיל 19) אזי הקרקטריסטיקה שלו היא 0 או מספר ראשוני. אותה תוצאה נכונה גם לחוג ראשוני (חוג ראשוני מוגדר כחוג אשר אם I,J אידיאלים $\neq 0$ אזי $\boxed{IJ \neq 0}$).

24. יהי D תחום בעל תכונת הכפולה המשותפת הימנית. יהי F ~~שדה המנות~~ חוג-עם-חילוק המנות של D, ויהי E חוג-עם-חילוק אחר המכיל את D ונוצר על ידי D (אין בין D ל-E חוג-עם-חילוק). הוכח כי F ו-E איזומורפיים.

25. יהי $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2} i$, הראה כי $\mathbb{Q}[\omega] \cong \mathbb{Q}[x]/I$ כאשר I האידיאל הנוצר על ידי x^2+x+1.

26. יהי $u = \sqrt{2}+\sqrt{3}$. מצא יוצר עבור האידיאל I שעבורו מתקיים $\mathbb{Q}[u] \cong \mathbb{Q}[x]/I$.

27. יהי I אידיאל בחוג R ו- $I[x_1, \dots, x_n]$ קבוצת כל הפולינומים מ- $R[x_1, \dots, x_n]$ אשר כל מקדמיהם שייכים ל- I . הראה כי קבוצה זו היא אידיאל וכן $R[x_1, \dots, x_n]/I[x_1, \dots, x_n] \cong R/I[x_1, \dots, x_n]$.

28. הוכח כי $M_n(R[x_1, \dots, x_n]) \cong M_n(R)[x_1, \dots, x_n]$

29. (א) יהי $f(x) = x^n + a_1x^{n-1} + \dots + a_n \in F[x]$, F שדה, $n \geq 1$, ויהי $u = x + (f(x))$ ב- $F[x]/(f(x))$, הראה כי כל איבר של $F[u]$ ניתן לכתיבה באופן יחיד בצורה $b_0 + b_1u + \dots + b_{n-1}u^{n-1}$, $b_i \in F$.
(ב) כאשר $F = \mathbb{Q}$ ו- $f(x) = x^3+3x-2$ מצא באופן מפורש הצגה מהצורה $b_0+b_1u+b_2u^2$ עבור $(2u^2+u-3)(3u^2-4u+1)$ וכן עבור $(u^2-u+4)^{-1}$.

30. הראה כי $F[u]$ מהתרגיל הקודם (חלק (א)) מכיל נילפוטנטים $\Longleftrightarrow$ ל- $f(x)$ יש פירוק מהצורה: $f(x) = g(x)^2h(x)$, $\deg g(x) \geq 1$.

31. הראה ש- x^3+x^2+1 אי פריק ב- $\mathbb{Z}/(2)[x]$ וכי $\mathbb{Z}/(2)[x]/(x^3+x^2+1)$ שדה של 8 איברים.

32. (א) הראה כי האידיאל I הנוצר על ידי 3 ועל ידי x^3-x^2+2x-1 אינו ראשי ב- $\mathbb{Z}[x]$.

~~33~~. (ב) האם $\mathbb{Z}[x]/I$ תחום? (רמז: הראה כי $\mathbb{Z}[x]/I \simeq \bar{\mathbb{Z}}[x]/\bar{I}$ כאשר $\bar{\mathbb{Z}} = \mathbb{Z}/(3)$ ו- $\bar{I} = (\bar{x}^3 - \bar{x}^2 + \bar{2}\bar{x} - \bar{1})$.

33. יהי F שדה אינסופי ו- $f(x_1,\dots,x_n) \in F[x_1,\dots,x_n]$ פולינום המתאפס בכל נקודה $(a_1,\dots,a_n)$ שבה פולינום אחר $g(x_1,\dots,x_n) \neq 0$ אינו מתאפס. אזי $f(x_1,\dots,x_n)=0$.

34. יהי F שדה סופי בעל q איברים, ויהי $f(x_1,\dots,x_n)$ פולינום המקיים $f(0,\dots,0)=0$ ואם $f(a_1,\dots,a_n) \neq 0$ לכל $(a_1,\dots,a_n) \neq (0,\dots,0)$. ויהי $g(x) = 1 - f(x_1,\dots,x_n)^{q-1}$. הוכח כי $g(a_1,\dots,a_n)=0$ פרט למקרה ש- $(a_1,\dots,a_n)=(0,\dots,0)$. הסק שהפונקציה הפולינומיאלית הנקבעת על ידי g שווה לפונקציה הנקבעת על ידי $(1-x_1^{q-1})\cdots(1-x_n^{q-1})$ ובפרט הסק כי $\deg g \geq n(q-1)$.

35. F כמו בתרגיל הקודם. ויהי $f(x_1,\dots,x_n)$ ממעלה m, $m < n$, ואם $f(0,\dots,0)=0$ הוכח שקיימת $(a_1,\dots,a_n) \neq (0,\dots,0)$ כך ש- $f(a_1,\dots,a_n)=0$. (זהו משפט של Artin–Chevalley).

~~37. הראה כי אם $s_k = \sum_{i=1}^{n} x_i^k$ אזי~~

~~$s_k - p_1 s_{k-1} + p_2 s_{k-2} + \dots + (-1)^{k-1} p_{k-1} s_1 + (-1)^k k p_k = 0$~~

~~$k=1,2,\dots$~~

36. הראה כי $\mathbb{Z}[\sqrt{10}]$ אינו בעל פריקות יחידה.

37. תהי D קבוצת כל המספרים בעלי הצורה $m+n\sqrt{-3}$ כאשר m,n שניהם שלמים או שניהם חצאי שלמים אי-זוגיים. הוכח כי D אוקלידי ביחס ל- $\delta(m+n\sqrt{-3}) = m^2+3n^2$

38. ויהי D תחום ראשי ו- $0\neq a\in D$ הו[כח כי] a ראשוני אם"ם $D/(a)$ שדה ואם a אינו ראשוני אזי $D/(a)$ אינו תחום.

40. יהי M מודול שמאלי מעל R. הוכח כי הקבוצה $B=\{b\in R \mid bx=0, \forall x\in M\}$ היא אידיאל ב- R. הראה בכל מקרה שאם C אידיאל ב- R וגם $C\subseteq B$ אזי ניתן להגדיר את M כמודול מעל R/C על ידי $(a+C)x=ax$, $a\in R$, $x\in M$.

41. תהי M חבורה קומוטטיבית סופית. האם אפשר להפוך את M למודול מעל $\mathbb{Q}$?

42. יהי n טבעי. מהו $\mathrm{Hom}(\mathbb{Z}, \mathbb{Z}/(n))$ ומהו $\mathrm{Hom}(\mathbb{Z}/(n), \mathbb{Z})$?

43. יהי R קומוטטיבי ויהי φ אנדומורפיזם של המודול $R^{(n)}$. הוכח שאם φ על אזי φ ~~אוטומורפיזם~~ חדחד ערכי.

44. מצאו בסיס עבור המודול החלקי ל- $\mathbb{Z}^{(3)}$
הנוצר על ידי:

$$f_1=(1,0,-1),\ f_2=(2,-3,1),\ f_3=(0,3,1),\ f_4=(3,1,5)$$

45. מצאו בסיס עבור המודול החלקי של $\mathbb{Q}[\lambda]^{(3)}$ הנוצר
על ידי:

$$f_1=(2\lambda-1,\lambda,\lambda^2+3),\ f_2=(\lambda,\lambda,\lambda^2),\ f_3=(\lambda+1,2\lambda,2\lambda^2-3)$$

46. מצאו בסיס של המודול החלקי ל- $\mathbb{Z}^{(3)}$ המורכב
מכל ה- (x_1,x_2,x_3) המקיימים:

$$x_1+2x_2+3x_3=0\ ,\quad x_1+4x_2+9x_3=0$$

47. מצאו צורה נורמלית של

$$A=\begin{pmatrix} \lambda-17 & 8 & 12 & -14 \\ -46 & \lambda+22 & 35 & -41 \\ 2 & -1 & \lambda-4 & 4 \\ -4 & 2 & 2 & \lambda-3 \end{pmatrix}$$

מצאו גם P,Q הפיכות כך ש- QAP נורמלית.

48. קבעו מבנה $M=D^{(3)}/K$ כאשר $D=\mathbb{Z}[\sqrt{-1}]$
ו-K נוצר על ידי

$$f_1=(1,3,6),\ f_2=(2+3i,-3i,12-8i),\ f_3=(2-3i,6+9i,-18i)$$

49. הגדרה את הדרגה $\mathrm{rank}M$ של מודול נוצר סופית M מעל
תחום ראשי אוקלידי D בתור הדרגה של המודול
החופשי $M/\mathrm{tor}M$. הוכיחו שאם $M\cong D^{(n)}/K$ אזי
$\mathrm{rank}M = n-\mathrm{rank}K$. הוכיחו גם שאם
N מודול חלקי ל- M אזי
$\mathrm{rank}M=\mathrm{rank}N+\mathrm{rank}(M/N)$.

44. מצאו בסיס עבור המודול החלקי ל-$\mathbb{Z}^{(3)}$ הנוצר על ידי:

$$f_1=(1,0,-1)\ ,\ f_2=(2,-3,1)\ ,\ f_3=(0,3,1)\ ,\ f_4=(3,1,5)$$

45. מצאו בסיס עבור המודול החלקי של $\mathbb{Q}[\lambda]^{(3)}$ הנוצר על ידי: $f_1=(2\lambda-1,\lambda,\lambda^2+3)$, $f_2=(\lambda,\lambda,\lambda^2)$, $f_3=(\lambda+1,2\lambda,2\lambda^2-3)$

46. מצאו בסיס של המודול החלקי ל-$\mathbb{Z}^{(3)}$ המורכב מכל ה-(x_1,x_2,x_3) המקיימים:

$$x_1+2x_2+3x_3=0\ ,\ x_1+4x_2+9x_3=0$$

47. מצאו צורה נורמלית של

$$A=\begin{pmatrix} \lambda-17 & 8 & 12 & -14 \\ -46 & \lambda+22 & 35 & -41 \\ 2 & -1 & \lambda-4 & 4 \\ -4 & 2 & 2 & \lambda-3 \end{pmatrix}$$

מצאו גם P,Q הפיכות כך ש- QAP נורמלית.

48. קבעו מבנה $M=D^{(3)}/K$ כאשר $D=\mathbb{Z}[\sqrt{-1}]$ ו-K נוצר על ידי

$$f_1=(1,3,6)\ ,\ f_2=(2+3i,-3i,12-8i)\ ,\ f_3=(2-3i,6+9i,-18i)$$

49. הגדר את הדרגה $\text{rank} M$ של מודול נוצר סופית M מעל תחום ראשי, קומוטטיבי D בתור הדרגה של המודול החופשי $M/\text{tor}M$. הוכח כי אם $M\cong D^{(n)}/K$ אזי $\text{rank} M = n-\text{rank} K$. הוכח גם כי אם N מודול חלקי ל-M אזי

$$\text{rank} M=\text{rank} N+\text{rank}(M/N).$$

50. מודול חלקי N של M נקרא טהור (pure) אם לכל $y\in N$ ו- $a\in D$ המשוואה $ax=y$ פתירה ב- M $\Leftrightarrow$ היא פתירה ב- N.

(א) הראה שאם N מחובר ישר של M אז N טהור.

(ב) הראה שאם N מודול חלקי טהור של M ואם $\operatorname{ann}(x+N)=(d)$ אזי ניתן לבחור $y\in x+N$ כך ש- $\operatorname{ann} y=(d)$.

51. (א) אם N מודול ~~מ~~ חלקי טהור של מודול פתול נוצר סופית M מעל תחום ראשי, הראה כי אזי N מחובר ישר.

(ב) אם M כמו ב- (א) ואם Dz מודול חלקי ציקלי כך ש- $\operatorname{ann} z\subset \operatorname{ann} x$ לכל $x\in M$ אזי Dz טהור ולכן מחובר ישר.

52. הוכח שכל מטריצה $A\in M_n(F)$ דומה למשוחלפת שלה.

53. תהי $A\in M_n(F)$ נילפוטנטית. הוכח שהיא דומה למטריצה אלכסונית בלוקים $\begin{pmatrix} N_1 & & & 0 \\ & N_2 & & \\ & & \ddots & \\ 0 & & & N_s \end{pmatrix}$ כאשר $N_i=\begin{pmatrix} 0 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & 0 \end{pmatrix}$.

54. כל $A\in M_n(\mathbb{R})$ דומה למטריצה אלכסונית בלוקים $\begin{pmatrix} B_1 & & & & & 0 \\ & \ddots & & & & \\ & & B_s & & & \\ & & & C_1 & & \\ & & & & \ddots & \\ 0 & & & & & C_t \end{pmatrix}$ כאשר B_i הם מהצורה $\begin{pmatrix} \alpha & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & \alpha \end{pmatrix}$ ו- C_j הם מהצורה

$$\begin{pmatrix} 0 & 1 & 1 & 0 & & & 0 \\ -\gamma & \beta & 0 & 1 & & & \\ & & 0 & 1 & 1 & 0 & \\ & & -\gamma & \beta & 0 & 1 & \\ 0 & & & & & \ddots & \end{pmatrix}$$

55. מצא את המטריצות ב- $M_5(\mathbb{Q})$ המתחלפות עם $\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$

56. מצא את המטריצות ב- $M_4(\mathbb{Q})$ המתחלפות עם $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & -3 & 3 \end{pmatrix}$.