מבוא לחוגים ומודולים - תרגול 9

אי-פריקות של פולינומים

משפט:

יהי F שדה, ויהי $p(x)$ פולינום מעל F ממעלה $n \leq 1$. אז ל-F יש לכל היותר n שורשים.

משפט:

יהי R חוג חילופי. אז $c \in R$ הוא שורש של $p(x)$ אם ורק אם $(x-c) \mid p(x)$

דוגמה:

מעל $\mathbb{Z}/6\mathbb{Z}$, ל-x^2+x יש 4 שורשים: $\bar{0},\bar{2},\bar{3},\bar{5}$

$$x^2+x = x(x-\bar{5}) = (x-\bar{2})(x-\bar{3})$$

מסקנה:

אם $p(x) \in F[x]$ פולינום ממעלה 2 או 3, אז $p(x)$ אי-פריק מעל F $\Leftrightarrow$ אין לו שורש ב-F.

איך מוצאים שורשים?

אם R תח"ש, F שדה השברים שלו, $p(x) = a_0 + a_1 x + \dots + a_n x^n \in R[x]$.

$\frac{\alpha}{\beta}$ שורש של $p(x)$ $\Leftarrow$ $\alpha \mid a_0, \beta \mid a_n$.

R תח"ש, F שדה השברים

האם פריק מעל R = פריק מעל F?

לא, למשל $R=\mathbb{Z}$, $F=\mathbb{Q}$, $\underset{2(x+4)}{2x+4}$ פריק מעל R, אי-פריק מעל F.

הגדרה:

$f(x)=a_0+a_1x+\cdots+a_nx^n$. ה<u>תכולה</u> של f, $c(f)$, היא המחלק המשותף המירבי של $a_0,\dots,a_n$.

f הוא <u>פרימיטיבי</u> אם $c(f)=1$.

משפט: (קריטריון אייזנשטיין)

יהי $P \triangleleft R$ אידיאל ראשוני, $f(x)=a_0+a_1x+\cdots+a_nx^n\in R[x]$ המקיים:

א. $a_n\notin P$. (למשל, אם f מתוקן)

ב. $a_0,\dots,a_{n-1}\in P$.

ג. $a_0\notin P^2$.

אז $f(x)$ אי-פריק מעל F. אם $f(x)$ פרימיטיבי מעל R, אז הוא אי-פריק מעל R.

משפט: (הלמה של גאוס)

יהי $f(x)\in R[x]$ פרימיטיבי. אז f אי-פריק מעל R $\Longleftrightarrow$ f אי-פריק מעל F.

חוג' פולינומים מעל תחומי שלמות

R תח"ש. מה התכונות של $R[x]$?

הערה:

$R[x]$ לעולם אינו שדה. כי למשל x לא הפיך.

טענה:

התנאים הבאים שקולים:

א. $R[x]$ אוקלידי:

ב. $R[x]$ תחום ראשי.

ג. R שדה.

הוכחה:

$\boxed{א \Leftarrow ב}$ תמיד נכון.

$\boxed{ג \Leftarrow א}$ ראינו כבר.

$\boxed{ב \Leftarrow ג}$ נתבונן באידאל $\langle x \rangle$.
$R[x]$ תחום ראשי

$R[x]/_{\langle x \rangle} \cong R$ תחו"ש $\Leftarrow$ $\langle x \rangle$ אידאל ראשוני

$\Leftarrow$ $\langle x \rangle$ מקסימלי $\Leftarrow$ $R[x]/_{\langle x \rangle} \cong R$ שדה. $\square$

משפט:

$R[x]$ תפ"י $\Leftrightarrow$ R תפ"י.

משפט: (משפט הבסיס של הילברט)

אם R חוג נותרי, אז גם $R[x]$ נותרי.

הערה:

$R[x]$ לעולם אינו ארטיני, כי $\langle x \rangle \supsetneq \langle x^2 \rangle \supsetneq \langle x^3 \rangle \supsetneq \cdots$

מודולים

הגדרה:

יהי R חוג. מודול שמאלי מעל R הוא חבורה אבלית $(M,+)$
עם פעולה $\mu: R \times M \longrightarrow M$, נסמן $\mu(r,a) = ra$, כך שלכל $a,b \in M$
ולכל $r,s \in R$:

א. $r(a+b) = ra + rb$.

ב. $(r+s)a = ra + sa$.

ג. $(rs)a = r(sa)$.

ד. $1_R \cdot a = a$.

(מודול "=" מרחב וקטורי מעל R)

הערה:

לכל $a\in M$, $0_R\cdot a=0_M$. לכל $r\in R$, $r\cdot 0_M=0_M$.

דוגמאות:

א. אם F שדה, F-מודול = מרחב וקטורי מעל F.

ב. $\mathbb{Z}$ - מודול = חבורות אבליות.

$$n\cdot a=\underbrace{a+a+\cdots+a}_{n\text{ פעמים}}$$

תרגיל:

תהי G חבורה אבלית, יהי R חוג, ונניח שיש הומומורפיזם $\varphi:R\longrightarrow End(G)$.
($End(G)$ = הומומורפיזמים מ-G לעצמה, זהו חוג ביחס לחיבור והרכבה).
הוכח שאפשר להגדיר על G מבנה של R-מודול.

הוכחה:

G היא כבר חבורה אבלית, רוצים לכל $r\in R$, $g\in G$ להגדיר מהו rg.

$$r\cdot g:=\varphi(r)(g)$$

נוודא למשל את האקסיומה הראשונה -

$$r\cdot(g_1+g_2)=\varphi(r)(g_1+g_2)\underset{\substack{\uparrow\\ \varphi(r)\text{ הומומורפיזם}}}{=}\varphi(r)(g_1)+\varphi(r)(g_2)=rg_1+rg_2$$

השאר - לבית.

הערה:

התנאי הזה הוא גם הכרחי כדי ש-G תהיה R-מודול.

הגדרה:

אם M מודול מעל R, תת-מודול של M הוא תת-חבורה $N\leq M$ שסגורה ביחס לכפל ב-R, כלומר לכל $r\in R$, $n\in N$, $rn\in N$.

דוגמה:

לא כל תת-חבורה היא תת-מודול. $R=\mathbb{Q}$, $M=\mathbb{Q}$, אבל $\mathbb{Z}\leq\mathbb{Q}$ תת-חבורה שאינה תת-מודול.

__דוגמאות:__

א. R הוא מודול מעל עצמו (שמאלי), $r\cdot a = ra$.

תת-מודולים (שמאליים) = אידאלים שמאליים.

ב. $R=\mathbb{Z}$. תת-מודולים של M = תת-חבורות של M.

__דוגמה:__

$R=F[x]$. איך נראה מודול מעל R? (F - שדה)

אם V מודול מעל R, הוא בפרט מרחב וקטורי מעל F.

בנוסף, ההעתקה $T: V \longrightarrow V$, $T(v) = xv$ היא העתקה לינארית (מורפיזם).

מודולים מעל $F[x]$ = מרחבים וקטוריים עם העתקה לינארית.

$$x^2\cdot v = x(xv) = T(T(v)) = T^2(v)$$

__תרגיל:__

תהי $T: V\longrightarrow V$ העתקה, ויהי $W\subseteq V$ תת-מרחב T-אינווריאנטי ($T(W)\subseteq W$).

אז W הוא תת-מודול של V (כמודול מעל $F[x]$).

__הוכחה:__

ראשית, כיוון ש-W הוא תת-מרחב, הוא בפרט תת-חבורה חיבורית של V.

לכן מספיק לוודא שלכל $w\in W$ ולכל $f(x)\in F[x]$, $f(x)\cdot w\in W$.

W הוא T-אינווריאנטי, לכן $T(W)\subseteq W$. באינדוקציה, לכל n מתקיים $T^n(W)\subseteq W$.

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \Longrightarrow f(x)\cdot w = a_0 \underset{W}{\underset{\Uparrow}{w}} + a_1 \underset{W}{\underset{\Uparrow}{T(w)}} + \cdots + a_n \underset{W}{\underset{\Uparrow}{T^n(w)}} \in W$$

$\square$

__הגדרה:__

יהי M מודול מעל R, ויהי $N\leq M$ תת-מודול. N היא תת-חבורה נורמלית של M, לכן M/N חבורה אבלית. מסתבר שגם הכפל ב-R מוגדר היטב, $r(m+N) = rm+N$. זה __מודול המנה__ של M ביחס ל-N.

אזהרה:

ראינו ש-R מודול מעל עצמו, ותת-מודולים = אידאלים שמאליים. מודול המנה הוא לא בהכרח חוג!

הגדרה:

יהי R חוג, ויהיו M,N מודולים מעל R. פונקציה $\varphi:M\to N$ היא <u>הומומורפיזם של מודולים</u> אם היא הומומורפיזם של חבורות וגם לכל $r\in R$, $m\in M$ מתקיים $\varphi(rm)=r\cdot\varphi(m)$.

כמו בחבורות ובחוגים, כל משפטי האיזומורפיזם שאנחנו מכירים מתקיימים, בפרט אם $\varphi: M\to N$ הומומורפיזם של מודולים אז

$$M/_{\ker\varphi}\cong \mathrm{Im}\,\varphi$$

תרגיל:

יהי R חוג חילופי. יהי n מספר טבעי, $E=R^{\{1,\dots,n\}}=\{f:\{1,\dots,n\}\to R\}$.
הראו ש-E הוא מודול מעל R, וגם $E\cong R^n$ כמודולים.

הוכחה:

נגדיר מבנה של מודול כך:

$$(f+g)(x)=f(x)+g(x)$$
$$(r\cdot f)(x)=r\cdot f(x)$$

אפשר לוודא שזה מקיים את כל האקסיומות.
נגדיר את האיזומורפיזם $\varphi:E\to R^n$ ע"י $\varphi(f)=(f(1),\dots,f(n))$.
נראה שזה הומומורפיזם של מודולים:

$$\varphi(f+g)=((f+g)(1),\dots,(f+g)(n))=(f(1)+g(1),\dots,f(n)+g(n))=$$
$$=(f(1),\dots,f(n))+(g(1),\dots,g(n))=\varphi(f)+\varphi(g)$$
$$\varphi(rf)=((rf)(1),\dots,(rf)(n))=(r\cdot f(1),\dots,r\cdot f(n))=$$
$$=r\cdot(f(1),\dots,f(n))=r\cdot\varphi(f)$$

φ חח"ע: $\varphi(f)=(0,\dots,0) \Leftarrow$ $f(x)=0$ לכל x $\Leftarrow f=0$.

φ על: אם נתון $(r_1,\dots,r_n)\in R^n$, נגדיר $f(x)=r_x$ $\Leftarrow \varphi(f)=(r_1,\dots,r_n)$.

לכן $E\cong R^n$.

$\square$

הגדרה:

מודול M "יקרא" פשוט אם אין לו תת-מודולים לא טריוויאליים.

הגדרה:

מודול M "יקרא" ציקלי אם קיים $a\in M$ שעבורו $M=Ra=\{ra \mid r\in R\}\leq M$.

דוגמאות:

א. $R=\mathbb{Z}$, מודול ציקלי = חבורה ציקלית.

מודול פשוט = $\mathbb{Z}/p\mathbb{Z}$ ל-p ראשוני (או $M=\{0\}$).

ב. נסתכל על R^n כמודול מעל $M_n(R)$ - זה מודול ציקלי,

$$R^n=M_n(R)\cdot e_1=M_n(R)\cdot\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}$$

אם $R=F$ שדה אז F^n מודול פשוט מעל $M_n(F)$.

טענה:

מודול M הוא פשוט אם ורק אם לכל $0\neq a\in M$ מתקיים $M=Ra$.

הוכחה:

$\boxed{\Leftarrow}$ אם M פשוט, נשים לב שלכל $0\neq a\in M$, $0\neq Ra\leq M$ (כי a נמצא שם),

לכן $M=Ra$.

$\boxed{\Rightarrow}$ יהי $0\neq N\leq M$ תת-מודול, ויהי $0\neq a\in N$. כיוון ש-N תת-מודול,

$M=Ra\subseteq RN=N \Leftarrow N=M$.

$\square$

טענה:

יהי M מודול ציקלי, ויהי $N\leq M$ תת-מודול. אז M/N מודול ציקלי.

הוכחה:

M ציקלי $\Leftarrow$ קיים $a\in M$ כך ש- $M=Ra$. נראה $M/N=R(a+N)$.

אכן, לכל $b+N\in M/N$, יש $r\in R$ כך ש- $b=ra$ $\Leftarrow$ $b+N=r(a+N)$.

לכן M/N נוצר ע"י $a+N$. $\square$

דוגמה:

הכיוון ההפוך לא נכון גם אם N היה ציקלי.

$R=\mathbb{Z}$, $M=\mathbb{Z}\times\mathbb{Z}$ לא מודול ציקלי. אבל $N=\mathbb{Z}\times\{0\}$ מודול ציקלי

(נוצר ע"י $(1,0)$), ו- $M/N\cong\mathbb{Z}$ גם מודול ציקלי.

משפט:

יהי M מודול מעל R. M ציקלי $\Longleftrightarrow$ קיים אידיאל שמאלי L של R

כך ש- $M\cong R/L$ כמודולים מעל R.

הגדרה:

נאמר שמודול M נפרש ע"י אוסף איברים $\{a_j\}_{j\in J}\subseteq M$ אם לכל $m\in M$

קיימים $j_1,\dots,j_n\in J$, $a_1,\dots,a_n\in R$ כך ש- $m=r_1a_{j_1}+\dots+r_na_{j_n}$.

אם הקבוצה סופית, נאמר ש- M נוצר סופית מעל R.

הגדרה:

תהי $\{a_j\}_{j\in J}\subseteq M$ קבוצה פורשת של איברים. אם הקבוצה בלתי-תלויה

לינארית מעל R, כלומר

$$\sum_{i=1}^{n} r_i a_i=0 \Longrightarrow r_1=\dots=r_n=0,$$

נקרא לקבוצה בסיס. מודול שיש לו בסיס נקרא מודול חופשי.

דוגמה:

$\mathbb{Z}/_{88212\mathbb{Z}}$ מודול ציקלי מעל $\mathbb{Z}$ שאינו חופשי, כי כל איבר בו תלוי ליניארית מעל $\mathbb{Z}$.

דוגמה:

במרחבים וקטוריים, $U\subseteq V,\ \dim U=\dim V<\infty \Rightarrow U=V$.

מעל חוגים זה לא נכון! $R=\mathbb{Z}$, $M=\mathbb{Z}$ (בסיס $\{1\}$), $N=2\mathbb{Z}$ (בסיס $\{2\}$). $M\neq N$.

דוגמה:

$R^n=\{(a_1,\dots,a_n)\mid a_i\in R\}$ מודול חופשי מעל R.

תרגיל:

מצאו בסיס לתת-המודול הבא של $\mathbb{Z}^3$ מעל $\mathbb{Z}$:

$$M=\left\{(x,y,z)\in\mathbb{Z}^3 \;\middle|\; \begin{matrix} x+2y+3z=0 \\ x+4y+9z=0 \end{matrix}\right\}$$

פתרון:

המודול M הוא מרחב הפתרונות של $A=\begin{pmatrix}1&2&3\\1&4&9\end{pmatrix}$. נדרג אותה ע"י פעולות שורה (פעולות עמודה משנות את מרחב הפתרונות):

$$\begin{pmatrix}1&2&3\\1&4&9\end{pmatrix}\xrightarrow{R_2\leftarrow R_2-R_1}\begin{pmatrix}1&2&3\\0&2&6\end{pmatrix}\xrightarrow{R_2\leftarrow \frac{R_2}{2}}\begin{pmatrix}1&2&3\\0&1&3\end{pmatrix}\longrightarrow\begin{pmatrix}1&0&-3\\0&1&3\end{pmatrix}$$

מותר לחלק ב-2 כי המשוואה השנייה היא $2y+6z=0 \Leftrightarrow y+3z=0$ כי $\mathbb{Z}$ תח"ש

ולכן $\{(3,-3,1)\}$ בסיס של M.

טענה:

כל מודול נוצר סופית הוא מנה של R^n לאיזשהו $n\in\mathbb{N}$.

הוכחה:

אם $a_1,\dots,a_n$ יוצרים את M, נגדיר $\varphi:R^n\longrightarrow M$ לפי $\varphi(r_1,\dots,r_n)=r_1a_1+\dots+r_na_n$.

אפשר לוודא ש-φ אפימורפיזם של מודולים $\Rightarrow R^n/_{\ker\varphi}\cong M$. $\square$