אלגברה לא קומוטטיבית - תרגול 2

9 במרץ 2015

1 פירוק לגורמים אלמנטריים

בהינתן חוג R, זו שאלה טבעית האם אפשר לסווג את כל המודולים מעל R עד כדי איזומורפיזם. למשל,

טענה: עבור שדה k, יש עד כדי איזומורפיזם בדיוק מרחב וקטורי אחד לכל עוצמה α והמרחבים $V^{\oplus\alpha}$ הם קבוצה מלאה של נציגים.

חוגים קצת יותר מסובכים משדות, אבל שעדיין ניתן לענות על השאלה הזאת עבורם הם:

הגדרה: חוג R נקרא תחום ראשי (PID - Principal Ideal Domain), אם הוא קומוטטיבי, ללא מחלקי אפס וכל אידאל בו נוצר ע"י איבר אחד.

שתי הדוגמאות המרכזיות הן:

1. $\mathbb{Z}$ - השלמים. המודולים מעל $\mathbb{Z}$ הן בדיוק חבורות אבליות.
2. $k[x]$ - חוג פולינומים מעל שדה. המודולים הם מרחבים וקטורים V מעל k עם אופרטור $T:V\to V$.

למעשה, מודולים כלליים הם עדיין קשים למיון ולכן נתמקד רק במודולים נוצרים סופית. מעתה, יהי R תחום ראשי ו-M מודול נ"ס. בחירה של יוצרים $x_1,...,x_n$ נותנת לנו העתקה על $f:R^n\twoheadrightarrow M$ וממשפט האיזומורפיזם הראשון, אנחנו מקבלים $M\simeq R^n/\ker f$. מכך נובע שכדי להבין את M, מספיק להבין את המודול $\ker f$ ואת האופן שבו הוא משוכן ב-R^n.

טענה: כל תת־מודול של R^n איזומורפי ל-R^m לאיזשהו $m\le n$. בפרט, הוא חופשי ונ"ס.

הוכחה: נוכיח את הטענה באינדוקציה על n. יהי $e_1,...,e_{n+1}$ הבסיס הסטנדרטי של R^{n+1} ונזהה את R^n עם הפרוש של $(e_1,...,e_n)$. נגדיר $M^{(n)}=M\cap R^n$. מהנחת האינדוקציה, $M^{(n)}$ חופשי ויש לו בסיס $(f_1,...,f_m)$ עבור $m\le n$. נגדיר את

$$I=\{r\in R\mid \exists y\in R^n \text{ s.t. } y+re_{n+1}\in M\}$$

כלומר, כל האיברים שיכולים להופיע בתור הקואורדינטה ה-$(n+1)$ של וקטור מ-M. זהו בברור אידאל ב־R ולכן נוצר ע"י איבר יחיד d. אם $d=0$, זה אומר ש-$M\subseteq R^n$ ובמקרה זה $f_1,...,f_m$ בסיס ל-M וסיימנו. אחרת, נבחר $f_{m+1}=y+de_{n+1}\in M$ כלשהו (שקיים מהגדרת d) ונוכיח ש- $(f_1,...,f_m,f_{m+1})$ בסיס של M.

<u>פרישה:</u>

אם $f\in M$, אזי הקואורדינטה ה-$(n+1)$ שלו היא כפולה של d (שהוא הקואורדינטה ה-$(n+1)$ של f_{m+1}) ולכן $f-cf_{m+1}\in M^{(n)}$ ומכאן שהוא נפרש ע"י $f_1,...,f_m$.

<u>אי־תלות:</u>

בהינתן

$$c_1f_1+\dots c_mf_m+c_{m+1}f_{m+1}=0$$

חייב להתקיים $c_{m+1}=0$ מהתבוננות בקואורדינטה ה-$(n+1)$ ולכן גם $c_1,\dots,c_m=0$ מהנחת האינדוקציה ($f_1,...,f_m$ בסיס).

קיבלנו אם כך שהמודול M הוא מנה של R^n בתת־מודול איסומורפי ל-R^m. או במילים אחרות, הוא יושב בסידרה מדוייקת

$$0\to R^m\overset{A}{\to}R^n\to M\to 0$$

כאשר ההעתקה A נתונה ע"י מטריצה $n\times m$ של איברים ב-R.

דוגמא:

אם A אלכסונית עם אלכסון $d_1,...,d_m$ אז

$$M\simeq R/d_1\oplus\cdots\oplus R/d_m\oplus R^{n-m}$$

עבור $d_i=0$, הגורם $R/d_i=R$ הוא חופשי ועבור $d_i\neq 0$, הגורם R/d_i הוא פיתול ציקלי.

שינוי בסיס עבור R^n ועבור R^m יתנו מטריצה A אחרת, אבל עם אותו קו־גרעין. הפעולה הראשונה מתאימה ל-$A\mapsto A\cdot Q$ כאשר $Q\in GL_m\left(R\right)$ והפעולה השניה מתאימה ל-$A\mapsto P\cdot A$ כאשר $P\in GL_n\left(R\right)$. המטרה הבאה שלנו היא

טענה: קיימות P,Q הפיכות כנ"ל עבורן PAQ אלכסונית עם $d_1\mid d_2\mid\cdots\mid d_m$. בפרט, מתקיים

$$M\simeq R/d_1\oplus\cdots\oplus R/d_m\oplus R^{n-m}$$

הוכחה: ע"י כפל ב-P ו-Q, בפרט אפשר לבצע כל פעולת שורה ועמודה אלמנטרית. אם במקום ה-$(1,1)$ נמצא איבר a שמחלק את כל שאר האיברים במטריצה, אז אפשר באמצעות פעולות שורה ועמודה אלמנטריות לאפס את השורה/עמודה הראשונה ולהמשיך את האלגוריתם באינדוקציה על המינור ה-$(1,1)$. מכיוון ש-a מחלק שם את הכל נקבל את הצורה הרצויה. אם a לא מחלק את כל אברי המטריצה, נראה שניתן להחליף אותו באיבר a' שמחלק אותו ממש. מכיוון שבתחום ראשי יש פריקות יחידה, התהליך הזה חייב להעצר. זה עובד כך. אם ישנו b איפשהו במטריצה שלא מתחלק ב-a, אפשר להניח בה"כ שהוא במקום $(2,1)$ (למה?). כעת, ישנם $s,t\in R$ עבורם

$$sa+tb=\gcd\left(a,b\right)=g$$

וגם $a=gx$ ו-$b=gy$. המטריצה $P_0=\begin{pmatrix}s&t\\-y&x\end{pmatrix}$ מקיימת

$$g\cdot\det P_0=g\left(sx+ty\right)=sgx+tgy=sa+ty=g$$

$$\det P_0=1$$

כלומר, P_0 הפיכה. כמו כן, מתקיים

$$\begin{pmatrix}s&t\\-y&x\end{pmatrix}\begin{pmatrix}a&*\\b&*\end{pmatrix}=\begin{pmatrix}g&*\\ *&*\end{pmatrix}$$

אם נשלים את P_0 למטריצה P ש-P_0 היא הפינה השמאלית עליונה שלה, יש לה אחדים על הלכסון ואפס בשאר המקומות, נקבל שלמטריצה PA יש g במקום ה-$(1,1)$ שלה כנדרש וזה מסיים את ההוכחה.

מסקנה: כל מודול M נוצר סופית מעל תחום ראשי מקיים $M\simeq R^n\oplus T\left(M\right)$ כאשר $T\left(M\right)$ הוא התת־מודול של M של כל אברי הפיתול. בפרט, אם M חסר פיתול הוא חופשי.

מודולים לא נוצרים סופית

עבור מודולים לא נוצרים סופית המצב הרבה יותר מסובך. למשל, מעל $\mathbb{Z}$, כשמדובר בחבורות אבליות, אנחנו מקבלים

טענה 1: החבורה $\mathbb{Q}$ היא חסרת פיתול ולא חופשית.

הוכחה: לכל איבר $x\in\mathbb{Q}$ ולכל $n\in\mathbb{Z}$ קיים $y\in\mathbb{Q}$ עבורו $ny=x$. כלומר, $\mathbb{Q}$ חבורה חליקה. מצד שני, בחבורה חופשית כל איבר שונה מאפס איננו חליק.

טענה 2: החבורה $\prod_{n=1}^{\infty}\mathbb{Z}$ היא חסרת פיתול ולא חופשית למרות שהיא לא חליקה.

הוכחה: נוכיח שכל הומומורפיזם $\varphi:\prod_{n=1}^{\infty}\mathbb{Z}\to\mathbb{Z}$ שמתאפס על תת החבורה $\bigoplus_{n=1}^{\infty}\mathbb{Z}$ הינו זהותית אפס. תהי A_p תת־החבורה של כל האיברים מהצורה

$$a=\left(a_0,pa_1,p^2a_2,...\right)$$

לכל n, אפשר לכתוב את a בתור סכום

$$a=\left(a_0,pa_1,...,p^{n-1}a_{n-1},0,0,...\right)+\left(0,0,...,0,p^na_n,p^{n+1}a_{n+1},...\right)\in\bigoplus_{n=1}^{\infty}\mathbb{Z}+p^n\prod_{n=1}^{\infty}\mathbb{Z}$$

ולכן $\varphi(a)\in p^n\mathbb{Z}$ לכל n ומכאן $\varphi(a)=0$. כעת, נבחר שני ראשוניים שונים p,q ומכיוון ש-$\gcd\left(p^n,q^n\right)=1$ מקבלים $A_p+A_q=\prod_{n=1}^{\infty}\mathbb{Z}$.

טענה 3: בחבורה $A=\prod_{p}\mathbb{Z}/p$ (כאשר המכפלה היא על כל הראשוניים) החלק הפיתולי $T(A)$ איננו מחובר ישר.

הוכחה: מתקיים $T(A)=\bigoplus_{p=1}^{\infty}\mathbb{Z}/p$ והסידרה הקצרה

$$0\to T(A)\to A\to C\to 0$$

לא מתפצלת כי C הוא חליק וב-A אין אברים חליקים.

2 פירוק פרימארי

את הפירוק לגורמים אלמנטריים שקיבלנו עבור מודול נ"ס M מעל תחום ראשי R אפשר גם לסדר קצת אחרת. לכל $a\in R$ עם פירוק לגורמים ראשוניים $a=p_1^{e_1}p_2^{e_2}\cdots p_n^{e_n}$, מתקיים ממשפט השאריות הסיני

$$R/a\simeq R/p_1^{e_1}\oplus\dots R/p_n^{e_n}$$

לכן אם

$$M\simeq R/a_1\oplus\cdots\oplus R/a_r$$

אפשר לפרק כל R/a_i לסכום ישר של מודולים מהצורה R/p^e עבור p ראשוני. כעת, לכל ראשוני p, האיברים ב-M שתחת זיהוי זה שייכים לאיזשהו גורם מהצורה R/p^e הם בדיוק אברי הפיתול מסדר שהוא חזקה של p. אם נסמן את תת־המודול של האיברים הללו ב-M_p נקבל ש-

$$M=M_{p_1}\oplus\cdots\oplus M_{p_r}$$

עבור איזשהו אוסף סופי של ראשוניים $p_1,\dots,p_r$ ב-R (שיכול לכלול את 0).

פירוק ז'ורדן: עבור k שדה סגור אלגברית, V מ"ו ממימד סופי מעל k ו-$T:V\to V$ אופרטור לינארי, האופרטור T נותן ל-V מבנה של מודול נ"ס מעל התחום הראשי $k[t]$. מכיוון ש-k ס"א, הראשוניים היחידים ב-$k[t]$ הם פולינום האפס והפולינומים $(t-\lambda)$ עבור $\lambda\in k$. אנחנו מקבלים אם כך פירוק מהצורה

$$V\simeq\bigoplus k[t]/(t-\lambda)^e$$

המודול $k[t]/(t-\lambda)^e$ הינו מרחב וקטורי ממימד e מעל k עם בסיס

$$1,(t-\lambda),(t-\lambda)^2,\dots,(t-\lambda)^{e-1}$$

ביחס לבסיס זה t מיוצג ע"י המטריצה

$$\begin{pmatrix}\lambda & 1 & 0 & \cdots & 0\\ 0 & \lambda & 1 & \cdots & 0\\ 0 & 0 & \lambda & \cdots & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & 0 & \cdots & \lambda\end{pmatrix}$$