

אלגברה ב3

© ארזים

9 בינואר 2017

1 חוגי דדקינד

משפט 1.1 יהי R חוג דדקינד, ויהי $0 \neq P \subseteq R$ אידאל ראשוני. אזי R_P ראשי.

הוכחה: ראינו כי R_P הוא חוג דדקינד. לכן יש בו אידאל ראשוני יחיד שאינו 0 - האידאל המקסימלי היחיד שלו, שנשמנו m .

ראשית, נראה כי m אידאל ראשי. יהי $a \in m$, $a \neq 0$. אזי

$$\sqrt{R_P a} = m$$

R_P הוא חוג נתר ולכן יש n טבעי עבורו $m^n \subseteq R_P a$ אם $n = 1$, $m = R_P a$ וסיימנו. נניח כעת כי $n \geq 2$, ונניח כי n מינימלי. לכן $m^{n-1} \not\subseteq R_P a$. נבחר $b \in m^{n-1} \setminus R_P a$. נסמן $x = \frac{a}{b}$ (איבר בשדה המנות F של R ושל R_P). כעת, $\frac{1}{x} = \frac{b}{a} \notin R_P$, כלומר $\frac{1}{x} \in F \setminus R_P$. בפרט, $\frac{1}{x}$ אינו שלם מעל R_P . מכאן, נקבל כי $x^{-1}m \not\subseteq m$, שכן אחרת, m הוא מודול נאמן מעל $R_P[x^{-1}] \subseteq F$. m הוא מודול נוצר סופית מעל R_P . ממשפט קודם, ינבע כי $\frac{1}{x}$ שלם מעל R_P וזו סתירה. כעת,

$$bm \subseteq m^n \subseteq R_P a$$

ולכן

$$\frac{b}{a}m \subseteq R_P$$

$x^{-1}m \subseteq R_P$ - אידאל בחוג R_P . אבל $x^{-1}m \not\subseteq m$. מכאן $x^{-1}m = R_P$ ולכן $m = R_P x$ אידאל ראשי.

כעת, נתבונן במנה $V = m/m^2$ כמרחב ווקטורי מעל השדה R_P/m . V אינו 0 שכן $m \neq m^2$. כיוון שמתקיים $m = R_P x$, V מרחב ווקטורי מממד 1 מעל R_P/m .

יהי $I \subsetneq R_P$, $0 \neq I$ אידאל. אזי $I \subseteq m$. כיוון שמתקיים $\sqrt{I} = m$, קיים n טבעי עבורו $m^n \subseteq I$. אם $m^n = I$, אזי $I = R_P x^n$ ראשי. אחרת, $I \not\subseteq m^n$, ולכן יש r מקסימלי עבורו $I \subseteq m^r$. יהי

$$y = tx^r \in I \setminus R_P x^{r+1}$$

לכן $t \notin R_P x = m$, כלומר $t \in R_P \setminus m = R_P^*$. נסיק כי $x^r \in I$ ואז $m^r = R_P x^r \subseteq I$.
 ■ לכן $I = R_P x^r = m^r$ ראשי.

מסקנה 1.2 כל אידאל לא טריוויאלי של R_P הוא חזקה של m .

משפט 1.3 יהי R חוג דדקינד, ויהי $0 \neq Q \subseteq R$ אידאל פרימרי. אזי יש אידאל ראשוני P (מקסימלי) עבורו

$$Q = p^e$$

הוכחה: יהי $P = \sqrt{Q}$. זהו אידאל ראשוני שאינו 0, ולכן מקסימלי. נסמן $S = R \setminus P$ ונתבונן בלוקליזציה R_P . זהו חוג ראשי, מקומי בעל אידאל מקסימלי $m = S^{-1}P$. אנו יודעים כי $S^{-1}Q \subseteq R_P$ אידאל פרימרי, שהרדיקל שלו הוא $S^{-1}P = m$. מהמסקנה,

$$S^{-1}Q = m^r = (S^{-1}P)^r = S^{-1}(P^r)$$

ואז $S^{-1}Q = S^{-1}P^r$. ראינו כי ההתאמה $Q \mapsto S^{-1}Q$ היא חד-חד-ערכית ועל בין אידאלים פרימריים של R לבין אידאלים פרימריים של R_P , ולכן נקבל $Q = P^r$.
 ■

משפט 1.4 יהי R חוג דדקינד ויהי $0 \neq I \subsetneq R$ אידאל. אזי יש הצגה יחידה $I = P_1^{e_1} \cdots P_k^{e_k}$, כאשר $P_1, \dots, P_k$ אידאלים ראשוניים (מקסימליים) שונים, $e_1, \dots, e_k \geq 1$.

הוכחה: ראינו כי בחוג נתר R , בו כל אידאל ראשוני שאינו 0 הוא מקסימלי, לכל אידאל יש פירוק יחיד למכפלת אידאלים פרימריים זרים בזוגות:

$$I = Q_1 \cdots Q_k$$

כעת נסמן $Q_i = P_i^{e_i}$ מהמשפט הקודם, כאשר $P_i = \sqrt{Q_i}$ ראשוני. אזי

$$I = P_1^{e_1} \cdots P_k^{e_k}$$

לכן קיבלנו קיום. עבור יחידות, נניח כי

$$I = (P'_1)^{e'_1} \cdots (P'_m)^{e'_m}$$

פירוק שכזה. כיוון שהאידאלים $Q'_i = (P'_i)^{e'_i}$ פרימריים, כחזקה של אידאלים מקסימליים, אזי

$$I = Q'_1 \cdots Q'_m$$

הוא פירוק פרימרי (מינימלי). מיחידות הפירוק הפרימרי, $m = k$, ולאחר סידור מחדש

$$P_i^{e_i} = (P'_i)^{e'_i}$$

לאחר השוואת הרדיקלים, $P_i = P'_i$. נקבל כי

$$P_i^{e_i} = P_i^{e'_i}$$

לכל i . נסמן $S = R \setminus P_i$, ונתבונן בחוג R_{P_i} עם האידאל

$$S^{-1}I = (S^{-1}P_1)^{e_1} \cdots (S^{-1}P_k)^{e_k} = (S^{-1}P_i)^{e_i}$$

באותו אופן

$$S^{-1}I = (S^{-1}P_i)^{e'_i}$$

נכתוב $S^{-1}P_i = R_{P_i}x_i$. לכן

$$R_{P_i}x_i^{e_i} = R_{P_i}x_i^{e'_i}$$

אם, למשל $e'_i > e_i$, אזי

$$\begin{aligned} x_i^{e_i} &= r_i x_i^{e'_i} \\ 1 &= r_i x_i^{e'_i - e_i} \end{aligned}$$

ולכן x_i הפיך - בסתירה. בכיוון ההפוך העניין דומה, ולכן $e'_i = e_i$. ■

משפט 1.5 יהי A חוג דדקינד ויהי F שדה המנות של A . יהי $F \subseteq K$ שדה הרחבה ממימד סופי וספרבילי. יהי R הסגור השלם של A בתוך K . אזי גם R הוא חוג דדקינד ששדה המנות שלו הוא K .

הוכחה: אנו יודעים כי R סגור בשלמות בתוך K . נראה כי K הוא שדה המנות של R . יהי $y \in K$, $y \neq 0$. y אלגברי מעל F . נתבונן במשוואה המינימלית של y מעל F :

$$y^n + \sum_{i=0}^{n-1} \frac{a_i}{b_i} y^i = 0$$

כאשר $a_i, b_i \in A$, $b_i \neq 0$, לכל $0 \leq i \leq n-1$. על ידי לקיחת מכנה משותף נוכל להניח כי $b_0 = \cdots = b_{n-1} = b$, ואז נכפול פי b^n .

$$(by)^n + \sum_{i=0}^{n-1} a_i b^{n-i} (by)^i = 0$$

ואז $by \in R$, כלומר $y \in \frac{1}{b}R$. אפשר לכתוב $y = \frac{r}{b}$, עבור $r \in R, b \in A$ ולכן K הוא שדה המנות של R .
יהי $Q \subseteq R, 0 \neq Q$ אידאל ראשוני. נסמן $Q \cap A = P$. זהו אידאל ראשוני של A . נראה כי $0 \neq P$. יהי $0 \neq y \in Q$. ראינו כי הפולינום המינימלי של y מעל F הוא בעל מקדמים מתוך A , כי שלם מעל A . נכתוב את המשוואה המינימלית:

$$y^n + \sum_{i=0}^{n-1} a_i y^i = 0$$

כאשר $a_i \in A$. ברור כי $a_0 \neq 0$, ממינימליות n . לכן

$$a_0 = -y^n - \sum_{i=1}^{n-1} a_i y^i \in Q \cap A = P$$

לכן P אידאל ראשוני שאינו 0 בחוג דדקינד A , ולכן P מקסימלי. ראינו בעבר כי במצב כזה P מקסימלי אם ורק אם Q מקסימלי, ולכן נקבל כי Q מקסימלי.
נותר להוכיח כי R חוג נתר. כיוון שנתון כי K הרחבה ספרבילית סופית של F , יש $\alpha \in K$ עבורו $K = F[\alpha]$. כשנכתוב $\alpha = \frac{r}{b}, r \in R, b \in A$, ולכן

$$F[\alpha] = F[r]$$

לכן נוכל להניח כי $\alpha \in R$, כלומר שלם מעל A . יהי $f(x) \in F[x]$ הפולינום האי פריק של α מעל F . כיוון שלקחנו α שלם מעל A , $f(x) \in A[x]$. יהי $F \subseteq L$ שדה הפיצול של $f(x)$ מעל F .
נניח כי ממעלה r , ולכן יש לו r שורשים שונים, שנשמנם $\alpha = \alpha_0, \dots, \alpha_{r-1} \in L$. כל שורש כזה מגדיר

$$\sigma_i : F[\alpha] \xrightarrow{\sim} F[\alpha_i]$$

איזומורפיזם של שדות מעל F , על ידי

$$\sum_{j=0}^{r-1} t_j \alpha_j \mapsto \sum_{j=0}^{r-1} t_j \alpha_i^j$$

נסמן

$$D = \prod_{i < j} (\alpha_i - \alpha_j) \in L$$

נראה כי $R \subseteq D^{-2}A[\alpha]$. יהי $0 \neq y \in R$.

$$y = \sum_{i=0}^{r-1} c_i \alpha^i$$

עבור $c_i \in F$, שכן $K = F[\alpha]$. כעת,

$$\sigma_j(y) = \sum_{i=0}^{r-1} c_i \alpha_j^i$$

נשים לב כי:

$$\begin{pmatrix} \sigma_0(y) \\ \vdots \\ \sigma_{r-1}(y) \end{pmatrix} = \begin{pmatrix} 1 & \alpha_0 & \dots & \alpha_0^{r-1} \\ 1 & \alpha_1 & \dots & \alpha_1^{r-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_{r-1} & \alpha_{r-1}^2 & \alpha_{r-1}^{r-1} \end{pmatrix} \begin{pmatrix} c_0 \\ \vdots \\ c_{r-1} \end{pmatrix}$$

מכלל קרמר, נקבל

$$c_i = \frac{A_i}{D}$$

כאשר A_i הוא אהדטרמיננטה של המטריצה בה מחליפים את העמודה i בעמודה שנמצאת באגף שמאל.

כל α_i שלם מעל A , כי הם שורשי $f(x)$. כיוון שגם y שלם מעל A , $\sigma_j(y)$ שלמים מעל A גם כן. A_i הוא סכום של מכפלות של האיברים הללו, ולכן A_i שלם מעל A . D שלם מעל A . נקבל כי

$$D^2 c_i = A_i D$$

כאשר אגף ימין שלם מעל A . נראה כי $D^2 \in A$. D^2 פולינום סימטרי בערכים $\alpha_0, \dots, \alpha_{r-1}$ עם מקדמים שלמים. ממשפט הפונקציות הסימטריות נקבל כי D^2 הוא פולינום במקדמים שלמים של הפולינומים הסימטריים האלמנטריים בערכים $\alpha_0, \dots, \alpha_{r-1}$. אלה הם (עד כדי סימן) המקדמים של $f(x)$ (נוסחאות וייטה), ולכן מתוך A . מכאן $D^2 \in A$ ובפרט $D^2 c_i \in F$ ושלם מעל A . A סגור בשלמות (בתוך F), ולכן $D^2 c_i \in A$. לכן

$$c_i \in D^{-2} A$$

נסיק כי

$$y \in D^{-2} A[\alpha]$$

לכן קיבלנו את ההכלה שרצינו. כעת, נסיים. $A[\alpha]$ מודול נוצר סופית מעל חוג נתר A (שכן α שלם מעל A). לכן $A[\alpha]$ הוא מודול נתר מעל A , ומכאן $A[\alpha]$ הוא חוג נתר. כעת, $A[\alpha] D^{-2}$ הוא מודול נוצר סופית (על ידי D^{-2}) מעל חוג נתר $A[\alpha]$, ולכן זהו מודול נתר מעל $A[\alpha]$. $A[\alpha] D^{-2} \subseteq R$ הוא תת מודול מעל $A[\alpha]$, ולכן R בעצמו מודול נתר מעל $A[\alpha]$. מכאן R חוג נתר. לכן סיימנו. ■

2 משפט האפסים של הילברט (Nullstellensatz)

משפט 2.1 (זריצקי) נתונים שדות $F \subseteq B$. נניח כי B נוצר סופית כאלגברה מעל F . אזי B ממימד סופי מעל F .

הוכחה: ההנחה אומרת שיש $\alpha_1, \dots, \alpha_n \in B$ עבורם

$$B = F[\alpha_1, \dots, \alpha_n]$$

נוכיח באינדוקציה על n . עבור $n = 1$, נקבל $B = F[\alpha_1]$. $\frac{1}{\alpha_1} \in B$, שכן B שדה, ואז נוכל להציג

$$\frac{1}{\alpha_1} = \sum_{i=0}^k a_i \alpha_1^i$$

כאשר $a_i \in F$. נקבל

$$\sum_{i=0}^k a_i \alpha_1^{i+1} - 1 = 0$$

לכן α_1 אלגברי מעל F . אזי

$$\dim B = \dim_F F[\alpha_1] \leq n + 1$$

ולכן B ממימד סופי מעל F .
באופן כללי, באינדוקציה, V ממימד סופי מעל שדה המנות של $A = F[\alpha_1]$, $K = F(\alpha_i)$ כי B נוצר סופית על ידי $n - 1$ איברים

$$B = K[\alpha_2, \dots, \alpha_n]$$

באינדוקציה, $\dim_K B < \infty$ ולכן $\alpha_1, \dots, \alpha_n$ אלגבריים מעל K .
נעצור כאן, ונמשיך בשיעור הבא.

■