9/3/08

אלגברה מ' 2 - שיעור 2

טענה: האידאל $I=\langle p(x)\rangle$ בחוג $F[x]$ הוא אידאל מקסימלי אם ורק אם $p(x)$ הינו אי-פריק מעל השדה F.

הוכחה: פולינום $p(x)$ יקרא אי-פריק אם אי-אפשר לרשום $p(x)=g(x)h(x)$, כאשר $g,h\in F[x]$ כך ש: $\deg p<\deg g,\deg h$. נניח כי I אידאל הושי הנוצר ע"י $p(x)$, וקיים $I\supseteq J=\langle g(x)\rangle$. אז $p(x)\in\langle g(x)\rangle$ ולכן ניתן לרשום $p(x)=h(x)g(x)$, ומתקיים $\deg p\geq\deg g,\deg h$.
אם $p(x)$ אי-פריק אז $\deg p=\deg h$ או $\deg p=\deg g$.
במקרה הראשון $J=F[x]$ (כי אז $g\in F$ ובמו אשר הפיק ב-$F[x]$), במקרה השני $J=I$. לכן I מקסימלי.
אם I מקסימלי ואם $p(x)=g(x)h(x)$ כאשר $\deg p\geq\deg g,\deg h$, אז מהטענה ההוכחה נובע כי I לא יכול להיות מקסימלי. ∎

הגדרה: תהי R טבעת חלקי אפס (אם $ab=0$ אז $a=0$ או $b=0$) נקרא **תחום שלמות**.

הגדרה: אידאל $R\supseteq I$ נקרא אידאל ראשוני אם כאשר $ab\in I$ אז $a\in I$ או $b\in I$.

תרגיל בית: $R\supseteq I$ הינו אידאל ראשוני אם ורק אם R/I הינו תחום שלמות.

דוגמה: יהי $F[x]\supseteq I$ אידאל השונה מאפס. אז I ראשוני אם ורק אם I מקסימלי.

תרגיל: מכל תחום אידאל מקסימלי הוא אידאל ראשוני

הוכחה: אם I מקסימלי אז $F[x]/I$ שדה ולכן הוא תחום שלמות. מהתרגיל I ראשוני. נניח כי I הוא ראשוני ונניח כי $I=\langle g(x)\rangle$. נוכיח כי $g(x)$ הוא אי-פריק. אם לא אז נרשום $p(x)q(x)=g(x)$, כאשר $\deg p,\deg q<\deg g$. מהיות I ראשוני נובע כי $p(x)\in I$ או $q(x)\in I$. בו סתירה למינימליות הדרגה של $g(x)$. ∎

שדה המנות של תחום שלמות

יהי R תחום שלמות. נגדיר: $L=\{(a,b)\in R\times R,\ b\neq 0\}$
נגדיר יחס על L ע"י: $(a_1,b_1)\sim(a_2,b_2)\iff a_1b_2=a_2b_1$
יחס זה הינו יחס שקילות (כדי להוכיח זאת צריך להשתמש בעובדה ש-R הינו תחום שלמות - מבו תרגיל בית).

נסמן את מחלקת השקילות של (a,b) ב- $\frac{a}{b}$. נגדיר פעולות:

$$\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd} \qquad \frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$$

בדוק שהגדרה זו אינה תלויה בבחירת הנציגים של מחלקת השקילות.

אם נסמן ב- Q את מחלקות השקילות עם הפעולות הנ"ל - אז נקבל שדה, הנכנע את R. Q נקרא שדה המנות של R.

<u>טענה</u>: ההעתקה $\varphi: R \to Q$ המוגדרת ע"י $\varphi(x)=\frac{x}{1}$ היא אי-זומורפיזם על התמונה.

<u>הוכחה</u>: נראה כי $\ker\varphi=0$. אם $x\in\ker\varphi$ אז $\varphi(x)=0$.

$$\frac{x}{1}=\frac{0}{1} \iff 1\cdot 0=1\cdot x \iff x=0$$

(קל לבדוק שהוא אכן הומומורפיזם). ∎

<u>דוגמאות</u>: 1) $R=\mathbb{Z}$ ואז $Q=\mathbb{Q}$.

2) $R=F[x]$ (F שדה) אז Q שדה כל הפונקציות הרציונליות, שמסומן $F(x)$.

פולינומים

(בחלק זה נעמד לפי ספרו של Rotman)

יהי R חוג ונסמן ב- $R[x]$ את חוג הפולינומים מעל R. אם R הוא שדה אז $R[x]$ הינו תחום ראשי, ואם רצוני שכל אידאל ראשוני הינו מקסימלי.

<u>הגדרה</u>: יהי R תחום שלמות ויהיו $f(x),g(x)\in R[x]$. ה- <u>gcd</u> של $f(x)$ ו- $g(x)$ ג'סומן ב- $(f(x),g(x))$ הינו הפולינום $d(x)\in R[x]$ המקיים:

1) $d\mid f, d\mid g$.

2) אם $c\mid f$ ואם $c\mid g$ אז $c\mid d$.

3) $d(x)$ הינו פולינום מתוקן - מקדם המוביל שווה ל- 1.

אם $(f,g)=1$ נאמר ש- f ו- g פולינומים <u>זרים</u>.

<u>משפט 14</u>: יהי F שדה ויהיו $f,g\in F[x]$ אז $d=(f,g)$ קיים, ומתקיים:

$$d(x)=a(x)f(x)+b(x)g(x)$$

עבור $a,b\in F[x]$.

הוכחה: נגדיר את הקבוצה I להיות אוסף כל הפולינומים מהצורה

$$I = \{a(x)f(x) + b(x)g(x) \;:\; a,b \in F[x]\}$$

I הינו אידאל.

$F[x]$ הינו pid ולכן קיים פולינום מתוקן $d(x)$ כך שמתקיים $I = \langle d(x) \rangle$. כיוון ש- $f,g \in I$ אז $d \mid f$, $d \mid g$.

מהגדרת I נובע כי קיימים a,b כך ש: $d = af + bg$.

אם $f \mid c$ וגם $g \mid c$ אז $f = cc'$, $g = cc''$ ולכן

$$d = af + bg = acc' + bcc'' = c(ac' + bc'')$$

כלומר $d \mid c$. ∎

כדי למצוא את ה- gcd משתמשים באלגוריתם החלוקה.

משפט 17: ישנו אלגוריתם לחישוב gcd של פולינומים.

רעיון ההוכחה: נניח כי $\deg f \geq \deg g$. מאלגוריתם החלוקה קיים פולינום q_1 כך ש:

$$f = q_1 g + r_1$$

כאשר r_1 פולינום שדרגתו קטנה ממש מדרגת g. אם $r_1 \neq 0$ אז נרשום $g = q_2 r_1 + r_2$, $\deg r_2 < \deg r_1$, ובאינדוקציה: $r_i = q_{i+2} r_{i+1} + r_{i+2}$, $\deg r_{i+2} < \deg r_{i+1}$

לכן קיים n כך ש: $r_{n+1} \cdot q_{n+2} = r_n$

אז (עד כדי קבוע) $d = r_{n+1}$. ∎

הגדרה: נאמר כי השדה K הינו **הרחבה** של השדה k אם קיים הומומורפיזם $k \to K$. נסמן כאן $k \subseteq K$.

מסקנה 18: יהיו $k \subseteq K$ שדות, ויהיו $f,g \in k[x] \subseteq K[x]$. אז חישוב ה- gcd של f ו-g בתוך $K[x]$ נותן לחישובו בתוך $k[x]$.

הוכחה: נרשום ב- $k[x]$: $f(x) = Q(x)g(x) + R(x)$ כאשר $Q,R \in k[x]$, וגם $\deg R < \deg g$. מעתה $k[x]$ נרשום $f(x) = q(x)g(x) + r(x)$ כאשר $q,r \in k[x]$, $\deg r < \deg g$. כיוון ש- $k[x] \subseteq K[x]$, אז השוויון הנ"ל נקרא גם ב- $K[x]$. לכן מיחידות ההצגה של אלגוריתם החלוקה ב- $K[x]$ (נקבל כי ב- $K[x]$, $Q(x) = q(x)$ וגם $R(x) = r(x)$.

משפט 20: יהי $f(x)\in F[x]$ ויהי $a\in F$. אז קיים $q(x)\in F[x]$ כך ש: $f(x)=q(x)(x-a)+f(a)$.

מסקנה 21: יהי $f(x)\in F[x]$. אז $a\in F$ הינו שורש של $f(x)$ אמ"מ $x-a$ מחלק את $f(x)$.

משפט 22: יהי F שדה ויהי $f(x)\in F[x]$ פולינום מדרגה $n\geq 0$.
אז ל-F יש לכל היותר n שורשים של $f(x)$.

הוכחה: נניח כי ל-F יש $n+1$ שורשים שונים של $f(x)$.
נסמן: $a_1,\dots,a_{n+1}$. ממסקנה 21 נובע כי: $f(x)=(x-a_1)g_1(x)$,
עבור $g_1(x)\in F[x]$. $x-a_2$ מחלק את $f(x)$ (מאותה מסקנה). כיוון ש:
$a_1\neq a_2$ אז הפולינום $x-a_1$ זר לפולינום $x-a_2$. לכן $x-a_2$ מחלק
את $g_1(x)$ וניתן לרשום: $g_1(x)=(x-a_2)g_2(x)$, $g_2(x)\in F[x]$
$f(x)=(x-a_1)(x-a_2)g_2(x)$
באינדוקציה (תרגיל 3) נקבל כי: $f(x)=(x-a_1)\cdots(x-a_{n+1})g_{n+1}(x)$
וזו סתירה.

הערה: המשפט האחרון אינו נכון אם F אינו שדה. ל-$\mathbb{Z}_8$ הפולינום x^2-1 יש
ארבעה שורשים שונים: $1,3,5,7$.

מסקנה 23: יהי F שדה ו-$p(x)\in F[x]$ פולינום אי-פריק שלו F. אז הקבוצה
$\frac{F[x]}{\langle p(x)\rangle}$ היא שדה, המכיל תת-שדה איזומורפי ל-F, ושם
$p(x)$ שורש של $p(x)$.

דוגמה: $\mathbb{C}\simeq\frac{\mathbb{R}[x]}{\langle 1+x^2\rangle}$

הוכחה: $p(x)$ אי-פריק $\Rightarrow\langle p(x)\rangle$ איבר מקסימלי $\Rightarrow\frac{F[x]}{\langle p(x)\rangle}$ הינו שדה.
נסמן ב-E. ההעתקה $E\to F$ המוגדרת ע"י $I+a\mapsto a$ (כאשר
$\langle p(x)\rangle=I$) הינו הומומורפיזם מח"ע. נסמן את התמונה ב-F' אז
$F'\simeq F$. נסמן $p(x)=\sum_{i=0}^{n}a_ix^i$, $a_i\in F$. הקבוצ $I+x$ הינו שורש
של $p(x)$: נבדוק להראות כי $I=(I+x)p$.

$$I=I+p(x)=I+\left(\sum_{i=0}^{n}a_ix^i\right)=\sum_{i=0}^{n}a_i(x+I)^i=p(x+I)$$