11/3/09

אלגברה ב' 2 - תרגול 2

בשדה יש רק 2 אידיאלים, אידאל ה-0 וכל השדה.

נראה שלחוג המטריצות $M_n(F)$ - על אף שאינו שדה - אין אידיאלים פרט ל-0 ולחוג עצמו. יהי $I \neq 0$ אידאל כלשהו, ונראה כי I מכיל איבר הפיך, ומכאן ינבע $I=M_n(F)$.

יהי $0 \neq a \in I$, ונניח כי $0 < \text{rank}\, a = r$. אזי לפי דירוג גאוס, קיימים g_1, g_2 כך ש:

$$g_1 a g_2 = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} \in I$$

באופן דומה נקבל כי המטריצה $\begin{pmatrix} 0 & \\ & I_r \\ & & 0 \end{pmatrix} \in I$.

מכאן נקבל כי אם $r < n$, $I \ni \begin{pmatrix} I_{r+1} & 0 \\ 0 & 0 \end{pmatrix}$. באינדוקציה נקבל כי $I_n \in I$.

לכן $I=M_n(F)$. ∎

<u>הגדרה:</u> <u>השדה הראשוני</u> של שדה F הוא חיתוך כל התת-שדות של F.

<u>תרגיל:</u> אם F שדה, אזי השדה הראשוני שלו הוא $\mathbb{Q}$ ~~או~~ $\mathbb{Z}_p$ כאשר p ראשוני.

<u>הגדרה:</u> אם השדה הראשוני של F הינו $\mathbb{Z}_p$, אזי <u>המציין</u> של F הוא p. אחרת, ~~[illegible]~~ המציין של F הוא 0 (מסמנים $(\text{char}(F))$.

<u>תרגיל:</u> נניח כי $\text{char}\, F = p$. אזי:

1) יהי $a \in F$. אזי:

$$pa = \underbrace{a+a+\dots+a}_{p} = \underbrace{(1+1+\dots+1)}_{p}a = 0 \cdot a = 0$$

2)
$$(a+b)^p = a^p + b^p$$

בפרט: ההעתקה $\sigma : F \to F$ המוגדרת ע"י $\sigma(a) = a^p$ הינה הומומורפיזם. σ נקרא <u>ההומומורפיזם של פרוביניוס</u>.

זה נכון כי:

$$(a+b)^p = a^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i} + b^p \underset{\substack{\uparrow \\ p \mid \binom{p}{i} \\ 1 \le i \le p-1}}{=} a^p + b^p$$

3)
$$(a+b)^{p^k} = a^{p^k} + b^{p^k}$$

באינדוקציה על k. $k=1$ הוכחנו.

$$(a+b)^{p^{k+1}} = \left((a+b)^{p^k}\right)^p \underset{\text{אינדוקציה}}{=} \left(a^{p^k}+b^{p^k}\right)^p \underset{\text{חלק 2}}{=} a^{p^{k+1}}+b^{p^{k+1}}$$

ראינו כי אם $(f,g)=1$ כאשר $f,g\in F[x]$ (F שדה) אז קיימים $a,b\in F[x]$ כך ש: $af+bg=1$.

זה אינו נכון בהכרח אם F אינו שדה אלא חוג. למשל, ניקח $R=\mathbb{Z}[x]$. אז x ו-2 הינם פולינומים זרים, אבל לא קיימים $a,b\in\mathbb{Z}[x]$ כך ש:
$x\cdot a(x)+2b(x)=1$

שוויון זה לא ייתכן, כי המקדם החופשי באגף ימין הינו 2α עבור α מסוים, ובאגף שמאל הוא 1, והרי ב-$\mathbb{Z}$ לא קיים פתרון למשוואה $2\alpha=1$.

<u>תרגיל:</u> מצאו את ה-gcd של $f=x^3-2x^2+1$, $g=x^2-x-3$ (ב-$\mathbb{Q}$).

<u>פתרון:</u>

$$\begin{array}{r|l} \multicolumn{2}{l}{x-1} \\ x^3-2x^2+1 & x^2-x-3 \\ x^3-x^2-3x & \\ \hline -x^2+3x+1 & \\ -x^2+x+3 & \\ \hline 2x-2 & \end{array} \qquad \begin{array}{r|l} \multicolumn{2}{l}{\frac{1}{2}x} \\ x^2-x-3 & 2x-2 \\ x^2-x & \\ \hline -3 & \end{array}$$

קיבלנו כי:

$$\underbrace{(x^3-2x^2+1)}_{f} = \underbrace{(x-1)}_{q_1}\underbrace{(x^2-x-3)}_{g} + \underbrace{(2x-2)}_{r_1}$$

$$\underbrace{(x^2-x-3)}_{g} = \underbrace{(\tfrac{1}{2}x)}_{q_2}\underbrace{(2x-2)}_{r_1} + \underbrace{(-3)}_{r_2}$$

לכן $\gcd(f,g)=1$.

<u>תרגיל:</u> נניח כי $f(x)\in F[x]$ פולינום אי-פריק מעל F. ראינו כי $\frac{F[x]}{\langle f(x)\rangle}$ הינו שדה. יהי $g(x)+I\neq 0$ איבר כלשהו. מהו ההופכי שלו?
(ניתן להניח כי דרגת $g(x)$ קטנה ממש מדרגת $f(x)$.)

<u>פתרון:</u> כיוון ש-$f(x)$ אי-פריק, $(g,f)=1$. לכן קיימים a,b כך ש:
$$ag+bf=1 \Rightarrow ag+I=1+I \Rightarrow (a+I)(g+I)=1+I$$
מכאן $a+I$ הוא ההופכי של $g+I$.

דוגמה: $\mathbb{Z}_2[x]/\langle x^2+x+1\rangle$. מהו ההופכי של $(1+x)+I$?

נחפש פתרון למשוואה:

$$a(x)(1+x)+b(x)(1+x+x^2)=1$$

$$\begin{array}{r} x \\ x+1 \overline{)\, x^2+x+1} \\ \underline{x^2+x} \\ 1 \end{array} \qquad \begin{array}{r} x+1 \\ 1 \overline{)\, x+1} \end{array}$$

כלומר,

$$(-x)(x+1)+1(x^2+x+1)=1$$

לכן ההופכי של $1+x+I$ הוא $-x+I$.