תרגול 7

פונקציית אוילר:

תזכורת: $\varphi(m)=\#(\mathbb{Z}/m\mathbb{Z})^*$

הגדרה: יהיו G_1,G_2 חבורות. המכפלה הישרה זו מכפלה קרטזית $G_1\times G_2$ עם חוק כפל $(a_1,a_2)(b_1,b_2)=(a_1b_1,a_2b_2)$.

המכפלה הישרה היא חבורה עם איבר יחידה (e_1,e_2).

הגדרה: יהיו R_1,R_2 חוגים. אז המכפלה הישרה זה $R_1\times R_2$ עם חוקי חיבור וכפל לפי הקואורדינטות:

$(a_1,a_2)+(b_1,b_2)=(a_1+b_1,a_2+b_2)$ ← איבר 0: $(0,0)$

$(a_1,a_2)\cdot(b_1,b_2)=(a_1b_1,a_2b_2)$ ← איבר יחידה: $(1,1)$

⚠ בחוג זה יש מחלקי אפס - $(1,0)(0,1)=(0,0)$ ← זה לא שדה.

למה: יהיו R_1,R_2 חוגים (חילופיים עם יחידה). אז $\boxed{(R_1\times R_2)^\times=R_1^\times\times R_2^\times}$

כלומר $(x_1,x_2)\in R_1\times R_2$ הפיך ⟺ x_1,x_2 הפיכים ב- R_1,R_2 בהתאמה.

הגדרה: יהיו G,H חבורות. הומומורפיזם $f:G\to H$ זה העתקה כך ש- $f(xy)=f(x)f(y)$.

דוגמא: $(\mathbb{R},+)\to(\mathbb{R}^*,\cdot)$, $x\mapsto e^x$ הומומורפיזם כי $e^{x+y}=e^xe^y$

הגדרה: איזומורפיזם של חבורות זה הומומורפיזם חח"ע ועל.

דוגמא: $(\mathbb{Z}/2\mathbb{Z},+)\to(\{1,-1\},\cdot)$

$\bar{0}\mapsto 1$

$\bar{1}\mapsto -1$

הגדרה: חבורות G,H איזומורפיות אם קיים איזומורפיזם $G\to H$.

כמובן: $G\cong H$ ← $\#G=\#H$.

הגדרה: יהיו R,S חוגים. הומומורפיזם $f:R\to S$ זו העתקה כך ש-

$f(x+y)=f(x)+f(y)\ \wedge\ f(xy)=f(x)f(y)\ \wedge\ f(1_R)=1_S$

הגדרה: איזומורפיזם של חוגים זה הומו' חח"ע ועל.

למה: אם $f:R\to S$ איזומורפיזם חוגים אז $f(R^\times)=S^\times$ ו- $f|_{R^\times}:R^\times\to S^\times$ הוא איזומורפיזם של חבורות.

משפט: אם $m_1,m_2\in\mathbb{Z}$, $m_1,m_2>1$, $\gcd(m_1,m_2)=1$ אזי $\boxed{\varphi(m_1m_2)=\varphi(m_1)\varphi(m_2)}$

הוכחה:

נגדיר $m=m_1m_2$. נתבונן על $f:\mathbb{Z}/m\mathbb{Z}\to\mathbb{Z}/m_1\mathbb{Z}\times\mathbb{Z}/m_2\mathbb{Z}$: $x+m_1m_2\mathbb{Z}\to(x+m_1\mathbb{Z},x+m_2\mathbb{Z})$

ההעתקה מוגדרת היטב. כיוון ש- m_1,m_2 זרים, לפי משפט השאריות הסיני f היא איזומורפיזם. אכן יהיו $y+m_1\mathbb{Z}$, $z+m_2\mathbb{Z}$. לפי משפט הסיני יש (קיים) $x\in\mathbb{Z}$ כך ש- $x\equiv y\ (m_1)$, $x\equiv z\ (m_2)$ אז $(y+m_1\mathbb{Z},z+m_2\mathbb{Z})\longmapsto x+m\mathbb{Z}$, x יחיד (מחמת) מודולו m.

$$\Leftarrow\quad \mathbb{Z}/m_1m_2\mathbb{Z}\cong\mathbb{Z}/m_1\mathbb{Z}\times\mathbb{Z}/m_2\mathbb{Z}$$
$$\Downarrow$$
$$(\mathbb{Z}/m_1m_2\mathbb{Z})^*\cong(\mathbb{Z}/m_1\mathbb{Z})^*\times(\mathbb{Z}/m_2\mathbb{Z})^*$$
$$\Downarrow$$
$$\varphi(m_1m_2)=\varphi(m_1)\cdot\varphi(m_2)\qquad\blacksquare$$

דוגמא: $\underset{4}{\varphi(12)}=\underset{2}{\varphi(3)}\underset{2}{\varphi(4)}$;

אם $m=p_1^{l_1}p_2^{l_2}\cdot\ldots\cdot p_r^{l_r}$ אז $\varphi(m)=\varphi(p_1^{l_1})\cdot\ldots\cdot\varphi(p_2^{l_2})$

p ראשוני, נרצה לחשב את $\varphi(p^l)$ - כמה לא זרים ל- p^l? p^{l-1} הם הכפולות של p.

לכן סה"כ: $\boxed{\varphi(p^l)=p^l-p^{l-1}}$.

$$\Leftarrow\quad \varphi(m)=\prod_{j=1}^{r}(p_j-1)p_j^{l_j-1}\quad\Leftarrow\quad \varphi(m)=\prod\left(1-\frac{1}{p_j}\right)\prod p_j^{l_j}=m\prod\left(1-\frac{1}{p_j}\right)$$

לכן למשל עבור $m=18=2^1\cdot3^2$: $\varphi(m)=18\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)=6$

מכאן ש- $(\mathbb{Z}/m\mathbb{Z})^*\cong(\mathbb{Z}/p_1^{l_1}\mathbb{Z})^*\times\ldots\times(\mathbb{Z}/p_r^{l_r}\mathbb{Z})^*$

פולינומים

אם k שדה נגדיר $k[x]=\{f:a_0+a_1x+\ldots+a_nx^n\}$. מתקיים: $k[x]$ הוא <u>חוג</u>,

$f=\sum a_ix^i$, $g=\sum b_ix^i\ \Rightarrow\ fg=\sum c_ix^i$ כאשר $c_i=\sum_{\substack{u+v=i\\(0\le u,v)}}a_ub_v$

דוגמא: $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$. נסתכל על הפולינום: $f(x)=x^p-x\in\mathbb{F}_p[x]$.

מתקיים: $f(0)=0-0=0$ וגם לכל $0\ne a\in\mathbb{Z}/p\mathbb{Z}$: $f(a)=a(a^{p-1}-1)\underset{\uparrow}{=}0$

לפי משפט פרמה הקטן

כלומר הפולינום משרה פונקציית אפס אך לפי הגדרה הוא אינו פולינום האפס!

• איבר יחידה: 1 • איבר אפס: 0 • הפיכים: $k[x]^\times=k^\times=k\setminus\{0\}$

טענה: $k[x]$ הוא תחום שלמות (אין מחלקי אפס)

אם $f\ne0$ אז $f(x)=a_0+\ldots+a_nx^n$, $g(x)=b_0+\ldots+b_mx^n\ \Rightarrow\ fg=a_0b_0+\ldots+a_nb_mx^{n+m}$

$a_nb_n\ne0$ כי $a_n\ne0$ ∧ $b_n\ne0$ $\Leftarrow$ $fg\ne0$ $\blacksquare$

המשך תרגול 7 8

הגדרה: $f(x)=a_0+a_1x+\dots+a_nx^n$, $f\neq 0$, $a_n\neq 0$. אזי המעלה $deg(f)=n$.

אם $f=0$ אז אין מעלה.

הגדרה: פולינום לא קבוע $p\in k[x]$ ייקרא אי פריק אם $p=ab$ $\Leftarrow$ $a\in k^\times$ או $b\in k^\times$

הערה: כל פולינום לא קבוע הוא מכפלה של פולינומים אי פריקים.

הוכחה באינדוקציה על המעלה.

הגדרה: יהי p פולינום אי פריק מתוקן. נגדיר $ord_p f=a$ אם $a\in\mathbb{Z}_{\geq 0}$, $p^a|f$ וגם $p^{a+1}\nmid f$.

a כזה קיים כי $p^0|f$, $p^{deg(f)+1}\nmid f$.

$ord_p f=0 \iff p\nmid f$