תזכורת:

R חוג, $I,J \trianglelefteq R$ אידיאלים. הגדרנו:

$$I+J=\{i+j : i\in I,\ j\in J\}$$

$$IJ=\{a_1i_1j_1+\ldots+a_ri_rj_r : a_k\in R,\ i_k\in I,\ j_k\in J\}$$

דוגמה: $R=\mathbb{Z}$ $\quad$ $I=n\mathbb{Z},\ J=m\mathbb{Z}$

$$I+J=\{nx+my : x,y\in\mathbb{Z}\}=\{x\in\mathbb{Z} : \gcd(n,m)\mid x\}=\gcd(n,m)\mathbb{Z}$$

$$I+J=\underbrace{(n,m)}_{\text{אידיאל נוצר}}=d\mathbb{Z}\qquad (d=\gcd(n,m))$$

$$IJ=nm\mathbb{Z}$$

הגדרה: R חוג, $I,J \trianglelefteq R$ אידיאלים. I,J נקראים זרים אם $I+J=R$

משפט (משפט השאריות הסיני):

R חוג חילופי. I,J אידיאלים זרים. אזי $R/IJ \simeq R/I \times R/J$

הוכחה:

נגדיר הומ' של חוגים $f:R\to R/I\times R/J$

$$f(r)=(r+I,\ r+J)$$

הגרעין של f:

$$r\in\ker f \iff f(r)=(0_{R/I},0_{R/J}) \iff r+I=0+I,\ r+J=0+J \iff r\in I \wedge r\in J \iff r\in I\cap J$$

כלומר, $\ker f=I\cap J$. נוכיח שתי טענות:

1) f על

2) $I\cap J=IJ$

ואז נקבל את המשפט כתוצאה של משפט האיזו' הראשון

הוכחת טענה 1:

לפי הנחת הזרות $1\in R=I+J$. לכן, יש $i\in I,\ j\in J$ כך ש $1=i+j$.

$$f(i)=(i+I,\ i+J)=(0_{R/I},1_{R/J})\qquad (1-i=j\in J \Rightarrow i+J=1+J\in 1_{R/J}$$

יהי $(r_1+I, r_2+J) \in R/I \times R/J$

$$f(r_2 i + r_1 j) = f(r_2)f(i) + f(r_1)f(j) = (r_2+I, r_2+J)(0,1) + (r_1+I, r_1+J)(1,0) =$$
$$= (0, r_2+J) + (r_1+I, 0) = (r_1+I, r_2+J)$$

לכן f על

הוכחת טענה 2:

צריך להוכיח $IJ = I\cap J$, $IJ \subseteq I\cap J$ תמיד נכון.

יהי $r\in I\cap J$. אזי $r = r\cdot 1 = r(i+j) = \underbrace{ri}_{\substack{r\in J \\ ri\in IJ}} + \underbrace{rj}_{\substack{r\in I \\ rj\in IJ}} \in IJ$

לכן $IJ = I\cap J$

תוצאה:

יהי R חוג חילופי, $I_1, \dots, I_n \triangleleft R$ זרים בזוגות. כלומר, $I_i + I_j = R$ לכל $i\neq j$. אזי
$$R/I_1\cdots I_n \simeq R/I_1 \times \dots \times R/I_n$$

הוכחה:

באינדוקציה על n.

$n=2$ הוכחנו. נניח שהמשפט ידוע עבור $n-1$. צריך להוכיח $I_n, I_1 \cdot \dots \cdot I_{n-1}$ זרים. כי אז,
$$R/I_1\cdot\dots\cdot I_n \simeq R/I_1\cdots I_{n-1} \times R/I_n \simeq R/I_1 \times \dots \times R/I_n$$

לפי ההנחה לכל $1\leq k\leq n-1$, האידיאלים I_n, I_k זרים. לכן קיימים $x_k\in I_k$, $y_k\in I_n$

כך ש $x_k+y_k = 1$. לכן,
$$1 = (x_1+y_1)\cdot\dots\cdot(x_{n-1}+y_{n-1}) = \underbrace{\underbrace{x_1\cdot\dots\cdot x_{n-1}}_{\in I_1\cdot\dots\cdot I_{n-1}} + \underbrace{(\text{מחוברים שונים, בכל אחד יש מחובר מ-} I_n)}_{\in I_n}}_{\in I_1\cdot\dots\cdot I_{n-1} + I_n}$$

לכן, $I_1\cdot\dots\cdot I_{n-1} + I_n = R$ ושני האידיאלים אכן זרים

תוצאה:

$n\in\mathbb{Z}$ $n = p_1^{e_1}\cdot\dots\cdot p_r^{e_r}$ פירוק לגורמים ראשוניים. לפי המשפט,
$$\mathbb{Z}_n \simeq \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_r^{e_r}\mathbb{Z}$$

הגדרה: R חוג, איבר $a\in R$ נקרא הפיך אם קיים $b\in R$ כך ש $ab=ba=1$

חבורה לכפל $R^* = \{a\in R : \text{הפיך } a\}$

ברור כי $(R\times S)^* = R^*\times S^*$ בפרט

$$\left(\mathbb{Z}/n\mathbb{Z}\right)^* \simeq \left(\mathbb{Z}/p_1^{e_1}\mathbb{Z}\right)^* \times \dots \times \left(\mathbb{Z}/p_r^{e_r}\mathbb{Z}\right)^*$$

העוצמה של $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$ היא $\varphi(n)$ $\Leftarrow$ $\varphi(n)=\varphi(p_1^{e_1})\cdot\ldots\cdot\varphi(p_r^{e_r})$

טענה:

R חוג, $I\triangleleft R$ אידיאל. אזי, $I=R \iff I$ מכיל איבר הפיך

הוכחה:

$(\Leftarrow)$ $I=R \Leftarrow 1\in I$, 1 הפיך

$(\Rightarrow)$ יהי $u\in R$ הפיך, יהי $uv=vu=1$ אזי $u\in I \Leftarrow 1=uv\in I \Leftarrow$ לכל $r\in R$, $r=r\cdot 1\in I$

$\Downarrow$

$R=I$

תוצאה:

יהי R חוג עם חילוק (כל איבר לא אפסי הוא הפיך). אזי האידיאלים היחידים של R הם $R,(0)$

טענה:

יהי R חוג חילופי. אזי R שדה $\iff$ האידיאלים היחידים שלו הם $R,(0)$

הוכחה:

$(\Leftarrow)$ כבר הוכחנו

$(\Rightarrow)$ נניח שאין אידיאלים מלבד $R,(0)$. יהי $0\neq a\in R$. אזי $Ra=R$.

לכן $1\in Ra \Leftarrow$ קיים $b\in R$ כך ש $ab=ba=1$

תוצאה:

יהי R חוג עם חילוק. אזי, כל הומו' $f:R\to S$ $(S\neq 0)$ של חוגים הוא חח"ע

הוכחה:

$\ker f\triangleleft R$, וגם $1\notin \ker f$ כי $f(1_R)=1_S\neq 0_S$. לכן $\ker f\neq R \Leftarrow \ker f=\{0_R\} \Leftarrow f$ חח"ע

בהגדרה: יהי R חוג. אידיאל אמיתי $M\triangleleft R$ נקרא מקסימלי אם $M\le I\triangleleft R \Leftarrow I=M$ או $I=R$

טענה:

R חוג. יהי $I\triangleleft R$ אידיאל. אזי קיים $M\triangleleft R$ מקסימלי כך ש $I\le M$

הוכחה:

הלמה של צורן, ניקח $I\in S=\{$ כל האידיאלים האמיתיים של R שמכילים את I $\}$

הלמה של צורן:

S קבוצה סדורה חלקית. אם לכל שרשרת $C\subseteq S$ (C שרשרת $\Leftrightarrow$ לכל $a,b\in C$, $a\le b$ או $b\le a$) יש חסם מלעיל (איבר $x\in S$ כך ש $a\le x$ לכל $a\in C$). אזי ל S יש איבר מקסימלי.

בחזרה להוכחה, צריך להוכיח שלכל שרשרת של אידאלים אמיתיים יש חסם מלעיל. תהי C שרשרת.

נגדיר $J=\bigcup_{I\in C} I$. נראה ש $J\in S$:

J סגור לחיבור: יהי $a,b\in J$, $a\in I_1\in C$, $b\in I_2$

בלי הגבלת הכלליות, $I_1\le I_2 \Leftarrow a,b\in I_2 \Leftarrow a+b\in I_2\subseteq J$

יהי $a\in J$, $r\in R$ אזי קיים $I\in C$ כך ש $a\in I$. אזי $ra\in I\subseteq J$

לכן J אידאל. אבל, $1\notin J$, כי J איחוד של אידאלים אמיתיים לכן J אמיתי וקיבלנו את כל התנאים של הלמה של צורן

טענה:

R חוג חילופי, $I\triangleleft R$ אידאל. אזי I מקסימלי $\Leftrightarrow$ R/I הוא שדה

הוכחה:

לפי משפט האיזו הרביעי (מהשיעור הקודם), יש התאמה $\{$אידאלים של $R/I\} \longleftrightarrow \{$אידאלים $I\le J\triangleleft R\}$, $J\longrightarrow J/I$

R/I שדה (R/I חילופי כי R חילופי) $\Leftrightarrow$ $\{(0_{R/I}), R/I\}$ הם כל האידאלים $\Leftrightarrow$ $J=I$ או $J=R$ $\Leftrightarrow$ I מקסימלי

מאינפי 1:

בתורת הקבוצות בונים את $\mathbb{Z}$.

$$\mathbb{Q} = \{(a,b)\in \mathbb{Z}\times\mathbb{Z} \mid b\neq 0\}/\sim$$

$$(a,b)\sim(c,d) \iff ad=bc \qquad \left(\frac{a}{b}=\frac{c}{d}\right)$$

איך מגדירים את $\mathbb{R}$?

סדרה (a_n) של איברים של $\mathbb{Q}$ נקראת סדרת קושי אם לכל $0<\varepsilon\in\mathbb{Q}$ קיים N כך שלכל $N<n,m$ מתקיים $|a_n-a_m|<\varepsilon$

R - החוג של סדרות קושי

$$(a_n)+(b_n)=(a_n+b_n)$$

$$(a_n)(b_n)=(a_nb_n)$$

סדרת קושי נקראת אפיסה אם לכל $0<\varepsilon\in\mathbb{Q}$ קיים N כך שלכל $N\le n$ מתקיים $|a_n|<\varepsilon$

$$I=\{\text{סדרות אפיסות}\}\triangleleft R$$

הגדרה: $\mathbb{R}=R/I$

תרגיל:

1. אידאל מקסימלי $\iff$ R שדה