

در این تحقیق یک حوزه صحیح پیدا کردیم که یک حوزه ایده ال اصلی (PID) است و حوزه اقلیدسی (ED) نمی باشد برای اثبات این موضوع دو قضیه فرعی را مطرح کردیم و از آن طریق حکم کلی را ثابت کردیم. که در ادامه به بررسی و اثبات آن دو قضیه فرعی می پردازیم:

مجموعه $\mathbb{Z}[W]$ ، $w = \frac{1}{2}(1 + i\sqrt{19})$ یک PID است که ED نمی باشد.

اثبات : روش کار این گونه است که:

- نخست ثابت می کنیم $\mathbb{Z}[W]$ یک PID است، برای این کار باید ثابت کنیم که دارای یک $DedeKind - Hosse$ نرم می باشد .
- سپس ثابت می کنیم که مجموعه $\mathbb{Z}[W]$ ، ED نیست. برای این کار ثابت می کنیم که هیچ $Universal side divisor$ ندارد .

به طور کلی اگر D یک حوزه صحیح باشد خواهیم داشت :

۱- هر دامنه اقلیدسی یک $Universal side divisor$ دارد.

$$\overline{D} = \{units, 0\} = unit_D \cup \{0\};$$

$u \in D - \overline{D}$ یک Usd ($Universal side divisor$) است اگر :

$$\forall x \in D \exists z \in \overline{D} \quad s.t. \quad u | x - z$$

۲- یک $DedeKind - Hosse$ نرم داشته باشد $\Leftrightarrow D$ یک PID است .

تابع $N : D \rightarrow \mathbb{N}$ یک $DedeKind - Hosse$ نرم است اگر :

$$\forall a, b \neq 0 \in D \quad b | a \quad OR \quad \exists s, t \in D \quad s.t. \quad 0 < N(sa - tb) < N(b)$$

حال ثابت می کنیم مورد ۱ را :

برای این کار فرض میکنیم D یک حوزه اقلیدسی (ED) با تابع ∂ باشد ثابت می کنیم دارای یک $universal\ side\ divisor$ است .

فرض کنیم $u \in D - \bar{D}$ به طوریکه $\partial(u)$ در میان تمام اعضای برد ∂ مینیمم باشد ، چنین چیزی امکان پذیر است زیرا برد ∂ در مجموعه اعداد حسابی قرار دارد فلذا خوش تعریف است و دارای عضو مینیمم می باشد.

فرض کنیم $x \in D$ دلخواه باشد . چون D یک حوزه اقلیدسی (ED) است ، پس داریم :

$$x = qu + r \quad \text{به طوریکه} \quad r = 0 \quad \text{یا} \quad \partial(r) < \partial(u).$$

اگر $r = 0$ آنگاه $u \mid x$ و از آن جا $u \mid x - 0$ و چون $0 \in \bar{D}$ پس حکم برقرار است .

اگر $r \neq 0$ آنگاه $r = x - uq$ پس دو حالت امکان پذیر است یا $r \in D - \bar{D}$ یا $r \in \bar{D}$ ، اگر $r \in D - \bar{D}$ آنگاه $N(r) < N(u)$ که این خلاف فرض است ، زیرا $N(u)$ مینیمم می باشد .

پس فرض اولیه که $r \in D - \bar{D}$ باطل و غلط است. فلذا $r \in \bar{D}$ و از آنجا $x - r = uq$ پس $u \mid x - r$ که حکم را نتیجه می دهد. در نتیجه حکم کلی برقرار است و u یک $universal\ side\ divisor$ است.

حال مورد ۲ را ثابت می کنیم:

($\Leftarrow$) فرض کنیم حوزه صحیح D یک $D - H$ نرم دارد. به نام N . ثابت میکنیم D یک PID است ؛ فرض کنیم $0 \neq I \leq D$. (I ایدآل D است) همچنین $b \in I$ به طوریکه $N(b)$ مینیمال باشد. چنین چیزی امکان پذیر است زیرا $\text{Im} N$ در اعداد طبیعی قرار دارد پس خوش تعریف می باشد و از آنجا دارای عضو مینیمم است.

اکنون فرض میکنیم $a \in I$ در نتیجه $\langle a, b \rangle \subseteq I$ حال خواهیم داشت:

$$b \mid a \Rightarrow a = br, r \in D \Rightarrow a \in \langle b \rangle \Rightarrow I \subseteq \langle b \rangle, \langle b \rangle \subseteq I \Rightarrow I = \langle b \rangle \Rightarrow D \text{ یک PID است}$$

حال اگر $b \nmid a$ آنگاه $\exists s, t \in D$ به طوریکه $0 < N(sa - tb) < N(b)$ از طرفی $sa - tb \in \langle a, b \rangle$ پس $sa - tb \in I$ اما ما $N(b)$ را عضو مینیمم گرفته بودیم و این موضوع که $N(sa - tb) < N(b)$ یک تناقض است.

پس این مورد امکان پذیر نیست و $b \mid a$ و حکم برقرار است.

($\Rightarrow$) فرض کنیم D یک PID است که نتیجه می دهد یک UFD نیز می باشد. ثابت میکنیم دارای یک $D-H$ نرم می باشد ، خواهیم داشت :

تابع N را تعریف می کنیم:

$$N: D \rightarrow \mathbb{N}, \quad N(0) = 0, \quad N(u) = 1, u \in \text{Unit}_D$$

$$N(a) = 2^n, \quad a = P_1 P_2 \dots P_n, \quad P_i \in D$$

($a \in D$) را میتوان به صورت حاصل ضرب عناصر اول نوشت زیرا D یک PID و از آن جا یک UFD است)

$$N(ab) = N(a).N(b) \quad ; \quad a, b \in D \quad \text{پس واضح است که داریم:}$$

فرض کنیم $0 \neq a, b \in D$ در نتیجه چون D یک PID است پس وجود دارد $r \in D$ به طوریکه $\langle a, b \rangle = \langle r \rangle$

اکنون دو حالت امکان پذیر است . $b|a$ و $b \nmid a$:

اگر $a|b$ آنگاه حکم بر قرار است پس فرض می کنیم $a \nmid b$ ، آنگاه :

$$b \nmid a \Rightarrow a \notin \langle b \rangle, a \in \langle r \rangle \Rightarrow r \notin \langle b \rangle, \langle a, b \rangle = \langle r \rangle \Rightarrow \langle b \rangle \subset \langle r \rangle \Rightarrow b = rx$$

$x \neq 0$ نمیتواند یکال باشد زیرا $\langle b \rangle \neq \langle r \rangle$

اکنون بنا بر تعریف تابع N ، داریم :

$$\begin{aligned} N(b) = N(b)N(x) &\Rightarrow N(b) = N(r)N(x) > N(r) \\ N(x) &= 2^n \end{aligned}$$

پس خواهیم داشت :

$$\left. \begin{aligned} N(b) &= N(r)N(x) > N(r) \\ r \in \langle r \rangle &= \langle a, b \rangle \Rightarrow \exists s, t \in D, r = sa - tb \end{aligned} \right\} \Rightarrow 0 < N(r) = N(sa - tb) < N(r)N(x) = N(b)$$

پس D دارای یک $D-H$ نرم است . در نتیجه حکم ثابت می شود .

اکنون به سراغ اثبات اصلی می رویم، داریم:

$$W = \frac{1}{2}(1+i\sqrt{19}) \text{ و } R = \mathbb{Z}[W]$$

ثابت می کنیم که R یک PID است اما ED نمی باشد.

نخست ثابت می کنیم که PID است. برای این کار باید نشان دهیم که دارای یک $D-H$ نرم است. داریم:

$$N: R \rightarrow \mathbb{N} \text{ و } N(a+bw) = a^2 + ab + 5b^2$$

دو عضو مخالف صفر چون β و α از R , $(\alpha, \beta \in R)$, را انتخاب می کنیم، اگر $\beta | \alpha$ آنگاه

حکم برقرار است و R دارای یک $D-H$ نرم است، پس فرض می کنیم $\beta \nmid \alpha$ یعنی $\frac{\alpha}{\beta} \notin R$.

پس $\frac{\alpha}{\beta} \in Q[i\sqrt{19}]$ داریم:

$$\begin{cases} \frac{\alpha}{\beta} = \frac{a+bw}{c} \\ c \neq 1 \end{cases}$$

$$\gcd(a, b, c) = 1$$

$$\exists x, y, z \in \mathbb{Z} \quad \text{s.t.} \quad ax + by + cz = 1$$

اکنون داریم:

$$\begin{cases} ay - 19bx = cq + r \\ |r| < \frac{c}{2} \end{cases}$$

حال سه عبارت جبری را داریم:

$$\left| \begin{array}{l} \frac{\alpha}{\beta} = \frac{a+bw}{c} \\ ax+by+cz=1 \\ ay-19bx=cq+r, \quad |r| < \frac{c}{2} \end{array} \right|$$

هدف این است که s, t پیدا کنیم تا در شرط $D-H$ نرم صدق کند، پس تعریف می کنیم:

$$t = q - zi\sqrt{19} \in R$$

$$s = y + xi\sqrt{19} \in R$$

در نتیجه داریم:

$$0 < N\left(\frac{\alpha}{\beta}s - t\right) = \frac{(ay-19bx-cq)^2 + 19(ax+by+cx)^2}{c^2} = \frac{r^2 + 19}{c^2} \leq \frac{1}{4} + \frac{19}{c^2}$$

اکنون تمام مقادیر صحیح ممکن برای c را بررسی می کنیم که آیا شرط $D-H$ نرم برقرار است یا خیر .

واضح است که برای $c \geq 5$ برقرار است چرا که با ضرب $N(\beta)$ در طرفین خواهیم داشت :

$$0 < N(xs - t\beta) \leq N(\beta) \left(\frac{1}{4} + \frac{19}{c^2}\right) \leq N(\beta)$$

که نتیجه می دهد R دارای $D-H$ نرم است در نتیجه بنا بر قضیه یک PID است .

(برای مقادیر منفی c همانند مقادیر مثبت آن عمل می کنیم و طبق تعریف c نمی تواند مساوی صفر باشد)

اکنون مقادیر باقی مانده برای c که می تواند ممکن باشد عبارتست از ۱، ۲، ۳ و ۴ . در ابتدا گفتیم که $c \neq 1$.

در ادامه ثابت می کنیم که به ازای مقادیر $c = 1, 2, 3$ ، R دارای یک $D-H$ نرم است .

از طرفی اگر $C=2$ آنگاه مقادیر s, t که در زیر بیان شده است نتیجه می دهد که R یک $D-H$ نرم است و بررسی آن واضح است. (کافی است s, t را در $N(s\alpha - t\beta) \leq N(\beta)$ قرار دهیم)

$$S=1, t = \frac{a-1+bi\sqrt{19}}{2} \in R$$

واضح است $S=1 \in R$ بررسی می کنیم که t هم عضو R باشد.

$$t = \frac{a-b}{2} + \frac{b}{2}i\sqrt{19} + \frac{b}{2} - \frac{b}{2} = \frac{a-b-1}{2} + \frac{b}{2}(1+i\sqrt{19}) = \frac{a-b-1}{2} + b'w$$

از طرفی اگر $c=2$ آنگاه واضح است که a, b نمی توانند هر دو همزمان زوج یا فرد باشد زیرا در اینصورت $\frac{\alpha}{\beta} \in R$ که این مخالف فرض است فلذا $a-b$ عددی فرد می باشد در نتیجه $a-b-1$ عددی زوج و از آن جا

$$t = \frac{a-b-1}{2} + b'w \in R \quad \text{پس} \quad \frac{a-b-1}{2} \in \mathbb{Z}$$

اگر: $c=3$

آنگاه:

$$a^2 + 19b^2 \equiv a^2 + b^2 \pmod{3}$$

از طرفی اگر $a^2 + b^2 \equiv 0 \pmod{3}$ آنگاه $a \equiv 0 \pmod{3}, b \equiv 0 \pmod{3}$

که نتیجه می دهد $\gcd(a, b, c) \geq 3$ که این خلاف فرض است زیرا $\gcd(a, b, c) = 1$

$$b \not\equiv 0 \pmod{3}, a \not\equiv 0 \pmod{3}$$

پس داریم:

همچنین:

$$3 \nmid a^2 + 19b^2 \Rightarrow a^2 + 19b^2 = 3q + r, r = \{1, 2\}$$

در نتیجه s و t که در شرط $D-H$ نرم صدق می کند تا R بنا بر قضیه یک PID شود،
می شود :

$$s = a - bi\sqrt{19}, t = q \in R$$

حال بررسی می کنیم اگر $c=4$. در این صورت a و b هر دو نمی توانند زوج باشند چرا که در این صورت $\gcd(a, b, c) \neq 1$ ، پس حالتی را بررسی می کنیم که یکی فرد و دیگری زوج است:

$$a^2 + 19b^2 \text{ فرد است} \Rightarrow a^2 + 19b^2 = 4q + r, r \in \{1, 2, 3\}$$

در نتیجه s و t که در شرط $D-H$ نرم صدق می کند تا R بنا بر قضیه یک PID شود،
می شود :

$$s = a - bi\sqrt{19}, t = q$$

حالت دوم ، اگر هر دو a و b فرد باشند آنگاه :

$$a^2 + 19b^2 \equiv 1 + 3 \pmod{8} \Rightarrow a^2 + 19b^2 = 8q + 4$$

در این صورت s و t که در شرط $D-H$ نرم صدق می کند تا R بنا بر قضیه یک PID شود،
می شود :

$$s = \frac{1}{2}a - bi\sqrt{19}, t = q$$

پس ثابت کردیم که برای تمامی مقادیر صحیح ممکن برای c, t, s موجود است که در شرط $0 \leq N(s\alpha - t\beta) \leq N(\beta)$ صدق کند تا R یک $D-H$ داشته باشد فلذا یک PID باشد .

حال ثابت می کنیم که ED, R نیست برای این کار ثابت می کنیم که هیچ $Universal \ side \ divisor$ ندارد. داریم :

$$Unit_R = \{+1, -1\} \Rightarrow \bar{R} = \{0, \pm 1\}$$

عضو $u \in R - \bar{R}$ را انتخاب می کنیم و فرض می کنیم که u یک $universal \ side \ divisor$ است.

پس برای هر عضو $x \in R$ باید داشته باشیم $u \mid x - z$ به طوری که وجود داشته باشد $z \in \bar{R}$.

عضو $x=2 \in R$ را در نظر می گیریم. چون u یک $universal\ side\ divisor$ است پس:

$$\begin{cases} u \mid 2-z \\ z \in \{0, \pm 1\} \end{cases} \Rightarrow \begin{cases} u \mid 2-0 \Rightarrow u = \pm 1, u = \pm 2 \\ u \mid 2-1 \Rightarrow u = \pm 1 \\ u \mid 2-(-1) \Rightarrow u = \pm 1, u = \pm 3 \end{cases}$$

از طرفی چون $u \notin \bar{R}$ پس نمی تواند ± 1 باشد فلذا تنها مقدار باقی مانده برای u که ممکن است ± 2 و ± 3 باشد. از طرفی داریم:

$$u = \pm 2, x = \frac{1}{2}(1+i\sqrt{19}) \Rightarrow \begin{cases} \frac{1}{2}(1+i\sqrt{19})-0 = \pm 2q \Rightarrow q = \frac{1}{\pm 2}(\frac{1}{2}(1+i\sqrt{19})) = \frac{1}{\pm 2}w = 0 + \frac{1}{\pm 2}w \notin R \\ \frac{1}{2}(1+i\sqrt{19})-1 = \pm 2q \Rightarrow q = \frac{1}{\pm 2}(\frac{1}{2}(1+i\sqrt{19})) - \frac{1}{\pm 2} = \frac{1}{\pm 2}w - \frac{1}{\pm 2} \notin R \\ \frac{1}{2}(1+i\sqrt{19})-(-1) = \pm 2q \Rightarrow q = \frac{1}{\pm 2}(\frac{1}{2}(1+i\sqrt{19})) + \frac{1}{\pm 2} = \frac{1}{\pm 2}w + \frac{1}{\pm 2} \notin R \end{cases} \Rightarrow \pm 2 \nmid x-z, \forall z \in \{0, \pm 1\}$$

$$u = \pm 3, w = x = \frac{1}{2}(1+i\sqrt{19}) \Rightarrow \begin{cases} \frac{1}{2}(1+i\sqrt{19})-0 = \pm 3q \Rightarrow q = \frac{1}{\pm 3}(\frac{1}{2}(1+i\sqrt{19})) = \frac{1}{\pm 3}w = 0 + \frac{1}{\pm 3}w \notin R \\ \frac{1}{2}(1+i\sqrt{19})-1 = \pm 3q \Rightarrow q = \frac{1}{\pm 3}(\frac{1}{2}(1+i\sqrt{19})) - \frac{1}{\pm 3} = \frac{1}{\pm 3}w - \frac{1}{\pm 3} \notin R \\ \frac{1}{2}(1+i\sqrt{19})-(-1) = \pm 3q \Rightarrow q = \frac{1}{\pm 3}(\frac{1}{2}(1+i\sqrt{19})) + \frac{1}{\pm 3} = \frac{1}{\pm 3}w + \frac{1}{\pm 3} \notin R \end{cases} \Rightarrow \pm 3 \nmid w-z, \forall z \in \{0, \pm 1\}$$

پس فرض خلف باطل است. پس R ، $Universal\ side\ divisor$ ندارد و بنا بر قضیه ED نمی باشد. و در نتیجه R یک PID است که ED نمی باشد.

□