השלמים של גאוס

תזכורות

1. תחום אוקלידי הוא תחום שלמות R שמוגדרת עליו פונקציה

$$d : R\backslash\{0\} \to \mathbb{N}$$

$$d(a) \leq d(a,b)$$

לכל $R\backslash\{0\} \ni a,b$ קיימים $r,q \in \mathbb{R}$ כך ש$a = qb + r$ וגם $d(q) < d(a) \vee r = 0$

2. תחום אוקלידי הוא ראשי.(אוקלידים⊃ראשיים⊃תחומי פריקות יחידה)

טענה

הוכח כי $\mathbb{Z}[i]$[השלמים של גאוס] הוא תחום פריקות יחידה.

הוכחה

בהרצאה הקודמת הוכחנו שהחוגים O_D הם אוקלידיים עבור

$$D = -1, m+2, \pm 3, 5, -7, -11, 13$$

$O_{-1} = \mathbb{Z}[i]$ ולכן אוקלידי ⇐ ראשי ⇐ תפ"ר

משפט(ווילסון)

p ראשוני $\Leftrightarrow (p-1)! \equiv -1 \pmod{p}$

הוכחה

כיוון הפוך הוא פשוט.

נביט במשוואה $x^2 - 1 = 0$ ב$\mathbb{Z}_p$. לפי המשפט היסודי של האלגברה יש למשוואה הזו שני פתרונות, והם $x = 1$ ו$x = -1$. אבל, כל מספר ב$\mathbb{Z}p$ שונה מאפשר הוא הפיך, ואם הוא שונה מ± 1 אז ההפוך שלו שונה ממנו.

במכפלה $1 \cdot 2 \cdot 3 \cdots (p-1)$ ישנם המספרים 1 ו$\overbrace{p-1}^{\equiv -1}$, וזוגות של מספרים הפכיים זה לזה ב$\mathbb{Z}p$, ולכן המכפלה יוצאת -1.

טענה

אם $p \equiv 1 \pmod{4}$ אזי קיים $x \in \mathbb{Z}$ כך ש$x \equiv -1 \pmod{p}$.

הוכחה

נסמן $x = 1 \cdot 2 \cdots \frac{p-1}{2} = \left(\frac{p-1}{2}\right)!$. נשים לב שלכל $1 \leq k \leq \frac{p-1}{2}$

$$-1 \equiv (p-1)! \equiv 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdots (p-3)(p-2)(p-1) = x^2 \cdot (-1)^2 = x^2$$

טענה

לכל ראשוני $\pi \in \mathbb{Z}[i]$, $N(\pi)$ הוא או ראשוני טבעי, או ריבוע של ראשוני טבעי.

הוכחה

נביט ב$N(\pi) \subseteq \mathbb{Z}$. יש לו פירוק כמכפלה של ראשוניים טבעיים $p_1 \cdots p_t$[אפשר חזרות].

$$\pi | \pi \cdot \overline{\pi} = N(\pi) = p_1 \cdots p_t$$

אבל π ראשוני כ$\mathbb{Z}[i]$, ולכן קיים $1 \leq i \leq t$ כך ש$\pi | p_i = p$.

$$N(\pi) | N(p) = p^2$$

$$N(\pi) \in \{\not{1}, p, p^2\}$$

(מחקנו את 1 כי π לא הפיך)

טענה

ראשוני טבעי p <u>שונה מ2</u> הוא ראשוני ב$\mathbb{Z}[i]$ אם ורק אם $p \equiv -1 \pmod 4$

הוכחה

$\Rightarrow$ נניח ש$p \equiv 1 \pmod 4$. אזי לפי טענה קודמת קיים $1 \leq x \leq p-1$ כך ש$x^2 \equiv -1 \pmod p$, ואז

$$p | x^2 + 1 = (x+i)(x-i)$$

אולם $p \nmid x+i$ וגם $p \nmid x-i$

$$p^{-1}(x+i) = \frac{x}{p} + \frac{1}{p} \overset{?}{\in} \mathbb{Z}[i]$$

$\Leftarrow p$ לא ראשוני.
נניח שp לא ראשוני. אזי הוא מתפרק כמכפלה של ראשוניים $p = \pi_1 \cdots \pi_t$ כאשר $t \geq 2$. אבל אז

$$N(p) = N(\pi_1) \cdots N(\pi_2)$$

$$t \not\geq 3 \Rightarrow t = 2$$

$$\left.\begin{array}{c} p = \pi_1 \cdot \pi_2 \\ N(\pi_1) = N(\pi_2) = p \end{array}\right\} \Rightarrow \pi_2 = \overline{\pi_2}$$

$$p = \pi \cdot \overline{\pi}$$

כעת נסמן $\pi = a + bi$, ולכן $p = a^2 + b^2$.
עכשיו, בה"כ a אי־זוגי וb זוגי $\Leftarrow 2|b \Leftarrow 4|b^2$

$$p \equiv a^2 \pmod 4 \Rightarrow p \equiv 1 \pmod 4$$

טענה

לכל p ראשוני טבעי כך ש$p \equiv 1 \pmod 4$ קיים פתרון יחיד למשוואה $p = a^2 + b^2$ כאשר $a, b \in \mathbb{Z}$

הוכחה

יהיו $a, b \in \mathbb{Z}$ כך ש$p = a^2 + b^2$. נסמן $x = a + bi$

$$p = x \cdot \overline{x}$$

ראינו קודם שקיים π ראשוני כך ש$p = \pi \cdot \overline{\pi}$, ובגלל ש$\mathbb{Z}[i]$ הוא תחום פריקות יחידה, $\{\pi \backslash \overline{\pi}\} \in \{x, \overline{x}\}$. אם נסמן $\pi = c + di$ אז

$$a = \mp c, d = \pm b$$

הקריטריון של אויילר

מספר טבעי הוא סכום של שני ריבועים אם ורק אם בפירוק שלו לגורמים ראשוניים(טבעיים) כל גורם ששארית החלוקה שלו ב4 היא 3 מופיע מספר זוגי של פעמים.

הוכחה

אם $n = a^2 + b^2$ אזי $n = (a + bi)(a - bi)$. יהי p גורם ראשוני של n כך ש$p \equiv -1 \pmod 4$. אזי p ראשוני ב$\mathbb{Z}[i]$, וזה אומר ש$p|a + bi$ או $p|a - bi$

$$\frac{a}{2}, \frac{b}{2} \in \mathbb{Z} \Leftrightarrow \frac{a}{2} + \frac{b}{2}i \in \mathbb{Z}[i]$$

החזקה המקסימלית d כך ש$p^d|a+bi$ שווה לחזקה המקסימלית d' כך ש$p^{d'} | \gcd(a, b)$ שווה לחזקה המקסימלית d'' כך ש$p^{d''}|a - bi$.

נפרק את $a+bi$ לגורמים ראשוניים ב$\mathbb{Z}[i]$.

$$a+bi = p^d \cdot \pi_1 \cdots \pi_t$$

$$\pi_1, \ldots \pi_t \neq p$$

$$a-bi = p^d \cdot \pi_1' \cdots \pi_{t'}'$$

$$\pi_1', \ldots \pi_{t'}' \neq p$$

ואז

$$n = p^{2d} \cdot \pi_1 \cdots \pi_t \cdot \pi_1' \cdots \pi_{t'}'$$

ומכיוון ש$\mathbb{Z}[i]$ הוא תחום פריקות יחידה, הגורם p מופיע $2d$ פעמים בn.
נניח ש$n = p_1 \cdot p_2 \cdots p_t \cdot m^2$ כאשר $p_1, \ldots p_t$ הם ראשוניים שונים ששארית החלוקה שלהם ב4 היא 1. עכשיו לכל $1 \leq i \leq t$ קיים π ראשוני ב$\mathbb{Z}[i]$ כך ש$\pi_i \cdot \overline{\pi_i} = p_i$

$$n = m^2 \cdot \pi_1\overline{\pi_1} \cdots \pi_t\overline{\pi_t} = \underbrace{(\pm m \cdot \pi_1 \cdot \pi_2 \cdots \pi_t)}_{y \in \mathbb{Z}[i]} \cdot \underbrace{\overline{(\pm m \cdot \pi_1 \cdot \pi_2 \cdots \pi_t)}}_{\overline{y}}$$

$$y = a+bi$$

$$n = y \cdot \overline{y} = a^2 + b^2$$

טענה

התכונות הבאות שקולות עבור p ראשוני טבעי שונה מ2:

1. $p \equiv 1 \pmod 4$
2. p לא ראשוני ב$\mathbb{Z}[i]$
3. יש איבר $x \in \mathbb{Z}[i]$ עם נורמה $N(x) = p$

הוכחה

(1) $\Leftrightarrow$ (2) ראינו

(2) $\Leftarrow$ (3) אזי $p = x \cdot \overline{x}$ $\Leftarrow$ p פריק $\Leftarrow$ לא ראשוני

(3) $\Leftarrow$ (2) ראינו ש$p = \pi \cdot \overline{\pi}$ ולכן $\pi = x$

משפט

הראשוניים של $\mathbb{Z}[i]$ הם(עד כדי חברות):

1. $1+i$
2. הראשוניים הטבעיים ששארית החלוקה שלהם ב4 היא 3
3. המספרים $a \pm bi$ כאשר a^2+b^2 ראשוני טבעי ששארית החלוקה שלו ב4 היא 1.

הוכחה

ראינו כבר שכל אלה ראשוניים. נסביר רק מדוע אין עוד פרט לאלה.

יהי $\pi \ni \mathbb{Z}[i]$ ראשוני. הנורמה שלו היא p או p^2, כאשר p ראשוני טבעי. אם $N(\pi)=p$ שונה מ2 אזי $p=\pi\cdot\overline{\pi}$ ולכן p לא ראשוני $\Leftarrow p\equiv 1 \pmod 4 \Leftarrow \pi$ הוא מקטגוריה 3.

אם $N(\pi)=p^2$ אזי $p\cdot p=p^2=\pi\cdot\overline{\pi}$ ומכיוון ש$\mathbb{Z}[i]$הוא תחום פריקות יחידה זה אומר ש$p\Leftarrow\pi=p$ ראושני ב$\mathbb{Z}[i]\Leftarrow(p\equiv -1 \pmod n)$ הוא מקטגוריה 2.

עבור $p=2$ לא קיים π ראשוני ב$\mathbb{Z}[i]$ מנורמה 4, בגלל ש$\mathbb{Z}[i]$ תחום פריקות יחידה[$=4=(1+i)^2(1-i)^2$]

נשאר למצוא את האיברים מנורמה 2, והם $1+i, 1-i, -1+i, -1-i$ - והם כולם חברים של $1+i$.

8.3 משוואת קו גאודזי על משטח

$$\mathbb{R}^2 \xrightarrow{x} \mathbb{R}^3$$

$$x\circ\alpha=\beta$$

$$\beta(t)=x(\alpha(t))$$

$$\alpha(t)=\left(\alpha^1(t),\alpha^2(t)\right)$$

משפט

כל עקומה רגולרית β על M מקיימת זהות

$$\beta''=\left(\alpha^{i'}\alpha^{j'}\Gamma_{ij}^{k}+\alpha^{k''}\right)x_k+\left(L_{ij}\alpha^{i'}\alpha^{j'}\right)n$$

$$\beta''=\frac{\mathrm{d}^2\beta}{\mathrm{d}t^2} \qquad \alpha^{i'}=\frac{\mathrm{d}\alpha^i}{\mathrm{d}t}$$

הוכחה

לפי הגדרה, $\beta = x \circ \alpha$.

$$\frac{\mathrm{d}\beta}{\mathrm{d}t} = \frac{\partial \underline{x}}{\partial u^i} \cdot \frac{\mathrm{d}\alpha^i}{\mathrm{d}t}$$

לפי נוסחת Leibniz

$$\frac{\mathrm{d}^2\beta}{\mathrm{d}t^2} = \frac{\mathrm{d}}{\mathrm{d}t}\left(\frac{\partial x}{\partial u^i} \cdot \frac{\mathrm{d}\alpha^i}{\mathrm{d}t}\right)$$

$$\frac{\mathrm{d}}{\mathrm{d}t}\left(\frac{\partial x \circ \alpha\,(t)}{\partial u^i}\right)\frac{\mathrm{d}\alpha^i}{\mathrm{d}t} + \frac{\partial x}{\partial u^1}\frac{\mathrm{d}^2\alpha^i}{\mathrm{d}t^2}$$

$$\frac{\partial^2 x}{\partial u^i \partial u^j}\frac{\mathrm{d}\alpha^j}{\mathrm{d}t}\frac{\mathrm{d}\alpha^i}{\mathrm{d}t} + \frac{\partial x}{\partial u^i}\frac{\mathrm{d}^2\alpha^i}{\mathrm{d}t^2}$$

$$\beta'' = x_{ij} d^{i'} \alpha^{j'} + x_i \alpha^{i''} = x_{ij} \alpha^{i'} \alpha^{j'} + x_k \alpha^{k''}$$

$$\left(x_{ij} = \Gamma^k_{ij} x_k + L_{ij} n\right)$$

$$\beta'' = \Gamma^k_{ij} x_k \alpha^{i'} \alpha^{j'} + L_{ij} n \alpha^{i'} \alpha^{j'}$$

$$\boxed{\beta'' = \left(\Gamma^k_{ij} \alpha^{i'} \alpha^{j'} + \alpha^{k''}\right) x_k + L_{ij} \alpha^{i'} \alpha^{j'} n}$$

הגדרה

עקומה $\beta = \underline{x} \circ \alpha$ נקראת קו גאודזי אם מתקיים אחד מן התנאים השקולים הבאים:

1. לכל $k = 1, 2$ מתקיים $\alpha^{k''} + \Gamma^k_{ij} \alpha^{i'} \alpha^{j'} = 0$
2. ווקטור β'' מאונך למשטח ומקיים $\beta'' = L_{ij} \alpha^{i'} \alpha^{j'}$

דוגמה

במישור $\forall_{i,j,k} \Gamma^k_{ij} \equiv 0$:

$$\begin{array}{ll} \forall_k & \alpha^{k''} = 0 \\ \forall_k & \alpha^{k'}\,(t) = a^k \\ \forall\,(t) & \alpha^k\,(t) = a^k t + b^k \end{array}$$

$$\begin{cases} \alpha^1\,(t) = a^1 + b^1 \\ \alpha^2\,(t) = a^2 t + b^2 \end{cases}$$

הוכחה של שקילות

אם מתקיימת (1) אזי לפי המשפט הקודם

$$\beta'' = L_{ij}\alpha^{i'}\alpha^{j'}n$$

למה: עקומה $\beta(t)$ המקיימת $\alpha^{k''} + \Gamma_{ij}^{k}\alpha^{i'}\alpha^{j'} = 0$ היא בהכרח פרמטריזציה במהירות קבועה.

הוכחה: צריך להוכיח שמתקיים $\frac{\mathrm{d}}{\mathrm{d}t}\|\beta'\| = 0$. באופן שקול, $\boxed{\frac{\mathrm{d}}{\mathrm{d}t}\|\beta'\|^2 = 0}$:

$$\frac{\mathrm{d}}{\mathrm{d}t}\left(\|\beta'\|^2\right) = \frac{\mathrm{d}}{\mathrm{d}t}\langle\beta'(t),\beta'(t)\rangle \overset{\text{Leibniz}}{=} \langle\beta''(t),\beta'(t)\rangle + \langle\beta'(t),\beta''(t)\rangle =$$

$$= 2\langle\beta''(t),\beta'(t)\rangle = 2\left\langle\left(\Gamma_{ij}^{k}\alpha^{i'}\alpha^{j'} + \alpha^{k''}\right)x_k + L_{ij}\alpha^{i'}\alpha^{j'}n, x_k\alpha^{k'}\right\rangle =$$

$$= 2\left\langle L_{ij}\alpha^{i'}\alpha^{j'}n, x_k\alpha^{k'}\right\rangle = 2L_{ij}\alpha^{i'}\alpha^{j'}\alpha^{k'}\underbrace{\langle n, x_k\rangle}_{=0}$$

לכן $\frac{\mathrm{d}}{\mathrm{d}t}\left(\|\beta'\|^2\right) = 0$.

8.4 קו גאודזי על משטח סיבוב

$$f(\varphi) > 0 \qquad (f(\varphi), g(\varphi))$$

הסיבוב של f סביב ציר הz הוא:

$$x(\theta,\varphi) = (f(\varphi)\cos\theta, f(\varphi)\sin\theta, g(\varphi))$$

$$\boxed{\Gamma_{12}' = \frac{\frac{\mathrm{d}f}{\mathrm{d}\varphi}}{f} \qquad \Gamma_{11}' = \Gamma_{22}' = 0}$$

$$\alpha^{k''} + \Gamma_{ij}^{k}\alpha^{i'}\alpha^{j'} = 0$$

$$k = 0$$

$$\alpha^{1''} + \Gamma_{ij}^{1}\alpha^{i'}\alpha^{j'} = 0$$

$$\alpha^{1''} + 2\Gamma^1_{12}\alpha^{1'}\alpha^{2'} = 0$$

$$\alpha^1 = \theta \qquad \alpha^2 = \varphi$$

$$\boxed{\theta'' + 2\Gamma'_{12}\theta'\varphi' = 0}$$

$$\frac{\mathrm{d}^2\theta}{\mathrm{d}t^2} + 2\Gamma'_{12}\frac{\mathrm{d}\theta}{\mathrm{d}t}\frac{\mathrm{d}\varphi}{\mathrm{d}t} = 0$$

$$\frac{\mathrm{d}^2\theta}{\mathrm{d}t^2} + 2\frac{\dfrac{\mathrm{d}f}{\mathrm{d}\varphi}}{f}\frac{\mathrm{d}\theta}{\mathrm{d}t}\frac{\mathrm{d}\varphi}{\mathrm{d}t} = 0$$

$$\frac{\mathrm{d}^2\theta}{\mathrm{d}t^2} + \frac{2}{f}\boxed{\frac{\mathrm{d}f}{\mathrm{d}\varphi}\frac{\mathrm{d}\varphi}{\mathrm{d}t}}\frac{\mathrm{d}\theta}{\mathrm{d}t} = 0$$

$$\frac{\mathrm{d}^2\theta}{\mathrm{d}t^2} + \frac{2}{f}\frac{\mathrm{d}f}{\mathrm{d}t}\frac{\mathrm{d}\theta}{\mathrm{d}t} = 0$$

$$f\frac{\mathrm{d}^2\theta}{\mathrm{d}t^2} + 2\frac{\mathrm{d}f}{\mathrm{d}t}\frac{\mathrm{d}\theta}{\mathrm{d}t} = 0$$

$$f^2\frac{\mathrm{d}^2\theta}{\mathrm{d}t^2} + 2f\frac{\mathrm{d}f}{\mathrm{d}t}\frac{\mathrm{d}\theta}{\mathrm{d}t} = 0$$

$$\left(f^2\frac{\mathrm{d}\theta}{\mathrm{d}t}\right)' = 0$$

$$\boxed{f^2\frac{\mathrm{d}\theta}{\mathrm{d}t} = \mathrm{Const}}$$

קיבלנו ש $\boxed{f^2\left(\varphi\left(t\right)\right)\dfrac{\mathrm{d}\theta}{\mathrm{d}t} = \mathrm{const}}$ לאורך קו גאודזי $\beta\left(t\right)$.

למה

זוית γ בין עקומה β לבין קו רוחב מקיימת

$$\cos\gamma = r\theta'$$

כאשר r הוא מרחק לציר z.

הוכחה

$$\cos\gamma = \left\langle \frac{\beta'}{\|\beta'\|}, \frac{x_1}{\|x_1\|} \right\rangle$$

נניח $\|\beta'\| = 1$ במהירות יחידה:

$$\cos\gamma = \left\langle \beta', \frac{x_1}{\|x_1\|} \right\rangle = \frac{1}{\|x_1\|}\langle \beta', x_1\rangle = \frac{1}{(g_{11})^{1/2}}\langle \beta', x_1\rangle = \frac{1}{r}\langle \beta', x_1\rangle =$$

$$= \frac{1}{r}\langle \beta', x_1\rangle = \frac{1}{r}\left\langle x_i\alpha^{i'}, x_1\right\rangle = \frac{1}{r}\left\langle x_1\alpha^{1'}, x_1\right\rangle = \frac{\alpha^{1'}}{r}g_{11} = \frac{\alpha^{1'}}{r}\cdot r^2 = r\alpha^{1'} = r\theta'$$

$$\boxed{(g_{ij}) = \begin{pmatrix} f^2 & 0 \\ 0 & \end{pmatrix} 1} \qquad f = r$$

$$f^2\frac{\mathrm{d}\theta}{\mathrm{d}t} = \mathrm{Const}$$

$$r^2\frac{\mathrm{d}\theta}{\mathrm{d}t} = \mathrm{Const}$$

אבל $r\theta' = \cos\gamma$

$$r\left(r\theta'\right) = \mathrm{Const}$$

$$\boxed{r\cos\gamma = \mathrm{Const}}$$

זה נקרא "יחס של Clairaut".

לאורך קו גאוזדי $\beta(t)$ מתקיים $f^2\left(\varphi(t)\right)\dfrac{\mathrm{d}\theta}{\mathrm{d}t} = \mathrm{Const}$

8.5 קואורדינטות פולריות וספיריות

השטח של D הוא אינטגרל כפול:

$$\mathrm{area}\,(D) = \iint_D 1\,\mathrm{d}x\,\mathrm{d}y = \iint_D r\,\mathrm{d}r\,\mathrm{d}\theta$$

הסיבה לכך שבקואורדינטות פולריות יש r בתוך המעגל היא ששטח הוא אינטגרל של אורך, וככל שמרחקים מהראשית, אורך המעגל גדל.

קואורדינטות ספריות

$$\theta, \varphi, \rho$$

$$0 \leq \theta \leq 2\pi$$

$$\varphi = \arccos \frac{z}{p} \qquad 0 \leq \varphi \leq \pi$$

$$\rho > 0$$

$$\mathrm{Vol}\,(D) = \iiint_D 1 \,\mathrm{d}x\,\mathrm{d}y\,\mathrm{d}z = \iiint_D \rho^2 \sin\varphi \,\mathrm{d}\rho\,\mathrm{d}\theta\,\mathrm{d}\varphi$$

הפעם יש $\rho^2 \sin\varphi$ בתוך האינטגרל, שכן זה שטח הפנים גדל ככל שמתרחקים מהראשית.

הגדרה

שטח של משטח M עם פרמטריזציה $x\left(u^1, u^2\right)$ כאשר $\underline{x} : U \to \mathbb{R}^3$(עם $U \subseteq \mathbb{R}^2$) הוא מתקבל ע"י אינטגרציה ביחס לאלמנט שטח:

$$\sqrt{\det\left(g_{ij}\right)}\,\mathrm{d}u^1\,\mathrm{d}u^2 = \sqrt{g_{11}g_{22} - g_{12}^2}\,\mathrm{d}u^1 du^2$$

דוגמה

על S^2: $\underline{x}\left(\theta, \varphi\right)$

$$\left(g_{ij}\right) = \begin{bmatrix} \sin^2\varphi & 0 \\ 0 & 1 \end{bmatrix}$$

לכן

$$\det\left(g_{ij}\right) = \sin^2\varphi$$

$$\sqrt{\det\left(g_{ij}\right)} = \sin u^2 \geq 0$$

לכן

$$\mathrm{area}\,(D) = \iint_D \sin u^2 \,\mathrm{d}u^1\,\mathrm{d}u^2$$