אלגוריתם אוקלידס בחוג השלמים

מחלק משותף מקסימאלי

יהיו $a,b \in \mathbb{Z}$. אם $0 < d \in \mathbb{Z}$ מקיים $\frac{d}{a},\frac{d}{b}$, ולכל $c \in \mathbb{Z}$ כך ש $\frac{c}{a},\frac{c}{b}$ מתקיים $\frac{c}{d}$, אז d נקרא מחלק משותף מקסימאלי של a,b. מסמנים $d = \gcd(a,b)$.

מחלק משותף מינימאלי

יהיו $a,b \in \mathbb{Z}$. אם $0 < l \in \mathbb{Z}$ מקיים $\frac{b}{a},\frac{a}{l}$, ולכל $c \in \mathbb{Z}$ כך ש $\frac{a}{c},\frac{b}{c}$ מ תקיים $\frac{l}{c}$ אז l נקרא כפולה משותפת מינימאלית של a,b. נזסמנים $l = lcm(a,b)$.

אלגוריתם למציאת מחלק משותף מקסימאלי

לכל $a,b \in \mathbb{Z}$ קיימים $r,q \in \mathbb{Z}$ כך ש: $|r| < |b|$ $a = b * q + r$.

דוגמא

נמצא את המחלק המשותף של 210 ו-135. כלומר, יש למצוא $\gcd(210,135)$.

$$210 = 135 * 1 + 75$$
$$135 = 75 * 1 + 60$$
$$75 = 60 * 1 + 15$$
$$60 = 15 * 4 + 0$$
$$\Rightarrow \gcd(210,135) = 15$$

ראינו ש-15 הוא מחלק משותף, ועכשיו נראה שהוא מקסימאלי.

משפט

אם d הוא מחלק משותף של a,b אז $d = \gcd(a,b)$ אם ורק אם קיימים $k,l \in \mathbb{Z}$ כך ש $d = ka + lb$.

הוכחת המשפט על הדוגמא

כיוון $\Leftarrow$:

$$15 = 75 - 60 = 75 - (137 - 75) = 2 * 75 - 135 = 2(210 - 135) - 135 = 2 * 210 - 3 * 135$$

כיוון $\Rightarrow$: נניח $\frac{c}{a}, b$. ושמתקיים $a = cr, b = cs$. אז $d = ka + lb = kcr + lcs = c(kr + ls) \Rightarrow \frac{c}{d}$.

טענה

אם $a = bq + r$ אז $\gcd(a,b) = \gcd(b,r)$.

אם $r = 0$ מקבלים $b = \gcd(a,b) = \gcd(b,0) = b$.

דוגמא

תרגול 01

אלגברה ליניארית 2

אלגוריתם אוקלידס, חלוקה עם שארית, חוגים

גיא רוזנדורן, 14/05/2008 16:09

אלגוריתם למציאת מחלק משותף מינימאלי

נשתמש בנוסחה $\text{lcm}(a,b) = \frac{a}{\gcd(a,b)} * b$.

אלגוריתם אוקלידס עבור חוג הפולינומים

עבור $f,g \in F[x]$ נגדיר $\text{lcm}(\quad), \gcd(\quad)$ באותה צורה כמו לשלמים כאשר מחליפים את $\mathbb{Z}$ ב $F[x]$ ואת "$0 <$" ב-"מתוקן" (מקדם עליון 1).

חלוקה עם שארית

לכל $f,g \in F[x]$ יש $q,r \in F[x]$ כך ש $f = g * q + r$ ו $\deg(r) < \deg(g)$.

דוגמא

$$f = x^3 + 6x^2 + 11x + 6$$
$$g = x^2 + 5x + 4$$

נעשה כמו בחילוק ארוך:

$$\begin{array}{l}
\qquad\qquad\qquad x + 1 = 9 \\
\hline
x^3 + 6x^2 + 11x + 6 \\
x^3 + 5x^2 + 4x \\
\qquad x^2 + 7x + 6 \\
\qquad x^2 + 5x + 4 \\
\qquad\qquad 2x + 2 = r
\end{array}$$

$$\begin{array}{l}
\hline
x^2 + 5x + 4 \\
x^2 + x \\
\qquad 4x + 4 \\
\qquad 4x + 4 \\
\qquad\qquad 0 = r
\end{array}$$

$$f = (x+1)g + (2x+2)$$
$$g = \left(\frac{1}{2}x + 2\right)(2x+2) = (x+4)(x+1) \Rightarrow \gcd(\quad) = x + 1$$
$$2(x+1) = f - (x-1)g$$
$$x + 1 = \frac{1}{2}f - \frac{x+1}{2} * g$$
$$\text{lcm}(f,g) = \text{lcm}(g,f) = \frac{g}{x+1} * f = (x+4)(x^3 + 6x^2 + 11x + 6)$$

חוגים

תרגיל

הראו כי לכל חוג $\mathbb{R}$ מתקיים $0 * a = a * 0 = 0$ לכל $a \in \mathbb{R}$.
לפי אקסיומת האפס $0 * a = (0+0)a$ ולפי אקסיומת הפילוג $(0+0)a = 0 * a + 0 * a$.
נסמן $x = 0 * a$ וקיבלנו $x = x + x$. נוסיף לשני הצדדים $(-x)$ ונקבל $x - x = x + (x - x)$, ולפי אקסיומת הפילוג קיבלנו $0 = x = 0 * a$.

הגדרות

חוג שבו $ab = ba$ נקרא חוג חילופי.
חוג שבו $ab = 0$ גורר $a = 0$ או $b = 0$ נקרא תחום שלמות.
חוג חילופי עם יחידה 1 שבו כל איבר שונה מאפס הפיך נקרא שדה.

דוגמאות

$\mathbb{Z}$ הוא תחום שלמות.
$\mathbb{Q}$ הוא שדה.
$M_2(\mathbb{R})$ זה לא תחום שלמות.
$\mathbb{Z}[i] = \{x + iy \in \mathbb{C} | x, y \in \mathbb{Z}\} \subseteq \mathbb{C}$ הוא חוג ולא שדה. נראה למה:
קיים איבר שונה מאפס ב $\mathbb{Z}[i]$ שההופכי שלו לא נמצא ב $\mathbb{Z}[i]$. ניקח את $(1+i)$:

$$\frac{1}{1+i} = \frac{1}{1+i} * \frac{1-i}{1-i} = \frac{1-i}{2} = \frac{1}{2} - \frac{1}{2}i \notin \mathbb{Z}[i]$$

$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \in \mathbb{C} | a, b \in \mathbb{Q}\} \subseteq \mathbb{C}$ חוג וגם שדה. נראה למה:

$$\frac{1}{a+b\sqrt{2}} = \frac{1}{a+b\sqrt{2}} * \frac{a-b\sqrt{2}}{a-b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} + \frac{-b}{a^2-2b^2} * \sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

הומומורפיזמים של חוגים

העתקה ϕ היא העתקה על חוגים המוגדרת ע"י $\phi: R \to S$ ששומרת על חיבור וכפל:

$$\phi(a+b) = \phi(a) + \phi(b)$$
$$\phi(ab) = \phi(a)\phi(b)$$

העתקה ϕ היא איזומורפיזם אם היא חד-חד-ערכית ועל אם ורק קיים איבר הופכי.
אוטומורפיזם של R זו העתקה איזומורפיזם $\phi: R \to R$.

תרגיל

יש להוכיח כי האוטומורפיזם ל $\mathbb{Z}$ הוא העתקת הזהות.

$$\phi: \mathbb{Z} \to \mathbb{Z} \Rightarrow \phi(0) = 0 \Rightarrow \phi(1) = \phi(1 * 1) = \phi(1)\phi(1) \Rightarrow \phi(1) = 1$$
$$\phi(2) = \phi(1+1) = \phi(1) + \phi(1) = 1 + 1 = 2$$
$$\vdots$$
$$\phi(n) = n$$

תרגול 01

אלגברה ליניארית 2

אלגוריתם אוקלידס, חלוקה עם שארית, חוגים

גיא רוזנדורן, 14/05/2008 16:09

תרגיל נוסף

נתונה העתקה $\phi:\mathbb{Z}[i]\to\mathbb{Z}[i]$.

טענה: ϕ והעתקת הזהות (I_d) הם האוטומורפיזם היחידים של $\mathbb{Z}[i]$.

הוכחה:

$$\phi(0)=0,\phi(1)=1$$
$$\forall n\in\mathbb{Z}\Rightarrow\phi(n)=n$$
$$\phi(i)^2=\phi(i^2)=\phi(-1)=-1\Rightarrow\phi(i)=\pm i$$

אם $\phi(i)=i$ אז:

$$\phi(a+bi)=\phi(a)+\phi(b)\phi(i)=a+bi\Rightarrow\phi=I_d$$

אם $\phi(i)=-i$ אז:

$$\phi(a+bi)=\cdots=a-bi$$

תרגיל

יש להוכיח:

$$\mathbb{Z}[i]\cong\left\{\begin{pmatrix}a&b\\-b&a\end{pmatrix}\middle|a,b\in\mathbb{Z}\right\}$$

נגדיר:

$$\phi(a+bi)=\begin{pmatrix}a&b\\-b&a\end{pmatrix}$$

רואים ישר שההעתקה היא חח"ע ועל.

נבדוק שהיא שומרת כפל וחיבור:

$$\phi(a+bi+c+di)=\phi(a+c+(b+d)i)=\begin{pmatrix}a+c&b+d\\-(b+d)&a+c\end{pmatrix}=\begin{pmatrix}a&b\\-b&a\end{pmatrix}+\begin{pmatrix}c&d\\-d&c\end{pmatrix}$$
$$=\phi(a+bi)+\phi(c+di)$$
$$\phi(a+bi)\phi(c+di)=\begin{pmatrix}a&b\\-b&a\end{pmatrix}\begin{pmatrix}c&d\\-d&c\end{pmatrix}=\begin{pmatrix}ac-bd&ad+bc\\-bc-ad&-bd+ac\end{pmatrix}=\phi(ab-bd+(ad+bc)i)$$
$$=\phi\big((a+bi)(c+di)\big)$$

תרגיל

יהי $\phi:F\to R$ הומומורפיזם של חוגים, ו F שדה.

יש להוכיח כי $\phi=0$ או ϕ שיכון (חח"ע).

$$\ker(\phi):=\{x\in F|\phi(x)=0\}$$

נראה ש $\ker(\phi)=0$ אם ורק אם ϕ שיכון, וש $\ker(\phi)=F$ אם ורק אם $\phi=0$.

אז $\phi(x*x^{-1})=\phi(x)\phi(x^{-1})=0=\phi(1)$ כאשר $\ker(\phi)\neq 0$.

$$\phi(a)=\phi(a1)=\phi(a)\phi(1)=0$$

תרגול 01

אלגברה ליניארית 2

אלגוריתם אוקלידס, חלוקה עם שארית, חוגים

גיא רוזנדורן, 14/05/2008 16:09

תוכן עניינים

אלגוריתם אוקלידס בחוג השלמים 1
מחלק משותף מקסימאלי 1
מחלק משותף מינימאלי 1
אלגוריתם למציאת מחלק משותף מקסימאלי 1
משפט 1
אלגוריתם למציאת מחלק משותף מינימאלי 2
אלגוריתם אוקלידס עבור חוג הפולינומים 2
חלוקה עם שארית 2
חוגים 3
הגדרות 3
הומומורפיזמים של חוגים 3