Квадратичен закон за реципрочност. Цели елементи.

3. Сума на Гаус. Квадратичен закон за реципрочност.

Нека $p > 0$ е просто число и $a \in \mathbb{Z}$ е цяло число. Полезно е да се дефинира

$$\left(\frac{a}{p}\right) = 0,$$

когато p дели цялото число a.
От сега нататък ще предполагаме, че $p > 0$ е нечетно просто число. Нека $\omega \in \mathbb{C}$ е примитивен p-ти корен на 1, например $\omega = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$.

Дефиниция 3.1. Функцията $g : \mathbb{Z}_p \to \mathbb{Z}[\omega]$, определена с формулата

$$g_a = \sum_{t\in\mathbb{Z}_p} \left(\frac{t}{p}\right)\omega^{at} \tag{3.1}$$

се нарича *квадратична сума на Гаус*.

Допускайки известна неточност, ще означаваме g_1 с g. Нека $p^* = (-1)^{\frac{p-1}{2}}p$. Ще покажем, че $g^2 = p^*$. Оттук следва, че $\sqrt{p^*} \in \mathbb{Z}[\omega]$. Нека $p \neq q > 0$ е друго нечетно просто число. Ще използуваме критерия на Ойлер

$$\left(\frac{p^*}{q}\right) \equiv (\sqrt{p^*})^{q-1} \mod q,$$

и аритметиката на $\mathbb{Z}[\omega]$, за да докажем квадратичния закон за реципрочност:

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right).$$

Да припомним, че символът на Льожандър е мултипликативна функция.

Лема 3.1. *Нека $a, b \in \mathbb{Z}_p$. Тогава*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Доказателство. Твърдението е очевидно, когато $a = 0$ или $b = 0$. От сега нататък ще предполагаме, че $a, b \in \mathbb{Z}_p^*$. Нека $\tau : \mathbb{Z}_p^* \to \mathbb{Z}_p^*$, е хомоморфизмът, зададен с формулата $\tau(x) = x^2$, $x \in \mathbb{Z}_p^*$. Тогава $\operatorname{im}\tau$ се състои от всички различни от нула квадратични остатъци. Тъй като $\ker\tau = \{1, -1\}$, то $|\operatorname{im}\tau| = \frac{p-1}{2}$. Следователно $|\mathbb{Z}_p^* : \operatorname{im}\tau| = 2$ и факторгрупата $\mathbb{Z}_p^*/\operatorname{im}\tau$ е изоморфна на цикличната група $C_2 = \{1, -1\}$. Нека $\sigma : \mathbb{Z}_p^* \to C_2$ е композицията $\mathbb{Z}_p^* \to \mathbb{Z}_p^*/\operatorname{im}\tau \cong C_2$. Сега би трябвало да е ясно, че

$$\left(\frac{a}{p}\right) = \sigma(a), \quad a \in \mathbb{Z}_p^*.$$

Тъй като σ е хомоморфизъм на групи, Лема 3.1 е доказана. □

Лема 3.2. $g_0 = 0$.

Доказателство. Това следва от факта, че броят на различните от нула квадратични остатъци е равен на броя на различните от нула квадратични неостатъци. □

Твърдение 3.3. $g_a = \left(\frac{a}{p}\right) g$.

Доказателство. Ако $a = 0$, твърдението съвпада с Лема 3.2. Ако $a \neq 0$, то изображението $\mathbb{Z}_p \to \mathbb{Z}_p$, определено с $t \mapsto at$, е биекция на $\mathbb{Z}_p$. Затова

$$\left(\frac{a}{p}\right) g_a = \sum_{t\in\mathbb{Z}_p} \left(\frac{a}{p}\right)\left(\frac{t}{p}\right)\omega^{at} = \sum_{t\in\mathbb{Z}_p} \left(\frac{at}{p}\right)\omega^{at} = \sum_{t\in\mathbb{Z}_p} \left(\frac{t}{p}\right)\omega^{t} = g_1 = g. \qquad \square$$

От Твърдение 3.3 следва, че

$$g_a g_{-a} = \left(\frac{a}{p}\right)\left(\frac{-a}{p}\right) g^2 = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right)^2 g^2 = \left(\frac{-1}{p}\right) g^2, \text{ когато } a \neq 0.$$

Следователно

$$\sum_{a\in\mathbb{Z}_p} g_a g_{-a} = \left(\frac{-1}{p}\right)(p-1)g^2 \tag{3.2}$$

Твърдение 3.4. $g^2 = p^*$.

Доказателство. Ще покажем, че лявата страна на (3.2) е равна на $p(p-1)$. От определението на g_a следва, че

$$\begin{aligned} g_a g_{-a} &= \sum_{x\in\mathbb{Z}_p} \left(\frac{x}{p}\right)\omega^{ax} \sum_{y\in\mathbb{Z}_p} \left(\frac{y}{p}\right)\omega^{-ay} \\ &= \sum_{x,y\in\mathbb{Z}_p} \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)\omega^{a(x-y)}. \end{aligned}$$

Сумирайки по a, получаваме

$$\sum_{a\in\mathbb{Z}_p} g_a g_{-a} = \sum_{a\in\mathbb{Z}_p}\sum_{x,y\in\mathbb{Z}_p} \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)\omega^{a(x-y)} = \sum_{x,y\in\mathbb{Z}_p} \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)\sum_{a\in\mathbb{Z}_p}\omega^{a(x-y)}.$$

Сега от тъждествата

$$\sum_{a\in\mathbb{Z}_p} \omega^{a(x-y)} = \begin{cases} p, & x = y, \\ 0, & x \neq y, \end{cases}$$

следва, че

$$\sum_{a\in\mathbb{Z}_p} g_a g_{-a} = \sum_{t\in\mathbb{Z}_p} \left(\frac{t}{p}\right)\left(\frac{t}{p}\right) p = p(p-1). \tag{3.3}$$

Накрая, сравнявайки (3.2) и (3.3) виждаме, че

$$g^2 = \left(\frac{-1}{p}\right) p = (-1)^{\frac{p-1}{2}} p = p^*. \qquad \square$$

Теорема 3.5 (квадратичен закон за реципрочност). *Ако $p > 0$ и $q > 0$ са нечетни прости числа, то*

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right).$$

Доказателство. Да означим с R пръстена $\mathbb{Z}[\omega]$. Според критерия на Ойлер

$$\left(\frac{p^*}{q}\right) \equiv (p^*)^{\frac{q-1}{2}} = g^{q-1} \mod q. \tag{3.4}$$

Умножавайки (3.4) с g, получаваме

$$g\left(\frac{p^*}{q}\right) \equiv g^q \mod qR. \tag{3.5}$$

От добре известното сравнение $(a+b)^q \equiv a^q + b^q \mod qR$, $a, b \in R$, следва, че

$$g^q = \left(\sum_{t\in\mathbb{Z}_p} \left(\frac{t}{p}\right)\omega^t\right)^q \equiv \sum_{t\in\mathbb{Z}_p} \left(\frac{t}{p}\right)^q \omega^{qt} = \sum_{t\in\mathbb{Z}_p} \left(\frac{t}{p}\right)\omega^{qt} = g_q = \left(\frac{q}{p}\right) g \mod qR. \tag{3.6}$$

Сега сравнения (3.5) и (3.6) показват, че

$$g\left(\frac{p^*}{q}\right) \equiv \left(\frac{q}{p}\right) g \mod qR. \tag{3.7}$$

За да се върнем в пръстена на целите числа, умножаваме (3.7) по g:

$$p^*\left(\frac{p^*}{q}\right) \equiv p^*\left(\frac{q}{p}\right) \mod qR,$$

откъдето според Лемма 1.8 следва, че

$$p^*\left(\frac{p^*}{q}\right) \equiv p^*\left(\frac{q}{p}\right) \mod q. \tag{3.8}$$

Тъй като q е нечетно просто число, от (3.8) получаваме

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right). \qquad \square$$

4. Цели елементи

Ще разглеждаме само комутативни пръстени с единичен елемент. Ако пръстенът S е подпръстен на пръстена R, ще казваме, че R е разширение на S.

Дефиниция. Нека R е разширение на пръстена S. Елементът $\alpha \in R$ се нарича *цял* над S, когато съществува моничен полином $f \in S[X]$, такъв че $f(\alpha) = 0$.

Забележка 4.1. Ясно е, че всеки елемент на S е цял над S.

Нека $\alpha_1, \ldots, \alpha_n \in R$. Ще означаваме с $S[\alpha_1, \ldots, \alpha_n]$ най-малкия подпръстен на R, който съдържа S и $\alpha_1, \ldots, \alpha_n$:

$$S[\alpha_1, \ldots, \alpha_n] = \{F(\alpha_1, \ldots, \alpha_n) : F \in S[X_1, \ldots, X_n]\}.$$

Лема 4.2. *Ако $\alpha \in R$ е цял над S, то пръстенът $S[\alpha]$ е крайнопороден S-модул.*

Доказателство. Нека $f \in S[X]$ е моничен полином от степен n, такъв че $f(\alpha) = 0$. Ще покажем, че за всеки елемент $\beta \in S[\alpha]$ съществуват елементи $r_0, r_1, \ldots, r_{n-1} \in S$, такива че

$$\beta = s_0 + s_1\alpha + \cdots + s_{n-1}\alpha^{n-1}. \tag{4.1}$$

Това ще докаже Лема 4.2, защото от (4.1) следва, че пръстенът $S[\alpha]$ се поражда като S-модул от $1, \alpha, \ldots, \alpha^{n-1}$.
Нека $\beta = F(\alpha)$, където $F \in S[X]$. Тъй като f е моничен полином, то съществуват полиноми $q, r \in S[X]$, такива че $F = qf + r$ и $\deg r < n$. Нека $r = s_0 + s_1X + \cdots + s_{n-1}X^{n-1}$, където $s_0, s_1, \ldots, s_{n-1} \in S$. Сега от $F = qf + r$ получаваме

$$\beta = F(\alpha) = q(\alpha)f(\alpha) + r(\alpha) = r(\alpha) = s_0 + s_1\alpha + \cdots + s_{n-1}\alpha^{n-1}. \qquad \square$$

Твърдение 4.3. *Ако $\alpha_1, \alpha_2, \ldots, \alpha_n \in R$ са цели елементи над S, то $S[\alpha_1, \ldots, \alpha_n]$ е крайнопороден S-модул.*

В доказателството на Твърдение 4.3 ще използуваме следната лема:

Лема 4.4 (транзитивност). *Нека $A \subset B \subset C$ са разширения на пръстени, такива че B е крайнопороден A-модул и C е крайнопороден B-модул. Тогава C е крайнопороден A-модул.*

Доказателство (лема 1.3). Нека $x_1, \ldots, x_k \in B$ пораждат B като A-модул и $y_1, \ldots, y_l \in C$ пораждат C като B-модул. За всеки $c \in C$ съществуват $b_j \in B$, $j = 1, \ldots, l$, такива че $c = \sum_{j=1}^{l} b_j y_j$. За всеки b_j, $j = 1, \ldots, l$, съществуват $a_{ij} \in A$, $i = 1, \ldots, k$, такива че $b_j = \sum_{i=1}^{k} a_{ij} x_i$, $j = 1, \ldots, l$. Следователно

$$c = \sum_{j=1}^{l} b_j y_j = \sum_{j=1}^{l} \sum_{i=1}^{k} a_{ij} x_i y_j. \tag{4.2}$$

Равенство (4.2) показва, че елементите $z_{ij} = x_i y_j \in C$, $i = 1, \ldots, k$, $j = 1, \ldots, l$, пораждат C като A-модул. □

Доказателство (Твърдение 1.2). Ще използуваме индукция по броя n на елементите $\alpha_1, \ldots, \alpha_n$. Нека $m \geq 2$ е естествено число. Да предположим, че Твърдение 4.3 е доказано когато $n < m$. Нека $\alpha_1, \ldots, \alpha_m \in R$ са цели над S. Да забележим, че α_m е цял над $S[\alpha_1, \ldots, \alpha_{m-1}]$, защото α_m е цял над S. Тъй като $S[\alpha_1, \ldots, \alpha_m] = S[\alpha_1, \ldots, \alpha_{m-1}][\alpha_m]$, пръстенът $S[\alpha_1, \ldots, \alpha_m]$ е крайнопороден $S[\alpha_1, \ldots, \alpha_{m-1}]$-модул. Освен това, $S[\alpha_1, \ldots, \alpha_{m-1}]$ е крайнопороден S-модул според индукционната хипотеза. Сега от Лема 4.4 следва, че $S[\alpha_1, \ldots, \alpha_m]$ е крайнопороден S-модул. □

В следващата лема R е комутативен пръстен.

Лема 4.5. *Нека $A \in M_{n\times n}(R)$ и нека наредената n-торка $x \in R^n$ е решение на хомогенната линейна система $Ax = 0$. Тогава* $\det(A)\, x = 0$.

Доказателство. Нека $\widetilde{A} \in M_{n\times n}(R)$ е присъединената матрица на A. Добре известно е, че $\widetilde{A}A = \det(A)E_n$. От $Ax = 0$ получаваме $\widetilde{A}(Ax) = 0$, откъдето $\det(A)\, x = 0$. □

Сега ще докажем обратното твърдение на Твърдение 4.3.

Теорема 4.6. *Нека R е разширение на пръстена S. Ако R е крайнопороден S-модул, то всеки елемент $\alpha \in R$ е цял над S.*

Доказателство. Нека $\alpha \in R$ и нека $x_j \in R$, $j = 1, \ldots, n$, пораждат R като S-модул. Тъй като $\alpha x_j \in R$ за всяко $j = 1, \ldots, n$, то съществуват елементи $a_{ij} \in S$, $1 \leq i, j \leq n$, такива че

$$\alpha x_j = \sum_{i=1}^{n} a_{ij} x_j, \qquad j = 1, \ldots, n. \tag{4.3}$$

Нека $A \in M_{n\times n}(S)$ е матрицата с коефициенти a_{ij}, $1 \leq i, j \leq n$. Уравнения (4.3) показват, че наредената n-торка $x = (x_1, \ldots, x_n) \in R^n$ е решение на хомогенната линейна система $(A - \alpha E_n)x = 0$. Следователно $\det(A - \alpha E_n)\, x = 0$ (виж Лемма 4.5), т.е. $\chi_A(\alpha)\, x = 0$, където $\chi_A \in S[X]$ е характеристичният полином на A. Тъй като $x_j \in R$, $j = 1, \ldots, n$, пораждат R като S-модул, то съществуват $a_j \in S$, $j = 1, \ldots, n$, такива че $1 = \sum_{j=1}^{n} a_j x_j$. Сега

$$\chi_A(\alpha) = \chi_A(\alpha) \cdot 1 = \sum_{j=1}^{n} a_j (\chi_A(\alpha) x_j) = 0.$$

Следователно α е корен на характеристичния полином $\chi_A \in S[X]$ на A, откъдето следва, че α е цял над S. □

Твърдение 4.7. *Нека R е разширение на пръстена S. Елементите $\alpha_1, \ldots, \alpha_n \in R$ са цели над S тогава и само тогава, когато пръстенът $S[\alpha_1, \ldots, \alpha_n]$ е крайнопороден S-модул. Нещо повече, в този случай всеки елемент на пръстена $S[\alpha_1, \ldots, \alpha_n]$ е цял над S.*

Доказателство. Следва непосредствено от Твърдение 4.3 и Теорема 4.6. □