Пръстени и полета. Теореми на Ойлер-Ферма и Уилсън.

В групите, алгебричните структури, които разглеждахме досега, беше въведена една бинарна операция, спрямо която групата е затворена като множество, т.е. на всеки два елемента от групата бинарната операция съпоставяше трети елемент, който също се намира в групата.

Нека сега разгледаме множеството R, в което са въведени две бинарни операции, наречени условно събиране $+$ и умножение $\cdot$. Ще казваме, че множеството R е *пръстен*, ако е затворено относно тези две операции и са изпълнени следните аксиоми:

I. R е абелева група относно събирането $+$, т.е.:

1. $(a+b)+c = a+(b+c)$ за $\forall a,b,c \in R$.

2. Съществува нулев елемент $0 \in R$[1], такъв че $a+0 = 0+a = a$ за $\forall a \in R$.

3. За всеки елемент $a \in R$ съществува проттивоположен елемент $-a \in R$, такъв че $a+(-a) = -a+a = 0$.

4. $a+b = b+a$ за $\forall a,b \in R$.

II. Операцията $\cdot$ е асоциативна, т.е.:

5. $(ab)c = a(bc)$ за $\forall a,b,c \in R$.

III. В сила са дистрибутивни закони за двете операции, т.е.:

6. $(a+b)c = ac+bc$ и $c(a+b) = ca+cb$ за $\forall a,b,c \in R$.

В допълнение: ако $ab = ba$ за $\forall a,b \in R$, то казваме, че R е *комутативен пръстен*; ако съществува единичен елемент $e \in R$, такъв че $ae = ea = a$ за $\forall a \in R$, казваме, че R е *пръстен с единица*. За удобство ще оазначаваме единичния елемент на R с 1 или с 1_R, за да подчертаем

[1]Понякога нулевият елемент на R ще записваме като 0_R, когато има нужда от допълнителна яснота.

неговата принадлежност.

Примери:

1. Множествата $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ и $\mathbb{C}$ са пръстени относно обичайните операции събиране и умножение на числа. При това те са комутативни пръстени с единица.

2. Подмножествата $m\mathbb{Z} = \{mz \mid z \in \mathbb{Z}\}$ на $\mathbb{Z}$ за $m = 0, 1, 2, \dots$ също са прсътени относно обичайните събиране и умножение на числа. При $m \geq 2$ е пример за пръстен, който не притежава единичен елемент.

3. Нека F е числово поле, $n \in \mathbb{N}$. Тогава $F_{n\times n}$ е пръстен относно операциите събиране и умножение на матрици с единичен елемент единичната матрица E. При $n > 1$ е пример за некомутативен пръстен.

Следствия от аксиомите:

а) Нулевият елемент 0_R и противоположният елемент $-a$ за $\forall a \in R$ са единствени. Всъщност това е следствие от аксиомите за групи.

б) Ако R е пръстен с единица 1_R, то тя е единствена.

в) $0.a = 0$ за $\forall a \in R$.

г) $(-a)b = a(-b) = -(ab)$ за $\forall a, b \in R$.

д) За $a, b \in R$ означаваме с $a - b$ елемента $a + (-b)$, наречен разлика на a и b.

е) От следствията от аксиомите за групи знаем, че за елемент $a \in R$ и числа $n, m \in \mathbb{Z}$ имаме, че $na + ma = (n + m)a$ и $m(na) = (mn)a$.

ж) Аксиома 5. ни дава, че за елементи $a_1, a_2, \dots, a_k \in R$, елементът $a_1a_2\dots a_k \in R$ е еднозначно определен.

з) За елемент $a \in R$ и число $k \in \mathbb{N}$ означаваме $a^k = \underbrace{aa\dots a}_{k \text{ пъти}}$. Оттук имаме, че $a^ka^l = a^{k+l}$ и $(a^k)^l = a^{kl}$.

Нека R е пръстен. Елементите $a, b \in R$ се наричат *делители на нулата*, ако $a \neq 0_R, b \neq 0_R$, но $ab = 0_R$.

Ако в пръстенът R няма делители на нулата, то той се нарича *област*[2]. Пример за област е пръстенът на целите числа $\mathbb{Z}$.

Нека R е пръстен с единица 1_R. Елементът $a \in R$ се нарича *обратим елемент*, ако съществува елемент $a^{-1} \in R$, такъв че $aa^{-1} = a^{-1}a = 1_R$. Например в пръстена $\mathbb{Z}$ обратимите елменти са само 1 и -1.

[2]Или още *област на цялост.*

Нека R е прсътен с поне два елемента, т.е. $|R| \geq 2$. Казваме, че R е *тяло*, ако всеки ненулев елемент $a \in R, a \neq 0_R$ е обратим.

Казваме, че R е *поле*, ако R е комутативен пръстен и R е тяло. Дотук ние използвахме понятието числово поле F, за което знаем, че $F \subseteq \mathbb{C}$, $|F| \geq 2$ и за всеки два елемента $a, b \in F$ е изпълнено $a+b, a-b, ab, \dfrac{a}{b} \in F$. По този начин се оказва, че всяко числово поле F е поле спрямо сегашната дефиниция. С други думи понятието числово поле е само частен случай на по-голям клас алгебрични структури, наречени полета.

Знаем, че $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ са полета т.к. са числови полета. Пример за тяло, което не е поле (т.е. не е комутативно) е множеството

$$\mathbb{H} = \left\{ \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \mid a, b \in \mathbb{C} \right\} \subseteq \mathbb{C}_{2\times 2},$$

наречено *тяло на кватернионите*. Наистина, ако $A = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \neq \mathbb{O}$, то $a \neq 0$ и/или $b \neq 0$, откъдето следва, че $\det A \neq 0$ и директно се проверява, че A^{-1}, за която знаем, че съществува, също принадлежи на $\mathbb{H}$.

Ако R е тяло (в частност поле), то R няма делители на нулата. Наистина, ако допуснем, че в R има елементи, които са делители на нулата, т.е. $a, b \in R$, такива че $a \neq 0_R, b \neq 0_R$, но $ab = 0_R$, то след като умножим двете страни отляво с елемента $a^{-1} \in R$, получаваме $a^{-1}(ab) = 0_R$ и асоциативното свойство на умножението в пръстените довежда до противоречието $1_R b = b = 0_R$. Следователно остава да е вярно, че в R няма делители на нулата.

Нека R е произволен пръстен. Знаем, че множеството R е абелева група спрямо операцията $+$, която ще наричаме *адитивна група на пръстена* R. Нека R е пръстен с единица 1_R и R^* е множеството на всички обратими елементи на R. Ясно е, че $1_R \in R^*$. Тогава R^* е група относно оерацията $\cdot$ в R: ако $a \in R^*$, то обратният му елемент a^{-1} също принадлежи на R^* и $aa^{-1} = a^{-1}a = 1_R$; ако $a, b \in R^*$, то $(ab)^{-1} = \underbrace{b^{-1}}_{\in R^*} \underbrace{a^{-1}}_{\in R^*}$ и следователно $ab \in R^*$. По този начин R^* е затворено относно операцията $\cdot$, чиято асоциативност е наследена от операцията $\cdot$ в R, притежава единичен елемент 1_R и всеки елемент притежава обратен. Така доказахме, че R^* е група относно операцията $\cdot$ в R, наречена *мултипликативна група на пръстена* R.

Примери:

1. $\mathbb{Z}^* = \{1, -1\}$.

2. $F^*_{n\times n}$ се състои от всички обратими матрици, т.е. с ненулеви детерминанти и следователно $F^*_{n\times n} = GL_n(F)$.

3. Ако R е тяло, то всеки негов ненулев елемент е обратим и следователно $R^* = R\backslash\{0_R\}$. Ако R е поле, то R е комутативно тяло и $R^* = R\backslash\{0_R\}$ е абелева група.

Нека R е пръстен, а $S \subseteq R$ е негово подмножество. Казваме, че S е *подпръстен* на R и означаваме $S \leq R$, ако за $\forall a, b \in S$ е изпълнено $a + b, a - b, ab \in S$. В такъв случай имаме, че $a - a = 0_R \in S$ и $0_R - a = -a \in S$ и S се оказва пръстен относно операциите $+$ и $\cdot$, наследени от R. Не е трудно да се провери, че сечението на фамилия подпръстени на R също е подпръстен на R.

Нека $n \in \mathbb{N}, n > 1$. В пръстена на целите числа $\mathbb{Z}$ остатъците при деление на n са $0, 1, \ldots, n-1$. Нека $\overline{r}$ е множествотона всички цели числа, които при деление с n дават остатък r, с други думи числата $z \in \mathbb{Z}$, такива че $z \equiv r(\mathrm{mod}\, n)$. Да разгледаме множеството

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

В него дефинираме операции $+$ и $\cdot$ по следния начин: $\overline{k} + \overline{l} = \overline{k+l}$ и $\overline{k} \cdot \overline{l} = \overline{k \cdot l}$. По този начин $\mathbb{Z}_n$ се превръща в пръстен с нулев елемент $\overline{0}$, единичен елемент $\overline{1}$ и при това е комутативен. Наричаме го *пръстен на класовете остатъци по модул* n. Ясно е, че $\mathbb{Z}_n$ има n на брой елемента.

Пример:

Да разгледаме пръстена от класовете остатъци по модул 6

$$\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}.$$

В него имаме, че $\overline{2}+\overline{3} = \overline{5}$; $\overline{4}+\overline{5} = \overline{9} = \overline{3}$, защото $9 \equiv 3(\mathrm{mod}\, 6)$; $\overline{4}\cdot\overline{5} = \overline{20} = \overline{2}$, защото $20 \equiv 2(\mathrm{mod}\, 6)$; $\overline{3} \cdot \overline{4} = \overline{12} = \overline{0}$ и следователно $\overline{3}$ и $\overline{4}$ са делители на нулата в $\mathbb{Z}_6$, а оттук вече самият пръстен няма как да е област.

Да си припомним, че за $n \in \mathbb{N}, n > 1$ с $\varphi(n)$ означаваме броя на естествените числа, ненадминаващи n, които са взаимно прости с n.

Теорема 1. *(1) За мултипликативната група на* $\mathbb{Z}_n$ *имаме, че* $\mathbb{Z}^*_n = \{\overline{k} \mid 0 \leq k \leq n-1 \text{ и } (k, n) = 1\}$ *и* $|\mathbb{Z}^*_n| = \varphi(n)$.

(2) $\mathbb{Z}_n$ е поле $\Leftrightarrow n$ е просто число.

Доказателство. (1) Да разгледаме произволен елемент $\overline{k} \in \mathbb{Z}_n, k = 1, 2, \ldots, n-1$ (няма нужда да разглеждаме $k = 0$, защото е ясно, че елементът $\overline{0} \notin \mathbb{Z}_n^*$). Нека k и n не са взаимно прости, т.е. $(k, n) = d > 1$ и $k = k_1 d$, а $n = n_1 d$ за $k_1, n_1 \in \mathbb{N}; k_1, n_1 > 1$. Ясно е, че $\overline{k} \neq \overline{0}$, защото $k < n$ и следователно $n \nmid k$. Също имаме и, че $\overline{n_1} \neq \overline{0}$, защото $d > 1 \Rightarrow n_1 < n$ и следователно $n \nmid n_1$. Но $\overline{k} \cdot \overline{n_1} = \overline{kn_1} = \overline{k_1 d n_1} = \overline{k_1 n} = \overline{0}$, поради очевидния факт, че $n \mid k_1 n$. Следователно $\overline{k}$ е делител на нулата в $\mathbb{Z}_n$ и няма как да е обратим елемент, т.е. $\overline{k} \notin \mathbb{Z}_n^*$. Нека сега k и n са взаимно прости, т.е. $(k, n) = 1$. От тъждеството на Безу имаме, че съществуват цели числа $u, v \in \mathbb{Z}$, такива че $uk + vn = 1$. Това означава, че $\overline{uk + vn} = \overline{uk} + \overline{vn} = \overline{uk} + \overline{0} = \overline{u} \cdot \overline{k} = \overline{1}$, с което открихме, че елементът $\overline{k}$ е обратим и неговият обратен е $\overline{u}$. И така $(k, n) = 1 \Rightarrow \overline{k} \in \mathbb{Z}_n^*$. По този начин доказахме, че $(k, n) = 1 \Leftrightarrow \overline{k} \in \mathbb{Z}_n^*$.

(2) $\mathbb{Z}_n$ е комутативен пръстен с единица. В такъв случай $\mathbb{Z}_n$ е поле $\Leftrightarrow$ всеки ненулев елемент на $\mathbb{Z}_n$ е обратим $\Leftrightarrow \mathbb{Z}_n^* = \mathbb{Z}_n \backslash \{\overline{0}\} \Leftrightarrow |\mathbb{Z}_n^*| = n - 1 \Leftrightarrow \varphi(n) = n - 1 \Leftrightarrow n$ е просто число. □

Вече можем да разгледаме първи пример на нечислово (и при това крайно) поле. Нека p е просто число. Горната теорема ни дава, че множеството

$$\mathbb{Z}_p = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$$

е поле с p на брой елемента. В полето с пет елемента

$$\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$$

например имаме, че $\overline{2} \cdot \overline{3} = \overline{2 \cdot 3} = \overline{6} = \overline{1}$ и $\overline{4}^2 = \overline{16} = \overline{1}$, с което става ясно, че всеки ненулев елемент е обратим.

Сега можем да докажем теоремите, които споменахме в първа глава.

Теорема на Ойлер-Ферма. *Ако $n \in \mathbb{N}, a \in \mathbb{Z}$ и $(a, n) = 1$, то $a^{\varphi(n)} \equiv 1 (\bmod\, n)$. В частност, ако n е просто, $a^{n-1} \equiv 1 (\bmod\, n)$.*

Доказателство. Разглеждаме пръстена $\mathbb{Z}_n$. Ако $b, c \in \mathbb{Z}$, то $\overline{b} = \overline{c} \Leftrightarrow b \equiv c (\bmod\, n)$. Нека $a \in \mathbb{Z}$ е такова, че $(a, n) = 1$. Тогава $\overline{a}$ е обратим елемент в $\mathbb{Z}_n$, т.е. $\overline{a} \in \mathbb{Z}_n^*$. Според Следствие 2 от Теоремата на Лагранж имаме, че $\overline{a}^{|\mathbb{Z}_n^*|} = \overline{1}$, но според Теорема 1 $|\mathbb{Z}_n^*| = \varphi(n)$ и следователно $\overline{a}^{\varphi(n)} = \overline{1}$. В $\mathbb{Z}$ това е равносилно с $a^{\varphi(n)} \equiv 1 (\bmod\, n)$. □

Теорема на Уилсън. *Ако p е просто число, то* $(p-1)! \equiv -1 (\operatorname{mod} p)$.

Доказателство. Разглеждаме полето $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$. Нека $\overline{k} \in \mathbb{Z}_p, \overline{k} \neq \overline{0}$. Т.к. сме в поле съществува обратен елемент $\overline{k}^{-1}$, такъв че $\overline{k} \cdot \overline{k}^{-1} = \overline{1}$. Да видим кога $\overline{k}^{-1} = \overline{k}$. Това означава, че $\overline{k}^2 = \overline{1}$, което е еквивалентно на $(\overline{k} - \overline{1})(\overline{k} + \overline{1}) = \overline{0}$. Т.к. $\mathbb{Z}_p$ е поле, в него няма делители на нулата и следователно или $\overline{k} - \overline{1} = \overline{0}$, или $\overline{k} + \overline{1} = \overline{0}$, т.е. $\overline{k} = \overline{1}$ или $\overline{k} = \overline{-1} = \overline{p-1}$. И така $\overline{k}^2 = \overline{1} \Leftrightarrow \overline{k} = \overline{1}$ или $\overline{k} = \overline{-1}$. Следователно елементите на $\mathbb{Z}_p$, които са различни от нула са елементите $\overline{1}, \overline{-1}$ и двойки елементи от вида $\{\overline{k}, \overline{k}^{-1}\}$, където $\overline{k} \neq \overline{k}^{-1}$. Това означава, че умножавайки всички ненулеви елементи на $\mathbb{Z}_p$ и групирайки двойките обратни елементи, получаваме

$$\overline{1} \cdot (\overline{-1}) \cdots (\underbrace{\overline{k} \cdot \overline{k}^{-1}}_{=\overline{1}}) \cdots = \overline{-1},$$

но както споменахме лявто произведение се състои от всички ненулеви елементи на полето, т.е. имаме

$$\overline{1} \cdot \overline{2} \cdots \overline{p-1} = \overline{-1},$$

което в пръстена на целите числа $\mathbb{Z}$ ни дава точно исканото равенство

$$(p-1)! \equiv -1 (\operatorname{mod} p).$$

□