Идеали. Факторпръстени. Теорема за хомомрфизмите на пръстени.

Нека R е произволен пръстен, а $I \subseteq R$ е непразно негово подмножество. Казваме, че I е *ляв идеал на* R, ако за $\forall a, b \in I$ е изпълнено че $a - b \in I$ и за $\forall a \in I, \forall r \in R$ е изпълнено, че $ra \in I$. Аналогично, казваме, че I е *десен идеал на* R, ако за $\forall a, b \in I$ е изпълнено, че $a - b \in I$ и за $\forall a \in I, r \in R$ е изпълнено, че $ar \in I$. Ако I е едновременно ляв и десен идеал на R, то казваме, че I е *двустранен идеал* или просто *идеал* на R и пишем $I \trianglelefteq R$.

Всеки идеал I на пръстена R е също и негов подпръстен, защото от дефиницията следва, че за $\forall a, b \in I$ е изпълнено $a - b \in I$ и $ab \in I$. Оттук следва и че I е подгрупа на адитивната група на R.

Примери:

1. Нулевият идеал $\{0_R\} \trianglelefteq R$ и целият пръстен $R \trianglelefteq R$ са тривиални примери за идеали.

2. Нека $R = \mathbb{Z}$, а $I = m\mathbb{Z} = \{mz \mid z \in \mathbb{Z}\}$ за $m = 0, 1, 2, \ldots$. Тогава за произволни два елемента $a, b \in I$ имаме, че $a = mz_1$ и $b = mz_2$ за $z_1, z_2 \in \mathbb{Z}$. Тогава $a - b = mz_1 - mz_2 = m(\underbrace{z_1 - z_2}_{\in\mathbb{Z}})$, което означава, че $a - b \in I$. За произволно $r \in R = \mathbb{Z}$ имаме, че $ra = rmz_1 = m(\underbrace{rz_1}_{\in\mathbb{Z}})$ и $ar = mz_1r = m(\underbrace{z_1r}_{\in\mathbb{Z}})$. С това $I \trianglelefteq R$, т.е. $m\mathbb{Z} \trianglelefteq \mathbb{Z}$.

3. Ясно е, че ако R е комутативен пръстен, то левите и десните идеали в него съвпадат и говорим просто за идеали на R.

4. Нека F е произволно поле. Да разгледаме матричния пръстен $R = F_{2\times 2}$, състоящ се от всички 2×2 матрици с елементи от полето F. Лесно се вижда, че множеството

$$I = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mid a, b \in F \right\}$$

е ляв, но не е десен идеал на R, а множеството

$$J = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in F \right\}$$

е десен, но не е ляв идеал на R. Изобщо в R няма двустранни идеали с изключение на тривиалните.

5. Сечението на идеали на R също е идеал на R.

Нека R е комутативен пръстен с единица 1_R. За произволен елемент $a \in R$ разглеждаме множеството

$$(a) = \{xa = ax \mid x \in R\}.$$

То е идеал на R, наречен *главен идеал на R, породен от a*. Наистина, за произволни два елемента $xa, ya \in (a)$, където $x, y \in R$ е изпълнено, че $xa - ya = (\underbrace{x-y}_{\in R})a \in (a)$, а за произволен елемент $r \in R$ е изпълнено $r(xa) = (\underbrace{rx}_{\in R})a \in (a)$ и така $(a) \trianglelefteq R$.

В пръстена на целите числа $\mathbb{Z}$ идеалите се изчерпват с $m\mathbb{Z}$ за $m \in \mathbb{Z}, m \geq 0$ и следователно всичките са главни идеали. Наистина, ако $I \trianglelefteq \mathbb{Z}$ е идеал на $\mathbb{Z}$, то тогава I е подгрупа на адитивната група на $\mathbb{Z}$. Знаем, че всички подгрупи на групата на целите числа се изчерпват с $m\mathbb{Z}$ за $m \in \mathbb{Z}, m \geq 0$ и следователно $I = m\mathbb{Z}$ за някое $m \in \mathbb{Z}, m \geq 0$. Имаме, че $m\mathbb{Z} = \{mz \mid z \in \mathbb{Z}\} = (m)$ според определението на главен идеал.

Твърдение 1. *Нека R е пръстен с единица 1_R, а $I \trianglelefteq R$ е идеал в R. Тогава*

а) Ако $1_R \in I$, то $I = R$;

б) Ако I съдържа обратим елемент на R, то $I = R$.

Доказателство. а) Нека $1_R \in I$. Тогава за $\forall r \in R$ е изпълнено $r = r.1_R \in I$ и по този начин $R \subseteq I$. Т.к. по определение $I \subseteq R$, то получихме $R = I$.

б) Нека $a \in I$ е обратим елемент на R. Тогава $\exists a^{-1} \in R : a^{-1}a = 1_R$. Сега от определението за идеал, имаме че $a^{-1}a \in I$, т.е. $1_R \in I$ и според а) следва, че $R = I$. □

Да отбележим, че ако един пръстен R е тяло (и в частност поле), то в R няма идеали различни от $\{0_R\}$ и R, т.е. няма нетривиални идеали. Наистина, нека $I \trianglelefteq R$ е идеал на R и да допуснем, че $I \neq \{0_R\}$. Тогава $\exists a \in I : a \neq 0_R$. Но R е тяло и в него всеки ненулев елемент е обратим, а оттам елементът a също е обратим. Сега от Твърдение 1 б) следва, че $I = R$. По този начин, ако $I \trianglelefteq R$, то или $I = \{0_R\}$, или $I = R$.

Твърдение 2. *Комутативен пръстен R с единица 1_R е поле $\Leftrightarrow$ R няма нетривиални идеали.*

Доказателство. Вече видяхме, че необходимостта е в сила. Остава да докажем обратната посока. Нека R е комутативен пръстен с единица и единствени идеали $\{0_R\}$ и R. Нека $a \in R, a \neq 0_R$ е ненулев елемент. Разглеждаме главният идеал, породен от a

$$(a) = \{ra \mid r \in R\}.$$

Имаме, че $a \in (a)$ и $a \neq 0_R$, откъдето следва, че $(a) \neq \{0_R\}$. В такъв случай, единствената възможност, която остава е $(a) = R$. Очевидно $1_R \in R$, което означава, че $1_R \in (a)$. Но тогава $\exists r \in R : ra = 1_R$. Това означава, че произволен ненулев елемент $a \in R$ е обратим. Така R е комутативно тяло, т.е. е поле. □

Когато разглеждахме група G, притежаваща нормална подгрупа $H \trianglelefteq G$, ние построихме нова група G/H, наречена факторгрупа на G по H. Сега ще извършим аналогична процедура спрямо даден прсътен.

Нека R е пръстен, а $I \trianglelefteq R$ е негов идеал. От определението за пръстен знаем, че R образува абелева група, относно операцията $+$, а от определението на идеал следва, че $I \leq R$ е подгрупа на R. Т.к. всяка подгрупа на абелева група е нормална, то получаваме, че $I \trianglelefteq R$ е нормална подгрупа на адитивната група на пръстена R. Разглеждаме факторгрупата на групата R по подгрупата I, а именно

$$R/I = \{a + I \mid a \in R\}.$$

R/I е абелева група спрямо операцията $+$, наследена от пръстена R, с нулев елемент I. В R/I дефинираме допълнително и операция $\cdot$ по

правилото $(a+I)\cdot(b+I) = ab+I$. Да проверим, че така въведеното умножение на елементи е коректно: нека $a_1 \in a+I, b_1 \in b+I$ са други представители на същите съседни класове. Това ни дава, че $a_1 = a+i_1$ за някакъв елемент $i_1 \in I$, а $b_1 = b+i_2$ за някакъв елемент $i_2 \in I$. Тогава $a_1b_1 - ab = (a+i_1)(b+i_2) - ab = ab + ai_2 + bi_1 + i_1i_2 - ab = \underbrace{ai_2}_{\in I} + \underbrace{bi_1}_{\in I} + \underbrace{i_1i_2}_{\in I}$, което означава, че $a_1b_1 - ab \in I$. Според свойствата на съседните класове получаваме, че $a_1b_1 + I = ab + I$. По този начин видяхме, че така дефинираната операция съпоставя един и същ съседен клас на представители от един и същ съседен клас, т.е. тя е коректно въведена.

Сега, спрямо двете операции $+$ и $\cdot$, множеството R/I се превръща в пръстен, наречен *факторпръстен на R по идеала I*. Ако пръстенът R е комутативен, то R/I също е комутативен, защото за $\forall a+I, b+I \in R/I$ имаме, че $(a+I)\cdot(b+I) = ab+I = ba+I = (b+I)\cdot(a+I)$. Ако R е пръстен с единица 1_R, то R/I е пръстен с единица $1_R + I$, защото $(1_R+I)\cdot(a+I) = 1_Ra + I = a + I = a1_R + I = (a+I)\cdot(1_R+I)$.

Пример:
За $R = \mathbb{Z}$ и $I = n\mathbb{Z}$ за $n \in \mathbb{Z}, n \geq 0$, имаме че

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

Нека R и R' са пръстени, а $\varphi : R \longrightarrow R'$ е изображение. Изображението φ е хомоморфизъм на прсътени, ако за $\forall a, b \in R$ е изпълнено $\varphi(a+b) = \varphi(a) + \varphi(b)$ и $\varphi(ab) = \varphi(a)\varphi(b)$. Ако в допълнение φ е биекция на R върху R', то φ е изоморфизъм на пръстени, а R и R' са изоморфни. Този факт отбелязваме с $R \cong R'$.

Нека $\varphi : R \longrightarrow R'$ е хомоморфизъм. Дефинираме множеството

$$\operatorname{Im}\varphi = \{\varphi(a) \in R' \mid a \in R\},$$

наречено *образ на φ* и множеството

$$\operatorname{Ker}\varphi = \{a \in R \mid \varphi(a) = 0_{R'}\},$$

наречено *ядро на φ*.

За произволни елементи $a, b \in \operatorname{Ker}\varphi$ имаме, че $\varphi(a-b) = \varphi(a) - \varphi(b) = 0_{R'} - 0_{R'} = 0_{R'}$, т.е. $a-b \in \operatorname{Ker}\varphi$. За произволен елемент $r \in R$ имаме още че $\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0_{R'} = 0_{R'}$ и $\varphi(ar) = \varphi(a)\varphi(r) = 0_{R'}\varphi(r) = 0_{R'}$, т.е. $ra, ar \in \operatorname{Ker}\varphi$. Всичко това означава, че $\operatorname{Ker}\varphi \trianglelefteq R$.

Твърдение 3. *Нека R е пръстен, а $I \trianglelefteq R$ е идеал на R. Тогава изображението*

$$\pi : R \longrightarrow R/I,$$

дефинирано с $\pi(a) = a + I$ за $\forall a \in R$ е хомоморфизъм на пръстени, наречен естествен хомоморфизъм[1] *на R върху R/I, с $\operatorname{Im}\pi = R/I$ и $\operatorname{Ker}\pi = I$.*

Доказателство. От материала за групи знаем, че R е група спрямо операцията $+$ и изображението π е хомоморфизъм на групата R във факторгрупата R/I (т.е. $\pi(a+b) = \pi(a)+\pi(b)$) с $\operatorname{Im}\varphi = R/I$ и $\operatorname{Ker}\varphi = I$. Остава ни да проверим единствено, че $\pi(ab) = ab + I = (a+I)\cdot(b+I) = \pi(a)\pi(b)$ за $\forall a, b \in R$, което означава, че π е хомоморфизъм на пръстени. □

Теорема за хомоморфизмите на пръстени.. *Нека R и R' са пръстени, а изображението*

$$\varphi : R \longrightarrow R'$$

е хомоморфизъм на пръстени. Тогава $\operatorname{Ker}\varphi \trianglelefteq R$ и $R/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi$.

Доказателство. От материала за групи знаем, че изображението

$$f : R/\operatorname{Ker}\varphi \longrightarrow \operatorname{Im}\varphi,$$

дефинирано с $f(a+\operatorname{Ker}\varphi) = \varphi(a)$ за $\forall a \in R$ е коректно и е изоморфизъм на групи. Остава да проверим единствено, че f е хоморфизъм на пръстени. Наистина, за произволни $a, b \in R$ имаме, че $f[(a+\operatorname{Ker}\varphi)\cdot(b+\operatorname{Ker}\varphi)] = f(ab + \operatorname{Ker}\varphi) = \varphi(ab) = \varphi(a)\varphi(b) = f(a + \operatorname{Ker}\varphi)f(b + \operatorname{Ker}\varphi)$. И така, f е изоморфизъм на пръстените $R/\operatorname{Ker}\varphi$ и $\operatorname{Im}\varphi$, т.е. $R/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi$. □

[1] Или още естествен епиморфизъм.