0.1 Прстени и идеали

0.1.1 Идеали прстена

На последњем часу смо дефинисали прстен, извели из аксиома правила рачунања и дали примере прстена. Затим смо увели појмове потпрстена и хомоморфизма прстена. Видели смо да је слика сваког хомоморфизма $f : R \to K$ један потпрстен прстена K. Његово језгро, које се дефинише као

$$Kerf = \{x \in R : f(x) = 0_K\}$$

је затворено за сабирање и множење, али ако би му припадала јединица прстена R, онда би било $f(a) = f(a \cdot 1_R) = f(a) \cdot 0_K = 0_K$ и за све елементе $a \in R$, па $1_R \in Kerf$ само у случају нула-хомоморфизма. Дакле, језгро није потпрстен, али има следећу особину: довољно је да неки елемент припада језгру да би његов производ са било којим елементом прстена био опет у језгру, јер

$$a \in Kerf \;\Rightarrow\; f(ax) = f(a) \cdot f(x) = f(a) \cdot 0_K = 0_K$$

за све $x \in R$. Исто важи и за xa. То нас мотивише да дефинишемо следећу подструктуру прстена:

Дефиниција 0.1. Нека је R прстен и I непразан подскуп од R. I је *идеал* прстена R ако важи:
1) $(I, +)$ је подгрупа адитивне групе прстена $(R, +)$,
2) за све $x \in R$ и $a \in I$ је $ax,\ xa \in I$.

Да је I идеал прстена R означавамо са $I \rhd R$.

Напомена 0.1. Први услов из дефиниције се може заменити условом $a, b \in I \;\Rightarrow\; a+b \in I$.

Зашто? Из другог услова ћемо добити: $0 \in R$ и $a \in I$ повлачи $a \cdot 0 = 0 \in I$, као и $(-a) = (-1) \cdot a \in I$ за све $a \in I$, па је $(I, +)$ заиста подгрупа од $(R, +)$.
Такође, ако је прстен R комутативан, што ће углавном бити случај, други услов постаје само $x \in R$ и $a \in I$ повлачи $ax \in I$.

Пример 0.2. Нека је R комутативан прстен и $a \in R$ произвољан елемент. Лако се провери да је скуп

$$< a >= aR = \{ax : x \in R\}$$

један идеал прстена R ($ax + ay = a(x + y) \in < a >$, као и $(ax)y = y(ax) = a(xy) \in < a >$) и кажемо да је то *главни идеал генерисан елементом a.*

Пример 0.3. У прстену $\mathbb{Z}$ сви идеали су главни.

Зашто? $I \rhd \mathbb{Z}$ повлачи $(I, +) \leq (\mathbb{Z}, +)$, а знамо да су подгрупе цикличне групе такође цикличне, па је I облика $n\mathbb{Z}$ за неки цео број n. Сада се лако провери да $n\mathbb{Z}$ задовољава и други услов из дефиниције идеала ($(nx)y = y(nx) = n(xy) \in n\mathbb{Z}$). Дакле, осим $\{0\}$ и целог прстена, идеали прстена целих бројева су $2\mathbb{Z}$, $3\mathbb{Z}$ итд.

Пример 0.4. Ако идеал садржи јединицу или било који инверзибилни елемент прстена, он је једнак целом прстену.

Зашто? $1 \in I,\ x \in R \ \Rightarrow\ 1 \cdot x \in I$, па би било $R \subset I$, тј. $I = R$. Слично, ако је неки инверзибилни елемент у I, онда ће производ њега и његовог инверза бити опет у I, а тај производ је 1.

Последица: Нека је $\mathbb{F}$ поље и $I \rhd \mathbb{F}$. Тада је $I = \{0\}$ или $I = \mathbb{F}$. (У пољу нема правих идеала.)

Пример 0.5. Језгро хомоморфизма прстена је идеал.

Видели смо већ да је за хомоморфизам $f : R \to K$, скуп

$$Kerf = \{x \in R : f(x) = 0_K\}$$

затворен за сабирање и да је довољно да један чинилац припада њему да би производ опет био ту. Као и код векторских простора и група, и овде важи:

$$f \text{ је "}1-1\text{"} \Leftrightarrow Kerf = \{0_R\}.$$

Пример 0.6. Ако је $\mathbb{F}$ поље, сваки идеал прстена $\mathbb{F}[X]$ је главни. Нека је $I \rhd \mathbb{F}[X]$. Ако

је $I = \{0\}$, он је главни, генерисан нула-полиномом. Нека је сада $I \neq \{0\}$ и нека је $a(x)$ не-нула полином из I чији је степен минималан. Узмимо било који полином $p(x)$ из I и еуклидски га поделимо полиномом $a(x)$: $p = aq + r$, при чему је степен полинома r строго мањи од степена полинома a. Из $a \in I$ следи да је и $aq \in I$, па даље из $p \in I$ добијамо $r = p - aq \in I$. Због степена сада мора бити $r \equiv 0$, што значи да је $p = aq$, односно да $p \in < a >$. Дакле, $I = < a >$.

Операције са идеалима

Нека су I и J идеали прстена R. Тада је њихов пресек такође један идеал:

$$a, b \in I \cap J \ \Rightarrow a, b \in I \wedge a, b \in J \Rightarrow a + b \in I \wedge a + b \in J \Rightarrow a + b \in I \cap J,$$

$$a \in I \cap J,\ x \in R \Rightarrow a \in I \wedge a \in J \wedge x \in R \Rightarrow ax, xa \in I \wedge ax, xa \in J \Rightarrow ax, xa \in I \cap J.$$

Ово је очекивано, али исто тако знамо да унија неће бити идеал (није ни подгрупа, знамо од раније). Зато правимо најмањи идеал који садржи два дата, и зовемо га збир идеала I и J:

$$I + J = \{a + b :\ a \in I,\ b \in J\}$$

Лако се провери да смо добили идеал:

$$a + b + a_1 + b_1 = (a + a_1) + (b + b_1)\ \in I + J$$

$$(a + b)x = ax + bx \in I + J$$

за $a \in I,\ b \in J,\ x \in R$.

Пошто у прстену, осим сабирања, постоји и множење, природно је да се питамо шта бисмо подразумевали под производом два идеала. Ако бисмо, по аналогији са сабирањем, IJ дефинисали као $IJ = \{ab : a \in I,\ b \in J\}$, наишли бисмо на проблем код провере да је овај скуп затворен за сабирање: $ab + a_1b_1$ не мора да буде облика нешто из I пута нешто из J. То превазилазимо тако што за елементе производа идеала узимамо суме коначно производа:

$$IJ = \{a_1b_1 + \cdots + a_nb_n :\ a_k \in I,\ b_k \in J\}$$

Сада се лако види да је збир два елемента из IJ опет елемент из IJ, а други услов је свакако испуњен: $x(a_1b_1 + \cdots + a_nb_n) = (xa_1)b_1 + \cdots + (xa_n)b_n$, а xa_k припада I. Исто и за множење здесна, само ће тада b_kx припадати J.

Важи: $IJ \subset I \cap J$.

Зашто? Нека је $a_1b_1 + \cdots + a_nb_n$ произвољан елемент из IJ. Пошто су сви a-ови у I, њихови производи са b-овима ће бити опет у I, а како је I затворен за сабирање, и цела сума $a_1b_1 + \cdots + a_nb_n$ ће припадати I. Исте аргументе користимо да покажемо да је ова сума у J: b_k припада J за свако k, па a_kb_k припада J за свако k, а онда и њихов збир. Дакле, елемент $a_1b_1 + \cdots + a_nb_n$ је и у I, и у J, па и у $I \cap J$. Обрнуто не важи у општем случају, а нешто касније ћемо видети у ком односу треба да буду два идеала да би њихов пресек био садржан у производу.

Пример 0.7. Пошто су у прстену $\mathbb{Z}$ сви идеали главни, збир, пресек и производ два идеала ће опет бити главни идеал. Тако је, на пример,

$$24\mathbb{Z} + 40\mathbb{Z} = 8\mathbb{Z},$$

$$24\mathbb{Z} \cap 40\mathbb{Z} = 120\mathbb{Z},$$

$$24\mathbb{Z} \cdot 40\mathbb{Z} = 960\mathbb{Z}.$$

Проверите да важи:

$$m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z},$$

$$m\mathbb{Z} \cap n\mathbb{Z} = s\mathbb{Z},$$

$$m\mathbb{Z} \cdot n\mathbb{Z} = mn\mathbb{Z},$$

где је $d = NZD(m, n)$, а $s = NZS(m, n)$.

0.1.2 Карактеристика прстена

Нека је R прстен и P било који његов потпрстен. По дефиницији, P садржи 1_R, па пошто је затворен за операције прстена, садржаће и $1_R + 1_R$, затим $1_R + 1_R + 1_R$ итд, као и (-1_R), $(-1_R) + (-1_R) \ldots$ Такође, $0_R \in P$, па P сигурно садржи скуп

$$\{m1_R :\ m \in \mathbb{Z}\}$$

Овај скуп је сам за себе један прстен који се зове *карактеристични потпрстен* прстена R и означава са R_0. То је, дакле, минимални потпрстен прстена R. У односу на његову

кардиналност разликујемо две врсте прстена. Прва могућност је да је $R_0 \cong \mathbb{Z}$, при чему је изоморфизам дат са $m \leftrightarrow m1_R$. Из инјективности овог пресликавања следи да је онда

$$k1_R = 0 \;\Leftrightarrow\; k = 0$$

Тада кажемо да је прстен R *карактеристике нула* и пишемо $charR = 0$. Дакле, $charR = 0$ значи да је $R_0 \cong \mathbb{Z}$ и да сабирањем 1_R саме са собом не можемо добити 0_R.
У супротном, односно ако је збир неколико 1_R једнак 0_R, *карактеристика прстена* је најмањи природан број k за који је $k1_R = 0_R$. Приметимо да је онда и за сваки елемент $x \in R$:

$$kx = k(1_R x) = 1_R x + \cdots + 1_R x = (1_R + \cdots + 1_R)x = (k1_R)x = 0_R x = 0_R$$

Такође, јасно је да је

$$charR = k \;\Leftrightarrow\; R_0 \cong \mathbb{Z}_k,$$

јер $m1_R = (kq + r)1_R = kq1_R + r1_R = r1_R$, где је $0 \leq r < k$.

Пример 0.8. $char\mathbb{Z} = 0$, $char\mathbb{Z}_k = k$

Пример 0.9. Ако је R прстен, онда прстени $R[X]$ и $M_n[R]$ имају исту карактеристику као и сам прстен R.
(Одмах се види, јер $1_{R[X]} = 1_R$, а јединична матрица E_n има на дијагонали 1_R.)

0.1.3 Делитељи нуле и област целих

Дефиниција 0.2. Елемент a прстена R је *леви делитељ нуле* у том прстену ако постоји елемент $b \in R \setminus \{0\}$ за који је $ab = 0$. (a је *десни делитељ нуле* ако постоји $b \in R \setminus \{0\}$ за који је $ba = 0$.)

Нула прстена је увек делитељ нуле. Ако је $a \neq 0$ делитељ нуле, кажемо да је a прави делитељ нуле (било леви било десни).
За прстен који нема праве делитеље нуле кажемо да је *област целих* или *домен*. Дакле, R је домен ако за било која два елемента важи:

$$ab = 0 \;\Rightarrow\; a = 0 \;\vee\; b = 0.$$

Пример 0.10. Прстен целих бројева је домен, док $\mathbb{Z}_n$, где n није прост број, није. На пример, у $\mathbb{Z}_{20}$ је $4 \cdot 5 = 0$. Такође, знамо да у прстену матрица (нпр. у $M_2[\mathbb{R}]$) постоје прави делитељи нуле, односно да постоје не-нула матрице такве да је њихов производ нула-матрица.

Делитељи нуле су блиско повезани са регуларношћу у прстену:

$$ax = ay \;\Leftrightarrow\; a(x - y) = 0,$$

па ако a није регуларан слева, постојаће различити x и y за које је $ax = ay$, а самим тим и елемент $b = x - y$ различит од нуле за који је $ab = 0$, и обрнуто. Дакле, a је леви делитељ нуле акко није регуларан слева (односно, a је десни дељитељ нуле акко није регуларан здесна.)

Видели смо да у прстенима $\mathbb{Z}_n$, где n није прост број, постоје прави делитељи нуле, док у $\mathbb{Z}_p$, где је p прост број, не постоје:

$$r \cdot_p s = 0 \text{ за неке } r, s \in \mathbb{Z}_p \;\Rightarrow\; p|rs \text{ у } \mathbb{Z} \;\Rightarrow\; p|r \vee p|s \;\Rightarrow\; r = 0 \vee s = 0$$

Важи и следеће:

Тврђење 0.1. *Ако је R домен, онда је његова карактеристика или нула или неки прост број.*

Доказ. Ако је $charR = 0$, онда је у реду. Нека је сада $charR = k > 0$. Покажимо да је k прост. Претпоставимо да је $k = rs$. Пошто је збир k јединица прстена R једнак 0_R, биће

$$0_R = k1_R = rs1_R = (r1_R)(s1_R),$$

па пошто R нема праве делитеље нуле, биће $r1_R = 0_R$ или $s1_R = 0_R$. По дефиницији карактеристике прстена, k је најмањи природан број за који је $k1_R = 0_R$, па из претходног следи да је $k \leq r$ или $k \leq s$. Сада из $k = rs$ имамо $k = r$ или $k = s$. Дакле, k нема прави растав, то јест, прост је. □