Algebrske strukture, 3.del

Obsegi in polja

Obsegi so zelo poseben tip kolobarjev. V kolobarjih lahko elemente seštevamo, odštevamo in množimo, v obsegih pa jih lahko tudi delimo (razen deljenja z nič seveda).

Definicija obsega

Obseg je tak kolobar, v katerem je množica neničelnih elementov grupa za množenje. Komutativnemu obsegu pravimo **polje**.

Opomba: Grupa je asociativen grupoid z enoto, v katerem je vsak element obrnljiv. Definicijo obsega lahko torej povemo tudi takole. **Obseg** je tak asociativen kolobar z enoto, v katerem je vsak neničeln element obrnljiv.

Primeri polj

Kolobarji $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ in $(\mathbb{C},+,\cdot)$ so polja. Za vsako polje F naj bo $F(x)$ množica vseh racionalnih funkcij v spremenljivki x s koeficienti iz F. Ta množica je polje za običajno seštevanje in množenje racionalnih funkcij. Torej so $(\mathbb{Q}(x),+,\cdot)$, $(\mathbb{R}(x),+,\cdot)$ in $(\mathbb{C}(x),+,\cdot)$ polja.

Primer obsega, ki ni polje

Množica vseh matrik oblike

$$\begin{bmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{bmatrix}$$

kjer $\alpha, \beta \in \mathbb{C}$, je obseg za običajno seštevanje in množenje matrik. Pravimo mu **obseg kvaternionov**.

Če vstavimo $\alpha = a + bi$ in $\beta = c + di$, velja

$$\begin{bmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{bmatrix} = a \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + b \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} + c \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} + d \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

Ta izraz lahko na kratko zapišemo kot $a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$. Matrika $\mathbf{1}$ je identična matrika, za matrike $\mathbf{i}, \mathbf{j}, \mathbf{k}$ pa velja

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{1}, \quad \mathbf{ij} = -\mathbf{ji} = \mathbf{k}, \quad \mathbf{jk} = -\mathbf{kj} = \mathbf{i}, \quad \mathbf{ki} = -\mathbf{ik} = \mathbf{j}.$$

Odtod med drugim sledi, da obseg kvaternionov ni komutativen.

Podobsegi in podpolja

Definicija podobsega in podpolja

Naj bo $(L, +, \cdot)$ obseg. Podmnožica $K \subseteq L$ je njegov **podobseg**, če je K podgrupa v $(L, +)$ in če je $K \setminus \{0\}$ podgrupa v $(L \setminus \{0\}, \cdot)$. Komutativen podobseg je **podpolje**.

Opomba: Na kratko povedano je $K \subseteq L$ podobseg v L, če je zaprta za odštevanje in deljenje.

Primeri podpolj

Očitno je $\mathbb{Q}$ podpolje polja $\mathbb{R}$ in $\mathbb{R}$ je podpolje polja $\mathbb{C}$.

Primer podpolja

Označimo s $\mathbb{Q}(\sqrt{3})$ množico vseh realnih števil oblike $a + b\sqrt{3}$, kjer $a, b \in \mathbb{Q}$. Pokažimo, da je $\mathbb{Q}(\sqrt{3})$ podpolje v $\mathbb{R}$.

Ker je

$$(a + b\sqrt{3}) - (c + d\sqrt{3}) = (a - c) + (b - d)\sqrt{3},$$

je množica $\mathbb{Q}(\sqrt{3})$ zaprta za odštevanje. Ker je

$$\frac{a + b\sqrt{3}}{c + d\sqrt{3}} = \frac{(a + b\sqrt{3})(c - d\sqrt{3})}{(c + d\sqrt{3})(c - d\sqrt{3})} = \frac{ac - 3bd}{c^2 - 3d^2} + \frac{bc - ad}{c^2 - 3d^2}\sqrt{3},$$

je množica $\mathbb{Q}(\sqrt{3}) \setminus \{0\}$ zaprta za deljenje. Pri tem smo upoštevali, da je $c + d\sqrt{3} \neq 0$ in $c^2 - 3d^2 \neq 0$, če $c \neq 0$ ali $d \neq 0$. V nasprotnem primeru bi namreč bilo $\sqrt{3}$ racionalno število.

Primer podpolja

Označimo s $\mathbb{Q}(\sqrt[3]{2})$ množico vseh realnih števil oblike $a + b\sqrt[3]{2} + c\sqrt[3]{4}$, kjer $a, b, c \in \mathbb{Q}$. Pokažimo, da je $\mathbb{Q}(\sqrt[3]{2})$ podpolje v $\mathbb{R}$.

Očitno je $\mathbb{Q}(\sqrt[3]{2})$ zaprta za odštevanje in množenje, torej je podkolobar. Pokazati je treba še, da za vsake $a, b, c \in \mathbb{Q}$, ki niso vsi nič, obstajajo taki $x, y, z \in \mathbb{Q}$, da je $(a + b\sqrt[3]{2} + c\sqrt[3]{4})^{-1} = x + y\sqrt[3]{2} + z\sqrt[3]{4}$. Treba je rešiti sistem $ax + 2cy + 2bz = 1$, $bx + ay + 2cz = 0$, $cx + by + az = 0$ z $\det \neq 0$.

Homomorfizmi obsegov in polj

Definicija homomorfizma obsegov

Homomorfizem obsegov je tak homomorfizem kolobarjev z enoto, ki slika iz obsega v obseg. Enako definiramo **homomorfizem polj**.

Opomba: Na dolgo povedano je homomorfizem polj iz polja $(K, +_K, \cdot_K)$ v polje $(L, +_L, \cdot_L)$ taka preslikava $f\colon K \to L$, ki za vsaka $x, y \in K$ zadošča $f(x +_K y) = f(x) +_L f(y)$ in $f(x \cdot_K y) = f(x) \cdot_L f(y)$ in tudi $f(1_K) = 1_L$.

Opomba: Definicijo homomorfizma polj iz polja $(K, +_K, \cdot_K)$ v polje $(L, +_L, \cdot_L)$ lahko povemo tudi takole: To je taka preslikava iz K v L, ki je homomorfizem grup iz $(K, +_K)$ v $(L, +_L)$ in iz $(K \setminus \{0\}, \cdot_K)$ v $(L \setminus \{0\}, \cdot_L)$.

Primer homomorfizma obsegov

Preslikava iz realnih števil v kvaternione, ki je definirana z

$$f(a) := \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$$

je homomorfizem obsegov.

Trditev

Vsak homomorfizem obsegov je injektiven.

Dokaz: Recimo, da je $f\colon K \to L$ homomorfizem obsegov in da je $f(a_1) = f(a_2)$ za neka $a_1, a_2 \in K$. Radi bi pokazali, da je $a_1 = a_2$. Označimo $a := a_1 - a_2$. Potem je $f(a) = f(a_1) - f(a_2) = 0_L$. Če $a_1 \neq a_2$, potem je $a \neq 0$, torej obstaja tak b iz K, da je $ab = 1_K$. Odtod sledi, da je $0_L = 0_L f(b) = f(a)f(b) = f(ab) = f(1_K) = 1_L$, kar je protislovje. Torej je res $a_1 = a_2$.

Opomba: Bijektivnemu homomorfizmu obsegov pravimo **izomorfizem obsegov**. Inverz izomorfizma obsegov je spet izomorfizem obsegov.

Opomba: Če je $f\colon K \to L$ homomorfizem obsegov, potem je $f(K)$ podobseg v L. Poleg tega je f bijektiven homomorfizem obsegov iz obsega K v obseg $f(K)$. Obsega K in $f(K)$ sta zato izomorfna. Torej lahko smatramo K za podobseg v L.

Kolobarji $\mathbb{Z}_n$ in $F[x]/(p)$

V tem razdelku bomo konstruirali dva tipa komutativnih kolobarjev, v nadaljevanju pa se bomo ukvarjali s tem, kdaj so ti kolobarji polja.

Kolobar $\mathbb{Z}_n$

Vzemimo neko naravno število n in označimo $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. Za vsaka $x, y \in \mathbb{Z}_n$ naj bo

$$x \oplus y := (x + y) \bmod n \quad \text{in} \quad x \odot y := (x \cdot y) \bmod n$$

kjer sta $+$ in $\cdot$ operaciji na $\mathbb{Z}$ in je $z \bmod n$ ostanek pri deljenju z z n. Trdimo, da je $(\mathbb{Z}_n, \oplus, \odot)$ komutativen in asociativen kolobar z enoto.

Komutativnost $\oplus$ in $\odot$ sledi direktno iz komutativnosti $+$ in $\cdot$. Pokažimo asociativnost $\oplus$. Vzemimo $x, y, z \in \mathbb{Z}_n$ in označimo $u = x \oplus y$ in $v = y \oplus z$. Vzemimo take $i, j, k, l \in \mathbb{N}$, da je

$$\begin{aligned} x + y &= in + u & \qquad u + z &= kn + (u \oplus z) \\ y + z &= jn + v & \qquad x + v &= ln + (x \oplus v) \end{aligned}$$

Odtod sledi

$$(x \oplus y) \oplus z = u \oplus z = u + z - kn = (x + y - in) + z - kn$$
$$x \oplus (y \oplus z) = x \oplus v = x + v - ln = x + (y + z - jn) - ln$$

torej je $(x \oplus y) \oplus z - x \oplus (y \oplus z) = (j + l - i - k)n$. Ker sta $(x \oplus y) \oplus z$ in $x \oplus (y \oplus z)$ med 0 in $n-1$ in ker je njuna razlika deljiva z n, sta enaka. Podobno dokažemo tudi asociativnost $\odot$ in distributivnost. Aditivna enota je 0, multiplikativna enota pa 1. Aditivni inverz elementa $x \neq 0$ je $n - x$.

Opomba: Preslikava

$$f : \mathbb{Z} \to \mathbb{Z}_n, \quad f(z) := z \bmod n$$

je homomorfizem kolobarjev z enoto iz $(\mathbb{Z}, +, \cdot)$ v $(\mathbb{Z}_n, \oplus, \odot)$.

Opomba: Če n ni praštevilo, potem kolobar $(\mathbb{Z}_n, \oplus, \odot)$ ni obseg. Iz razcepa $n = rs$, kjer $r, s < n$, namreč sledi, da je $r \odot s = 0$ in $r \neq 0$ in $s \neq 0$.

Konstrukcijo iz prejšnjega primera lahko razširimo tudi na polinome.

Kolobar $F[x]/(p)$

Naj bo F polje. Označimo s $F[x]$ množico vseh polinomov v spremenljivki x s koeficienti iz F. Običajno seštevanje in množenje polinomov označimo s $+$ in $\cdot$. Potem je $(F[x], +, \cdot)$ komutativen in asociativen kolobar z enoto.

Vzemimo nek nekonstanten polinom $p \in F[x]$ in označimo z $F[x]/(p)$ množico vseh polinomov iz $F[x]$, ki so nižje stopnje kot p. Za vsaka polinoma $r, s \in F[x]/(p)$ definirajmo polinoma

$$r \oplus s := r + s \quad \text{in} \quad r \odot s := (r \cdot s) \bmod p$$

kjer je $q \bmod p$ ostanek pri deljenju polinoma q s polinomom p.

Podobno kot v prejšnjem primeru pokažemo, da je $(F[x]/(p), \oplus, \odot)$ komutativen in asociativen kolobar z enoto.

Opomba: Preslikava

$$\phi\colon F[x] \to F[x]/(p), \quad \phi(q) := q \bmod p$$

je homomorfizem kolobarjev z enoto iz $(F[x], +, \cdot)$ v $(F[x]/(p), \oplus, \odot)$.

Definicija razcepnega in nerazcepnega polinoma

Polinom $p \in F[x]$ je **razcepen**, če obstajata taka polinoma $p_1, p_2 \in F[x]$ stopnje ≥ 1, da je $p = p_1 p_2$. Polinom, ki ni razcepen, je **nerazcepen**.

Opomba: Konstantni in linearni polinomi so nerazcepni.

Primer

Polinom $x^2 - 3$ leži tako v $\mathbb{Q}[x]$ kot v $\mathbb{R}[x]$. V $\mathbb{Q}[x]$ je nerazcepen, ker nima racionalne ničle. V $\mathbb{R}[x]$ je razcepen, ker velja $x^2 - 3 = (x + \sqrt{3})(x - \sqrt{3})$.

Opomba: Preslikavi $\phi\colon \mathbb{Q}[x]/(x^2 - 3) \to \mathbb{Q}(\sqrt{3})$, $\phi(q) = q(\sqrt{3})$ in $\psi\colon \mathbb{R}[x]/(x^2 - 3) \to \mathbb{R} \times \mathbb{R}$, $\psi(q) = (q(\sqrt{3}), q(-\sqrt{3}))$ sta izomorfizma kolobarjev. Ker je $\mathbb{Q}(\sqrt{3})$ polje, je tudi $\mathbb{Q}[x]/(x^2 - 3)$ polje. $\mathbb{R} \times \mathbb{R}$ ni polje.

Trditev

Če je polinom $p \in F[x]$ razcepen, potem kolobar $(F[x]/(p), \oplus, \odot)$ ni obseg.

Dokaz je podoben kot pri $\mathbb{Z}_n$. Če je p razcepen v $F[x]$, potem obstajata taka neničelna polinoma $p_1, p_2 \in F[x]/(p)$, da je $p_1 \odot p_2 = 0$.

Linearna diofantska enačba

V dokazu glavnega izreka bomo potrebovali naslednji tehnični rezultat.

Izrek o linearni diofantski enačbi

Če sta celi števili a_1 in a_2 tuji (= njun največji skupni delitelj je 1), potem obstajata taki celi števili x in y, da velja $a_1 x + a_2 y = 1$.

Dokaz: Brez škode lahko predpostavimo, da sta a_1 in a_2 naravni števili. Po izreku o deljenju z ostankom obstajajo taka naravna števila $k_1, \ldots, k_n$ in $a_3, \ldots, a_{n+1}$, da velja:

$$a_1 = k_1 a_2 + a_3 \quad \text{kjer } a_3 < a_2 \tag{1}$$

$$a_2 = k_2 a_3 + a_4 \quad \text{kjer } a_4 < a_3 \tag{2}$$

$$\vdots$$

$$a_{n-1} = k_{n-1} a_n + a_{n+1} \quad \text{kjer } a_{n+1} < a_n \tag{n-1}$$

$$a_n = k_n a_{n+1} \tag{n}$$

Postopek smo nadaljevali toliko časa, dokler ni ostanek padel na nič. Ker se ostanek v vsakem koraku zmanjša, je korakov samo končno mnogo.

Pokažimo najprej, da je $a_{n+1} = 1$. Iz enačbe (n) sledi, da a_{n+1} deli a_n Odtod in iz enačbe (n-1) sledi, da a_{n+1} deli a_{n-1}. Odtod in iz enačbe (n-2) sledi, da a_{n+1} deli a_{n-2}. Ta postopek nadaljujemo, dokler ne pridemo do prve enačbe. Torej a_{n+1} deli tako a_1 kot a_2. Ker sta a_1 in a_2 tuji, odtod sledi, da je $a_{n+1} = 1$.

Pokažimo sedaj, da za vsako naravno število $m = 1, \ldots, n$ obstajata taki celi števili x_m in y_m, da velja

$$a_1 x_m + a_2 y_m = a_{m+1}. \qquad (*)$$

Pri $m = 1$ lahko vzamemo kar $x_1 = 0$ in $y_1 = 1$. Iz enačbe (1) sledi $a_3 = a_1 - k_2 a_2$, torej lahko vzamemo $x_2 = 1$ in $y_2 = -k_2$. Izpeljimo sedaj še rekurzivni zvezi za x_m in y_m. Iz enačbe (m-1) sledi, da je $a_{m+1} = a_{m-1} - k_{m-1} a_m$, kar je po indukcijski predpostavki enako $(a_1 x_{m-2} + a_2 y_{m-2}) - k_{m-1}(a_1 x_{m-1} + a_2 y_{m-1})$. Če to primerjamo z željeno relacijo $(*)$, dobimo $x_m = x_{m-2} - k_{m-1} x_{m-1}$ in $y_m = y_{m-2} - k_{m-1} y_{m-1}$. Ko je m enak n, dobimo ravno izrek: $a_1 x_n + a_2 y_n = a_{n+1} = 1$. $\square$

Naš glavni rezultat je:

Izrek o $\mathbb{Z}_p$

Če je p praštevilo, potem je kolobar $\mathbb{Z}_p$ polje.

Dokaz. Vemo že, da je $\mathbb{Z}_p$ komutativen in asociativen kolobar z enoto. Pokazati moramo še, da ima vsak neničelni element multiplikativen inverz. Vzemimo $a_2 = p$ in naj bo a_1 poljuben neničeln element v $\mathbb{Z}_p$. Vidimo, da sta a_1 in a_2 tuji števili. Po izreku o linearni diofantski enačbi obstajata taki celi števili x in y, da je $a_1 x + a_2 y = 1$. Odtod sledi, da je $a_1^{-1} = x \bmod p$.

Podobno dokažemo tudi naslednji rezultat:

Izrek o $F[x]/(p)$

Če je $p \in F[x]$ nerazcepen polinom stopnje ≥ 1, potem je $F[x]/(p)$ polje.

Dokaz: Dva polinoma sta tuja, če nimata skupnega faktorja stopnje ≥ 1. Če vzamemo $p_2 = p$ iz izreka in $p_1 \neq 0$ polinom, ki je nižje stopnje kot p, potem sta p_1 in p_2 tuja. Za vsaka tuja polinoma p_1 in p_2 konstruramo kot zgoraj taka polinoma q_1 in q_2, da je $p_1 q_1 + p_2 q_2 = 1$ in dobimo izrek.

Primer

Poiščimo inverz elementa 12 v polju $\mathbb{Z}_{41}$.

Iščemo tak $x \in \mathbb{Z}$, da je $12x \bmod 41 = 1$. To velja natanko tedaj, ko obstaja tak $y \in \mathbb{Z}$, da velja $12x + 41y = 1$. Evklidov algoritem nam da

$$\begin{aligned} 41 &= 3 \cdot 12 + 5 &\quad\Rightarrow\quad& 5 = 41 - 3 \cdot 12 \\ 12 &= 2 \cdot 5 + 2 &\quad\Rightarrow\quad& 2 = 12 - 2 \cdot 5 \\ 5 &= 2 \cdot 2 + 1 &\quad\Rightarrow\quad& 1 = 5 - 2 \cdot 2 \end{aligned}$$

Ko vstavimo prvo enačbo v drugo, dobimo

$$2 = 12 - 2 \cdot (41 - 3 \cdot 12) = -2 \cdot 41 + 7 \cdot 12$$

Ko to in prvo enačbo vstavimo v tretjo enačbo, dobimo

$$1 = (41 - 3 \cdot 12) - 2 \cdot (-2 \cdot 41 + 7 \cdot 12) = 5 \cdot 41 + (-17) \cdot 12$$

Torej je $x = -17$, kar pa ni v $\mathbb{Z}_{41}$. Sledi $12^{-1} = x \bmod 41 = 24$.

Primer

Izračunajmo inverz polinoma $x^3 - 2x + 2$ v polju $\mathbb{Q}[x]/(x^4+1)$.

Najprej uporabimo Evklidov algoritem

$$\begin{aligned} x^4 + 1 &= x(x^3 - 2x + 2) + 2x^2 - 2x + 1 \\ x^3 - 2x + 2 &= \frac{x+1}{2}(2x^2 - 2x + 1) + \frac{3-3x}{2} \\ 2x^2 - 2x + 1 &= -\frac{4x}{3}\left(\frac{3-3x}{2}\right) + 1 \end{aligned}$$

Iz prve enačbe dobimo

$$2x^2 - 2x + 1 = (x^4 + 1) - x(x^3 - 2x + 2)$$

Iz druge enačbe potem dobimo

$$\begin{aligned} \frac{3-3x}{2} &= (x^3 - 2x + 2) - \frac{x+1}{2}(2x^2 - 2x + 1) \\ &= (x^3 - 2x + 2) - \frac{x+1}{2}((x^4 + 1) - x(x^3 - 2x + 2)) \\ &= -\frac{x+1}{2}(x^4 + 1) + \frac{x^2 + x + 2}{2}(x^3 - 2x + 2) \end{aligned}$$

Upoštevajmo sedaj oba izraza v tretji enačbi. Dobimo

$$\begin{aligned}1 &= (2x^2-2x+1)+\frac{4x}{3}\left(\frac{3-3x}{2}\right)\\ &= ((x^4+1)-x(x^3-2x+2))\\ &\quad + \frac{4x}{3}\left(-\frac{x+1}{2}(x^4+1)+\frac{x^2+x+2}{2}(x^3-2x+2)\right)\\ &= \frac{3-2x(x+1)}{3}(x^4+1)+\frac{-3x+2x(x^2+x+2)}{3}(x^3-2x+2)\end{aligned}$$

Inverz polinoma x^3-2x+2 v $\mathbb{Q}[x]/(x^4+1)$ je torej

$$\frac{-3x+2x(x^2+x+2)}{3}=\frac{2x^3+2x^2+x}{3}.$$

Produkt polinoma in njegovega inverza je res enak 1 v $\mathbb{Q}[x]/(x^4+1)$, ker

$$\frac{2x^3+2x^2+x}{3}(x^3-2x+2)=\frac{2x^2+2x-3}{3}(x^4+1)+1.$$

Polja s p^n elementi

Radi bi opisali vsa končna polja. Ideja konstrukcije je naslednja:

- Vzemi praštevilo p in naravno število n. Vemo, da je $\mathbb{Z}_p$ polje.
- Dokaži, da v $\mathbb{Z}_p[x]$ obstaja nerazcepen polinom $q(x)$ stopnje n.
- Dokaži, da je $\mathbb{Z}_p[x]/(q(x))$ polje s p^n elementi.

Izrek o klasifikaciji končnih obsegov pravi:

- Vsako končno polje je izomorfno enemu od zgornjih polj.
- Dve končni polji z enakim številom elementov sta izomorfni.

Podrobnosti bomo izpustili. Raje si oglejmo primer.

Polje s štirimi elementi

Iščemo polje, ki ima štiri elemente. Kolobar $\mathbb{Z}_4$ sicer ima štiri elemente, ampak ni polje. Iskano polje je $\mathbb{Z}_2[x]/(x^2+x+1)$.

Množica $\mathbb{Z}_2[x]/(x^2+x+1)$ se sestoji iz vseh polinomov v $\mathbb{Z}_2[x]$, ki so nižje stopnje kot x^2+x+1. To so polinomi $0, 1, x, x+1$.

Operaciji na množici $\mathbb{Z}_2[x]/(x^2+x+1)$ sta seštevanje in množenje modulo x^2+x+1. Njuni tabeli sta:

$\oplus$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\odot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Pokazali smo že, da je $(\mathbb{Z}_2[x]/(x^2+x+1), \oplus, \odot)$ komutativen in asociativen kolobar z enoto. Iz tabele za $\odot$ se vidi, da ima vsak neničeln element inverz. Torej je ta kolobar polje.

Opomba: Tudi brez tabele za $\odot$ lahko dokažemo, da je ta kolobar polje. Zadošča dokazati, da je $x^2 + x + 1$ nerazcepen polinom v $\mathbb{Z}_2[x]$.

V $\mathbb{Z}_2[x]$ imamo dva polinoma stopnje 1 in štiri polinome stopnje 2. Polinoma stopnje 1 sta x in $x + 1$. Razcepni polinomi stopnje 2 so torej x^2, $x(x + 1) = x^2 + x$ in $(x + 1)^2 = x^2 + 1$. Polinom $x^2 + x + 1$ ni eden od teh, torej je nerazcepen.