Algebra I

Fyrirlestrar Reynis Axelssonar

Hörður Freyr Yngvason

Haustönn 2009

Efnisyfirlit

Hluti I

Einfaldir hlutir úr einfaldari talnafræði

Kafli 1

Inngangsefni

1.1 Deilanleiki

Táknum með $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ mengi allra náttúrlegu talnanna og með $\mathbb{Z} = \{n \in \mathbb{R} : n \in \mathbb{N}, -n \in \mathbb{N}\}$. Látum $a, b, \in \mathbb{Z}$. Við segjum að talan a *gangi upp í* tölunni b ef til er heiltala c þ.a. $b = ac$ og við skrifum þá

$$a \mid b.$$

Látum $m \in \mathbb{Z}$; við setjum

$$m\mathbb{Z} := \{nm : n \in \mathbb{Z}\}.$$

Eftirfarandi skilyrði eru jafngild:

(i) $a \mid b$,

(ii) $b \in a\mathbb{Z}$,

(iii) $b\mathbb{Z} \subset a\mathbb{Z}$.

Setning 1.1 (Einfaldari reglur). (1) Fyrir öll $a \in \mathbb{Z}$ er $1 \mid a$ og $-1 \mid a$. Ef $a \mid 1$, þá er $a = 1$ eða $a = -1$.

(2) Ef $a \in \mathbb{Z}$, þá $a \mid 0$. Ef $0 \mid a$ þá er $a = 0$.

(3) Ef $a \mid b$ og $b \mid c$ þá $a \mid c$.

(4) Ef $a \mid b$ og $b \mid a$, þá er $a = b$ eða $a = -b$.

(5) Fyrir öll $a \in \mathbb{Z}$ er $a \mid a$.

(6) Ef $a \mid b$ og $a \mid c$ þá

$$a \mid nb + mc$$

fyrir öll $n, m \in \mathbb{Z}$.

Sönnun. Er auðveld. ∎

Setning 1.2 (Um deilingu með afgangi). Látum $m \in \mathbb{Z}, m \geq 1$. Fyrir sérhverja tölu n eru til heilar tölur q, r þ.a.

$$n = qm + r \qquad \text{og} \qquad 0 \leq r < m.$$

Tölurnar q og r ákvarðast ótvírætt af þessum skilyrðum.

Til að sanna þetta notum við:

Setning 1.3 (Um minnsta stak). Ef A er hlutmengi í $\mathbb{N}$ og $A \neq \emptyset$ þá hefur A minnsta stak, þ.e. til er stak $a \in A$ þ.a. $a \leq x$ fyrir öll $x \in A$.

Gefum okkur þetta án sönnunar!

Sönnun (Sönnun á setningu 1.2). Látum $n, m \in \mathbb{Z}, m \geq 1$. Setjum

$$A := \{x \in \mathbb{N} : \text{Til er } q \in \mathbb{Z} \text{ þ.a. } x = n - qm\}.$$

Þá er $A \neq \emptyset$, því að $n + m = n - (-1)m \in \mathbb{N}$ og því $n + m \in A$. Þar með hefur A minnsta stak r; og til er $q \in \mathbb{Z}$ þ.a. $r = n - qm$. Þá er $0 \leq r < m$: Vegna $r \in \mathbb{N}$ er $r \geq 0$; ef við hefðum $r \geq m$ þá væri $r_1 = r - m \geq 0$ og þá er $r_1 \in \mathbb{N}$, ef q er þ.a. $r = n - qm, q \in \mathbb{Z}$, þá er $r_1 = n - qm - m = n - (q+1)m$, svo að $r_1 \in A$, $0 \leq r_1 < r$ í mótsögn við skilgreiningu.

Ótvíræðni: Ef $n = qm + r = q_1 m + r_1$ þar sem $q, q_1 \in \mathbb{Z}, r, r_1 \in \mathbb{Z}, 0 \leq r < m, 0 \leq r_1 < m$, þá er $r - r_1 \in \mathbb{Z}, -m < r - r_1 < m$. En $r - r_1 = (q_1 - q)m$, og eina heila margfeldið af m sem er stærra en $-m$ og minna en m er 0, svo að $r - r_1 = 0$. En þá er $(q_1 - q)m = r - r_1 = 0$, svo að $q - q_1 = 0$. Því er $r_1 = r$ og $q_1 = q$. ∎

Setning 1.4. Látum A vera hlutmengi í $\mathbb{Z}$ þ.a. eftirfarandi tveimur skilyrðum sé fullnægt:

(i) $A \neq \emptyset$

(ii) Ef $x, y \in A$, þá er $x - y \in A$.

Þá er til nákvæmlega ein náttúrleg tala m þ.a. $a = m\mathbb{Z}$.

Sönnun. Athugum: Þar sem $A \neq \emptyset$ hefur A stak x; skv. (ii) er þá $0 = x - x \in A$. Höfum þá líka: Ef $x \in A$, þá er $-x = 0 - x \in A$. Ef $x, y \in A$ þá er $-y \in A$ og því $x + y = x - (-y) \in A$. Fáum nú: Ef $x \in A$, þá er $2x = x + x \in A$ svo að $3x = 2x + x \in A$, $4x = 3x + x \in A$ og með þrepun fæst $nx \in A$ fyrir öll $n \in \mathbb{N}$. Þá er líka $(-n)x = -nx \in A$ fyrir öll $n \in \mathbb{N}$. Höfum því sýnt: Ef $x \in A$, þá er $x\mathbb{Z} \subset A$. Fyrir $x \in A$ er $-x \in A$ og annaðhvort er $x \geq 0$ eða $-x \geq 0$ svo að $x \in \mathbb{N}$ eða $-x \in \mathbb{N}$. Ef $A = \{0\}$, þá er $A = 0\mathbb{Z}$. Gerum ráð fyrir að $A \neq \{0\}$. Þá er

$$A \cap \mathbb{N} \neq \emptyset.$$

En þá hefur $A \cap \mathbb{N}$ minnsta stak m. Höfum sýnt að $m\mathbb{Z} \subset A$. Látum nú $n \in A$. Skv. setningu um deilingu með afgangi eru til heilar tölur q, r þ.a. $n = qm + r$ og $0 \leq r < m$. En $n \in A$, og $m \in A$ og því $qm \in A$, svo að $r = n - qm \in A$ og $r \geq 0$ svo að $r \in A \cap \mathbb{N}, r < m$. Þetta er í mótsögn við skilgreiningu á m nema $r = 0$. Því verður $r = 0$ að gilda, svo að $n = qm \in m\mathbb{Z}$. Höfum þá að $A \subset m\mathbb{Z}$ og $m\mathbb{Z} \subset A$ svo að $A = m\mathbb{Z}$.

Ef $A = m\mathbb{Z} = m_1\mathbb{Z}$ með $m, m_1 \in \mathbb{Z}$, þá $m \mid m_1$ og $m_1 \mid m$ svo $m = m_1$ eða $m = -m_1$, en $m_1 \geq 0$ svo $m = m_1$. ∎

Látum $a, b \in \mathbb{Z}$ og setjum

$$A := a\mathbb{Z} + b\mathbb{Z} = \{aj + bk : j, k \in \mathbb{Z}\}$$

Þá fullnægir mengið A skilyrðunum (i) og (ii); (i) er augljóst og ef $x = aj + bk$ og $y = aj_1 + bk_1$ þá er $x - y = a(j - j_1) + b(k - k_1) \in A$. Þar með er til nákvæmlega ein náttúrleg tala d þ.a.

$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}.$$

Höfum $a\mathbb{Z}, b\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. Fáum:

(i) $d \mid a$ og $d \mid b$.

(ii) Ef $c \mid a$ og $c \mid b$ þá $c \mid d$.

Eiginleiki (i) er augljós af $a\mathbb{Z} \subset d\mathbb{Z}$ og $b\mathbb{Z} \subset d\mathbb{Z}$. Ef $c \mid a$ og $c \mid b$, þá er $a\mathbb{Z} \subset c\mathbb{Z}$ og $b\mathbb{Z} \subset c\mathbb{Z}$. Þá er ljóst að

$$d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} \subset c\mathbb{Z}$$

svo að $c \mid d$. Líka: Ef d_1 fullnægir:

(i') $d_1 \mid a$ og $d_1 \mid b$.

(ii') Ef $c \mid a$ og $c \mid b$ þá $c \mid d_1$.

þá gefa (i) og (ii') að $d \mid d_1$ og (i') og (ii) að $d_1 \mid d$; ef d og d_1 eru bæði í $\mathbb{N}$ þá fæst $d = d_1$. M.ö.o. d er *eina* náttúrlega talan sem fullnægir skilyrðunum (i) og (ii).

1.2 Stærsti samdeilir

Skilgreining 1.1. Látum $a, b \in \mathbb{Z}$. Náttúrlega talan d sem fullnægir (i) og (ii) kallast *stærsti samdeilir* a og b; og er táknuð

$$\mathrm{ssd}(a, b).$$

Hjálparsetning 1.1. Látum $a, b, q, r \in \mathbb{Z}$ vera þ.a.

$$a = bq + r.$$

Þá er

$$\mathrm{ssd}(a, b) = \mathrm{ssd}(b, r)$$

Sönnun. Ef $c \mid a$ og $c \mid b$, þá $c \mid r$ vegna $r = a - bq$. Eins ef $c \mid b$ og $c \mid r$, þá $c \mid a$. Höfum því

$$(c \mid a \text{ og } c \mid b) \text{ þ.þ.a.a. } (c \mid b \text{ og } c \mid r)$$ ∎

Athugasemd. Ef $a, b \in \mathbb{N}$ og $a \mid b, b \neq 0$, þá er $a \leq b$. Ef önnur talnanna a, b er núll, þá er stærsti samdeilirinn algildi hinnar tölunnar. Sér í lagi er $\mathrm{ssd}(0, 0) = 0$. Það er því ljóst hver stærsti samdeilirinn er nema hvorug talnanna sé núll. Líka er $a\mathbb{Z} = (-a)\mathbb{Z}$, svo

$$\mathrm{ssd}(-a, b) = \mathrm{ssd}(a, -b) = \mathrm{ssd}(-a, -b) = \mathrm{ssd}(a, b).$$

Þurfum bara að finna stærsta samdeili *jákvæðu* talnanna.

Setning 1.5 (Reiknirit Evklíðs). Látum $a, b \in \mathbb{Z}$, $0 < b < a$. Deilum b upp í a með afgangi:

$$a = bq_1 + r_1, \qquad 0 \leq r_1 < b;$$

deilum r_1 upp í b með afgangi:

$$b = r_1 q_2 + r_2, \qquad 0 \leq r_2 < r_1;$$

deilum r_2 upp í r_2 með afgangi:

$$r_1 = r_2 q_3 + r_3$$

o.s.frv. Deilum almennt r_{k+1} upp í r_k með afgangi, fáum

$$r_k = r_{k+1}q_{q+2} + r_{k+2}, \qquad 0 \leq r_{k+2} < r_{k+1}$$

meðan r_k verður ekki núll. Fáum stranglega fallandi runu (r_k) af náttúrlegum tölum; hún endar með að við fáum $r_{k+1} = 0$. Þá er

$$\mathrm{ssd}(a, b) = r_k.$$

Sönnun. Skv. hjálparsetningu er

$$\mathrm{ssd}(a, b) = \mathrm{ssd}(b, r_2) = \mathrm{ssd}(r_1, r_2) = \mathrm{ssd}(r_2, r_3) = \cdots = \mathrm{ssd}(r_k, r_{k+1}) = \mathrm{ssd}(r_k, 0) = r_k.$$

■

Athugasemd. Látum $d = \mathrm{ssd}(a, b)$. Það þýðir að $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. Sér í lagi hefur jafnan

$$ax + by = d$$

lausn í heilum tölum x og y. Þessi jafna kallast *Bézout-jafnan* fyrir a og b. Með því að „fara afturábak“ gegnum reiknirit Evklíðs fæst *ein* lausn á Bézout-jöfnunni.

Dæmi 1.1. Reiknum stærsta samdeili talnanna 75 og 261:

$$\begin{aligned} 261 &= 3 \cdot 75 + 36 \\ 75 &= 2 \cdot 36 + 3 \\ 36 &= 3 \cdot 12 + 0, \end{aligned}$$

Svo stærsti samdeilirinn er 3. Höfum þá:

$$\begin{aligned} 75 &= 2 \cdot 36 + 3, \\ 261 &= 3 \cdot 75 + 36, \end{aligned}$$

það gefur:

$$\begin{aligned} 3 &= 75 - 36 \cdot 2 \\ &= 75 - (261 - 3 \cdot 75) \cdot 2 \\ &= 75 \cdot 7 - 261 \cdot 2, \end{aligned}$$

svo að $x = 7, y = -2$ er ein lausn Bézout-jöfnunnar

$$75x + 261y = 3.$$

□

Skilgreining 1.2. Segjum að heilu tölurnar a, b séu *ósamþátta* ef $\text{ssd}(a, b) = 1$.

Athugasemd. Tölurnar a, b eru ósamþátta þ.þ.a.a. jafnan

$$ax + by = 1$$

hafi lausn í heilum tölum x, y. Almennt hefur jafna

$$ax + by = c$$

lausn í heilum tölum þ.þ.a.a. $\text{ssd}(a, b) \mid c$.

1.3 Frumtölur

Skilgreining 1.3. *Frumtala* er náttúrleg tala $p > 1$ þ.a. engin náttúrleg tala gangi upp í p nema 1 og p.

Athugasemd. Tölurnar sem ganga upp í frumtölu p eru þá $1, p, -1$ og $-p$.

Hjálparsetning 1.2 (Hjálparsetning Evklíðs). Ef p er frumtala, a og b eru heilar tölur og $p \mid ab$, þá $p \mid a$ eða $p \mid b$.

Sönnun. Gerum ráð fyrir að $p \mid ab$ en að p gangi ekki upp í a, þá er $\text{ssd}(p, a) = 1$, því að $\text{ssd}(p, a)$ gengur upp í p, er því 1 eða p en getur ekki verið p. Þar með eru til heilar tölur x og y þ.a.

$$px + ay = 1.$$

En þá er $b = p(bx) + ab \cdot y$, og $p \mid ab$, svo að $p \mid b$. ∎

Skilgreining 1.4. Látum $n \in \mathbb{N}, n \geq 1$. *Frumþáttun* tölunnar er að skrifa n sem margfeldi

$$n = p_1 \cdots p_r$$

þar sem $p_1, \ldots, p_r$ eru frumtölur, sem kallast þá *frumþættir* frumþáttunarinnar.

Leyfum $r = 1$, þá er n frumtala; þægilegt er að leyfa $r = 0$ með því samkomulagi að $\prod_{k=1}^{0} p_k = 1$. Þá má segja:

Setning 1.6 (Undirstöðusetning reikningslistarinnar). Sérhver náttúrleg tala n þ.a. $n \geq 1$ hefur frumþáttun og frumþættirnir ákvarðast ótvírætt burtséð frá röð.

Skilgreining 1.5. Getum því kallað þá frumþætti *tölunnar* n.

Setning 1.7 (Evklíð). Til eru óendanlega margar frumtölur.

Sönnun. Gerum ráð fyrir að þær séu endanlega margar, segjum $p_1, \ldots, p_r$. Setjum

$$x := p_1 \cdots p_r + 1.$$

Nú er til frumtala p sem gengur upp í x. En $p \neq p_j$ fyrir $j = 1, \ldots, r$: Ef $p_j \mid x$ þá gengi p_j upp í $x - p_1 \cdots p_r = 1$. ∎

Sönnun (á undirstöðusetningu reikningslistarinnar). (1) Tala $n \geq 1$ hefur frumþáttun. Annars væri til *minnsta* tala n sem hefur ekki frumþáttun. Hún er þá ekki talan 1 og ekki frumtala og því má skrifa $n = km$, þar sem k, m eru náttúrlegar tölur ólíkar n og 1; en þá eru $k, m < n$ og því hafa k og m frumþáttanir $k = p_1 \cdots p_r$ og $m = q_1 \cdots q_s$, en þá er

$$n = p_1 \cdots p_r \cdot q_1 \cdots q_s$$

frumþáttun á n; mótsögn.

(2) Látum $n = p_1 \cdots p_r = q_1 \cdots q_s$ vera frumþáttanir. Þá gildir $p_r \mid q_1 \cdots q_s$; skv. hjálparsetningu Evklíðs og þrepun, þá gengur p_r upp í einni af tölunum $q_1, \ldots, q_s$. Með því að breyta um röð á $q_1, \ldots, q_s$ má gera ráð fyrir að $p_r \mid q_s$. En q_s er frumtala, $p_r > 1$, svo að $p_r = q_s$. En þá er $p_1 \cdots p_{r-1} = q_1 \cdots q_{s-1}$. Með þrepun sést að $r - 1 = s - 1$ og $p_1, \ldots, p_{r-1}$ eru tölurnar $q_1, \ldots, q_{s-1}$. En þá er $r = s$ og $p_1, \ldots, p_r$ og $q_1, \ldots, q_s$ eru sömu tölurnar, en hugsanlega í annarri röð. ∎

Látum $a \in \mathbb{Z}$ og $m \in \mathbb{N}, m \geq 1$. Skrifum

$$a \bmod m$$

fyrir afganginn sem fæst þegar við deilum m upp í a; m.ö.o. ef $a = mq + r$ og $0 \leq r < m$; þá er

$$a \bmod m := r.$$

Athugasemd. Í kennslubók stendur (bls. 9):

> When $a = qn+r$, where q is the quotitent and r is the remainder upon dividing a by n, we write $a \bmod n = r$ ~~or $a \equiv r \bmod n$~~ [1].

Hins vegar:

1.4 Samleifing, mátreikningur

Skilgreining 1.6. Látum $m \in \mathbb{N}, m \geq 1$, og $a, b, \in \mathbb{Z}$. Við skrifum

$$a \equiv b \pmod{m} \tag{1.1}$$

ef $m \mid a - b$ og segjum að a og b séu *samleifa* m.t.t. m (eða *mátað við* m); fullyrðingin (1.1) kallast *samleifing*.

Athugasemd. Höfum $a \equiv b \pmod{m}$ þ.þ.a.a. $a \bmod m = b \bmod m$.

Athugasemd. Ef $a \equiv b \pmod{m}$ þá segjum við að a og b séu *leifar* hvors annars m.t.t. m; *leifar* tölunnar a m.t.t. m eru allar tölur b þ.a. $a \equiv b \pmod{m}$, og afgangurinn $a \bmod m$ er sú leif r sem fullnægir $0 \leq r < m$.

Setning 1.8 (Reiknireglur). Látum $m \in \mathbb{N}$, $m \geq 1$ og $a, b, c, d \in \mathbb{Z}$.

(1) $a \equiv a \pmod{m}$

(2) Ef $a \equiv b \pmod{m}$, þá er $b \equiv a \pmod{m}$.

(3) Ef $a \equiv b \pmod{m}$ og $b \equiv c \pmod{m}$, þá er $a \equiv c \pmod{m}$.

(4) Ef $a \equiv c \pmod{m}$ og $b \equiv d \pmod{m}$, þá er

$$\begin{aligned} a + b &\equiv c + d \pmod{m}, \\ a - b &\equiv c - d \pmod{m}, \\ ab &\equiv cd \pmod{m} \end{aligned}$$

og fyrir allar náttúrlegar tölur n er

$$a^n \equiv c^n \pmod{m}.$$

(5) Ef $a \equiv b \pmod{m}$ og $d \in \mathbb{N}$ þannig að $d \mid m$ þá er

$$a \equiv b \pmod{d}.$$

[1] Við munum ekki nota yfirstrikaða hlutann, hunsum hann

Sönnun. Er einföld; t.d. fæst þriðja reglan í (4) með

$$ab - cd = ab - cb + cb - cd = (a - c)b + c(b - d).$$ ∎

Liðir (1)-(3) segja að samleifing sé dæmi um *jafngildisvensl*.

Skilgreining 1.7. *Vensl* R á mengi X er mengi af tvenndum (x, y), þar sem $x, y \in X$; m.ö.o. er $R \subset X \times X$. Við skrifum xRy í stað $(x, y) \in R$.

Venja er að nota sérstök tákn fyrir vensl í stað bókstafa. Samleifing $(\mathrm{mod}\ m)$ skilgreinir vensl á $\mathbb{Z}$. Sem mengi eru venslin $\{(a, b) \in \mathbb{Z} \times \mathbb{Z} : a \equiv b\ (\mathrm{mod}\ m)\}$.

Skilgreining 1.8. Látum X vera mengi. *Jafngildisvensl* á menginu X eru vensl á X þ.a. eftirfarandi þremur skilyrðum sé fullnægt:

(i) $x \sim x$ fyrir öll $x \in X$.

(ii) Ef $x \sim y$, þá er $y \sim x$.

(iii) Ef $x \sim y$ og $y \sim z$, þá er $x \sim z$.

Skilgreining 1.9. Látum X vera mengi. *Deildaskipting* mengisins X er mengi $\mathcal{D}$ af hlutmengjum í X sem eru ekki tóm þ.a. sérhvert stak í X sé innihaldið í *nákvæmlega einu* af mengjunum sem eru stök í $\mathcal{D}$; köllum stökin í $\mathcal{D}$ *deildir* deildaskiptingarinnar. Þetta þýðir:

(i) Ef $A \in \mathcal{D}$, þa er $\emptyset \neq A \subset X$.

(ii) Ef $A, B \in \mathcal{D}$, $A \neq B$, þá er $A \cap B = \emptyset$.

(iii) $X = \bigcup_{A \in \mathcal{D}} A$.

Skilgreining 1.10. Látum nú $\sim$ vera jafngildisvensl á mengi X og $x \in X$. Mengið

$$[x] := \{y \in X : x \sim y\}$$

kallast *jafngildisflokkur* staksins x með tilliti til jafngildisvenslanna $\sim$.

Setning 1.9. Látum $\sim$ vera jafngildisvensl á mengi X. Þá mynda jafngildisflokkarnir deildaskiptingu á X. Fyrir sérhverja deildaskiptingu $\mathcal{D}$ mengisins X eru til nákvæmlega ein jafngildisvensl $\sim$ á X þ.a. $\mathcal{D}$ sé mengi jafngildisflokkanna með tilliti til $\sim$.

Sönnun. (1) Látum $\sim$ vera jafngildisvensl á X. Höfum $x \sim x$ svo að $x \in [x]$ og því er $[x] \neq \emptyset$. G.r.f. að $x, y \in X$ og $[x] \cap [y] \neq \emptyset$ og veljum z úr $[x] \cap [y]$. Ef $t \in [x]$, þá er $x \sim t$; en líka er $x \sim z$ og $y \sim z$. Af $x \sim z$ leiðir $z \sim x$. Af $y \sim z$ og $z \sim x$ leiðir $y \sim x$. Af $y \sim x$ og $x \sim t$ leiðir $y \sim t$. Því er $t \in [y]$. Höfum sýnt að $[x] \subset [y]$. Af samhverfuástæðum er líka $[y] \subset [x]$, og því $[x] = [y]$. Vegna $x \in [x]$ er X sammengi allra flokkanna.

(2) Látum $\mathcal{D}$ vera deildaskiptingu mengisins X. Skrfium $x \sim y$ þ.þ.a.a. x og y séu í sömu deild skiptingarinnar. Þá er ljóst að $\sim$ eru jafngildisvensl og að jafngildisflokkarnir eru deildir $\mathcal{D}$. ∎

Dæmi 1.2. Jafngildisflokkur heillar tölu a m.t.t. jafngildisvenslanna $? \equiv ? \pmod{m}$ er mengið

$$a + m\mathbb{Z} = \{a + mk : k \in \mathbb{Z}\},$$

sem er mengi allra heilla talna sem eru samleifa $a \pmod{m}$. Jafngildisflokkarnir eru m talsins, nefnilega

$$0 + m\mathbb{Z}, 1 + m\mathbb{Z}, 2 + m\mathbb{Z}, \ldots, (m-1) + m\mathbb{Z}.$$

Þeir kallast *leifaflokkarnir* $\pmod{m}$. □

Hluti II

Grúpur

Kafli 2

Grúpur

2.1 Reikniaðgerðir

Skilgreining 2.1. *Reikniaðgerð* á mengi X er vörpun $X \times X \to X$. Reikniaðgerðir eru (eins og vensl) táknaðar með sérstökum táknum eins og „ $\cdot$ “ eða „+“. Ef $\top$ er reikniaðgerð á X þá skrifum við

$$x \top y \qquad \text{í stað} \qquad \top(x, y).$$

Reikniaðgerð $\top$ á X kallast *tengin* ef

$$(x \top y) \top z = x \top (y \top z)$$

fyrir öll $x, y, z \in X$. Hún kallast *víxlin* ef

$$x \top y = y \top x$$

fyrir öll $x, y \in X$. Stak e í X kallast *hlutleysa* fyrir $\top$ ef

$$x \top e = e \top x = x$$

fyrir öll $x \in X$.

Setning 2.1. Reikniaðgerð getur ekki haft nema eina hlutleysu.

Sönnun. Ef e og e' eru hlutleysur fyrir aðgerð $\top$, þá er

$$e = e \top e' = e'.$$

■

Skilgreining 2.2. Látum $\top$ vera reikniaðgerð með hlutleysu e á mengi X og $x \in X$. Stak x' í X kallast *umhverfa* staksins x m.t.t. $\top$ ef

$$x \top x' = x' \top x = e.$$

Setning 2.2. Látum $\top$ vera *tengna* reikniaðgerð með hlutleysu e á mengi X. Stak úr X hefur í hæsta lagi eina umhverfu m.t.t. $\top$.

Sönnun. Látum x' og x'' vera umhverfur staksins x m.t.t. $\top$. Þá er

$$x' = x' \top e = x' \top (x \top x'') = (x' \top x) \top x'' = e \top x'' = x''. \qquad \blacksquare$$

2.2 Grúpur

Skilgreining 2.3. *Grúpa* er mengi G með reikniaðgerð á G þ.a. aðgerðin sé tengin, hafi hlutleysu og þ.a. sérhvert stak í G hafi umhverfu m.t.t. aðgerðarinnar.

Grúpa kallast *víxlin* ef aðgerð hennar er víxlin, og grúpan kallast þá líka *víxlgrúpa* eða *Abelgrúpa*.

Athugasemd (um rithátt). Þótt reikniaðgerðir séu ofboðslega margar, þá eru þær flestar táknaðar með annaðhvort „ $\cdot$ “ eða „+“. Aðgerð táknuð með „ $\cdot$ “ kallast *margföldun*, aðgerð táknuð með „+“ kallast *samlagning*. Ef aðgerð er skrifuð sem margföldun, þá er venja að sleppa margföldunarmerkinu og skrifa ab í stað $a \cdot b$; *ef* það veldur ekki misskilning. Venja er, þegar talað er um almennar grúpur, að skrifa aðgerðina sem margföldun og láta lesanda eftir að sjá hvernig niðurstöður verða ef aðgerðin er táknuð öðruvísi.

Umhverfa staks x m.t.t. margföldunar er rituð x^{-1}. Umhverfa x m.t.t. samlagningar er rituð $-x$.

Dæmi 2.1. (1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ eru grúpur m.t.t. samlagningar en ekki m.t.t. margföldunar.

(2) $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$, $\mathbb{C} \setminus \{0\}$ eru víxlnar grúpur m.t.t. margföldunar.

(3) Látum X vera mengi og $\mathfrak{S}(X)$ vera mengi allra gagntækra varpana $f : X \to X$. Þá er $\mathfrak{S}(X)$ grúpa m.t.t. samskeytingar varpana $\circ$, þar sem

$$(f \circ g)(x) = f(g(x)) \qquad \text{fyrir öll } x \in X.$$

Hlutleysan er $\mathrm{id}_X : X \to X$ sem er gefin með

$$\mathrm{id}_X(x) := x$$

fyrir öll x úr X; umhverfa gagntækrar vörpunar f er *andhverfa* hennar.

Vorum að athuga $\mathfrak{S}(X)$, sem var mengi allra gagntækra varpana $f : X \to X$, þar sem X er gefið mengi; fyrir $f, g \in \mathfrak{S}(X)$ er samskeytingin $f \circ g$ þ.a.

$$(f \circ g)(x) := f(g(x))$$

fyrir öll $x \in X$, líka gagntæk vörpun, þannig að vörpunin

$$\mathfrak{S}(X) \times \mathfrak{S}(X) \to \mathfrak{S}(X), (f, g) \mapsto f \circ g$$

er reikniaðgerð á menginu $\mathfrak{S}(X)$ sem gerir $\mathfrak{S}(X)$ að grúpu. Athugum sérstaklega

$$\mathfrak{S}_n := \mathfrak{S}(\{1, \ldots, n\}.$$

Köllum þetta *uppstokkanagrúpu* mengisins $\{1, \ldots, n\}$; notum orðið líka fyrir almennari mengi X. Vörpunin $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ má lýsa með „töflu“, nefnilega þannig að við skrifum

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}.$$

Til dæmis er

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$$

vörpunin $\sigma : \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$ þannig að $\sigma(1) = 4, \sigma(2) = 2, \sigma(3) = 1, \sigma(4) = 3$. Í neðri línunni koma fyrir allar tölurnar $1, \ldots, n$ en venjulega í annarri röð. Þess vegna er svona vörpun stundum kölluð *umröðun*; en almennar notum við orðið *uppstokkun*. Ef t.d.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 3 & 4 \end{pmatrix},$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$$

þá er auðvelt að reikna

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix}.$$

Fyrir σ, τ úr $\mathfrak{S}_n$ er venja að skrifa $\tau\sigma$ í stað $\tau \circ \sigma$.

(4) Látum $m \in \mathbb{N}, m \geq 1$ og setjum $Z_m := \{0, 1, \ldots, m-1\}$. Skilgreinum reikniaðgerð $\dot{+}$ á Z_m með

$$a \dot{+} b := (a + b) \bmod m.$$

Þetta gerir Z_m að grúpu: Við sjáum að

$$(a \dot{+} b) \dot{+} c = (a + b + c) \bmod m = a \dot{+} (b \dot{+} c),$$

núll er hlutleysa, og fyrir j úr Z_m er $m - j$ umhverfa staksins j, því að

$$j \dot{+} (m - j) = (j + m - j) \bmod m = m \bmod m = 0. \qquad \square$$

2.3 Hlutgrúpur

Skilgreining 2.4. Látum G vera mengi með reikniaðgerð $\top$. Við segjum að hlutmengi H í G sé *lokað* með tilliti til $\top$ ef $a \top b \in H$ fyrir öll $a, b \in H$. Þá gefur reikniaðgerðin af sér reikniaðgerð

$$H \times H \to H, (a, b) \mapsto a \top b$$

á H með einskroðun.

Skilgreining 2.5. Látum nú G vera grúpu. *Hlutgrúpa* í G er hlutmengi H í G sem er lokað m.t.t. reikniaðgerðarinnar og þannig að aðgerðin á H, sem aðgerðin á G gefur af sér geri, H að grúpu.

Athugasemd. Ef H er hlutgrúpa í grúpu G, þá er hlutleysan í H hlutleysan í G: Ef e' er hlutleysan í H og e er hlutleysan í G, þá er

$$e' \cdot e' = e' = e \cdot e'.$$

Látum nú e'' vera umhverfu e' í G; þá fæst

$$e' = e'e = e'(e'e'') = (e'e')e'' = e'e'' = e.$$

Sér í lagi er $e \in H$. Þá er líka ljóst að umhverfa staks í H er líka umhverfa þess í G: Ef $x \in H$, x' er umhverfa x í H og x'' er umhverfan í G, þá er

$$x' = x'ex'(xx'') = (x'x)x'' = ex'' = x''.$$

Ef tengin aðgerð á mengi G gefur af sér aðgerð á hlutmengi H, þá verður sú aðgerð líka tengin. En þá er ljóst:

Setning 2.3. Hlutmengi H í grúpu G er hlutgrúpa í G þ.þ.a.a. eftirfarandi þremur skilyrðum sé fullnægt:

(i) $e \in H$, þar sem e er hlutleysan í G

(ii) Ef $a, b \in H$, þá er $ab \in H$.

(iii) Ef $a \in H$, þá er umhverfan $a^{-1} \in H$.

Athugasemd. Ef aðgerð í grúpu er skrifuð sem margföldun, þá er umhverfa staks x táknuð x^{-1}; en ef hún er skrifuð sem samlagning, þá er umhverfan táknuð $-x$.

Ef aðgerðin er skrifuð sem samlagning (sem er venjulega ekki gert nema hún sé víxlin), þá er hlutleysan yfirleitt kölluð *núll* eða *núllstak* og táknuð með 0; við skrifum $a - b$ í stað $a + (-b)$; höfum þá reikniaðgerð

$$G \times G \to G, (a, b) \mapsto a - b$$

sem kallast *frádráttur*; hún er yfirleitt ekki tengin, né hefur hlutleysu. Ef aðgerðin er skrifuð sem samlagning, þá verða skilyrðin í síðustu setningu svona:

(i) $0 \in H$.

(ii) Ef $a, b \in H$, þá er $a + b \in H$.

(iii) Ef $a \in H$, þá er $-a \in H$.

Gífurlegur fjöldi dæma um grúpur fæst með því að athuga hlutgrúpur í $\mathfrak{S}(X)$ fyrir sérstök mengi X.

Dæmi 2.2. (1) Látum V vera línulegt rúm yfir $\mathbb{R}$; þá myndar mengi allra gagntækra $\mathbb{R}$-*línulegra* varpana $\phi : V \to V$ hlutgrúpu í $\mathfrak{S}(V)$. Við getum kallað hana

$$GL_{\mathbb{R}}(V)$$

(GL stendur fyrir *general linar group*). Nú má lýsa línulegu vörpuninni $\phi : V \to V$ á n-víðu rúmi V með $n \times n$ fylki A, og samskeyting varpana samsvarar fylkjamargföldun. Nú skilgreinir $n \times n$ fylki A gagntæka vörpun $V \to V$ m.t.t. grunns í V þ.þ.a.a. $\det A \neq 0$. Við sjáum að mengi allra $n \times n$-fylkja A yfir $\mathbb{R}$ þannig að $\det A \neq 0$ myndar grúpu m.t.t. fylkjamargföldunar; köllum hana

$$GL(n, \mathbb{R}).$$

Eins fæst

$$GL(n, \mathbb{C})$$

fyrir umhverfanleg $n \times n$-tvinntalnafylki.

Látum $SL(n, \mathbb{R})$ vera mengi allra $n \times n$-fylkja A yfir $\mathbb{R}$ þ.a. $\det A = 1$. Þá er $SL(n, \mathbb{R})$ hlutgrúpa í $GL(n, \mathbb{R})$: Hlutleysan i $GL(n, \mathbb{R})$ er einingarfylkið I, og $\det I = 1$, svo að $I \in SL(n, \mathbb{R})$, þá er $\det(AB) = \det A \cdot \det B = 1 \cdot 1 = 1$, svo að $AB \in SL(n, \mathbb{R})$, og $\det A^{-1} = \frac{1}{\det A} = \frac{1}{1} = 1$, svo að $A^{-1} \in SL(n, \mathbb{R})$. Líka getum við athugað $SL(n, \mathbb{Z})$, sem er mengi allra $n \times n$-fylkja með stök í $\mathbb{Z}$. Það er ljóst að $I \in SL(n, \mathbb{Z})$; ef $A, b \in SL(n, \mathbb{Z})$ þá er $AB \in SL(n, \mathbb{R})$; og $A^{-1} = \frac{1}{\det A} \cdot \operatorname{adj} A = \operatorname{adj} A$ hefur líka heiltölustuðla, svo að $A^{-1} \in SL(n, \mathbb{Z})$.

(2) Látum V vera línulegt rúm. *Vildarvörpun* $\psi : V \to V$ er vörpun af gerðinni $\psi(x) = \varphi(x) + b$, þar sem $\varphi : V \to V$ er línuleg vörpun og b er fasti í V. *Gagntækar* vildarvarpanir $V \to V$ mynda grúpu með tilliti til samskeytinga. Látum nú $V = \mathbb{R}^n$. Vörpun $\psi : \mathbb{R}^n \to \mathbb{R}^n$ kallast *firðrækin* eða *flutningur* ef $\|\psi(x) - \psi(y)\| = \|x - y\|$ fyrir öll $x, y \in \mathbb{R}^n$. Sýna má (og á að gera í línulegri algebru) að þetta eru nákvæmlega allar vildarvarpanir $\psi(x) = \varphi(x) + b$, þar sem φ er *þverstöðluð* línuleg vörpun; það þýðir að hún varpi þverstöðluðum grunni í $\mathbb{R}^n$ á þverstaðlaðan grunn í $\mathbb{R}^n$; jafngilt er að $\langle \phi(x), y \rangle = \langle x, \phi(y) \rangle$ fyrir öll $x, y \in \mathbb{R}^n$; og þetta jafngildir því að fylkið A fyrir φ í venjulega grunninum sé þverstaðlað, sem þýðir að ${}^tA \cdot A = I$, þar sem ${}^tA$ er bylta fylkið af A. Flutningarnir mynda grúpu með tilliti til samskeytingar!

Látum nú $X \subset \mathbb{R}^n$; þá er

$$S(X) := \{\varphi : \mathbb{R}^n \to \mathbb{R}^n : \varphi \text{ er flutningur þannig að } \varphi[X] = X\}$$

augljóslega hlutgrúpa í flutningsgrúpunni: $\mathrm{id}_{\mathbb{R}^n}[X] = X$; ef $\varphi[X] = X$ og $\psi[X] = X$, þá er $(\varphi \circ \psi)[X] = \varphi[\psi[X]] = \varphi[X] = X$; og $\varphi^{-1}[X] = \varphi^{-1} \circ \varphi[X] = X$. Köllum þetta *samhverfugrúpu* mengisins X.

Flutningar í $\mathbb{R}^n$ eru hliðranir, snúningar um punkt, speglanir um línu og rennispeglanir; rennispeglun er speglun um línu ásamt hliðrun í stefnu línunnar. Samhverfugrúpa jafnhliða þríhyrnings hefur sex stök, nefnilega snúning um $0°$ (það er samsemdavörpunin $\mathrm{id}_{\mathbb{R}^n}$, setjum $p_0 = \mathrm{id}_{\mathbb{R}^n}$), um $120°$, köllum hana ρ_1, og um $240°$, köllum hana ρ_2, tölusetjum hornpunktana með $1, 2, 3$, látum σ_k vera speglunina um hæðina hjá hornpunkti númer k. Sjáum að

ρ_0 varpar $1, 2, 3$ á $1, 2, 3$ í þessari röð,

ρ_1 varpar $1, 2, 3$ á $2, 3, 1$ í þessari röð,

ρ_2 varpar $1, 2, 3$ á $3, 1, 2$ í þessari röð,

σ_1 varpar $1, 2, 3$ á $1, 3, 2$ í þessari röð,

σ_2 varpar $1, 2, 3$ á $3, 2, 1$ í þessari röð,

σ_3 varpar $1, 2, 3$ á $2, 1, 3$ í þessari röð.

□

$\circ$	ρ_0	ρ_1	ρ_2	σ_1	σ_2	σ_3
ρ_0	ρ_0	ρ_1	ρ_2	σ_1	σ_2	σ_3
ρ_1	ρ_1	ρ_2	ρ_0	σ_3		
ρ_2	ρ_2	ρ_0	ρ_1	σ_2		
σ_1	σ_1					
σ_2	σ_2					
σ_3	σ_3					

Tafla 2.1: Margföldunartafla fyrir samhverfugrúpu þríhyrningsins, *óklárað*.

Athugasemd. Ef við höfum endanlega grúpu, þá má tölusegja stökin og búa til „margföldunartöflu“ yfir reikniaðgerðina. Við sjáum strax af slíkri töflu hvort við höfum hlutleysu og hvort aðgerðin er víxlin (það þýðir að taflan er samhverf um *aðalhornalínuna*). Það er ekki ljóst hvernig sjá má af töflunni hvort aðgerðin er tengin.

Grúputafla hefur þann eiginleika að í hverri línu og hverjum dálki kemur sérhvert stak úr grúpunni fyrir nákvæmlega einu sinni. Það er vegna þess að í grúpu gilda *styttireglur*:

Setning 2.4 (Styttireglur). (i) Ef $ab = ac$, þá er $b = c$.

(ii) Ef $ba = ca$, þá er $b = c$.

Sönnun. Ef $ab = ac$ þá er $b = eb = a^{-1}ab = a^{-1}ac = ec = c$; hitt er eins! ∎

Mengi með reikniaðgerð, sem er *tengin*, kallast *hálfgrúpa*. Ef við höfum hálfgrúpu H með hlutleysu e og látum G vera mengi allra staka í H sem hafa umhverfu í H þá er G lokað með tilliti til aðgerðarinnar og myndar grúpu; því að

$$(ab)^{-1} = b^{-1}a^{-1} \qquad \text{og} \qquad (a^{-1})^{-1} = a.$$

Nákvæmar:

Setning 2.5. Látum H vera *hálfgrúpu* með hlutleysu e og skrifum reikniaðgerðina í H sem margföldun. Þá gildir:

(i) Hlutleysan e hefur umhverfu og $e^{-1} = e$.

(ii) Ef a og b hafa umhverfur a^{-1} og b^{-1} þá hefur ab umhverfu og $(ab)^{-1} = b^{-1}a^{-1}$.

(iii) Ef a hefur umhverfu a^{-1} þá hefur a^{-1} umhverfu, og $\left(a^{-1}\right)^{-1} = a$.

Sönnun. (i) Er afleiðing af því að $ee = e$.

(ii) Höfum

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$$

og

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b{-}1b = e$$

svo að $b^{-1}a^{-1}$ er umhverfa staksins ab.

(iii) Jöfnurnar $aa^{-1} = a^{-1}a = e$ segja ekki bara að a^{-1} sé umhverfa staksins a heldur líka að a sé umhverfa staksins a^{-1}. ∎

Fylgisetning 2.1. Látum H vera hálfgrúpu með hlutleysu og G vera mengi allra staka í H sem hafa umhverfu, þá gefur reikniaðgerðin í H af sér reikniaðgerð á G með einskorðun; og aðgerðinni á G, sem fæst þannig, gerir G að grúpu.

Fylgisetning 2.2. Ef $a_1, \ldots, a_n$ eru stök í grúpu G, þá er

$$(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots a_1^{-1},$$

þ.e. umhverfa margfeldis endanlega margra staka í grúpu er margfeldið af umhverfunum í „öfugri röð“.

Dæmi 2.3. (1) Rauntalnamengið er hálfgrúpa m.t.t. margföldunar og hefur hlutleysu 1; grúpan af umhverfum er $\mathbb{R}\setminus\{0\}$. Eins eru $\mathbb{Q}, \mathbb{C}$ hálfgrúpur m.t.t. margföldunar og grúpurnar með umhverfunum eru $\mathbb{Q}\setminus\{0\}, \mathbb{C}\setminus\{0\}$. Heilu tölurnar, $\mathbb{Z}$, mynda hálfgrúpu með hlutleysu 1 með tilliti til margföldunar og grúpan af hlutleysunum er $\{-1, 1\}$.

(2) Látum X vera mengi og H vera mengi allra varpana $f : X \to X$. Þá myndar H hálfgrúpu m.t.t. samskeytingar varpana; hlutleysan er samsemdavörpunin $\mathrm{id}_X : X \to X; \mathrm{id}_X(x) := x$ fyrir öll $x \in X$ og grúpan af umhverfunum er grúpan $\mathfrak{S}(X)$ af *gagntækum* vörpunum $X \to X$.

(3) Látum $\mathbb{R}^{n\times n}$ vera mengi allra $n \times n$-fylkja yfir $\mathbb{R}$. Það er hálfgrúpa m.t.t. margföldunar fylkja, hlutleysan er einingarfylkið I. Grúpan af umhverfunum er $GL(n, \mathbb{R}) := \{A \in \mathbb{R}^{n\times n} : \det(A) \neq 0\}$. Látum $\mathbb{Z}^{n\times n}$ vera mengi allra $n \times n$-fylkja með heiltölustökum; það er hálfgrúpa m.t.t. fylkjamargföldunar (ef við margföldum saman tvö fylki með heilum stuðlum fæst aftur fylki með heilum stuðlum), hlutleysan er einingarfylkið I. Grúpan af umhverfunum er

$$\{A \in \mathbb{Z}^{n\times n} : \det(A) = 1 \text{ eða } \det(A) = -1\}.$$

Sönnum þetta: Ef $A \in \mathbb{Z}^{n\times n}$ og $\det(A) \neq 0$, þá er

$$A^{-1} := \frac{1}{\det(A)} \cdot \operatorname{adj}(A)$$

umhverfan í $\mathbb{R}^{n\times n}$, þar sem $\operatorname{adj}(A)$ er bylta hjáþáttafylkið. Höfum ljóslega $\operatorname{adj}(A) \in \mathbb{Z}^{n\times n}$, ef $\det(A) = 1$ eða $\det(A) = -1$ þá er $\operatorname{adj}(A) \in \mathbb{Z}^{n\times n}$ og er umhverfa A í $\mathbb{Z}^{n\times n}$. Öfugt, ef A hefur umhverfu $B \in \mathbb{Z}^{n\times n}$, þá er $AB = I$, svo að $\det(A)\det(B) = \det I = 1$ og $\det(A)\det(B) \in \mathbb{Z}$; en þá er $\det(A) = 1$ eða $\det(A) = -1$. □

Höfum minnst á *styttiregluna*. Getum sett hana fram aðeins almennar:

Setning 2.6 (Almennari styttiregla). Látum H vera hálfgrúpu með hlutleysu e og a vera stak í H sem hefur umhverfu a^{-1}.

(i) Ef $x, y \in H$ og $ax = ay$, þá er $x = y$.

(ii) Ef $x, y \in H$ og $xa = ya$, þá er $x = y$.

Athugasemd. Við orðum þetta þannig: Umhverfanlegt stak er styttanlegt bæði frá hægri og vinstri.

Sönnun. (i) Ef $ax = ay$, þá er

$$x = ex = (a^{-1}a)x = a^{-1}(ax) = a^{-1}ay = (a^{-1}a)y = ey = y.$$

(ii) Ef $xy = ya$, þá er

$$x = xe = x(aa^{-1} = (xa)a^{-1} = (ya)a^{-1} = y(aa^{-1}) = ye = y.$$ ■

Athugasemd. Ef $xa = ay$ er ekki hægt að álykta að $x = y$, þótt að a sé umhverfanlegt, *nema* að reikniaðgerðin sé víxlin.

Höfum því sýnt:

Setning 2.7. Hlutmengi H í grúpu G er hlutgrúpa í G þ.þ.a.a. eftirfarandi skilyrðum sé fullnægt:

(i) $e \in H$, þar sem e er hlutleysan í G.

(ii) Ef $a, b \in H$, þá er $ab \in H$.

(iii) Ef $a \in H$, þá er $a^{-1} \in H$

Setning 2.8. Skilyrðin (i), (ii) og (iii) í síðustu setningu eru jafngild eftirfarandi skilyrðum:

(i') $H \neq \emptyset$.

(ii') Ef $a, b \in H$, þá er $ab^{-1} \in H$.

Sönnun. Gefum okkur að (i)-(iii) gildi. Vegna $e \in H$ skv. (i) er $H \neq \emptyset$, svo að (i') gildir. Látum $a, b \in H$. Skv. (iii) er $b^{-1} \in H$, þá höfum við $a, b^{-1} \in H$, svo að $ab^{-1} \in H$ skv. (iii) og þar með gildir (ii').

Gefum okkur nú að (i') og (ii') gildi. Þá er $H \neq \emptyset$ svo til er $c \in H$. Skv. (ii') er þá $e = cc^{-1} \in H$, svo að (i) gildir. Látum nú $a \in H$. Við vitum að $e \in H$ svo að $e, a \in H$ og þá $a^{-1} = ea^{-1} \in H$ skv. (ii'). Látum þá $a, b \in H$, vitum að $b^{-1} \in H$, af $a, b^{-1} \in H$ leiðir að $ab = a(b^{-1})^{-1} \in H$ skv. (ii') svo að (iii) gildir líka. ∎

Athugasemd. Ef aðgerðin í G er skrifuð sem samlagning þá líta skilyrðin svona út:

(i) $0 \in H$.

(ii) Ef $a, b \in H$, þá er $a + b \in H$.

(iii) Ef $a \in H$ þá er $-a \in H$.

og hin skilyrðin verða

(i') $H \neq \emptyset$.

(ii') Ef $a, b \in H$, þá er $a - b \in H$.

2.4 Rásaðar grúpur

Rifjum upp að alveg í upphafi sönnuðum við: Ef A er mengi af heilum tölum, $A \neq \emptyset$ og fyrir öll $a, b \in A$ er $a - b \in A$, þá er til nákvæmlega ein náttúrleg tala m þ.a. $A = m\mathbb{Z}$. Þetta má nú orða svo:

Setning 2.9 (Mikilvæg setning). Hlutgrúpurnar í samlagningargrúpunni $\mathbb{Z}$ eru nákvæmlega mengin $m\mathbb{Z}$, þar sem $m \in \mathbb{N}$ (ath. að $0 \in \mathbb{N}$).

Dæmi 2.4. Látum

$$Z_m := \{0, 1, \ldots, m-1\}$$

þar sem $m \in \mathbb{N}, m \geq 2$. Við skilgreindum samlagningu á Z_m og gerðum það að samlagningargrúpu. Við getum líka skilgreint margföldun á Z_m með

$$a \odot b := ab \bmod m.$$

Þessi reikniaðgerð gerir Z_m að víxlinni hálfgrúpu með hlutleysu 1, höfum

$$(a \odot b) \odot c = a \odot (b \odot c) = (a \cdot b \cdot c) \mod m.$$

Grúpan af umhverfanlegu stökunum er táknuð með

$$\mathcal{U}(m).$$

Hvaða stök hafa umhverfu? Við höfum

$$a \in \mathcal{U}(m) \quad \text{þ.þ.a.a.} \quad \text{ssd}(a, m) = 1.$$

Hvað þýðir það að a hafi umhverfu? Það þýðir að til sé x þ.a. $ax \equiv 1 \pmod m$ og það þýðir aftur að til eru x og y þ.a. $1 - ax = my$, þ.e. $1 = ax + my$, sem þýðir að $\text{ssd}(a, m) = 1$. □

Skilgreining 2.6. Látum G vera grúpu með hlutleysu e og skrifum aðgerðina sem margföldun. Fyrir $a \in G$ og $n \in \mathbb{N}$ skilgreinum við *veldið* a^n með þrepun þannig að

$$a^0 := e,$$
$$a^{n+1} := a^n a.$$

Setjum líka

$$a^{-n} := (a^{-1})^n$$

og höfum þá skilgreint a^n fyrir öll $n \in \mathbb{Z}$. Ef aðgerðin í G er skrifuð sem samlagning, þá skrifum við na í stað a^n; skilgreiningin verður þá

$$0_{\mathbb{N}} a := 0_G$$
$$(n+1)a := na + a$$
$$(-n)a := n(-a).$$

Látum G vera grúpu og $a \in G$. Þá gildir

$$a^{n+m} = a^n \cdot a^m$$
$$a^{nm} = (a^n)^m$$

Athugasemd (Viðvörun). Almennt er $(ab)^n$ *ekki* jafnt $a^n b^n$. Ef það gildir fyrir $n = 2$, þ.e. $a^2b^2 = \left(a^b\right)^2 = abab$, þá getum við stytt a frá vinstri og b frá hægri og fáum

$$ab = ba.$$

Ef hins vegar $ab = ba$, þá er auðvelt að sjá með þrepun að $(ab)^n = a^n b^n$. Sér í lagi gildir þetta fyrir öll stök í víxlgrúpum.

Skilgreining 2.7. Látum a vera stak í grúpu G. Setjum

$$\langle a \rangle := \{a^n : n \in \mathbb{Z}\}.$$

Setning 2.10. Mengið $\langle a \rangle$ er hlutgrúpa í G, og raunar minnsta hlutgrúpa í G sem inniheldur a.

Sönnun. Það er ljóst að $a \in \langle a \rangle$, svo að $\langle a \rangle \neq \emptyset$. Ef $x, y \in \langle a \rangle$ þá má skrifa $x = a^n, y = a^m$ þar sem $n, m \in \mathbb{Z}$ og þá er $xy^{-1} = a^{n-m} \in \langle a \rangle$. Þá er $\langle a \rangle$ hlutgrúpa. Ef H er hlutgrúpa í G þ.a. $a \in H$, þá er ljóst með þrepun að $a^n \in H$ fyrir öll $n \in \mathbb{N}$ og $a^{-n} = \left(a^{-1}\right)^n \in H$ fyrir öll $n \in \mathbb{N}$, svo að $\langle a \rangle \subset H$. ∎

Skilgreining 2.8. Segjum að $\langle a \rangle$ sé hlutgrúpan í G sem stakið a *spannar*. Látum almennar A vera hlutmengi í grúpu G. Þá er til minnsta hlutgrúpa í G sem inniheldur A sem hlutmengi; við getum skilgreint hana sem sniðmengið af öllum hlutgrúpum sem innihalda A sem hlutmengi. Við táknum þessa grúpu með

$$\langle A \rangle$$

og segjum að $\langle A \rangle$ sé *hlutgrúpan í G sem A spannar*.

Setning 2.11. Grúpan $\langle A \rangle$ er mengi allra margfelda $a_1 a_2 \cdots a_r$, þar sem $a_1, \ldots, a_r \in A \cup A^{-1}$, þar sem $A^{-1} := \left\{a^{-1} : a \in A\right\}$.

Skilgreining 2.9. Ef A er endanlegt, $A = \{a_1, \ldots, a_n\}$, þá skrifum við $\langle A \rangle = \langle a_1, \ldots, a_n \rangle$.

Athugasemd. Höfum $\langle a \rangle = \langle \{a\} \rangle$ fyrir $a \in G$.

Skilgreining 2.10. (1) Við segjum að grúpa G sé *rásuð* ef til er stak $a \in G$ þ.a. $G = \langle a \rangle$.

(2) Við segjum að grúpa G sé *endanlega spönnuð* ef til eru endanlega mörg $a_1, \ldots, a_n$ þ.a. $G = \langle a_1, \ldots, a_n \rangle$.

Athugasemd. Látum G vera grúpu með hlutleysu e. Þá eru $\{e\}$ og G hlutgrúpur í G; $\{e\}$ er minnsta hlutgrúpan en G sú stærsta. Hlutgrúpan í G er *eiginleg* ef hún er ekki G sjálft, þ.e. hún er eiginlegt hlutmengi í G. Á ensku er grúpa kölluð *trivial* ef hún hefur bara eitt stak; slík grúpa kallast *örgrúpa*.

Á ensku er fjöldatala grúpu kölluð *order* grúpunnar; við notum bara *fjöldatala*. En það sem á ensku er kallað *order of an element in a group* köllum við *raðstig*.

Skilgreining 2.11. *Raðstig* staks a í grúpu G er fjöldatala mengisins $\langle a \rangle$.

Setning 2.12. Látum a vera stak í grúpu G. Stakið a hefur endanlegt raðstig þá og því aðeins að til sé náttúrleg tala n þannig að $n \geq 1$ og $a^n = e$, þar sem e er hlutleysan, og raðstigið er þá minnsta slíka talan n.

Sönnun. Athugum fyrst: Ef vörpunin $\varphi : \mathbb{Z} \to G, \varphi(n) := a^n$ er eintæk, þá er raðstigið óendanlegt. Ef hins vegar til eru heilar tölur n, m þ.a. $n \neq m$ og $a^n = a^m$, þá má g.r.f. að $n < m$, fyrir $k := m - n$ er þá $a^k = a^m \cdot a^{-n} = e$ og $k \geq 1$. Gerum nú á hinn bókinn gráð fyrir að til sé tala $k \geq 1$ þannig að $a^k = e$ og látum k vera *minnstu* slíka tölu. Ef nú $n \in \mathbb{Z}$, þá getum við skrifað

$$n = kq + r$$

þar sem $q, r \in \mathbb{Z}$ og $0 \leq r < k$. Þá er

$$a^n = a^{kq+r} = a^{kq} a^r = \left(a^k\right)^q a^r = e^q a^r = a^r.$$

Því er

$$\langle a \rangle = \left\{a^0 = e, a^1 = a, \ldots, a^{k-1}\right\}$$

sem hefur nákvæmlega r stök, því að stökin $a^0, a^1, \ldots, a^{k-1}$ eru öll ólík; annars væru til ólíkar tölur $(i, j) \in \{0, \ldots, k-1\}$ þ.a. $i \leq j$ og $a^i = a^j$, en þá er $1 \leq j - i \leq k - 1$ og $a^{j-i} = a^j \left(a^j\right)^{-1} = e$ í mótsögn við skilgreiningu á k. ∎

Athugasemd. Sönnunin sýnir: Ef raðstig staksins a er endanleg tala k, þá er

$$\langle a \rangle = \left\{ a^0, a^1, \ldots, a^{k-1} \right\}.$$

Athugum betur vörpunina $\varphi : \mathbb{Z} \to G, \varphi(n) := a^n$. Hún fullnægir skilyrðinu

$$\varphi(n+m) = \varphi(n)\varphi(m) \tag{2.1}$$

fyrir öll n, m; þetta er bara reglan $a^{n+m} = a^n a^m$. Af (2.1) leiðir $\varphi(n) = \varphi(n+0) = \varphi(n)\varphi(0)$, svo að $\varphi(0) = e$; ef $\varphi(n) = \varphi(m) = e$, þá er

$$\varphi(n-m) = \varphi(n)\varphi(-m) = \varphi(n)\varphi(m)^{-1} = e \cdot e^{-1} = e.$$

Þetta þýðir að

$$H := \{n \in \mathbb{Z} : \varphi(n) = e\}$$

er hlutgrúpa í samlagningargrúpunni $\mathbb{Z}$. Hún er af gerðinni $k\mathbb{Z}$, þar sem $k \in \mathbb{N}$. Ef $k = 0$, þ.e. ekkert veldi a^n fyrir $n \neq 0$ er e, þá sýnir röksemdafærslan í síðustu setningu að vörpunin φ er eintæk, og þá er raðstig a óendanlegt. Ef $k \geq 1$, þá er k minnsta tala þ.a. $k \geq 1$ og $a^k = e$, svo að k er raðstigið.

Vörpunin φ er dæmi um *grúpumótun*.

Kafli 3

Grúpumótanir

3.1 Eiginleikar grúpumótana

Skilgreining 3.1. Látum G_1, G_2 vera grúpur. *Grúpumótun* $\varphi : G_1 \to G_2$ er vörpun þannig að

$$\varphi(xy) = \varphi(x)\varphi(y) \tag{3.1}$$

fyrir öll $x, y \in G_1$.

Athugasemd. Ef aðgerðin í G_1 er skrifuð sem samlagning, þá verður jafnan (3.1) að

$$\varphi(x + y) = \varphi(x) \cdot \varphi(y).$$

Eins, ef aðgerðin í G_1 er skrifuð sem $\cdot$ og sú í G_2 er skrifuð sem $+$ þá verður hún að

$$\varphi(x \cdot y) = \varphi(x) + \varphi(y)$$

o.s.frv.

Dæmi 3.1. (1) Vigurrúm yfir $\mathbb{R}$ eða $\mathbb{C}$ er grúpa m.t.t. samlagningar, og línuleg vörpun er grúpumótun.

(2) Látum $\mathbb{R}_+^* := \{x \in \mathbb{R} : x > 0\}$; þetta er hlutgrúpa í $\mathbb{R}^* := \mathbb{R} \setminus \{0\}$ m.t.t. margföldunar. Varpanirnar

$$\exp : \mathbb{R} \to \mathbb{R}_+^*, \quad \exp x := \sum_{n \geq 0} \frac{x^n}{n!}$$

$$\log : \mathbb{R}_+^* \to \mathbb{R}$$

eru grúpumótanir. Hér lítum við á $\mathbb{R}$ sem grúpu m.t.t. samlagningar en $\mathbb{R}_+^*$ m.t.t. margföldunar. □

Setning 3.1. (1) Ef G er grúpa, þá er $\mathrm{id}_G : G \to G, x \mapsto x$ grúpumótun.

(2) Ef $\varphi : G \to H$ og $\psi : H \to K$ eru grúpumótanir, þá er samskeytingin $\psi \circ \varphi : G \to K$ grúpumótun.

(3) Ef $\varphi : G \to H$ er gagntæk grúpumótun, þá er andhverfan $\varphi^{-1} : H \to G$ líka grúpumótun.

Sönnun. (1) Augljóst.

(2) Fyrir $a, b \in G$ er

$$\psi\circ\varphi(ab) = \psi(\varphi(ab)) = \psi(\varphi(a)\varphi(b)) = \psi(\varphi(a))\psi(\varphi(b)) = (\psi\circ\varphi(a))(\psi\circ\varphi(b)).$$

(3) Ef $c, d \in H$, þá eru $\varphi^{-1}(c), \varphi^{-1}(d) \in G$ og

$$\varphi(\varphi^{-1}(c)\varphi^{-1}(d)) = \varphi(\varphi^{-1}(c))\varphi(\varphi^{-1}(d)) = cd = \varphi(\varphi^{-1}(cd))$$

og þar eð φ er eintæk fæst $\varphi^{-1}(cd) = \varphi^{-1}(c)\varphi^{-1}(d)$. ∎

Setning 3.2. Látum $\varphi : G_1 \to G_2$ vera grúpumótun og e_k vera hlutleysuna í G_k fyrir $k = 1, 2$. Þá gildir:

(1) $\varphi(e_1) = e_2$

(2) $\varphi(a^{-1}) = \varphi(a)^{-1}$ fyrir öll $a \in G$.

(3) $\varphi(a^n) = \varphi(a)^n$ fyrir öll $a \in G$ og $n \in \mathbb{Z}$.

Sönnun. (1) Höfum

$$\varphi(e_1)\varphi(e_1) = \varphi(e_1e_1) = \varphi(e_1) = e_2\varphi(e_1)$$

styttum $\varphi(e_1)$ frá hægri og fáum $\varphi(e_1) = e_2$.

(2) Höfum $aa^{-1} = a^{-1}a = e_1$. Af (1) leiðir að

$$\varphi(a)\varphi(a^{-1}) = \varphi(a^{-1})\varphi(a) = e_2$$

og það þýðir að $\varphi(a^{-1})$ er umhverfa staksins $\varphi(a)$.

(3) Höfum

$$\varphi(a^0) = \varphi(e_1) = e_2 = \varphi(a)^0,$$
$$\varphi(a^{k+1}) = \varphi(a \cdot a^k) = \varphi(a) \cdot \varphi(a^k)$$

svo að þrepun gefur $\varphi(a^n) = \varphi(a)^n$ fyrir öll $n \in \mathbb{N}$. En skv. (2) er þá líka $\varphi(a^{-n}) = \varphi((a^{-1})^n) = \varphi(a^{-1})^n = (\varphi(a)^{-1})^n = \varphi(a)^{-n}$ fyrir öll $n \in \mathbb{N}$, svo að $\varphi(a^n) = \varphi(a)^n$ fyrir öll $n \in \mathbb{Z}$. ∎

3.2 Tenging við heiltölurnar

Fylgisetning 3.1. Látum G vera grúpu og $a \in G$. Þá er til nákvæmlega ein grúpumótun $\varphi : \mathbb{Z} \to G$ þannig að $\varphi(1) = a$; hún er gefin með $\varphi(n) = a^n$ fyrir öll n.

Athugasemd. $\mathbb{Z}$ er hér *samlagningargrúpa* heilu talnanna, þ.a. grúpumótun $\varphi : \mathbb{Z} \to G$ er vörpun þ.a. $\varphi(n+m) = \varphi(n)\varphi(m)$ fyrir öll $n, m \in \mathbb{Z}$.

Sönnun (á fylgisetningu). Skv. veldareglu er $a^{n+m} = a^n a^m$, svo a vörpun $\varphi_a : \mathbb{Z} \to G, \varphi_a(n) := a^n$ er grúpumótun þ.a. $\varphi(1) = a$, þá segir liður (3) í síðustu setningu að $\varphi(n) = \varphi(n \cdot 1) = \varphi(1)^n = a^n$ fyrir öll n. ∎

Fylgisetning 3.2. Grúpa G er rásuð þ.þ.a.a. til sé átæk grúpumótun $\varphi : \mathbb{Z} \to G$.

Sönnun. Slík grúpumótun er af gerðinni $\varphi_a : \mathbb{Z} \to G, n \mapsto a^n$; og myndmengi hennar er $\{a^n : n \in \mathbb{Z}\}$; höfum $\langle a \rangle = G$ þ.þ.a.a. φ_a sé átæk. ∎

Dæmi 3.2. Vörpunin

$$\mathbb{Z} \to Z_m, n \mapsto n \bmod m$$

er átæk grúpumótun, svo að Z_m er rásuð grúpa. *Ath:* Samlagning í Z_m var skilgreind með $k \bmod m + j \bmod m = (j+k) \bmod m$. □

3.3 Kjarni, mynd og einsmótanir

Setning 3.3. Látum $\varphi : G_1 \to G_2$ vera grúpumótun.

(1) Ef H er hlutgrúpa í G_1, þá er myndin $\varphi[H] = \{\varphi(h) : h \in H\}$ hlutgrúpa í G_2.

(2) Ef K er hlutgrúpa í G_2, þá er frummyndin $\varphi^{-1}[K] = \{x \in G_1 : \varphi(x) \in K\}$ hlutgrúpa í G_1.

Sönnun. (1) Látum e_k vera hlutleysuna í $G_k, k = 1, 2$. Höfum $e_2 = \varphi(e_1) \in \varphi[H]$, því að $e_1 \in H$, svo að $\varphi[H] \neq \emptyset$. Ef $c, d \in \varphi[H]$, þá eru til $a, b \in H$ þ.a. $\varphi(a) = c$ og $\varphi(b) = d$. Þá er

$$cd^{-1} = \varphi(a)\varphi(b)^{-1} = \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1}) \in \varphi[H],$$

vegna $ab^{-1} \in H$. Því er $\varphi[H]$ hlutgrúpa í G_2.

(2) Vegna $\varphi(e_1) = e_2 \in K$ er $e_1 \in \varphi^{-1}[K]$, svo að $\varphi^{-1}[K] \neq \emptyset$. Ef $a, b \in \varphi^{-1}[K]$, þá er $\varphi(a) \in K$ og $\varphi(b) \in K$, svo að

$$\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} \in K$$

og því $ab^{-1} \in \varphi^{-1}[K]$. ∎

Skilgreining 3.2. Látum $\varphi : G_1 \to G_2$ vera grúpumótun. Við köllum

$$\operatorname{Im}\varphi := \varphi[G_1] = \{\varphi(g) : g \in G_1\}$$

mynd eða *myndgrúpu* mótunarinnar φ, og

$$\operatorname{Ker}\varphi := \varphi^{-1}[\{e_2\}] = \{x \in G_1 : \varphi(x) = e_2\}$$

þar sem e_2 er hlutleysan í G_2, köllum við *kjarna* grúpumótunarinnar φ.

Fylgisetning 3.3. Ef $\varphi : G_1 \to G_2$ er grúpumótun, þá er $\operatorname{Im}\varphi$ hlutgrúpa í G_2 og $\operatorname{Ker}\varphi$ er hlutgrúpa í G_1.

Setning 3.4. Látum $\varphi : G_1 \to G_2$ vera grúpumótun.

(1) Vörpunin φ er átæk þ.þ.a.a. $\operatorname{Im}\varphi = G_2$.

(2) Vörpunin φ er eintæk þ.þ.a.a. $\operatorname{Ker}\varphi = \{e_1\}$, þar sem e_1 er hlutleysan í G_1.

Sönnun. (1) er nánast skilgreiningin á átækni.

(2) Ef φ er eintæk og $x \in \operatorname{Ker}\varphi$, þá er $\varphi(x) = e_2 = \varphi(e_1)$, svo að $x = e_1$ og því er $x \in \{e_1\}$. Ljóst er að $e_1 \in \operatorname{Ker}\varphi$, og því er $\operatorname{Ker}\varphi = \{e_1\}$.

Ef nú á hinn bóginn $\operatorname{Ker}\varphi = \{e_1\}$ og $a, b \in G$ eru stök þ.a. $\varphi(a) = \varphi(b)$, þá er $\varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1}) = \varphi(a)\varphi(b)^{-1} = e_2$ svo að $ab^{-1} \in \operatorname{Ker}\varphi = \{e_1\}$, þ.e. $ab^{-1} = e_1$ og þá $a = b$. Því er φ eintæk. ∎

Skilgreining 3.3. *Gagntæk* grúpumótun $\varphi : G_1 \to G_2$ kallast *grúpueinsmótun* og við segjum að tvær grúpur G_1 og G_2 séu *einsmóta* og skrifum

$$G_1 \approx G_2 \quad \text{eða} \quad G_1 \cong G_2$$

ef til er einsmótun $\varphi : G_1 \to G_2$.

Setning 3.5. Látum G_1, G_2, G_3 vera grúpur.

(1) $G_1 \cong G_2$.

(2) Ef $G_1 \cong G_2$ þá er $G_2 \cong G_1$.

(3) Ef $G_1 \cong G_2$ og $G_2 \cong G_3$, þá er $G_1 \cong G_3$.

Sönnun. (1) $\mathrm{id}_{G_1} : G_1 \to G_1$ er grúpueinsmótun.

(2) Ef $\varphi : G_1 \to G_2$ er grúpueinsmótun þá er $\varphi^{-1} : G_2 \to G_1$ grúpueinsmótun.

(3) Ef $\varphi : G_1 \to G_2$ og $\psi : G_2 \to G_3$ eru grúpueinsmótanir, þá er $\varphi \circ \psi : G_1 \to G_3$ grúpueinsmótun. ∎

Athugasemd. Gerum ráð fyrir að $\varphi : G_1 \to G_2$ sé *eintæk* grúpumótun. Þá er $\operatorname{Im}\varphi$ hlutgrúpa í G_2 og vörpunin $\overline{\varphi} : G_1 \to \operatorname{Im}\varphi, x \mapsto \varphi(x)$ er *gagntæk* og því grúpueinsmótun, G_1 er því einsmóta hlutgrúpu í G_2.

Dæmi 3.3. Látum D_n vera samhverfugrúpu reglulegs n-hyrnings (*tvíflötungsgrúpa*) og tölusetjum hornpunkta marghyrningsins með $v_1, \ldots, v_n$. Flutningur φ sem tekur marghyrninginn á sjálfan sig ákvarðast af því hvernig hornpunktarnir varpast. Finnum gagntæka vörpun $\sigma_\varphi : \{1, \ldots, n\} \to \{1, \ldots, n\}$ þannig að

$$\sigma_\varphi(k) = j \quad \text{þ.þ.a.a.} \quad \varphi(v_k) = v_j.$$

Nú er ljóst að

$$\sigma_\varphi \circ \sigma_\psi = \sigma_{\varphi\circ\psi}$$

þetta þýðir að vörpunin

$$\Sigma : D_n \to \mathfrak{S}_n, \varphi \mapsto \sigma_\varphi$$

er *eintæk grúpumótun*, svo að D_n verður einsmóta hlutgrúpunni

$$\operatorname{Im}\Sigma = \{\sigma_\varphi : \phi \in D_n\}$$

í $\mathfrak{S}_n$. □

Smá mengjafræði. Látum $\varphi : X \to Y$ vera vörpun milli mengja. Ef $A \subset X$ þá er

$$A \subset \varphi^{-1}[\varphi[A]]; \tag{3.2}$$

ef nefnilega $a \in A$, þá er $\varphi(a) \in \varphi[A]$, og það þýðir að $a \in \varphi^{-1}[\varphi[A]]$. Jafnaðarmerki þarf ekki að gilda í (3.2); en gildir þó ef φ er *eintæk* vörpun. Ef $B \subset Y$, þá er

$$\varphi[\varphi^{-1}[B]] \subset B; \tag{3.3}$$

ef nefnilega $x \in \varphi[\varphi^{-1}[B]]$, þá er til $y \in \varphi^{-1}[B]$ þ.a. $x = \varphi(y)$; en $y \in \varphi^{-1}[B]$ þýðir að $\varphi(y) \in B$, svo að $x \in B$. Jafnaðarmerki þarf ekki að gilda í (3.3); en gildir þó ef φ er *átæk*. Af (3.2) leiðir að $\varphi[A] \subset \varphi[\varphi^{-1}[\varphi[A]]]$. Notum svo (3.3) á $B := \varphi[A]$ og fáum

$$\varphi[\varphi^{-1}[\varphi[A]]] \subset \varphi[A].$$

Við fáum því

$$\varphi[\varphi^{-1}[\varphi[A]]] = \varphi[A]$$

fyrir öll hlutmengi A í X
Afleiðing: Látum $\varphi : X \to Y$ vera vörpun og A_1, A_2 vera hlutmengi í X. Við höfum $\varphi[A_1] = \varphi[A_2]$ þ.þ.a.a. $\varphi^{-1}[\varphi[A_1]] = \varphi^{-1}[\varphi[A_2]]$.

Setning 3.6. Látum $\varphi : G_1 \to G_2$ vera grúpumótun með kjarna $K := \operatorname{Ker}\varphi = \{x \in G_1 : \varphi(x) = e_2\}$, e_2 hlutleysan í G_2. Ef H er hlutgrúpa í G_1, þá er

$$\varphi^{-1}[\varphi[H]] = HK = KH.$$

Athugasemd (Upprifjun). Fyrir hlutmengi A, B í grúpu G er

$$AB := \{ab : a \in A, b \in B\}.$$

Ef aðgerðin í G er skrifuð sem samlagning, þá skrifum við

$$A + B := \{a + b : a \in A, b \in B\}.$$

Sönnun (Sönnun á síðustu setningu). Látum $x \in \varphi^{-1}[\varphi[H]]$. Þá er $\varphi(x) \in \varphi[H]$, svo að til er h úr H þannig að $\varphi(x) = \varphi(h)$. Látum $k := h^{-1}x$. Þá er

$$\varphi(k) = \varphi(h)^{-1}\varphi(x) = \varphi(h)^{-1}\varphi(h) = e_2,$$

svo að $k \in K$ og $x = hk \in HK$. Þetta sýnir að $\varphi^{-1}[\varphi[H]] \subset HK$. Eins er $k_1 := xh^{-1} \in K$, og $x = k_1 h \in KH$, svo að $\varphi^{-1}[\varphi[H]] \subset KH$.

Ef nú $x \in HK$, þá eru til h úr H og k úr K þannig að $x = hk$, og þá er

$$\varphi(x) = \varphi(h)\varphi(k) = \varphi(h) \cdot e_2 = \varphi(h) \in \varphi[H],$$

svo að $x \in \varphi^{-1}[\varphi[H]]$. Þetta sýnir að $HK \subset \varphi^{-1}[\varphi[H]]$. Eins sést að $KH \subset \varphi^{-1}[\varphi[K]]$. ∎

Fylgisetning 3.4. Látum $\varphi : G \to H$ vera grúpumótun og H_1, H_2 vera hlutgrúpur í G. Höfum

$$\varphi[H_1] = \varphi[H_2] \quad \text{þ.þ.a.a.} \quad H_1K = H_2K.$$

3.4 Meira um rásaðar grúpur

Látum nú G vera rásaða grúpu og a vera stak í G þannig að $G = \langle a \rangle$. Þá höfum við grúpumótun

$$\varphi_a : \mathbb{Z} \to G, j \mapsto a^j$$

Höfum að til er nákvæmlega eitt stak $n \in \mathbb{N}$ þ.a. $\operatorname{Ker} \varphi_a = n\mathbb{Z}$; ef $n = 0$ þá hefur a óendanlegt raðstig; en ef $n \geq 1$, þá hefur a raðstig n og $|G| = |\langle a \rangle| = n$. Látum $k \in \mathbb{Z}$ og athugum

$$\langle a^k \rangle.$$

Þetta er hlutgrúpa í $\langle a \rangle = G$ og

$$\langle a^k \rangle = \varphi_a[k\mathbb{Z}].$$

Ef nú $k, j \in \mathbb{Z}$, þá segir fylgisetning 3.4 að

$$\langle a^k \rangle = \langle a^j \rangle \quad \text{þ.þ.a.a.} \quad k\mathbb{Z} + n\mathbb{Z} = j\mathbb{Z} + n\mathbb{Z}.$$

En nú er $k\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$ þar sem $d = \operatorname{ssd}(k, n)$. Fáum

Fylgisetning 3.5. Látum G vera grúpu, $a \in G$ vera stak með raðstig $n \geq 1$ og látum $j, k \in \mathbb{Z}$. Við höfum

$$\langle a^k \rangle = \langle a^j \rangle \quad \text{þ.þ.a.a.} \quad \operatorname{ssd}(k, n) = \operatorname{ssd}(j, n).$$

Fylgisetning 3.6. Látum a vera stak af raðstigi $n \in \mathbb{N}$ í grúpu G, k vera heila tölu og $d := \operatorname{ssd}(k, n)$. Þá er

$$\langle a^k \rangle = \langle a^d \rangle.$$

Sönnun. $d = \operatorname{ssd}(d, k)$, því að $d \mid k$ ∎

Fylgisetning 3.7. Látum a vera stak af raðstigi $n \in \mathbb{N}$ í gúpu G, k vera heila tölu. Við höfum

$$\langle a^k \rangle = \langle a \rangle \quad \text{þ.þ.a.a.} \quad \operatorname{ssd}(k, n) = 1.$$

Athugasemd. Sjáum: Stak $k \in Z_n$, sem var grúpan $\{0, \ldots, n-1\}$ með samlagningu $\bmod n$ spannar grúpuna Z_n þ.þ.a.a. $\operatorname{ssd}(k, n) = 1$, og það þýðir að $k \in \mathcal{U}(n)$, þar sem $\mathcal{U}(n)$ var grúpan af stökum í $\{0, \ldots, n-1\}$ sem hafa umhverfu m.t.t. margföldunar $\bmod n$.

Skilgreining 3.4. Látum $n \in \mathbb{N}, n \geq 1$. Við táknum með $\varphi(n)$ fjölda allra talna úr $\{0, \ldots, n-1\}$ þannig að $\text{ssd}(k, n) = 1$.

Ef við setjum $\mathbb{N}^+ := \{n \in \mathbb{N} : n \geq 1\}$, þá fáum við fall $\varphi : \mathbb{N}^+ \to \mathbb{N}$, $n \mapsto \varphi(n)$, sem kallast *φ-fall Eulers* (á ensku stundum kallað *Euler's totient function*).

Við sjáum:

(1) Talan $\varphi(n)$ er fjöldatala grúpunnar $\mathcal{U}(n)$.

(2) Talan $\varphi(n)$ er fjöldi staka a í rásaðri grúpu G með fjöldatölu n þannig að a spanni alla gúpuna.

Setning 3.7. Látum a vera stak með endanlegt raðstig $n \in \mathbb{N}$ í grúpu G og $k \in \mathbb{Z}$. Þá hefur a^k raðstigið $\frac{n}{d}$, þar sem $d = \text{ssd}(k, n)$.

Sönnun. Fyrir $j \in \mathbb{Z}$ fæst $a^{kj} = e$, e er hlutleysan í G, þ.þ.a.a. $kj \in n\mathbb{Z}$, það jafngildir $\frac{k}{d}j \in \frac{n}{d}\mathbb{Z}$ eða m.ö.o. að $\frac{n}{d} \mid \frac{k}{d}j$. En $\frac{n}{d}$ og $\frac{k}{d}$ eru ósamþátta, svo að þetta jafngildir $\frac{n}{d} \mid j$, sem þýðir að $j \in \frac{n}{d}\mathbb{Z}$. ∎

Fylgisetning 3.8. Raðstig staks í endanlegri rásaðri grúpu gengur upp í fjöldatölu grúpunnar.

Setning 3.8. Látum G vera rásaða grúpu með fjöldatölu $n \in \mathbb{N}$. Þá er sérhver hlutgrúpa í G rásuð og fjöldatala hennar gengur upp í fjöldatölu G. Fyrir sérhverja tölu j þ.a. $j \mid n$ hefur G *nákvæmlega eina* hlugrúpu með fjöldatölu j.

Sönnun. Látum a spanna G og athugum $\varphi_a : \mathbb{Z} \to G, j \mapsto a^j$. Ef H er hlutgrúpa í G, þá er $\varphi_a^{-1}[H]$ hlutgrúpa í $\mathbb{Z}$ þ.a. $n\mathbb{Z} \subset \varphi_a^{-1}[H]$; og þar sem φ_a er átæk er $H = \varphi_a[\varphi_a^{-1}[H]]$; hlutgrúpurnar í G eru því nákvæmlega grúpurnar $\varphi_a[k\mathbb{Z}]$, þar sem $n\mathbb{Z} \subset k\mathbb{Z}$, þ.e. $k \mid n$. Grúpan $\varphi_a[k\mathbb{Z}]$ hefur $\frac{n}{k}$ stök; því að hún er spönnuð af a^k sem hefur raðstig $\frac{n}{k}$, því að $k = \text{ssd}(k, n)$. ∎

Stefnum að merkilegri niðurstöðu:

Setning 3.9. Grúpa er rásuð þ.þ.a.a. hún sé einsmóta $\mathbb{Z}$ eða einhverri af grúpunum Z_n, þar sem $n \geq 1$. Sér í lagi eru rásaðar grúpur með sömu fjöldatölu einsmóta.

Mjökum okkur í átt að sönnun:

3.4.1 Ámótanir

Skilgreining 3.5. Átæk grúpumótun er stundum kölluð (grúpu)*ámótun*, og eintæk grúpumótun er kölluð (grúpu)*ímótun*.

Eftirfarandi setning er ekki í kennslubókinni eftir Gallian, en skiptir miklu máli og mun birtast síðar.

Setning 3.10 (Ámótunarsetningin). Látum $\varphi : G \to G_1$ vera *átæka* grúpumótun og $\psi : G \to G_2$ vera grúpumótun. Þá er jafngilt:

(i) Til er grúpumótun $\chi : G_1 \to G_2$ þ.a. $\psi = \chi \circ \varphi$.

(ii) $\operatorname{Ker}\varphi \subset \operatorname{Ker}\psi$.

Ef öðru (og þar með báðum) af þessum skilyrðum er fullnægt, þá ákvarðast vörpunin χ í skilyrði (i) ótvírætt, og hún er eintæk þ.þ.a.a. $\operatorname{Ker}\varphi = \operatorname{Ker}\psi$, en hún er átæk þ.þ.a.a. vörpunin ψ sé átæk.

Sönnun. Ef (i) er fullnægt og $x \in \operatorname{Ker}\varphi$, þ.e. $\varphi(x) = e_1$, þar sem e_1 er hlutelysan í G_1, þá er $\psi(x) = \chi(\varphi(x)) = \chi(e_1) = e_2$, þar sem e_2 er hlutleysan í G_2. Því gildir (ii).

Ef hins vegar (ii) er fullnægt, þá skilgreinum við vörpun $\chi : G_1 \to G_2$ þannig: Látum $x \in G_1$, þar eð φ er átæk er til stak $y \in G$ þannig að $\varphi(y) = x$, veljum eitt slík stak y og setjum $\chi(x) := \psi(y)$. Við sýnum að vörpunin χ sé *vel skilgreind*; m.ö.o. að skilgreiningin á $\chi(x)$ sé óháð valinu á y: Gerum ráð fyrir að einnig gildi að $\varphi(y_1) = x$. Þá er

$$\varphi(y_1 y^{-1}) = \varphi(y_1)\varphi(y^{-1}) = xx^{-1} = e_1,$$

svo að $y_1 y^{-1} \in \operatorname{Ker}\varphi \subset \operatorname{Ker}\psi$ og þá

$$e_2 = \psi(y_1 y^{-1}) = \psi(y_1)\psi(y^{-1}),$$

svo að $\psi(y_1) = \psi(y)$.

Sýnum nú að χ er *grúpumótun:* Látum $x_1, x_2 \in G_1$, veljum $y_1, y_2 \in G$ þ.a. $\varphi(y_1) = x_1$ og $\varphi(y_2) = x_2$. Þá er $\varphi(y_1y_2) = \varphi(y_1)\varphi(y_2) = x_1x_2$, svo að skv. skilgreiningu á χ er

$$\chi(x_1x_2) = \psi(y_1y_2) = \psi(y_1)\psi(y_2) = \chi(x_1)\chi(x_2).$$

Ef $y \in G$, og $x = \varphi(y)$, þá er $\psi(y) = \chi(x) = \chi(\varphi(y))$ og því er $\psi = \chi \circ \varphi$. Þar með er skilyrði (i) fullnægt.

Ef χ_1 er önnur grúpumótun $G_1 \to G_2$ þ.a. $\psi = \chi_1 \circ \varphi$, þá látum við $x \in G_1$ og finnum y þ.a. $\varphi(y) = x$. Þá er

$$\chi_1(x) = \chi_1(\varphi(y)) = (\chi_1 \circ \varphi)(y) = \psi(y) = \chi(x)$$

og því er $\chi_1 = \chi$.

Ef vörpunin χ er eintæk og $x \in \operatorname{Ker}\psi$, þá er $e_2 = \psi(x) = \chi(\varphi(x))$ en við höfum líka $\chi(e_1) = e_2$ og vegna eintækni er $\varphi(x) = e_1$, þ.e. $x \in \operatorname{Ker}\varphi$. Þar með er $\operatorname{Ker}\varphi = \operatorname{Ker}\psi$. Ef á hinn bóginn $\operatorname{Ker}\varphi = \operatorname{Ker}\psi$ og $x \in G_1$ er þannig að $\chi(x) = e_2$, þá veljum við $y \in G$ þannig að $\varphi(y) = x$. Þá er $\psi(y) = (\chi \circ \varphi)(y) = \chi(\varphi(y)) = \chi(x) = e_2$, svo að $x \in \operatorname{Ker}\psi = \operatorname{Ker}\varphi$ og því er $e_1 = \varphi(y) = x$. Þar með er $\operatorname{Ker}\chi = \{e_1\}$, svo χ er eintæk.

Þar sem φ er átæk er $\varphi[G] = \chi[\varphi[G]] = \chi[G_1]$, þ.e. $\operatorname{Im}(\varphi) = \operatorname{Im}(\psi)$, svo að χ er átæk þ.þ.a.a. ψ sé átæk. ∎

Fylgisetning 3.9. Látum $\varphi : G \to G_1$ og $\psi : G \to G_2$ vera átækar grúpumótanir þannig að $\operatorname{Ker}\varphi = \operatorname{Ker}\psi$. Þá eru grúpurnar G_1 og G_2 einsmóta.

Sönnun. Ámótunarsetningin segir að til sé grúpumótun $\chi : G_1 \to G_2$ þ.a. $\psi = \chi \circ \varphi$, og hún er eintæk vegna $\operatorname{Ker}\varphi = \operatorname{Ker}\psi$ og átæk þar sem ψ er átæk, svo að χ er einsmótun. ∎

Látum G vera rásaða grúpu. Þá höfum við *átæka* grúpumótun $\varphi : \mathbb{Z} \to G$. Sáum: G hefur óendanlega fjöldatölu þ.þ.a.a. $\operatorname{Ker}\varphi = 0$ en endanlega fjöldatölu n þ.þ.a.a. $\operatorname{Ker}\varphi = n\mathbb{Z}$, þar sem $n \in \mathbb{N}$, $n \geq 1$. Fáum:

Fylgisetning 3.10. Tvær rásaðar grúpur eru einsmóta þ.þ.a.a. þær hafi sömu fjöldatölu.

Með öðrum orðum:

Fylgisetning 3.11. Látum G vera rásaða grúpu. Ef hún er óendanleg, þá er hún einsmóta samlagningargrúpunni $\mathbb{Z}$. Ef hún hefur endanlega fjöldatölu n, $n \geq 1$, þá er hún einsmóta samlagningargrúpunni Z_n, sem var mengið $\{0, \ldots, n-1\}$ með samlagningu mod n.

Kafli 4

Uppstokkunargrúpur

4.1 Upprifjun og Cayley's theorem

Við höfum skilgreint uppstokkunargrúpu $\mathfrak{S}_n$; hún er grúpa allra gagntækra varpana $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$, þar sem aðgerðin er samskeyting varpana, köllum stökin í $\mathfrak{S}_n$ *uppstokkanir* mengisins $\{1, \ldots, n\}$. Fyrir $\sigma\tau \in \mathfrak{S}_n$ skrifum við

$$\sigma\tau \quad \text{í stað} \quad \sigma \circ \tau.$$

Athugasemd. Látum G vera (endanlega) grúpu. Fyrir $x \in G$ athugum við *vinstri* hliðrunina

$$v_g : G \to G, v_g(x) := gx.$$

Þá er

$$v_{gh}(x) = (gh)x = g(hx) = v_g(v_h(x)),$$

þ.e. $v_{gh} = v_g \circ v_h$. Sjáum að $v_g \circ v_{g^{-1}} = v_{g^{-1}} \circ v_g = v_e = \mathrm{id}_G$, þar sem e er hlutleysan í G. Því er $v_g : G \to G$ *gagntæk* og vörpunin $v : G \to \mathfrak{S}(G), g \mapsto v_g$ er *grúpumótun*. Hún er augljóslega eintæk: Ef $v_g = v_h$, þá er $g = v_g e = v_h e = h$. Þar með sést að G er einsmóta myndgrúpunni $\mathrm{Im}(v)$. Sjáum því: Sérhver grúpa er einsmóta hlutgrúpu í grúpu $\mathfrak{S}(X)$ af gagntækum vörpunum frá mengi X í sjálft sig.

Ef X, Y eru mengi og $\varphi : X \to Y$ er gagntæk vörpun, þá fæst *grúpueinsmótun*

$$\Phi : \mathfrak{S}(G) \to \mathfrak{S}(Y), \sigma \mapsto \varphi \circ \sigma \circ \varphi^{-1}$$

því að

$$\Phi(\sigma \circ \tau) = \varphi \circ \sigma \circ \tau\varphi^{-1} = \varphi \circ \sigma \circ \varphi^{-1} \circ \tau \circ \varphi^{-1} = \Phi(\sigma) \circ \Phi(\tau)$$

og Φ hefur andhverfu $(Y) \to (X), \tau \mapsto \varphi^{-1}\tau \circ \varphi$. Ef nú G er *endanleg* grúpa, þá höfum við gagntæka vörpun $G \to \{1, \ldots, n\}$ fyrir eitthvert $n \in \mathbb{N}$, $n \geq 1$. Þetta sýnir:

Setning 4.1 (Cayley's theorem). Sérhver endanleg grúpa er einsmóta hlutgrúpu í $\mathfrak{S}_n$ fyrir eitthvert $n \in \mathbb{N}$, $n \geq 1$.

Setning 4.2. Grúpan $\mathfrak{S}_n$ er endanlegt mengi með fjöldatölu $n!$.

4.2 Brautir og rásir

Skilgreining 4.1. Látum $\sigma \in \mathfrak{S}_n$, þ.e. σ er gagntæk vörpun $\{1, \ldots, n\} \to \{1, \ldots, n\}$. Látum $x \in \{1, \ldots, n\}$. *Braut* staksins x m.t.t. σ er mengið

$$[x]_\sigma := \left\{\sigma^k(x) : k \in \mathbb{Z}\right\}.$$

Þetta er hlutmengi í $\{1, \ldots, n\}$. Hlutmengi í $\{1, \ldots, n\}$ kallast *braut uppstokkunarinnar* σ ef það er af gerðinni $[x]_\sigma$ fyrir eitthvert $x \in \{1, \ldots, n\}$.

Við getum skilgreint jafngildisvensl $\sim$ á menginu $\{1, \ldots, n\}$ þannig að við setjum $x \sim y$ þ.þ.a.a. til sé $k \in \mathbb{Z}$ þannig að $y = \sigma^k(x)$. Til að sjá að þetta eru jafngildisvensl:

(a) $x = \sigma^0(x)$, því að $\sigma^0 = \mathrm{id}_{\{1,\ldots,n\}}$ svo að $x \sim x$.

(b) Ef $x \sim y$ þá er til $k \in \mathbb{Z}$ þannig að $y = \sigma^k(x)$, en þá er $x = \sigma^{-k}(y)$, svo að $y \sim x$.

(c) Ef $x \sim y$ og $y \sim z$, þá eru til $k, j \in \mathbb{Z}$ þ.a. $y = \sigma^k(x)$ og $z = \sigma^j(y)$. En þá er $z = \sigma^j(\sigma^k(x)) = \sigma^{j+k}(x)$, svo að $x \sim z$.

Nú er ljóst að $[x]_\sigma = \{y : x \sim y\}$ svo að $[x]_\sigma$ er jafngildisflokkur x m.t.t. σ. Fáum:

Setning 4.3. Brautir uppstokkunarinnar σ mynda deildaskiptingu mengisins $\{1, \ldots, n\}$.

Látum x vera *kyrrapunkt* vörpunarinnar σ; það þýðir að $\sigma(x) = x$. Þá er $[x]_\sigma = \{x\}$. Ef x er ekki kyrrapunktur, þá hefur mengið $[x]_\sigma$ ólíka punkta, en það er *endanlegt* og inniheldur alla punkta $\sigma^k(x)$ fyrir öll $k \in \mathbb{Z}$, svo að til eru $k, j \in \mathbb{Z}$ þannig að $j < k$ og $\sigma^j(x) = \sigma^k(x)$, og þá er $\sigma^{k-j}(x) = x$, sjáum því að til er tala $m \geq 1$ þ.a. $\sigma^m(x) = x$. Nú er ljóst að mengið $\left\{k \in \mathbb{Z} : \sigma^k(x) = x\right\}$ er *hlutgrúpa* í $\mathbb{Z}$: Ef m er *minnsta* talan þ.a. $\sigma^m(x) = x$ og $m \geq 1$, þá er $\left\{k \in \mathbb{Z} : \sigma^k(x) = x\right\} = m\mathbb{Z}$. Sjáum þá: Ef við setjum

$$x_k := \sigma^{k-1}(x) \quad \forall k = 1, \ldots, m,$$

þá eru stökin $x_1, \ldots, x_m$ ólík og

$$[x]_\sigma = \{x_1 = x, x_2, \ldots, x_m\},$$

og við höfum

$$\begin{aligned} \sigma(x_k) &= x_{k+1} \quad \text{fyrir } k = 1, \ldots, m-1, \\ \sigma(x_m) &= x_1. \end{aligned}$$

Skilgreining 4.2. Uppstokkun α í $\mathfrak{S}_n$ kallast *rás* ef hún hefur *nákvæmlega eina* braut sem hefur fleiri en eitt stak; köllum hana *aðalbraut* rásarinnar. Ef fjöldatala aðalbrautarinnar er m, þá segjum við að α sé m-rás.

Tvær rásir α og β kallast *sundurlægar* ef aðalbrautir þeirra eru sundurlægar.

Ef α er m-rás, þá eru til m ólík stök $x_1, \ldots, x_m$ í $\{1, \ldots, n\}$ þ.a.

$$\begin{aligned} \alpha(x_k) &= x_{k+1} \quad \text{fyrir } k = 1, \ldots, m-1, \\ \alpha(x_m) &= x_1, \\ \alpha(x) &= x \quad \text{ef } x \notin \{x_1, \ldots, x_m\}. \end{aligned}$$

Táknum þá α með

$$(x_1, \ldots, x_m)_n \quad \text{eða} \quad (x_1, \ldots, x_m)$$

og sleppum gjarnan kommunum ef $n < 10$. Í $\mathfrak{S}_9$ er $(7\,8\,1\,2) = (7, 8, 1, 2)_9$ rásin

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 7 & 3 & 4 & 5 & 6 & 8 & 1 & 9 \end{pmatrix}$$

Látum nú α, β vera *sundurlægar* rásir, A vera aðalbraut α og B vera aðalbraut β. Þá er

$$\alpha\beta(x) = \begin{cases} \alpha(x), & \text{ef } x \in A, \\ \beta(x), & \text{ef } x \in B, \\ x, & \text{ef } x \notin A \cup B. \end{cases}$$

Af samhverfuástæðum gildir sama um $\beta\alpha$, svo að $\alpha\beta = \beta\alpha$. Höfum þá:

Setning 4.4. Sundurlægar rásir víxlast.

Látum nú $\sigma \in \mathfrak{S}_n$ og $A_1, \ldots, A_r$ vera upptalningu á þeim brautum σ sem hafa fleiri en eitt stak. Fyrir $k = 1, \ldots, r$ er þá $\alpha_k : \{1, \ldots, n\} \to \{1, \ldots, n\}$ sem skilgreind er með

$$\alpha_k(x) := \begin{cases} \sigma(x), & \text{ef } x \in A_k, \\ x, & \text{ef } x \notin A_k \end{cases}$$

rás með aðalbraut A_k og við höfum

$$\sigma = \alpha_1 \alpha_2 \cdots \alpha_r.$$

Ef á hinn bóginn σ er margfeldi $\sigma = \alpha_1 \cdots \alpha_r$ af rásum sem eru sundurlægar tvær og tvær, þá eru brautir σ nákvæmlega mengin $A_1, \ldots, A_r$, þar sem A_k er aðalbraut α_k, $k = 1, \ldots, r$ ásamt einstökunum $\{x\}$ þar sem $x \notin A_1 \cup \cdots \cup A_r$. Við höfum

$$\sigma|A_k = \alpha_k|A_k$$

fyrir $k = 1, \ldots, r$ og

$$\sigma|B = \mathrm{id}\,|B$$

þar sem $B := \{1, \ldots, n\} \setminus (A_1 \cup \cdots \cup A_r)$. Höfum þá

Setning 4.5. Sérhverja uppstokkun σ má skrifa sem samskeytingu

$$\sigma = \alpha_1 \cdots \alpha_r$$

af rásum sem eru sundurlægar tvær og tvær (og víxlast þá tvær og tvær); og framsetningin ákvarðast ótvírætt burtséð frá röð.

Athugasemd. $\mathrm{id}_{\{1,\ldots,n\}}$ er samskeyting *tómu fjölskyldunnar* af rásum.

Dæmi 4.1. Við höfum

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 5 & 3 & 8 & 4 & 6 & 1 & 2 & 7 \end{pmatrix} = (1\,9\,7)(2\,5\,4\,8).$$

□

Setning 4.6. Sérhver rás er samskeyting af 2-rásum, t.d.

$$(x_1 \cdots x_r) = (x_1\, x_r)(x_1\, x_{r-1})(x_1\, x_{r-2}) \cdots (x_1\, x_3)(x_1\, x_2).$$

Setning 4.7. Sérhver uppstokkun er samskeyting af 2-rásum.

Athugasemd (Viðvörun). Þessar tvírásir víxlast almennt ekki tvær og tvær, og framsetningin er alls ekki ákvörðuð ótvírætt.

4.3 Formerki uppstokkunar

Setning 4.8. Til er nákvæmlega ein grúpumótun

$$\operatorname{sign} : \mathfrak{S}_n \to \{1, -1\}$$

þannig að $\operatorname{sign} \tau = -1$ fyrir sérhverja tvírás. Hún er gefin með

$$\operatorname{sign} \sigma = (-1)^{n-b(\sigma)}$$

þar sem $b(\sigma)$ er fjöldi brauta uppstokkunarinnar σ (*einstökungar meðtaldir!*).

Fylgisetning 4.1. Ef $\sigma \in \mathfrak{S}_n$ og

$$\sigma = \tau_1 \cdots \tau_r$$

þar sem $\tau_1, \ldots, \tau_r$ eru 2-rásir, þá er

$$\operatorname{sign} \sigma = (-1)^r .$$

Fylgisetning 4.2. Ef $\sigma \in \mathfrak{S}_n$ og

$$\sigma = \tau_1 \cdots \tau_r = \tau_1' \cdots \tau_s'$$

þar sem $\tau_1, \ldots, \tau_r, \tau_1', \ldots, \tau_s'$, þá er

$$r \equiv s \pmod 2$$

þ.e. annaðhvort eru tölurnar r og s báðar jafnar eða báðar oddatölur.

Skilgreining 4.3. Uppstokkun σ kallast *jafnstæð* ef $\operatorname{sign}\sigma = 1$ er *oddstæð* ef $\operatorname{sign}\sigma = -1$.

Sönnun (á setningu 4.8). Ef slík vörpun sign er til, þá er hún gefin með formúlunni í fylgisetningu 4.1 og ákvarðast því ótvírætt ef hún er til.

Látum $\sigma \in \mathfrak{S}_n$ og $b := b(\sigma)$ tákna fjölda braut uppstokkunarinnar σ. Þar sem tvírás hefur nákvæmlega $n-1$ brautir. Skilgreinum $\operatorname{sign}\sigma$ með formúlunni í setningunni og sjáum að

$$\operatorname{sign}\tau = (-1)^{n-(n-1)} = -1$$

ef τ er 2-rás. Til að sanna að sign sé grúpumótun sýnum við fyrst: Ef $\sigma \in \mathfrak{S}_n$ og τ er tvírás, þá er

$$\operatorname{sign}(\sigma\tau) = -\operatorname{sign}\sigma.$$

Athugum tvö tilvik: Skrifum $\tau = (u\ v)$.

1. tilvik: Stökin u, v eru á sömu braut σ. Skrifum brautina $\{x_1, \ldots, x_r\}$, þar sem $\sigma(x_i) = x_{i+1}$ fyrir $i = 1, \ldots, r-1$, $\sigma(r) = x_1$; megum gera ráð fyrir að $n = x_1$ og $r = x_k$, $2 \le k \le r$. Þá hefur $\sigma\tau$ sömu brautir og σ nema hvað brautir $\{x_1, \ldots, x_r\}$ skiptast í tvennt, nefnilega $\{x_1, x_{k+1}, \ldots, x_r\}$ og $\{x_2, \ldots, x_k\}$.

2. tilvik: Skoðum nú tilvikið þegar $\tau = (u\ v)$ þar sem u, v eru í ólíkum brautum uppstokkunarinnar σ. Getum gert ráð fyrir að brautirnar séu $\{x_1, \ldots, x_r\}$ og $\{y_1, \ldots, y_s\}$, þar sem $\sigma(x_j) = x_{j+1}$ fyrir $j = 1, \ldots, r-1$, $\sigma(x_r) = x_1$, $\sigma(y_k) = y_{k+1}$ fyrir $k = 1, \ldots, s-1$, $\sigma(y_k) = y_1$ og við getum tölusett þannig að $x_r = u$ og $y_s = v$. Brautirnar tvær sameinast í eina braut uppstokkunarinnar $\sigma\tau$, nefnilega $\{x_1, \ldots, x_r, y_1, \ldots, y_s\}$ þar sem $\sigma\tau(x_j) = x_{j+1}$ fyrir $j = 1, \ldots, r-1$, $\sigma\tau(x_r) = y_1$, $\sigma\tau(y_k) = y_{k+1}$ fyrir $k = 1, \ldots, s-1$, $\sigma\tau(y_s) = x_1$ en aðrar brautir $\sigma\tau$ eru eins og brautir σ. Brautir $\sigma\tau$ eru því einni færri en brautir σ, svo að $\operatorname{sign}(\sigma\tau) = -\operatorname{sign}(\sigma)$.

Athugum nú að $\mathrm{id}_{\{1,\ldots,n\}}$ hefur n brautir sem allar eru einstökungar, svo að $\operatorname{sign}(\mathrm{id}_{\{1,\ldots,n\}}) = (-1)^{n-n} = 1$. Ef nú $\tau_1, \ldots, \tau_s$ eru 2-rásir, þá fæst með þrepun að

$$\operatorname{sign}(\tau_1 \cdots \tau_s) = \operatorname{sign}(\mathrm{id}_{\{1,\ldots,n\}}\, \tau_1 \cdots \tau_s) = (-1)^s \operatorname{sign}(\mathrm{id}_{\{1,\ldots,n\}}) = (-1)^s.$$

Látum nú $\sigma, \tau \in \mathfrak{S}_n$ og skrifum $\tau = \tau_1 \cdots \tau_s$ þar sem $\tau_1, \ldots, \tau_s$ eru 2-rásir, þá er

$$\operatorname{sign}(\sigma\tau) = \operatorname{sign}(\sigma\tau_1 \cdots \tau_s) = (-1)^s \operatorname{sign}(\sigma) = \operatorname{sign}(\sigma)\operatorname{sign}(\tau)$$

og við höfum sýnt að $\operatorname{sign} : \mathfrak{S}_n \to \{-1, 1\}$ er grúpumótun. ∎

Skilgreining 4.4. Talan $\operatorname{sign}(\sigma)$ kallast *formerki* uppstokkunarinnar σ. Tvírás er líka kölluð *umskipting* (e. *transposition*). Rifjum upp að uppstokkun σ kallast *jafnstæð* ef $\operatorname{sign}(\sigma) = 1$ en *oddstæð* ef $\operatorname{sign}(\sigma) = -1$. Táknum með $\mathfrak{A}_n$ mengi allra *jafnstæðra* uppstokkana í $\mathfrak{S}_n$.

Setning 4.9. Mengið $\mathfrak{A}_n$ er hlutgrúpa í $\mathfrak{S}_n$ og fyrir $n \geq 2$ er fjöldatala þess $\frac{1}{2}n!$.

Sönnun. Höfum $\mathfrak{A}_n = \operatorname{Ker}(\operatorname{sign})$, svo að $\mathfrak{A}_n$ er hlutgrúpa í $\mathfrak{S}_n$. Látum $n \geq 2$ og τ vera tvírás. Þá er

$$\mathfrak{S}_n \setminus \mathfrak{A}_n = \tau\mathfrak{A}_n := \{\tau\rho : \rho \in \mathfrak{A}_n\}$$

ef nefnilega $\sigma \in \tau\mathfrak{A}_n$, $\sigma = \tau\rho$ með $\rho \in \mathfrak{A}_n$, þá er $\operatorname{sign}(\sigma) = \operatorname{sign}(\tau) \cdot \operatorname{sign}(\rho) = (-1) \cdot 1 = -1$, svo að $\sigma \in \mathfrak{S}_n \setminus \mathfrak{A}_n$. Ef hins vegar $\sigma \in \mathfrak{S}_n \setminus \mathfrak{A}_n$, þ.e. $\operatorname{sign}(\sigma) = -1$, setjum $\rho := \tau\sigma$, þá er $\sigma = \tau^2\sigma = \tau\rho$ og $\operatorname{sign}(\rho) = \operatorname{sign}(\tau)\operatorname{sign}(\sigma) = (-1)(-1) = 1$, svo að $\rho \in \mathfrak{A}_n$. En $\tau\mathfrak{A}_n$ hefur jafnmörg stök og $\mathfrak{A}_n$, því að vörpunin $\mathfrak{A}_n \to \tau\mathfrak{A}_n, \rho \mapsto \tau\rho$ er gagntæk með andhverfu $\tau\mathfrak{A}_n \to \mathfrak{A}_n, \sigma \mapsto \tau\sigma$ (vegna $\tau^2 = \mathrm{id}_{\{1,\ldots,n\}}$), þess vegna hafa $\mathfrak{A}_n$ og $\tau\mathfrak{A}_n$ jafnmörg stök, þau eru sundurlæg, og sammengið $\mathfrak{S}_n$ hefur $n!$ stök, svo að $\mathfrak{A}_n$ hefur $\frac{1}{2}n!$ stök. ∎

Athugasemd. Mengið $\tau\mathfrak{A}_n$ er svokallað *hjámengi* hlutgrúpunnar $\mathfrak{A}_n$ í $\mathfrak{S}_n$.

Kafli 5

Hjámengi

5.1 Hjámengi

Skilgreining 5.1. Látum H vera hlutgrúpu í grúpu G og x vera stak í G. Við köllum mengið

$$xH := \{xh : h \in H\}$$

vinstra hjámengi hlutgrúpunnar H gegnum stakið x, og mengið

$$Hx := \{hx : h \in H\}$$

kallast *hægra hjámengi* hlutgrúpunnar H gegnum stakið x.

Athugasemd. Höfum $x \in xH$ og $x \in Hx$ vegna $x = xe$ og $x = ex$, þar sem e er hlutleysan í G, og $e \in H$. Ef aðgerðin í G er skrifuð sem samlagning, þá eru hjámengin skrifuð

$$x + H = \{x + h : h \in H\}$$

$$H + x = \{h + x : h \in H\}.$$

Ef grúpan G er víxlin, þá er $xH = Hx$ fyrir öll $x \in G$ og allar hlutgrúpur H í G. Þá þarf ekki að gera neinn greinamun á hægri og vinstri hjámengjum.

Dæmi 5.1. Látum $G = \mathbb{R}^2$ með samlagningu. Þetta er línulegt rúm yfir $\mathbb{R}$, og línuleg hlutrúm eru hlutgrúpur. Sér í lagi er sérhver lína gegnum núllpunktinn hlutgrúpa í $\mathbb{R}^2$; látum H vera slíka línu og $x \in \mathbb{R}^2$. Þá er hjámengið $x + H$ línan gegnum x samsíða línunni H. □

Látum nú H vera hlutgrúpu í grúpu G og $x \in G$. Fyrir öll $y \in G$ gildir $y \in xH$ þ.þ.a.a. til sé $h \in H$ þ.a. $y = xh$; og það er jafngilt $x^{-1}y \in H$ (það

er líka jafngilt því að $y^{-1}x = (x^{-1}y)^{-1} \in H$). Skrifum nú

$$x \sim y \quad \text{þ.þ.a.a.} \quad x^{-1}y \in H,$$

þetta eru jafngildisvensl:

(a) $x^{-1}x = e \in H$, svo að $x \sim x$.

(b) Ef $x \sim y$, þá er $x^{-1}y \in H$, þá er $y^{-1}x = (x^{-1}y)^{-1} \in H$, svo að $y \sim x$.

(c) Ef $x \sim y$ og $y \sim z$, þá er $x^{-1}y \in H$ og $y^{-1}z \in H$, en þá er $x^{-1}z = x^{-1}yy^{-1}z \in H$, svo að $x \sim z$.

Höfum sýnt:

Setning 5.1. Vinstra hjámengið xH er jafngildisflokkur staksins x mt.t. jafngildisvenslanna $\sim$, þar sem

$$x \sim y \quad \text{þ.þ.a.a.} \quad x^{-1}y \in H.$$

Sér í lagi mynda vinstri hjámengin deildaskiptingu mengisins G.

Fylgisetning 5.1. Höfum $y \in xH$ þ.þ.a.a. $yH = xH$.

Höfum líka $yx^{-1} \in H$. Fáum samsvarandi setningu:

Setning 5.2. Hægra hjámengið Hx er jafngildisflokkur staksins x m.t.t. jafngildisvenslanna $\sim_1$, þar sem

$$x \sim_1 y \quad \text{þ.þ.a.a.} \quad yx^{-1} \in H.$$

Sér í lagi mynda hægri hjámengin deildaskiptingu mengisins.

Fylgisetning 5.2. Höfum $y \in Hx$ þ.þ.a.a. $Hy = Hx$.

Látum $x \in G$, þá fæst gagntæk vörpun

$$H \to xH, y \mapsto xy$$

umhverfan er $xH \to H, z \mapsto x^{-1}z$.

Fylgisetning 5.3. Látum G vera endanlega grúpu og H vera hlutgrúpu í G. Þá hafa öll vinstri hjámengin xH jafnmörg stök. Ef h er fjöldatala h, g fjöldatala G og m fjöldi hjámengja, þá er $g = mh$. Sér í lagi gildir

$$h \mid g.$$

5.2 Vísitala og tenging við rásaðar grúpur

Skilgreining 5.2. Látum H vera hlutgrúpu í grúpu G. Við segjum að H hafi *endanlega vísitölu* í G ef vinstri hjámengi grúpunnar H í G eru endanlega mörg, og fjöldi þeirra kallast þá vísitala H í G og er táknuð

$$(G : H),$$

í bók er skrifað $|G : H|$.

Athugasemd. Vörpunin $\psi : G \to G, \psi(x) := x^{-1}$ varpar xH á Hx^{-1}; svo að ψ gefur af sér gagntæka vörpun milli mengis allra vinstri hjámengja og mengis allra hægri hjámengja; þau eru því jafnmörg.

Getum nú orðað seinustu setningu öðruvísi: Ef grúpan G er endanleg, þá er

$$\#G = (G : H)\#H.$$

Athugasemd. Táknum með $\#G$ fjöldatölu (endanlegs) mengis.

Fylgisetning 5.4. Ef G er endanelg grúpa og H er hlutgrúpa í G, á er

$$(G : H) = \frac{\#G}{\#H}.$$

Fylgisetning 5.5. Sérhver grúpa með fjöldatölu sem er frumtala er rásuð.

Sönnun. Látum G vera grúpu, $\#G = p$, þar sem p er frumtala. Sér í lagi er $p > 1$, svo að til er stak a í G annað en hlutleysan. Þá er $\langle a \rangle$ hlutgrúpa með fjöldatölu ≥ 2 sem gengur upp í p, svo að $\#\langle a \rangle = p$, og þá $\langle a \rangle = G$. ∎

Fylgisetning 5.6. Ef a er stak í endanlegri grúpu G, þá gengur raðstig þess upp í $\#G$.

Sönnun. Raðstigið er $\#\langle a \rangle$. ∎

Fylgisetning 5.7. Ef G er endanleg grúpa með hlutleysu e og $n = \#G$, þá er

$$a^n = e.$$

Sönnun. Látum r vera raðstig a, þá er til m þ.a. $n = mr$, svo að

$$a^n = (a^r)^m = e^m = e.$$ ∎

5.2.1 Fermat, Fermat-Euler

Fylgisetning 5.8 (Litla Fermat-setningin). Ef a er heil tala sem er ekki heilt margfeldi af frumtölu p, þá er

$$a^{p-1} \equiv 1 \pmod{p}.$$

Sönnun. Tölurnar $1, \ldots, p-1$ mynda trúpu m.t.t. margföldunar $(\bmod\ p)$. ∎

Fylgisetning 5.9 (Fermat-Euler). Ef $m \geq 1$ og $a \in \mathbb{Z}$ er þannig að $\text{ssd}(a, m) = 1$, þá er

$$a^{\varphi(m)} \equiv 1 \pmod{m},$$

hér er φ fall Eulers.

Sönnun. $a \bmod m$ er í grúpu $\mathcal{U}(m)$ sem hefur margföldun $\bmod p$ sem aðgerð, og $\#\mathcal{U}(m) = \varphi(m)$. ∎

5.3 Normlegar hlutgrúpur

Skilgreining 5.3. Hlutgrúpa H í grúpu G kallast *normleg* í G ef $xH = Hx$ fyrir öll x úr G.

Athugasemd. Skilgreindum almennt $AB := \{ab : a \in A, b \in B\}$ fyrir hlutmengi A, B í G; höfum reiknireglunа

$$(AB)C = A(BC) = \{abc : a \in A, b \in B, c \in C\}.$$

Höfum líka

$$xH = \{x\}H \qquad \text{og} \qquad Hx = H\{x\}.$$

Af því leiðir t.d.

$$xH = Hx \qquad \text{þ.þ.a.a.} \qquad xHx^{-1} = H.$$

Af $\{x\}H = H\{x\}$ leiðir nefnilega $\{x\}H\{x^{-1}\} = H\{x\}\{x^{-1}\} = H\{e\} = H$, og af $H = \{x\}H\{x^{-1}\}$ leiðir $H\{x\} = \{x\}H\{x^{-1}\}\{x\} = xH$.

Innskot: Eftirfarandi skilgreiningu setti Reynir fram í dæmatíma 23. september, hún á eiginlega betur heima hér í fyrirlestrunum:

Skilgreining 5.4. (i) Látum G vera grúpu. Einsmótun $\phi : G \to G$ kallast *sjálfmótun* grúpunnar G og mengi allra sjálfmótana G er táknað

$$\operatorname{Aut} G.$$

Þetta er hlutgrúpa í $\mathfrak{S}(G)$ og kallast *sjálfmótanagrúpa* grúpunnar G.

(ii) Skilgreinum fyrir sérhvert $x \in G$ vörpun

$$\iota_x : G \to G, \quad g \mapsto xgx^{-1}.$$

Þetta er sjálfmótun.[1]Köllum slíkar sjálfmótanir *innri sjálfmótanir* grúpunnar G. Innri sjálfmótanirnar mynda hlutgrúpu í $\operatorname{Aut} G$, hún er táknuð

$$\operatorname{Inn}(G).$$

Höldum nú áfram þaðan sem frá var horfið, en skiljum betur eftirfarandi setningu:

Fylgisetning 5.10. Hlutgrúpa H í G er normleg í G þ.þ.a.a.

$$\iota_x[H] = H$$

fyrir allar innri sjálfmótanir ι_x grúpunnar G.

[1]Sjá nánar dæmablað 4, dæmi 21

Athugum að fyrir sérhverja hlutgrúpu H í grúpu G er $HH = H$: Höfum $H \subset HH$ vegna þess að $h = eh = he$ og $e \in H$; og $HH \subset H$ því að H er lokað m.t.t. margföldunar.

Látum nú N vera *normlega* hlutgrúpu í G. Þá er

$$(xN)(yN) = x(Ny)N = x(yN)N = xyNN = xyN.$$

Við höfum þá

$$xNx^{-1}N = xx^{-1}N = eN = N$$

og líka $x^{-1}NxN = x^{-1}xN = eN = N$. Líka er $xNN = xN$ og

$$N(xN) = (Nx)N = (xN)N = xNN = xN.$$

Höfum sýnt:

Setning 5.3. Látum N vera normlega hlutgrúpu í grúpu N og G/N vera mengi (vinstri) hjámengja grúpunnar N í G. Þá verður G/N að grúpu með reikniaðgerð sem gefin er með

$$xN \cdot yN = xyN.$$

Hlutleysan í grúpunni G/N er

$$eN = N,$$

og margföldunarumhverfa xN er $x^{-1}N$. Vörpunin

$$\pi : G \to G/N$$

er átæk grúpumótun með kjarna N.

Skilgreining 5.5. Köllum grúpu G/N, þar sem N er normleg hlutgrúpa í G, *deildagrúpu* af grúpunni G, og vörpunina $\pi : G \to G/N$ náttúrlega ofanvarpið.

Eftir var að sanna fullyrðinguna um π, en

$$\pi(xy) = xyN = xN \cdot yN = \pi(x)\pi(y)$$

svo að π er grúpumótun, og við höfum $x \in \operatorname{Ker}\pi$ þ.þ.a.a. $xN = N$, en það jafngildir $x \in N$.

Athugasemd. Fyrir grúpu G þar sem aðgerðin er skrifuð sem samlagning er aðgerðin á G/N gefin með

$$(x+N)+(y+N)=(x+y)+N.$$

Athugasemd (Mikilvægt). Allar hlutgrúpur í *víxl*grúpu eru normlegar!

Dæmi 5.2. Látum $m \in \mathbb{N}, m \geq 1$. Stökin í $\mathbb{Z}/m\mathbb{Z}$ eru m talsins, nefnilega hjámengin

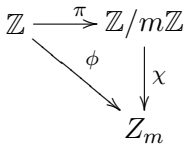
$$0+m\mathbb{Z}=m\mathbb{Z}, 1+m\mathbb{Z}, \ldots, (m-1)+m\mathbb{Z}.$$

Höfum

$$k+m\mathbb{Z}=\{x\in\mathbb{Z} : x \equiv k \pmod{m}\}.$$

Náttúrlega ofanvarpið $\pi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ er átæk grúpumótun með kjarna $m\mathbb{Z}$. Nú höfum við líka aðra átæka grúpumótun $\phi : \mathbb{Z} \to Z_m, k \mapsto k \bmod m$, með kjarna $m\mathbb{Z}$.

Skv. *ámótunarsetningunni* er til nákvæmlega ein grúpumótun $\chi : \mathbb{Z}/m\mathbb{Z} \to Z_m$, og hún er *grúpueinsmótun*. Fyrir $m = 0$ er ljóst að $m\mathbb{Z} = \{0\}$ og $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}$. Sjáum: Grúpa er rásuð þ.þ.a.a. hún sé einsmóta deildagrúpu af $\mathbb{Z}$.



□

Með öðrum orðum:

Setning 5.4. Látum $\pi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ vera náttúrlega ofanvarpið,

$$\pi(x) = x + m\mathbb{Z} \qquad \forall x \in \mathbb{Z}$$

og $\varphi : \mathbb{Z} \to Z_m$ vera vörpunina sem er gefin með $\varphi(x) = x \bmod m$. Þá eru π og φ átækar grúpumótanir með sama kjarna, nefnilega $m\mathbb{Z}$, svo að til er nákvæmlega ein grúpumótun

$$\chi : \mathbb{Z}/m\mathbb{Z} \to Z_m$$

þannig að $\varphi = \chi \circ \pi$, þ.e. $x \bmod m = \chi(x + m\mathbb{Z})$ og hún er *einsmótun*.

Sönnun. Þetta er bein afleiðing af *ámótunarsetningunni* (bls. 41) ■

5.4 Setningar um einsmótanir

Önnur afleiðing ámótunarsetningarinnar er:

Setning 5.5 (Fyrsta einsmótunarsetningin). Látum $\varphi : G \to H$ vera grúpumótun, þá er $\operatorname{Ker}\varphi$ normleg hlutgrúpa í G og við höfum náttúrlega einsmótun[2]

$$G/\operatorname{Ker}\varphi \to \operatorname{Im}(\varphi),$$

þ.e. $\operatorname{Im}(\varphi) \cong G/\operatorname{Ker}\varphi$.

Sönnun. Látum $x \in \operatorname{Ker}\varphi$ og $g \in G$. Þá er

$$\begin{aligned}\varphi(gxg^{-1}) &= \varphi(g)\varphi(x)\varphi(g^{-1})\\ &= \varphi(g)e_H\varphi(g^{-1})\\ &= \varphi(g)\varphi(g^{-1})\\ &= \varphi(gg^{-1})\\ &= \varphi(e_G)\\ &= e_H,\end{aligned}$$

svo að $gxg^{-1} \in \operatorname{Ker}\varphi$, þetta sýnir að $\operatorname{Ker}\varphi$ er normleg hlutgrúpa. Látum $\pi : G \to G/\operatorname{Ker}\varphi$ vera náttúrlega ofanvarpið, það hefur kjarnann $\operatorname{Ker}\varphi$ og er átæk vörpun. Vörpunin $\tilde{\varphi} : G \to \operatorname{Im}(\varphi)$, $\tilde{\varphi}(x) := \varphi(x)$ fyrir öll x, er líka átæk grúpumótun með kjarnann $\operatorname{Ker}\varphi$. Þá er til nákvæmlega ein grúpumótun $\chi : G/\operatorname{Ker}\varphi \to \operatorname{Im}(\varphi)$ þannig að örvaritið

$$\begin{array}{ccc} G & \xrightarrow{\pi} & G/\operatorname{Ker}\varphi \\ & \searrow^{\tilde{\varphi}} & \downarrow{\scriptstyle \chi} \\ & & \operatorname{Im}(\varphi) \end{array}$$

sé víxlið, þ.e. $\chi \circ \pi = \tilde{\varphi}$, og hún er einsmótun skv. ámótunarsetningunni. ∎

Athugasemd. *Örvarit* er fjölskylda af mengjum ásamt vörpunum á milli þeirra, þeim má lýsa með myndum á borð við

$$\begin{array}{ccccc} X & \xrightarrow{\varphi} & Y & \xrightarrow{\psi} & Z \\ {\scriptstyle\alpha}\downarrow & & {\scriptstyle\beta}\downarrow & & {\scriptstyle\gamma}\downarrow \\ U & \xrightarrow{\chi} & V & \xrightarrow{\theta} & T \end{array}$$

[2] *Náttúrleg einsmótun* er einsmótun sem telst venjulega gefin og við þurfum ekki að velja neitt af handahófi (gróf lýsing).

Að svona örvarit sé *víxlið* þýðir: Fyrir sérhver tvö mengi í örvaritinu eru allar varpanir frá öðru í hitt, sem fást sem samskeytingar af vörpunum í örvaritinu, sama vörpunin. Að örvaritið hér að ofan sé víxlið þýðir að

$$\beta \circ \varphi = \chi \circ \alpha \quad \text{og} \quad \gamma \circ \psi = \theta \circ \beta$$

því af því leiðir að

$$\gamma \circ \psi \circ \varphi = \theta \circ \beta \circ \varphi = \theta \circ \chi \circ \alpha.$$

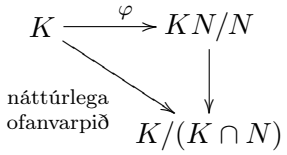
Setning 5.6 (Önnur einsmótunarsetningin). Látum K vera hlutgrúpu í grúpu G og N vera normlega hlutgrúpu í G. Þá er

$$K/(K \cap N) \cong KN/N.$$

Sönnun. Þar sem N er normleg er $kN = Nk$ fyrir öll $k \in K$ og þá $KN = NK$, svo að skv. gömlu heimadæmi er KN hlutgrúpa í G. Hún inniheldur N sem hlutgrúpu, og þar sem N er normleg í G er hún normleg í KN, svo að við getum myndað deildagrúpuna KN/N og höfum náttúrlega ofanvarpið $\pi : KN \to KN/N$. Fáum líka vörpun $\varphi : K \to KN/N, k \mapsto \pi(k)$ (athugum að $K \subset KN$), höfum $\varphi = \pi|K$. Þá er φ átæk: Látum $\zeta \in KN/N$, þá má skrifa $\zeta = xN$, þar sem $x \in KN$, og $x = kn$, þar sem $k \in K$ og $n \in \mathbb{N}$. Þá er $nN = N$, svo að

$$\varphi(x) = kN = k(nN) = (kn)N = xN = \zeta.$$

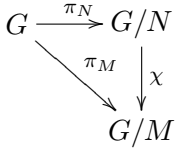
Nú er $\varphi(k) = N$ þ.þ.a.a. $k \in K \cap N$ ef $k \in K$, svo að $\operatorname{Ker} \varphi = K \cap N$. Þá er $K \cap N$ normleg hlutgrúpa í K, og við höfum átækar varpanir



með sama kjarna $K \cap N$, svo að $K/K \cap N \cong KN/N$. ∎

Setning 5.7 (Þriðja einsmótunarsetningin). Látum M og N vera normlegar hlutgrúpur í G þannig að $N \subset M$. Þá er $(G/N)/(M/N) \cong G/M$.

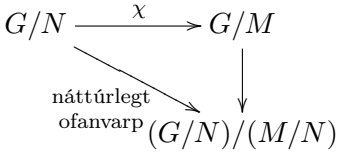
Sönnun. Athugum að náttúrlegu ofanvörpin $\pi_M : G \to G/M$ og $\pi_N : G \to G/N$ eru átækar grúpumótanir og $\operatorname{Ker}\pi_N = N \subset M = \operatorname{Ker}\pi_M$. Skv. ámótunarsetningunni er til nákvæmlega ein grúpumótun $\chi : G/N \to G/M$ þ.a. örvaritið



sé víxlið, þ.e. $\chi(xN) = xM$ fyrir öll $x \in G$. Höfum þá $\chi(xN) = M$ þ.þ.a.a. $x \in M$, og það þýðir að $xN \in M/N$. M.ö.o. er

$$\operatorname{Ker}\chi = M/N$$

því M/N er normleg hlutgrúpa í G/N og við höfum nú þegar átækar grúpumótanir



með sama kjarna, nefnilega M/N; því er $G/M \cong (G/N)/(M/N)$. ∎

Kafli 6

Bein margfeldi af grúpum

6.1 (Ytri) bein margfeldi og beinar summur

Látum $G_1, \ldots, G_n$ vera grúpur. Þá má skilgreina reikniaðgerð á margfeldismenginu

$$G_1 \times \cdots \times G_n = \{(g_1, \ldots, g_n) : g_k \in G_k, k = 1, \ldots, n\}$$

með því að setja

$$(g_1, \ldots, g_n)(h_1, \ldots, h_n) = (g_1 h_1, \ldots, g_n h_n),$$

þetta gerir $G_1 \times \cdots \times G_n$ að grúpu, hlutleysan er $(e_1, \ldots, e_n)$ þar sem e_k er hlutleysan í G_k fyrir $k = 1, \ldots, n$. Umhverfa staks $g = (g_1, \ldots, g_n)$ er $g^{-1} = (g_1^{-1}, \ldots, g_n^{-1})$, þar sem g_k^{-1} er umhverfa g_k í G_k.

Skilgreining 6.1. Köllum mengið $G_1 \times \cdots \times G_n$ með þessari margföldun *(ytra) margfeldi* af grúpunum $G_1, \ldots, G_n$ og táknum það með

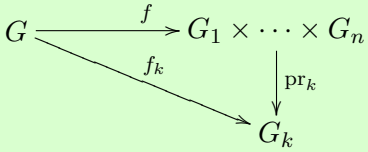
$$G_1 \times \cdots \times G_n \quad \text{eða} \quad \prod_{k=1}^{n} G_k.$$

Ef grúpurnar $G_1, \ldots, Gn$ *eru víxlnar*, þá táknum við það líka með

$$G_1 \oplus \cdots \oplus G_n \quad \text{eða} \quad \bigoplus_{k=1}^{n} G_k$$

og köllum það *(ytri) beinu summuna* af $G_1, \ldots, G_n$.

Setning 6.1. Látum $G_1, \ldots, G_n$ vera grúpur, náttúrlegu ofanvörpin $\mathrm{pr}_k : G_1 \times \cdots \times G_n \to G_k$ eru grúpumótanir og fullnægja eftirfarandi: Ef G er grúpa og $f_k : G \to G_k$ er grúpumótun fyrir $k = 1, \ldots, n$, þá er til nákvæmlega ein grúpumótun $f : G \to G_1 \times \cdots \times G_n$ þannig að örvaritið



sé víxlið fyrir öll $k = 1, \ldots, n$. Vörpunin f er gefin með

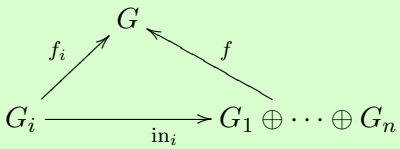
$$f(g) = (f_1(g), \ldots, f_n(g)) .$$

Sönnun. Augljóst, það þarf bara að sýna að þetta sé grúpumótun. ∎

Setning 6.2. Látum $G_1, \ldots, G_n$ vera víxlgrúpur, skrifaðar sem samlagningargrúpur og táknum með 0_i hlutleysuna í G_i, $i = 1, \ldots, n$. Varpanirnar

$$\mathrm{in}_i : G_i \to G_1 \oplus \cdots \oplus G_n, \quad \mathrm{in}_i(g_i) := (0_1, \ldots, 0_{i-1}, g_i, 0_{i+1}, \ldots, 0_n)$$

eru grúpumótanir. Látum $f_i : G_i \to G$ vera grúpumótun frá G_i í *víxl*grúpu G fyrir $i = 1, \ldots, n$. Þá er til nákvæmlega ein grúpumótun $f : G_1 \oplus \cdots \oplus G_n \to G$ þannig að örvaritið



sé víxlið fyrir öll $i = 1, \ldots, n$, þ.e. $f \circ in_i = f_i$. Vörpunin f er gefin með

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{n} f_i(x_i).$$

Sönnun. Ef til er grúpumótun f þ.a. $f \circ \mathrm{in}_i$ fyrir öll i, þá er

$$f(x_1, \ldots, x_n) = f\left(\sum_{i=1}^{n} \mathrm{in}_i(x_i)\right) = \sum_{i=1}^{n} f \circ \mathrm{in}_i(x_i) = \sum_{i=1}^{n} f_i(x_i),$$

svo að f ákvarðast ótvírætt og er gefið með formúlunni í setningunni, ef það er til. Skilgreinum nú á hinn bóginn vörpun f með formúlunni, þá er f

grúpumótun því að

$$\begin{aligned} f((x_1,\ldots,x_n)+(y_1,\ldots,y_n)) &= f(x_1+y_1,\cdots,x_n+y_n)\\ &= \sum_{i=1}^{n} f(x_i+y_i)\\ &= \sum_{i=1}^{n} (f_i(x_i)+f_i(y_i))\\ &= \sum_{i=1}^{n} f_i(x_i) + \sum_{i=1}^{n} f_i(y_i)\\ &= f(x_1,\ldots,x_n)+f(y_1,\ldots,y_n). \end{aligned}$$

Auk þess er

$$\begin{aligned} f\circ \mathrm{in}_i(x) &= f(0_1,\ldots,0_{i-1},x,0_{i+1},\ldots,0)\\ &= f_1(0_1)+\cdots+f_{i-1}(0_{i-1})+f_i(x)+f_{i+1}(0_{i+1})+\cdots+f_n(0_n)\\ &= f_i(x) \end{aligned}$$

fyrir öll $x \in G_i$, svo að $f\circ \mathrm{in}_i = f$ fyrir öll $i \in I$. ∎

Athugasemd. Við notuðum regluna $\sum_{i=1}^{n}(x_i+y_i) = \sum_{i=1}^{n} x_i + \sum_{i=1}^{n} y_i$, sem gildir í víxlgrúpum. Ef aðgerðin er skrifuð sem margföldun, þá verður þetta

$$\prod_{i=1}^{n}(a_ib_i) = \left(\prod_{i=1}^{n} a_i\right)\left(\prod_{i=1}^{n} b_i\right).$$

Hér er $\prod_{i=1}^{n} a_i := a_1\cdots a_n$, nánar tiltekið er $\prod_{i=1}^{0} a_i := e$, þ.e. hlutleysan í G, $\prod_{i=1}^{n+1} a_i = (\prod_{i=1}^{n}) a_{n+1}$ þrepunarskilgreining.

Athugasemd. Reglan $\prod_{i=1}^{n} a_ib_i = (\prod_{i=1}^{n} a_i)(\prod_{i=1}^{n} b_i)$ gildir *alls ekki* í grúpum sem eru ekki víxlnar. Fyrir $n=2$ segir hún

$$a_1b_1a_2b_2 = a_1a_2b_1b_2$$

sem jafngildir $b_1a_2 = a_2b_1$. Þess vegna gildir síðasta setning ekki fyrir óvíxlnar grúpur.

6.2 Kínverska leifasetningin

Setning 6.3. [Kínverska leifasetningin] Látum $m_1,\ldots,m_r$ vera náttúrlegar tölur þ.a. $m_k \geq 1$ fyrir öll $k=1,\ldots,r$ og $\mathrm{ssd}(m_j,m_k)=1$ ef $j\neq k$. Setjum $m := m_1\cdots m_r$. Þar sem $m_i \mid m$ er til nákvæmlega ein grúpumótun

$$\psi_i : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m_i\mathbb{Z} \quad \text{þ.a.} \quad \psi_i(x+m\mathbb{Z}) = x+m_i\mathbb{Z}$$

fyrir öll $x \in \mathbb{Z}$. Þá er vörpunin

$$\psi := (\psi_1, \ldots, \psi_n) : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_r\mathbb{Z}$$

grúpumótun.

Sönnun. Ákvörðum $\operatorname{Ker}\psi$. Látum $\xi \in \operatorname{Ker}\psi$, $\xi = x + m\mathbb{Z}$ með $x \in \mathbb{Z}$. Að $\psi(\xi) = 0$ þýðir að $\psi_i(\xi) = 0$ fyrir öll $i = 1, \ldots, r$, þ.e.

$$x + m_i\mathbb{Z} = m_i\mathbb{Z} \qquad \text{þ.e.} \qquad x \in m_i\mathbb{Z}$$

eða m.ö.o. $m_i \mid x$ fyrir öll $i = 1, \ldots, r$. Vegna $\operatorname{ssd}(m_j, m_k) = 1$ ef $j \neq k$ leiðir af því að $m = m_1 \cdots m_r \mid x$, þ.e. $x \in m\mathbb{Z}$, og það þýðir að $\xi = 0$. Því er $\operatorname{Ker}\psi = \{0\}$, og það þýðir að vörpunin ψ er eintæk. Nú er $\#(\mathbb{Z}/m\mathbb{Z}) = m$ og $\#(\mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_r\mathbb{Z}) = m_1 \cdots m_r = m$. En eintæk vörpun milli tveggja mengja sem hafa jafnmörg stök er gagntæk! ∎

Fylgisetning 6.1. Látum $m_1, \ldots, m_r$ vera eins og í setningu og $x_k \in \{0, \ldots, m_k - 1\}$ fyrir $k = 1, \ldots, r$. Þá er til nákvæmlega ein tala x í $\{0, \ldots, m - 1\}$, þar sem $m := m_1 \cdots m_r$, þannig að

$$x \bmod m_k = x_k$$

fyrir $k = 1, \ldots, r$.

Varpanirnar ψ_k í kínversku leifasetningunni varðveita *margföldun*: Við höfum margföldun á $\mathbb{Z}/n\mathbb{Z}$, $n \geq 1$, þannig að

$$(x + n\mathbb{Z})(y + n\mathbb{Z}) = xy + n\mathbb{Z}.$$

Þetta samsvarar margföldun mod n. Stökin sem hafa margföldunarumhverfu mynda grúpu $\mathcal{U}(n)$.

Setning 6.4 (Viðbót við kínversku leifasetninguna). Vörpunin ψ varpar $\mathcal{U}(m)$ gagntækt á margfeldið

$$\mathcal{U}(m_1) \times \cdots \times \mathcal{U}(m_r).$$

Sönnun. Ef x hefur margföldunarumhverfu y, þá er

$$\psi(xy) = (\psi_1(xy), \ldots, \psi_r(xy)) = (\psi_1(x)\psi_1(y), \ldots, \psi_r(x)\psi_r(y)).$$

En $\psi(1+m\mathbb{Z}) = (1+m_1\mathbb{Z},\ldots,1+m_r\mathbb{Z})$, svo að $\psi(y)$ er margföldunarumhverfa $\psi(x)$; öfugt, ef $\psi(x) = (\psi_1(x),\ldots,\psi_r(x))$ hefur margföldunarumhverfu $z = (z_1,\ldots,z_r)$, þá er til y úr $\mathbb{Z}/m\mathbb{Z}$ þ.a. $\psi(y) = z$, og þá er $\psi(xy) = (1+m_1\mathbb{Z},\ldots,1+m_r\mathbb{Z})$, svo að $xy = 1+m\mathbb{Z}$, þ.e. x hefur margföldunarumhverfu y. ∎

6.2.1 Tenging við φ-fall Eulers

Munum að $\varphi(n) = \#\mathcal{U}(n)$ (með φ fyrir φ-fall Eulers).

Fylgisetning 6.2. Látum m vera náttúrlega tölu ≥ 1, með frumþáttun $m = p_1^{n_1}\cdots p_r^{n_r}$, þar sem $p_1,\ldots,p_r$ eru *ólíkar* frumtölur. Þá er

$$\varphi(m) = \varphi(p_1^{n_1})\cdots\varphi(p_r^{n_r}).$$

Athugasemd. Stak k í $\{1,\ldots,p^n-1\}$, þar sem p er frumtala, er ósamþátta p^n þ.þ.a.a. það sé ekki margfeldi af p. Margfeldin af p í þessu mengi eru pj þar sem $j = 1,\ldots,p^{n-1}-1$ og þau eru $p^{n-1}-1$ talsins. Því er

$$\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1) = p^n\left(1-\frac{1}{p}\right).$$

Fylgisetning 6.3. Látum m vera eins og í fylgisetningu 6.2. Þá er

$$\begin{aligned}\varphi(m) &= (p^{n_1}-p^{n_1-1})\cdots(p^{n_r}-p^{n_r-1})\\ &= m\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_r}\right).\end{aligned}$$

6.3 (Innri) bein margfeldi og beinar summur

Skilgreining 6.2. Látum $H_1,\ldots,H_n$ vera hlutgrúpur í grúpu G. Við segjum að G sé *(innra) beint margfeldi* af hlutgrúpunum $H_1,\ldots,H_n$ ef vörpunin

$$H_1\times\cdots\times H_n \to G, \quad (g_1,\ldots,g_n)\mapsto g_1\cdots g_n$$

er grúpueinsmótun. Skrifum þá gjarnan

$$G = H_1\times\cdots\times H_n$$

og ef G er *víxlin* þá skrifum við

$$G = H_1 \oplus \cdots \oplus H_n$$

og segjum að G sé *(innri) bein summa* af hlutgrúpunum $H_1, \ldots, H_n$.

Athugasemd. Þetta er ekki sami ritháttur og í bókinni, þar er

$$H_1 \times \cdots \times H_n \cong H_1 \oplus \cdots \oplus H_n$$

innri og ytri summa, sem Reyni Axelssyni finnst fráleitt.

Athugasemd. Ef aðgerðin í G er víxlin og skrifuð sem samlagning og $H_1, \ldots, H_n$ eru hlutgrúpur í G, þá er vörpunin

$$H_1 \oplus \cdots \oplus H_n, \quad (g_1, \ldots, g_n) \mapsto g_1 + \cdots + g_n$$

sjálfkrafa grúpumótun. Það þýðir $G = H_1 \oplus \cdots \oplus H_n$ að sérhvert stak g í G megi skrifa með *nákvæmlega einum hætti* sem summu $g = g_1 + \cdots + g_n$ þar sem $g_k \in H_k$ fyrir öll $k = 1, \ldots, n$.

Athugum að ef G er ekki víxlin er ekki sjálfgefið að þetta sé grúpumótun því fyrir hlutgrúpur H, K í G fæst ef

$$\varphi : H \times K \to G, \quad \varphi(h, k) := hk,$$

að

$$\varphi((h_1, k_1), (h_2, k_2)) = \varphi(h_1 h_2, k_1 k_2) = h_1 h_2 k_1 k_2$$

en

$$\varphi(h_1, k_1)\varphi(h_2, k_2) = h_1 k_1 h_2 k_2.$$

Setning 6.5. Látum $H_1, \ldots, H_n$ vera hlutgrúpur í grúpu G. Grúpan G er bein innri summa af þessum hlutgrúpum $H_1, \ldots, H_n$ þ.þ.a.a. eftirfarandi skilyrðum sé fullnægt:

(i) Ef $i, j \in \{1, \ldots, n\}$, $i \neq j$, þá víxlast sérhvert stak úr H_i við sérhvert stak úr H_j.

(ii) $G = H_1 \cdots H_n$, m.ö.o. má skrifa sérhvert stak g úr G sem margfeldi $g = g_1 \cdots g_n$ með $g_k \in H_k$ fyrir $k = 1, \ldots, n$.

(iii) $(H_1 \cdots H_{j-1} H_{j+1} \cdots H_n) \cap H_j = \{e\}$ fyrir öll $j \in \{1, \ldots, n\}$.

Sönnun. Höfum að (i) jafngildir því að vörpunin

$$\varphi : H_1 \times \cdots \times H_n \to G, \quad (g_1, \ldots, g_n) \mapsto g_1 \cdots g_n$$

sé grúpumótun: Ef (i) gildir þá er

$$\begin{aligned}\varphi((g_1, \ldots, g_n)(h_1, \ldots, h_n)) &= \varphi(g_1h_1, \ldots, g_nh_n) \\ &= g_1h_1 \cdots g_nh_n \\ &\overset{\text{(i)}}{=} g_1 \cdots g_n \cdot h_1 \cdots h_n \\ &= \varphi(g_1, \ldots, g_n) \cdot \varphi(h_1, \ldots, h_n).\end{aligned}$$

Ef hins vegar (i) gildir ekki og til eru i, j, $i < j$, og stök x úr H_i og y úr H_j þannig að $xy \neq yx$ þá er

$$\begin{aligned}&\varphi((e, \ldots, e, \underset{\substack{\uparrow \\ i\text{-ta sæti}}}{y}, e, \ldots, e)(e, \ldots, e, \underset{\substack{\uparrow \\ j\text{-ta sæti}}}{x}, e, \ldots, e)) \\ &= \varphi(e, \ldots, e, x, e, \ldots, e, y, e, \ldots, e) \\ &= xy\end{aligned}$$

en

$$\varphi(e, \ldots, e, y, e, \ldots, e)\varphi(e, \ldots, x, e, \ldots, e) = yx \neq xy$$

svo að φ er ekki grúpumótun. Ljóst er að (ii) jafngildir því að φ sé átæk. Skilyrði (iii) segir að $\operatorname{Ker}\varphi = \{e\}$. Ef $(g_1, \ldots, g_n) \in \operatorname{Ker}\varphi$, þ.e. $g_1 \cdots g_n = e$, þá er (að skilyrði (i) gefnu):

$$g_i^{-1} = g_1 \cdots g_{i-1}g_{i+1} \cdots g_n \in (H_1 \cdots H_{i-1}H_{i+1} \cdot H_n) \cap H_i;$$

ef (iii) gildir fæst $g_i^{-1} = e$ og þá $g_j = e$ fyrir öll $j = 1, \ldots, n$. Öfugt, ef $\operatorname{Ker}\varphi = \{(e, \ldots, e)\}$ og $x \in (H_1 \cdots H_{i-1}H_{i+1} \cdots H_n) \cap H_i$ þá má skrifa $x = g_1 \cdots g_{i-1}g_{i+1} \cdots g_n$ með $g_j \in H_j$, $j \neq i$. Þá er (að (i) gefnu)

$$\begin{aligned}&\varphi(g_1, \ldots, g_{i-1}, x^{-1}, g_{i+1}, \ldots, g_n) \\ &= g_1 \cdots g_{i-1}x^{-1}g_{i+1} \cdots g_n \\ &= e\end{aligned}$$

og þá

$$(g_1, \cdots, g_{i-1}, x^{-1}, g_{i+1}, g_n) = (e, \ldots, e),$$

sér í lagi er $x^{-1} = e$ og þá $x = e$. Því er

$$(H_1 \cdots H_{j-1}H_{j+1} \cdots H_n) \cap H_j = \{e\}.$$

■

Athugasemd (Viðvörun!). Það er ekki nóg að krefjast í stað skilyrðis (iii) að $H_i \cap H_j = \{e\}$ fyrir $i \neq j$. Mótdæmi fæst með því að láta H_1, H_2, H_3 vera þrjár ólíkar línur gegnum núllpunktinn í $G := \mathbb{R}^2$: Þá er $H_i + H_j = \mathbb{R}^2$ ef $i \neq j$ og þá $(H_i + H_j) \cap H_k = H_k$ ef $\{i, j, k\} = \{1, 2, 3\}$.

Það má þó veikja skilyrði (iii) aðeins:

Setning 6.6. Í síðustu setningu má í stað skilyrðanna (i) og (iii) setja

(i') Grúpurnar $H_1, \ldots, H_n$ eru normlegar í G.

(iii') $(H_1 \cdots H_{j-1}) \cap H_j = \{e\}$ fyrir $j = 1, \ldots, n$

Sönnun. Sönnum með þrepun: Ef $H_1, \ldots, H_n$ fullnægja (i') og (iii') þá er $H_1 \cdots H_n$ bein summa af $H_1, \ldots, H_n$ og normleg hlutgrúpa í G. En þetta þarf bara að sýna fyrir $n = 2$, því að í þrepunarskrefinu þá notum við tilvikið $n = 2$ á $H_1 \cdots H_{j-1}$ og H_j. Látum þá H, K vera normlegar hlutgrúpur í G þannig að $H \cap K = \{e\}$; sýnum að öll stök úr H víxlist við öll stök úr K: Látum $h \in H, k \in K$. Þá er

$$hkh^{-1}k^{-1} \in H \cap K = \{e\}$$

því að $h \in H$ og $kh^{-1}k^{-1} \in H$ af því að $h^{-1} \in H$ og h normleg, svo að $hkh^{-1}k^{-1} = h(kh^{-1}k^{-1}) \in H$; en líka $hkh^{-1} \in K$ af því að K er normleg, svo að $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} \in K$. En þá er $hkh^{-1}k^{-1} = e$ og þá $hk = kh$ Þar með gildir (i) í síðustu setningu. Fyrir $n = 2$ eru skilyrði (iii) og (iii') sama skilyrðið. ∎

Athugasemd. Höfum nú sýnt að okkar skilgreining á að grúpa sé innra margfeldi af hlutgrúpum sé jafngild skilgreiningunni í kennslubókinni.

Kafli 7

Flokkunarsetning fyrir endanlegar víxlgrúpur

Setning 7.1. Sérhver endanleg víxlgrúpa er einsmóta grúpu af gerðinni

$$\mathbb{Z}/p_1^{r_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_n^{r_n}\mathbb{Z}$$

þar sem $p_1, \ldots, p_n$ eru frumtölur og $r_j \geq 1$ fyrir $j = 1, \ldots, n$. Talnarunan $p_1^{r_1}, \ldots, p_n^{r_n}$ ákvarðast ótvírætt burtséð frá röð (sérhver víxlgrúpa er bein summa af rásuðum víxlgrúpum, gætum svo notað kínversku leifasetninguna á það)

Við sönnum þessa setningu með röð af hjálparsetningum. Skrifum víxlgrúpu sem samlagningargrúpu, svo að við skrifum nx í stað x^n og $\mathbb{Z}x$ í stað $\langle x \rangle$ (hlutgrúpan sem er spönnuð af x), þ.e.

$$\mathbb{Z}x = \{nx : n \in \mathbb{Z}\}.$$

Hjálparsetning 7.1. Látum $\varphi : G \to H$ vera grúpumótun og x vera stak í G með endanlegt raðstig, þá hefur $\varphi(x)$ endanlegt raðstig sem gengur upp í raðstig x.

Sönnun. Athugum að G og H þurfa ekki að vera víxlnar, svo við skrifum aðgerðir sem margföldun. Látum $\psi : \mathbb{Z} \to G$, $n \mapsto x^n$; þá er raðstig x talan j þ.a. $\operatorname{Ker}\psi = \mathbb{Z}j$. Nú er

$$\varphi\psi(n) = \varphi(x^n) = (\varphi(x))^n$$

svo að raðstig $\varphi(x)$ er talan k þ.a. $\mathrm{Ker}(\varphi \circ \psi) = \mathbb{Z}k$. En ljóst er að $\mathrm{Ker}\,\psi \subset \mathrm{Ker}(\varphi \circ \psi)$, svo að $\mathbb{Z}j \subset \mathbb{Z}k$, þ.e. $k \mid j$. ∎

Hjálparsetning 7.2. Látum G vera endanlega víxlgrúpu með fjöldatölu n og p vera frumtölu sem gengur upp í n, þá hefur G stak af raðstigi p.

Sönnun. Notum þrepun yfir n. Ljóst ef $n = 1$. Gerum ráð fyrir að $n > 1$. Látum $x \in G$, $x \neq 0$, setjum $H := \mathbb{Z}x$, sem er rásuð; látum q vera frumþátt í $\#H$. Þá hefur H stak y af raðstigi q. Ef $q = p$, þá þarf ekki að gera meira. Annars setjum við

$$G' := G/\mathbb{Z}y,$$

sem hefur fjöldatölu $\frac{1}{q}\#G < \#G$. Skv. þrepunarforsendu hefur G' stak af raðstigi p, því að $p \mid \frac{1}{q}\#G$. Skrifum það $z + \mathbb{Z}y$. Þá er $pz \in \mathbb{Z}y$, svo að $pqz = 0$ í G. Nú er raðstig z margfeldi af p og því p eða pq. Ef það er p, þá erum við búin; annars hefur qz raðstig p. ∎

Hjálparsetning 7.3. Látum G vera víxlgrúpu með fjöldatölu mn, þar sem $\mathrm{ssd}(m, n) = 1$. Setjum

$$H := \{x \in G : mx = 0\}, \quad K := \{x \in G : nx = 0\}.$$

Þá er $G = H \oplus K$ og $\#H = m$, $\#K = n$.

Sönnun. Til eru j, k úr $\mathbb{Z}$ sem leysa Bézout-jöfnuna $1 = jn + km$. Fyrir x úr G er þá

$$x = jnx + kmx \in H + K,$$

því að $nx \in H$ og $mx \in K$ vegna $mnx = 0$. Þar með er $H + K = G$. Ef $x \in H \cap K$, þá er $mx = nx = 0$, svo að raðstig x gengur upp í m og n og er þá 1 vegna $\mathrm{ssd}(m, n) = 1$; svo að $x = 0$. Því er $H \cap K = \{0\}$; og við höfum $G = H \oplus K$.

Þá er $\#H \cdot \#K = \#G = mn$. Ef p er frumtala sem gengur upp í $\#K$, þá er til stak x úr K með raðstig p, svo að $p \mid n$ og þá p $p \nmid m$. Því hefur $\#K$ engan frumþátt úr m. Eins hefur $\#H$ engan frumþátt úr n, svo að $\#H = m$ og $\#K = n$. ∎

Afleiðing (með þrepun): Ef G er víxlgrúpa með fjöldatölu n og $n = p_1^{\gamma_1} \cdots p_s^{\gamma_s}$ er frumþáttun n, þar sem $p_1, \ldots, p_s$ eru ólíkar frumtölur, þá er $G = G_1 \oplus \cdots \oplus G_s$, þ.a. $\#G_j = p_j^{\gamma_j}$ fyrir $j = 1, \ldots, s$.

Hjálparsetning 7.4. Ef p er frumtala og G er víxlgrúpa með fjöldatölu p^n, þá er G annaðhvort rásuð eða $G = H \oplus K$ þar sem H er rásuð hlutgrúpa í G af sem stærstri fjöldatölu.

Sönnun. Þrepun yfir n. Látum p^m vera hæsta raðstig staks í G, H vera hlutgrúpu spannaða af slíku staki. Við höfum þá $p^m x = 0$ fyrir öll x úr G.

Fyrra tilvik. Ekkert stak úr $G \setminus H$ hefur raðstig p. Athugum þá grúpumótunina

$$\varphi_1 : G \to G, \quad x \mapsto px.$$

Þá er $\operatorname{Ker} \varphi_1$ mengi allra staka í G af raðstigi 1 eða p, svo að $\operatorname{Ker} \varphi_1 \subset H$. En H er rásuð grúpa með fjöldatölu p^m og hefur nákvæmlega p stök þ.a. $px = 0$. Þau mynda hlutgrúpuna $H_1 := p^{m-1}H = \{p^{m-1}x : x \in H\}$. Þá er $G/H_1 \cong pG$, svo að $(G : pG) = \#H_1 = p$. Ef $m = 1$, þá er $pG = \{0\}$ og $G = H$. Annars athugum við grúpumótunina

$$\varphi_2 : pG \to pG, \quad x \mapsto px.$$

Höfum aftur $\operatorname{Ker} \phi_2 \subset H$ og þá $\operatorname{Ker} \phi_2 \subset H_1$; en $H_1 = p^{m-1}H \subset p^{m-1}G \subset pG$, svo að $\operatorname{Ker} \phi_2 = H_1$. Því fæst $pG/H_1 \cong p^2G$, og $\big(pG : p^2G\big) = \#H_1 = p$. Ef $m = 2$, þá er $p^2G = \{0\}$ og $\#G = p^2$, svo að $G = H$. Annars athugum við

$$\varphi_3 : p^2G \to p^2G, \quad x \mapsto px;$$

o.s.frv. Þetta endar á að við fáum $p^{m-1}G = \{0\}$ og $G = H$.

Seinna tilvik. Til er stak úr $G \setminus H$ sem hefur raðstig p. Það spannar hlutgrúpu L í G þ.a. $L \cap H = \{0\}$, því að sniðmengið $L \cap H$ er eiginleg hlutgrúpa í L og $\#L = p$. Athugum ofanvarpið $\pi : G \to G/L$. Það varpar H gagntækt á rásaða hlutgrúpu $\hat{H}$ með stærðstu fjöldatölu í G/L. Skv. þrepunarforsendu er til hlutgrúpa $\hat{K}$ í G/L þ.a. $G/L = \hat{H} \oplus \hat{K}$. Setjum $K := \pi^{-1}[\hat{K}]$ og sýnum að $G = H \oplus K$: Látum $x \in G$, skrifum $\pi(x) = \hat{h} + \hat{k}$ með $\hat{h} \in \hat{H}$ og $\hat{k} \in \hat{K}$; látum h vera stak í H þ.a. $\pi(h) = \hat{h}$ og setjum $k := x - h$; þá er $\pi(k) = \pi(x) - \hat{h} = \hat{k} \in \hat{K}$, svo að $k \in K$ og $x = h + k$; við höfum því að $G = H + K$. Látum $x \in H \cap K$, þá er $\pi(x) \in \hat{H} \cap \hat{K} = \{0\}$, svo að $x \in L$ og þá $x \in H \cap L = \{0\}$. Því er $H \cap K = \{0\}$; við höfum því að $G = H \oplus K$. ∎

Fylgisetning 7.1. Endanleg víxlgrúpa er einsmóta beinni summu af rásuðum grúpum sem hafa fjöldatölu sem er veldi af frumtölu.

Hjálparsetning 7.5. Ef $G = H_1 \oplus \cdots \oplus H_r = K_1 \oplus \cdots \oplus K_s$ þar sem H_j, K_k eru rásaðar grúpur með fjöldatölur sem eru (jákvæð) veldi af frumtölu p, þá er $r = s$ og eftir umröðun er $H_j \cong K_j$ fyrir $j = 1, \ldots, r$.

Sönnun. Athugum $\varphi : G \to G, x \mapsto px$; setjum $G[p] := \operatorname{Ker} \varphi$. Þá er ljóst að

$$G[p] = H_1[p] \oplus \cdots \oplus H_r[p] \cong K_1[p] \oplus \cdots \oplus K_s[p]$$

og $H_j \cong \mathbb{Z}/p\mathbb{Z}$; svo að

$$G \cong (\mathbb{Z}/p\mathbb{Z})^r \cong (\mathbb{Z}/p\mathbb{Z})^s ,$$

svo að $r = s$. Einnig er

$$G/G[p] \cong pG \cong pH_1 \oplus \cdots \oplus pH_r \cong pK_1 \oplus \cdots \oplus pK_r.$$

En $\#(pH_j) = \frac{1}{p}\#H_j$ og því hefur $G/G[p]$ færri stök en G. Getum nú notað þrepun! ∎

Skilgreining 7.1. *Einföld grúpa* er grúpa sem hefur enga normlega hlutgrúpu.

Hluti III

Baugar

Kafli 8

Baugar

8.1 Baugar, baugamótanir

Skilgreining 8.1. *Baugur* er mengi R ásamt tveimur reikniaðgerðum á R, samlagningu og margföldun, þannig að gildi:

(i) Mengið R er víxlgrúpa m.t.t. samlagningar.

(ii) Margföldunin er tengin.

(iii) Um samlagningu og margföldun gilda *dreifireglur*:

Vinstri dreifireglan $a(b+c) = ab + ac$ fyrir öll $a, b, c \in R$.

Hægri dreifireglan $(a+b)c = ac + bc$ fyrir öll $a, b, c \in R$.

Ef margföldunin hefur hlutleysu, þá kallast hún *einingarstak* baugsins R og er táknuð 1_R eða 1; og baugurinn kallast *einbaugur*. Ef margföldunin í baugnum er víxlin, þá kallast baugurinn *víxlinn* eða *víxlbaugur*.

Athugasemd. Nú til dags er venja að skilgreina ávallt bauga sem einbauga.

Skilgreining 8.2. Látum S, R vera bauga. *Baugamótun* $\varphi : R \to S$ er vörpun þ.a.

$$\varphi(a+b) = \varphi(a) + \varphi(b)$$

og

$$\varphi(ab) = \varphi(a) + \varphi(b)$$

fyrir öll a, b úr R. Ef R, S eru einbaugar, þá er *einbaugamótun* $\varphi : R \to S$ baugamótun þ.a. $\varphi(1_R) = 1_S$. Gagntæk baugamótun kallast *baugaeinsmótun*.

Dæmi 8.1. (1) Heilu tölurnar $\mathbb{Z}$, ræðu tölurnar $\mathbb{Q}$, rauntölurnar $\mathbb{R}$ og tvinntölurnar $\mathbb{C}$ eru víxlnir einbaugar m.t.t. venjulegu reikniaðgerðanna. Ívörpin $\mathbb{Z} \hookrightarrow \mathbb{Q}, x \mapsto x$, $\mathbb{Z} \hookrightarrow \mathbb{R}$, $\mathbb{Z} \hookrightarrow \mathbb{C}$, $\mathbb{Q} \hookrightarrow \mathbb{R}$, $\mathbb{Q} \hookrightarrow \mathbb{C}$, $\mathbb{R} \hookrightarrow \mathbb{C}$ eru einbaugamótanir. Náttúrlegu tölurnar $\mathbb{N}$ mynda ekki baug (þær eru ekki víxlgrúpa m.t.t. samlagningar).

(2) Ef R er baugur og X er mengi, þá má gera mengið R^X af öllum vörpunum $f : X \to R$ að baug með því að setja

$$(f+g)(x) := f(x) + g(x)$$
$$(fg)(x) := f(x)g(x)$$

fyrir öll x úr X. Ef R er einbaugur, þá verður R^X einbaugur, eingarstakið er fastavörpun með gildið 1_R. Sértilvik eru mengi allra raunfalla $\mathbb{R}^X$ á X og allra tvinnfalla $\mathbb{C}^X$ á X.

(3) Á grúpunum $\mathbb{Z}/m\mathbb{Z}$ er vel skilgreind margföldun þannig að

$$[x]_m \cdot [y]_m = [xy]_m$$

fyrir öll $x, y \in \mathbb{Z}$; hér höfum við skrifað $[x]_m := x + m\mathbb{Z}$; þetta gerir $\mathbb{Z}/m\mathbb{Z}$ að einbaug með einingarstakið $[1]_m$.

(4) Látum R vera baug; fjölskylda $(a_{jk})_{\{1,\ldots,m\}\times\{1,\ldots,n\}}$ kallast $m \times n$-fylki yfir R ef $a_{jk} \in R$ fyrir öll j, k. Fyrir $m \times n$-fylki $A = (a_{jk})$ og $n \times p$-fylki $B = (b_{kl})$ skilgreinum við fylkið AB sem $m \times p$-fylkið $C = (c_{jl})$ þar sem

$$c_{jl} := \sum_{k=1}^{n} a_{jk} b_{kl}.$$

Táknum með $R^{m\times n}$ mengi $m \times n$-fylkja yfir R. Sjáum: Ef $m \in \mathbb{N}$, þá gerir þessi margföldun, ásamt samlagningunni

$$A + B := (a_{jk} + b_{jk})$$

mengið $R^{m\times m}$ að baug; ef R er einingarbaugur, þá er $R^{m\times m}$ einbaugur; eiingarstak hans er $m \times m$-einingarfylkið $I := (\delta_{jk})$, þar sem δ_{jk} er *Kroneckertáknið* í R,

$$\delta_{jk} = \begin{cases} 1_R & \text{ef } j = k \\ 0_R & \text{ef } j \neq k. \end{cases}$$

Þótt R sé víxlinn þarf $R^{m\times m}$ ekki að vera víxlinn ef $m \geq 2$; þetta er sér í tilvikið fyrir $\mathbb{R}^{m\times m}$, baug $m \times m$-raunfylkja, sem er óvíxlinn baugur ef $m \geq 2$. □

8.2 Reiknireglur

Setning 8.1. Látum R vera baug með núllstaki 0_R.

(1) Fyrir öll a úr R er

$$0_R a = a 0_R = 0_R.$$

(2) (Formerkjareglur) Fyrir öll a, b úr R er

$$(-a)b = a(-b) = -ab,$$

$$(-a)(-b) = ab.$$

Sönnun. Þetta er afleiðing af dreifireglunni.

(1) Höfum

$$\begin{aligned} 0_R + 0_R a &= 0_R a \\ &= (0_R + 0_R)a \\ &= 0_R a + 0_R a, \qquad \text{(dreifiregla)} \end{aligned}$$

styttireglan í samlagningargrúpunni gefur $0_R = 0_R a$. Eins fæst $a0_R = 0_R$ með hinni dreifireglunni (ath. að ef baugurinn er víxlinn eru dreifireglurnar jafngildar, en ef ekki þá þurfum við á þeim báðum að halda).

(2) Höfum

$$\begin{aligned} ab + (-a)b &= (a + (-a))b \qquad \text{(dreifiregla)} \\ &= 0_R b \\ &= 0_R, \end{aligned}$$

svo að $(-a)b$ er samlagningarumhverfa ab, þ.e. $(-a)b = -ab$. Eins fæst að $a(-b) = -ab$ með hinni dreifireglunni. En þá er

$$(-a)(-b) = -a(-b) = -(-ab) = ab.$$

■

Setning 8.2 (Almenn dreifiregla). Ef $a_1, \ldots, a_m, b_1, \ldots, b_n \in R$, R er baugur, þá er

$$\left(\sum_{j=1}^{m} a_j\right)\left(\sum_{k=1}^{m}\right) = \sum_{i=1}^{m}\sum_{k=1}^{n} a_j b_k.$$

Sönnun. Fæst með þrepun, fyrst yfir n, svo yfir m. ■

Setning 8.3. Látum $R_1, \ldots, R_n$ vera bauga; samlagningargrúpan

$$\prod_{k=1}^{n} R_k = R_1 \times \cdots \times R_n$$

verður að baug með margföldueninni

$$(a_1, \ldots, a_n)(b_1, \ldots, b_n) := (a_1 b_1, \ldots, a_n b_n).$$

Ofanvörpin

$$\mathrm{pr}_k : \prod_{k=1}^{n} R_k \to R_k, (a_1, \ldots, a_n) \mapsto a_k$$

verða baugamótanir. Ef $R_1, \ldots, R_n$ eru einbaugar, þá er $\prod_{k=1}^{n} R_k$ einbaugur með einingarstakið $(1_{R_1}, 1_{R_2}, \ldots, 1_{R_n})$ og ofanvörpin verða baugamótanir.

Sönnun. Augljóst (þarf að fara í gegnum að dreifireglurnar gildi, en það er einfalt). ∎

Setning 8.4 (Viðbót við kínversku leifasetninguna). Látum $m_1, \ldots, m_r$ vera náttúrlegar tölur þ.a. $m_k \geq 1$ og $\mathrm{ssd}(m_j, m_k) = 1$ ef $j \neq k$. Samlagningargrúpueinsmótunin

$$\mathbb{Z}/m_1 \cdots m_r\mathbb{Z} \to \mathbb{Z}/m_1 \times \cdots \times \mathbb{Z}/m_r\mathbb{Z}, [x]_{m_1 \cdots m_r} \mapsto ([x]_{m_1}, \ldots, [x]_{m_r})$$

er í raun *einbaugaeinsmótun*.

Sönnun. Augljóst! (Það var augljóst að hún er baugamótun en var ekki augljóst að hún væri gagntæk, en við erum búin að sanna það). ∎

Athugasemd. Í kennslubók er þess krafist að í einbaug R sé $1_R \neq 0_R$; þetta er ekki sniðugt.

Athugum hins vegar: Ef $1_R = 0_R$ og $a \in R$, þá er

$$a = 1_R a = 0_R a = 0_R,$$

svo að $R = \{0_R\}$; m.ö.o. hefur R bara eitt stak, sem er bæði núllstak og einingarstak! Slíkur baugur kallast *núllbaugur*. Við teljum núllbaug vera einbaug en bókin ekki.

8.3 Deilibaugar, heilbaugar og svið

Skilgreining 8.3. Látum R vera einbaug. Stak a í R kallast *eind* ef það hefur margföldunarumhverfu. Skv. gamalli setningu (um hálfgrúpur með hlutleysu) mynda eindirnar grúpu m.t.t. margföldunar; við köllum hana *eindagrúpu* (eða bara *margföldunargrúpu*) baugsins og táknum hana með

$$R^*$$

Dæmi 8.2. $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$, en $\mathbb{Z}^* = \{1, -1\}$. Athugum að grúpan $(\mathbb{Z}/m\mathbb{Z})^*$ er einsmóta $\mathcal{U}(m)$, sem var grúpa staka úr $\{0, \ldots, m-1\}$ þ.a. $\text{ssd}(k, m) = 1$ með margföldun mod m. □

Skilgreining 8.4. Við segjum að baugur sé *deilibaugur* ef hann er einbaugur og $R^* = R \setminus \{0\}$; þetta þýðir að $1_R \neq 0_R$ og sérhvert stak nema núllstakið hafi margföldunarumhverfu. Víxlinn deilibaugur kallast *svið* (~~sumir segja *kroppur*~~).

Athugasemd. Ef $1_R \neq 0_R$ í baug R, þá er $0_R \cdot a = 0_R \neq 1_R$ fyrir öll a úr R þannig að 0_R getur alls ekki haft margföldunarumhverfu.

Dæmi 8.3. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ eru svið, en $\mathbb{Z}$ ekki. Eitt einfaldasta dæmið um deilibaug sem er ekki víxlinn er *fertölur Hamiltons* (sjá dæmablað). □

Skilgreining 8.5. Látum R vera baug. *Hlutbaugur* í R er hlutmengi S í R sem er lokað m.t.t. bæði samlagningar og margföldunar og verður baugur m.t.t. aðgerðanna sem þannig fást á S.

Hluteinbaugur í einbaug R er hlutbaugur S í R sem er einbaugur og þannig að $1_S = 1_R$.

Athugasemd. $\{0\}$ er hlutbaugur í $\mathbb{Z}$ og einbaugur, en ekki hluteinbaugur í $\mathbb{Z}$; annað dæmi: $\{0\} \times \mathbb{Z}$ er hlutbaugur í $\mathbb{Z} \times \mathbb{Z}$ og einbaugur, *líka* í skilningi bókarinnar, með hlutleysu $(0, 1)$; en ekki hluteinbaugur í $\mathbb{Z} \times \mathbb{Z}$, því að hlutleysan í $\mathbb{Z} \times \mathbb{Z}$ er $(1, 1)$.

Skilgreining 8.6. Látum R vera baug.

(1) Við segjum að stak a í R sé *núlldeilir frá vinstri* ef til er stak b í R þ.a. $b \neq 0$ en $ab = 0$.

(2) Við segjum að stak a í R sé *núlldeilir frá hægri* ef til er stak b í R þ.a. $b \neq R$ en $ba = 0$.

(3) Við segjum að stak a í R sé *styttanlegt frá vinstri* ef $ab = ac$ leiðir til $b = c$ fyrir öll b, c úr R.

(4) Við segjum að stak a í R sé *styttanlegt frá hægri* ef $ba = ca$ leiðir til $b = c$ fyrir öll b, c úr R.

Ef baugurinn er *víxlinn*, þá er enginn munur á núlldeilum frá hægri og frá vinstri, og við tölum einfaldlega um *núlldeila* ; eins er stak styttanlegt frá vinstri þ.þ.a.a. það sé styttanlegt frá hægri; og við köllum það einfaldlega *styttanlegt* .

Athugasemd. Skv. þessari skilgreiningu er núllstakið núlldeilir þ.þ.a.a. R sé ekki núllbaugur (skv. bók telst 0 ekki vera núlldeilir).

Setning 8.5. Stak a í baug er styttanlegt frá vinstri þ.þ.a.a. það sé ekki núlldeilir frá vinstri; það er styttanlegt frá hægri þ.þ.a.a. það sé ekki núlldeilir frá hægri.

Sönnun. Sönnum fyrri fullyrðinguna. Ef a er styttanlegt frá vinstri og b er stak þ.a. $ab = 0$, þá er $ab = 0 = a \cdot 0$ og þá $b = 0$. Því er a ekki núlldeilir frá vinstri. Ef hins vegar a er ekki núlldeilir frá vinstri og $ab = ac$, þá er $a(b - c) = ab - ac = 0$ og þar sem a er ekki núlldeilir frá vinstri er $b - c = 0$ og því $b = c$. ∎

Athugasemd. *Eind* er alltaf styttanleg, bæði frá hægri og frá vinstri. Í deilibaug er núllstakið því einni núlldeilirinn (hvort sem er frá hægri eða frá vinstri).

Skilgreining 8.7. *Heilbaugur* er víxlinn einbaugur sem er ekki núllbaugur þannig að öll stök nema núllstakið séu styttanleg, þ.e. núllstakið er eini núlldeilirinn.

Dæmi 8.4. (1) Sérhvert svið er heilbaugur.
(2) Baugur heilu talnanna $\mathbb{Z}$ er heilbaugur. □

Látum R vera baug, $a \in R$ og athugum vörpunina $v_a : R \to R, v_a(x) := ax$. Að a sé styttanlegt *frá vinstri* þýðir að vörpunin v_a sé *eintæk*. Ef R er *víxlinn*

einbaugur og vörpunin v_a er *átæk*, þá er til stak b í R þannig að $v_a(b) = 1$, þ.e. $ab = 1$, það þýðir að a sé eind, þ.e. hafi margföldunarumhverfu.

Ef nú R er *endanlegt* mengi, þá er vörpun $R \to R$ átæk þ.þ.a.a. hún sé eintæk . Fáum:

Setning 8.6. Endanlegur heilbaugur er svið.

Dæmi 8.5. Látum $m \geq 1$. Fyrir $m = 1$ er $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/\mathbb{Z} = \{0\}$ núllbaugur, sem er einbaugur en ekki heilbaugur. Fyrir $m \geq 2$ er $\mathbb{Z}/m\mathbb{Z}$ heilbaugur þ.þ.a.a. ekki séu til stök í baugnum sem eru ekki núll en margfeldi þeirra sé núll; það þýðir að fyrir öll $x, y \in \mathbb{Z}$ þ.a. $m \mid xy$ gildi $m \mid x$ eða $m \mid y$. Og þetta þýðir að m sé frumtala. Sjáum: $\mathbb{Z}/m\mathbb{Z}$ er heilbaugur þ.þ.a.a. m sé frumtala, og þá er $\mathbb{Z}/m\mathbb{Z}$ *svið*. □

Athugasemd. Að R sé heilbaugur þýðir að R sé víxlinn einbaugur þ.a. $1_R \neq 0_R$ og eftirfarandi skilyrði sé fullnægt:

Ef $a, b \in R$ og $ab = 0$, þá er $a = 0$ eða $b = 0$.

Skilgreining 8.8. *Kennitala baugs* R er minnsta jákvæða heila talan n þannig að $na = 0$ fyrir öll a úr R *ef* slík tala er til; annars er kennitalan 0. Kennitalan er táknuð með

$$\operatorname{char} R.$$

Fyrir einbauga er þetta einfaldara:

Setning 8.7. Látum R vera einbaug. Þá er til nákvæmlega ein einbaugamótun $\varphi : \mathbb{Z} \to R$; hún er gefin með

$$\varphi(n) = n \cdot 1_R.$$

Látum φ vera þessa einbaugamótun. Þá er $\operatorname{char} R$ talan n þ.a.

$$\operatorname{Ker} \varphi = n\mathbb{Z}.$$

M.ö.o. er $\operatorname{char} R$ raðstig 1_R í samlagningargrúpunni R ef það er endanlegt, en 0 ef það er óendanlegt.

Sönnun. Athugum: Ef $n \cdot 1_R = 0$, þá er

$$na = n \cdot (1_R a) = (n1_R)a = 0a = 0$$

fyrir öll a úr R. Öfugt, ef $na = 0$ fyrir öll a úr R, þá er sér í lagi $n1_R = 0$. ■

Kafli 9

Íðul

Skilgreining 9.1. Látum R vera baug. Hlutmengi $\mathfrak{A}$ í R kallast

(i) *Íðal frá vinstri (vinstra íðal)* ef það er hlutgrúpa í samlagningargrúpu R og $ra \in \mathfrak{A}$ fyrir öll $r \in R$ og $a \in \mathfrak{A}$.

(ii) *Íðal frá hægri (hægra íðal)* ef það er hlutgrúpa í samlagningargrúpunni R og $ar \in \mathfrak{A}$ fyrir öll $r \in R$ og $a \in \mathfrak{A}$.

(iii) *Tvíhliða íðal* ef það er íðal frá vinstri og frá hægri.

Athugasemd. Að $\mathfrak{A}$ sé vinstra íðal í einbaug R er jafngilt því að gildi:

(i) $0 \in \mathfrak{A}$.

(ii) Ef $a, b \in \mathfrak{A}$, þá er $a + b \in \mathfrak{A}$.

(iii) Ef $r \in R$ og $a \in \mathfrak{A}$ þá er $ra \in \mathfrak{A}$.

Ástæðan er að af (iii) leiðir að fyrir öll $a \in \mathfrak{A}$ er $-a = (-1)a \in \mathfrak{A}$.

9.1 Deildabaugar

Setning 9.1. Látum R vera baug og $\mathfrak{A}$ vera hlutgrúpu í samlagningargrúpunni R. Þá er jafngilt:

(i) $\mathfrak{A}$ er tvíhliða íðal í R.

(ii) Skilgreina má margföldun á deildagrúpunni $R/\mathfrak{A}$ þannig að

$$(a + \mathfrak{A}) \cdot (b + \mathfrak{A}) = ab + \mathfrak{A}$$

fyrir öll $a, b \in R$.

Ef þessum skilyrðum er fullnægt, þá verður $R/\mathfrak{A}$ að baug með þessari margföldun úr (ii), og $R/\mathfrak{A}$ verður einbaugur ef R er einbaugur.

Sönnun. (i)⇒(ii). Sýna þarf: Ef $\mathfrak{A}$ er tvíhliða íðal og $a+\mathfrak{A} = c+\mathfrak{A}$ og $b+\mathfrak{A} = d+\mathfrak{A}$, þá er

$$ab+\mathfrak{A} = cd+\mathfrak{A}$$

því þá er þetta vel skilgreind margföldun. En $a+\mathfrak{A} = c+\mathfrak{A}$ þýðir að $a-c \in \mathfrak{A}$, og $b+\mathfrak{A} = c+\mathfrak{A}$ þýðir að $(b-d) \in \mathfrak{A}$. En þá er

$$ad-cd = \underbrace{(a-c)}_{\in\mathfrak{A}}\underbrace{b}_{\in R} + \underbrace{c}_{\in R}\underbrace{(b-d)}_{\in\mathfrak{A}} \in \mathfrak{A}$$

af því að $\mathfrak{A}$ er *tvíhliða íðal*. Þetta sýnir að margföldunin í (ii) er vel skilgreind. Gerum nú ráð fyrir að (ii) gildi. Sýnum fyrst að $R/\mathfrak{A}$ verður að baug: Vitum að $R/\mathfrak{A}$ jer víxlgrúpa með tilliti til samlagningar. Nú fæst

$$\begin{aligned}(a+\mathfrak{A})((b+\mathfrak{A})(c+\mathfrak{A})) &= (a+\mathfrak{A})(bc+\mathfrak{A})\\ &= a(bc)+\mathfrak{A}\\ &= (ab)c+\mathfrak{A}\\ &= (ab+\mathfrak{A})(c+\mathfrak{A})\\ &= ((a+\mathfrak{A})(b+\mathfrak{A}))(c+\mathfrak{A})\end{aligned}$$

svo að tengireglan gildir. Einnig er

$$\begin{aligned}(a+\mathfrak{A})((b+\mathfrak{A})+(c+\mathfrak{A})) &= (a+\mathfrak{A})((b+c)+\mathfrak{A})\\ &= a(b+c)+\mathfrak{A}\\ &= (ab+ac)+\mathfrak{A}\\ &= (ab+\mathfrak{A})+(ac+\mathfrak{A})\\ &= (a+\mathfrak{A})(b+\mathfrak{A})+(a+\mathfrak{A})(c+\mathfrak{A})\end{aligned}$$

svo að vinstri dreifireglan gildir. Eins sést að hægri dreifireglan gildir. Ef R er einbaugur, þá er

$$\begin{aligned}(1_R+\mathfrak{A})(a+\mathfrak{A}) &= 1_R a+\mathfrak{A} = a+\mathfrak{A}\\ (a+\mathfrak{A})(1_R+\mathfrak{A}) &= a1_R+\mathfrak{A} = a+\mathfrak{A}\end{aligned}$$

svo að $1_R+\mathfrak{A}$ er einingarstak í $R/\mathfrak{A}$. Þá gildir sér í lagi að

$$\begin{aligned}ra+\mathfrak{A} &= (r+\mathfrak{A})(a+\mathfrak{A}) = 0_{R/\mathfrak{A}}\\ ar+\mathfrak{A} &= (a+\mathfrak{A})(r+\mathfrak{A}) = 0_{R/\mathfrak{A}}\end{aligned}$$

svo að $ra, ar \in \mathfrak{A}$ og því er $\mathfrak{A}$ tvíhliða íðal í R; þar með gildir (ii)⇒(i). ∎

Skilgreining 9.2. Látum $\mathfrak{A}$ vera tvíhliða íðal í baug R, við köllum baug-inn $R/\mathfrak{A}$ með margföldun úr síðustu setningu *deildabaug* af R með tilliti til $\mathfrak{A}$.

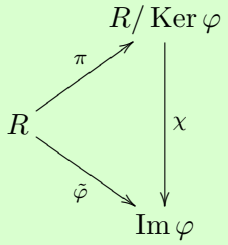
Athugasemd. Látum $\mathfrak{A}$ vera tvíhliða íðal í R. Skilyrði (ii) segir að náttúrlega ofanvarpið

$$\pi : R \to R/\mathfrak{A}, \quad r \mapsto r + \mathfrak{A}$$

sé *baugamótun*. Ef R er einbaugur, þá er $\pi(1_R) = 1_R + \mathfrak{A}$ *einingarstakið* í $R/\mathfrak{A}$, svo að π er þá *einbaugamótun*.

Athugasemd. Fyrir víxlbauga er enginn munur á hægri og vinstri íðulum, og þau eru þá tvíhliða; tölum þá einfaldlega um *íðul*.

Setning 9.2. Látum $\varphi : R \to S$ vera [ein]baugamótun. Þá er $\operatorname{Ker}\varphi$ tví-hliða íðal í R og $\operatorname{Im}\varphi$ er hlut[ein]baugur í S; grúpueinsmótunin χ sem gerir örvaritið



víxlið, þar sem π er náttúrlega ofanvarpið og $\tilde{\varphi} : R \to \operatorname{Im}\varphi, x \mapsto \varphi(x)$, er [ein]baugaeinsmótun.

Sönnun. Ef nú $x, y \in R/\operatorname{Ker}\varphi$, þá eru til $a, b \in R$ þannig að $x = a + \operatorname{Ker}\varphi = \pi(a)$ og $y = b + \operatorname{Ker}\varphi = \pi(b)$; þá er

$$\begin{aligned}
\chi(xy) &= \chi(\pi(a)\pi(b)) \\
&= \chi(\pi(ab)) \\
&= \tilde{\varphi}(ab) \\
&= \varphi(ab) \\
&= \varphi(a)\varphi(b) \\
&= \tilde{\varphi}(a)\tilde{\varphi}(b) \\
&= \chi(\pi(a))\chi(\pi(b)) \\
&= \chi(x)\chi(y)
\end{aligned}$$

svo að χ er baugamótun. Ef φ er einbaugamótun, þá er

$$1_S = \varphi(1_R) \in \operatorname{Im}\varphi,$$

svo að $\operatorname{Im}\varphi$ er hluteinbaugur í S og

$$\chi(1_{R/\operatorname{Ker}\varphi}) = \chi(\pi(1_R)) = \varphi(1_R) = 1_S = 1_{\operatorname{Im}\varphi}.$$ ∎

Athugasemd. Ef $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$ eru vinstri [hægri, tvíhliða] íðul í baug R, þá er hlutgrúpan

$$\mathfrak{A}_1 + \cdots + \mathfrak{A}_n = \{a_1 + \cdots + a_n : a_k \in \mathfrak{A}_k \text{ fyrir } k = 1, \ldots, n\}$$

vinstra [hægra, tvíhliða] íðal í R. Einnig er

$$\mathfrak{A}_1 \cap \cdots \cap \mathfrak{A}_n$$

vinstra [hægra, tvíhliða] íðal í R. Látum R vera *einbaug*, fyrir $a \in R$ er

$$Ra := \{ra : r \in R\}$$

vinstra íðal í R, og

$$aR := \{ar : r \in R\}$$

hægra íðal í R. Ef $a_1, \ldots, a_n \in R$, þá er

$$Ra_1 + \cdots + Ra_n$$

minnsta vinstra íðal í sem inniheldur $a_1, \ldots, a_n$; köllum það *vinstra íðalið sem* $a_1, \ldots, a_n$ *spanna*. Eins er

$$a_1R + \cdots + a_nR$$

minnsta hægra íðalið sem inniheldur $a_1, \ldots, a_n$, köllum það *hægra íðalið sem* $a_1, \ldots, a_n$ *spanna*. Köllum svona íðul *endanlega spönnuð*.

9.2 Höfuðíðalbaugar

Setning 9.3. Látum R vera [ein]baug. Þá er

$$Z(R) := \{a \in R : ab = ba \quad \forall b \in R\}$$

víxlinn hlut[ein]baugur í R.

Sönnun. Ljóst er að $0_R \in Z(R)$; fyrir $a_1, a_2 \in Z(R)$ er

$$(a_1 + a_2)b = a_1b + a_2b = ba_1 + ba_2 = b(a_1 + a_2)$$

fyrir öll $b \in R$, svo að $a_1 + a_2 \in Z(R)$; annað sést með svipuðum hætti. ∎

Skilgreining 9.3. Köllum $Z(R)$ *miðju* baugsins R.

Ef $a \in Z(R)$, þá er $Ra = aR$, svo að Ra er tvíhliða íðal.

Skilgreining 9.4. Íðal $\mathfrak{A}$ í baug R kallast *höfuðíðal* ef til er stak $a \in Z(R)$ þannig að

$$\mathfrak{A} = Ra = aR.$$

Skilgreining 9.5. Baugur R kallast *höfuðíðalbaugur* ef hann er víxlinn einbaugur, $1_R \neq 0_R$ og sérhvert íðal í R er höfuðíðal.

Dæmi 9.1. Við þekkjum allar hlutgrúpurnar í $\mathbb{Z}$; það eru mengin $m\mathbb{Z}$ þar sem $m \in \mathbb{N}$, en þessar hlutgrúpur eru allar íðul í $\mathbb{Z}$. Sér í lagi er $\mathbb{Z}$ *höfuðíðalbaugur*. Deildabaugarnir eru baugarnir $\mathbb{Z}/m\mathbb{Z}, m \in \mathbb{N}$. □

Athugasemd. Í skilgreiningu á höfuðíðalbaug er venja að krefjast þess einnig að hann hafi enga núlldeila nema núllstakið.

Rifjum upp að *heilbaugur* var víxlinn einbaugur sem var ekki núllbaugur og hefur enga núlldeila nema núllstakið. Þá má orða skilgreininguna þannig:

Skilgreining 9.6 (endurbætt). *Höfuðíðalbaugur* er heilbaugur þannig að sérhvert íðal hans sé höfuðíðal.

Athugasemd. Samkvæmt skilgreiningu bókar er íðal í R hlutbaugur í R, en oftast ekki *hluteinbaugur*: Ef $\mathfrak{A}$ er íðal (frá vinstri, hægri eða tvíhliða) og $1_R \in \mathfrak{A}$, þá er $\mathfrak{A} = R$. Ef t.d. $\mathfrak{A}$ er íðal frá vinstri, þá er

$$r = r \cdot 1_R \in \mathfrak{A}$$

fyrir öll $r \in R$ ef $1_R \in \mathfrak{A}$.

Setning 9.4. Látum $\mathfrak{A}$ vera tvíhliða íðal í baug R. Íðölin (frá vinstri, hægri eða tvíhliða) í deildabaugnum $R/\mathfrak{A}$ eru mengin $\mathfrak{B}/\mathfrak{A}$, þar sem $\mathfrak{B}$ er íðal (frá vinstri, hægri eða tvíhliða) í R þ.a. $\mathfrak{A} \subset \mathfrak{B}$.

Sönnun. Látum $\pi : R \to R/\mathfrak{A}$ vera náttúrlega ofanvarpið og $\mathfrak{C}$ vera íðal af einhverri gerð í $R/\mathfrak{A}$; þá er $\mathfrak{B} := \pi^{-1}[\mathfrak{C}]$ íðal í R af sömu gerð, $\mathfrak{A} \subset \mathfrak{B}$, og þar sem π er átæk er $\mathfrak{C} = \pi[\pi^{-1}[\mathfrak{C}]] = \pi[\mathfrak{B}] = \mathfrak{B}/\mathfrak{A}$. Augljóst er að fyrir íðal $\mathfrak{B}$ þ.a. $\mathfrak{A} \subset \mathfrak{B}$ er $\mathfrak{B}/\mathfrak{A}$ íðal í $R/\mathfrak{A}$ af sömu gerð. ∎

Athugasemd. Ef $\varphi : R \to S$ er baugamótun og $\mathfrak{C}$ er íðal (af einhverri gerð) í S, þá er frummyndin $\varphi^{-1}[\mathfrak{C}]$ íðal í R af sömu gerð; segjum að $\mathfrak{C}$ sé íðal frá vinstri og $r \in R$, $a \in \varphi^{-1}[\mathfrak{C}]$, þá er $\varphi(ra) = \varphi(r)\varphi(a) \in \mathfrak{C}$, því að $\varphi(r) \in S$ og $\varphi(a) \in \mathfrak{C}$, svo að $ra \in \varphi^{-1}[\mathfrak{C}]$. Ef hins vegar $\mathfrak{A}$ er íðal í R, þá þarf myndin $\varphi[\mathfrak{A}]$ ekki að vera íðal í S, *nema* vörpunin φ sé átæk.

Setning 9.5. Einbaugur R er deilibaugur þ.þ.a.a. R sé ekki núllbaugurinn og R hafi engin vinstri íðul nema $\{0\}$ og R.

Sönnun. Ef R er deilibaugur og $\mathfrak{A}$ er íðal í R þannig að $\mathfrak{A} \neq \{0\}$, þá inniheldur $\mathfrak{A}$ stak a þ.a. $a \neq 0$, og a hefur umhverfu b; en þá er $1_R = ba \in \mathfrak{A}$ og þá $\mathfrak{A} = R$.

Öfugt ef $R \neq \{0\}$ og hefur engin vinstri íðul nema $\{0\}$ og R, látum $a \in R$, $a \neq 0$; þá er Ra vinstra íðal þannig að $a \in Ra$, svo að $Ra \neq \{0\}$ og því $Ra = R$; sér í lagi er $1_R \in Ra$, svo að til er $b \in R$ þannig að $ba = 1_R$; en þá er $b \neq 0$, því að $0_R \cdot a = 0_R \neq 1_R$; og sama röksemdafærsla sýnir að til er $c \in R$ þannig að $cb = 1_R$. En þá er

$$c = c1_R = c(ba) = (cb)a = 1_R a = a,$$

svo að $ab = ba = 1_R$ og b er því umhverfa fyrir a. ∎

Athugasemd. Eins sést: R er deilibaugur þ.þ.a.a. $R \neq \{0\}$ og R hafi engin *hægri* íðul nema $\{0\}$ og R. Það er *ekki nóg* að R hafi engin *tvíhliða* íðul nema $\{0\}$ og R; R getur samt haft fullt af hægri og vinstri íðulum.

Fylgisetning 9.1. *Víxlinn* einbaugur K er svið þ.þ.a.a. hann sé ekki núllbaugur og hafi engin íðul nema $\{0\}$ og K.

Athugasemd. Skrifum $\{0\} = K \cdot 0$ og $K = K \cdot 1$, svo að $\{0\}, K$ eru alltaf höfuðíðul, svo svið er höfuðíðalbaugur.

9.3 Háíðul og frumíðul

Skilgreining 9.7. *Háíðal* [frá vinstri, frá hægri, tvíhliða] er eiginlegt íðal [frá vinstri, frá hægri, tvíhliða] sem er ekki innihaldið í stærra eiginlegu íðali [frá vinstri, frá hægri, tvíhliða].

Athugasemd. Notum hugtakið aðallega fyrir víxlbauga og getum þá talað um „háíðal“ án þess að taka fram tegundina. En

Setning 9.6. Tvíhliða íðal $\mathfrak{A}$ er háíðal *frá vinstri* þ.þ.a.a. $R/\mathfrak{A}$ sé deilibaugur (og þá er það háíðal frá hægri).

Sönnun. Því að vinstri íðulin í $R/\mathfrak{A}$ eru íðulin $\mathfrak{B}/\mathfrak{A}$ þar sem $\mathfrak{B}$ er vinstra íðal í R; og $\mathfrak{B}/\mathfrak{A}$ er eiginlegt í $R/\mathfrak{A}$ þ.þ.a.a. $\mathfrak{B}$ sé eiginlegt í R. ∎

Fylgisetning 9.2. Látum R vera víxlinn einbaug. Íðal $\mathfrak{A}$ í R er háíðal þ.þ.a.a. $R/\mathfrak{A}$ sé svið.

Skilgreining 9.8. Látum R vera víxlinn einbaug. Íðal $\mathfrak{A}$ í R kallast *frumíðal* ef það er *eiginlegt* og eftirfarandi skilyrði er fullnægt:

Ef $a, b \in R$ og $ab \in \mathfrak{A}$, þá er $a \in \mathfrak{A}$ eða $b \in \mathfrak{A}$.

Athugasemd. $a \in \mathfrak{A}$ jafngildir $\pi(a) = 0$, þar sem $\pi : R \to R/\mathfrak{A}$ er ofanvarpið. Því er ljóst:

Setning 9.7. Íðal í víxlnum einbaug er frumíðal þ.þ.a.a. $R/\mathfrak{A}$ sé heilbaugur.

Athugasemd. Þar sem svið er heilbaugur er sérhvert háíðal frumíðal, en ekki öfugt.

Dæmi 9.2. Núllíðalið $\mathbb{Z} \cdot 0$ í $\mathbb{Z}$ er frumíðal. Fyrir $m \in \mathbb{N}, m \geq 1$ er jafngilt:

(i) $m\mathbb{Z}$ er frumíðal,

(ii) $m\mathbb{Z}$ er háíðal,

(iii) m er frumtala.

því að $\mathbb{Z}/m\mathbb{Z}$ er heilbaugur þ.þ.a.a. m sé frumtala; og endanlegur heilbaugur er svið. □

Athugasemd. Hluteinbaugur R í sviði K er heilbaugur, því stak a í R þannig að $a \neq 0$ hefur umhverfu í K og er því styttanlegt í K og þar með líka í R.

9.4 Brotasvið

Skilgreining 9.9. Látum R vera heilbaug. *Brotasvið* fyrir R er svið K þannig að R sé hluteinbaugur í K og sérhvert stak í K megi skrifa sem ab^{-1} þar sem $a, b \in R$ og $b \neq 0$ (umhverfan er tekin í K).

Setning 9.8. Sérhver heilbaugur hefur brotasvið sem ákvarðast ótvírætt burtséð frá einsmótun.

Sönnun. Setjum $M := R \times (R \setminus \{0\})$. Skilgreinum vensl á M með

$$(a, b) \sim (c, d) \quad \text{þ.þ.a.a.} \quad ad = bc.$$

Þetta eru jafngildisvensl: $(a, b) \sim (a, b)$ vegna $ab = ab$; ef $(a, b) \sim (c, d)$, þ.e. $ad = bc$, þá er $cb = da$ og því $(c, d) \sim (a, b)$, því að R er víxlinn; ef $(a, b) \sim (c, d)$ og $(c, d) \sim (e, f)$, þá er $ad = bc$ og $cf = de$ og því

$$afd = adf = bcf = bde = bed$$

en d er styttanlegt, svo að $af = de$ og því $(a, b) \sim (e, f)$. Táknum jafngildisflokk (a, b) með $\frac{a}{b}$. Nú má skilgreina samlagningu og margföldun á mengi jafngildisflokkanna þannig að

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Til að sjá að þetta sé skynsamleg skilgreining þarf að sýna: Ef $\frac{a}{b} = \frac{e}{f}$ og $\frac{c}{d} = \frac{g}{h}$, þá er

$$\frac{ad + bc}{bd} = \frac{eh + fg}{fh} \qquad \text{og} \qquad \frac{ac}{bd} = \frac{eg}{fh}$$

En forsendan þýðir að $af = be$ og $ch = dg$, svo að

$$(ad + bc)fh = adfh + bcfh = afdh + bfch = bedh + bfdg = bd(eh + fg)$$

sem þýðir að $\frac{ad+bc}{bd} = \frac{eh+fg}{fh}$; og

$$acfh = afch = bedg = bdeg$$

sem þýðir að $\frac{ac}{bd} = \frac{eg}{fh}$. Nú er auðvelt að sjá að þessar reikniaðgerðir gera K að víxlbaug með einingarstaki $\frac{1}{1}$ og núllstaki $\frac{0}{1}$; til dæmis sést tengireglan fyrir samlagningu þannig:

$$\begin{aligned}\left(\frac{a}{b}+\frac{c}{d}\right)+\frac{e}{f} &= \frac{ad+bc}{bd}+\frac{e}{f}\\ &= \frac{(ad+bc)f+bde}{bdf}\\ &= \frac{adf+bcf+bde}{bdf}\\ &= \frac{adf+b(cf+de)}{bdf}\\ &= \frac{a}{b}+\frac{cf+de}{df}\\ &= \frac{a}{b}+\left(\frac{c}{d}+\frac{e}{f}\right),\end{aligned}$$

aðrar reglur sjást á svipaðan hátt. Þar eð R er heilbaugur er ljóst að $\frac{a}{b} = \frac{0}{1}$ þ.þ.a.a. $1a = b0$, þ.e. $a = 0$. Ef nú $\frac{a}{b} \neq \frac{0}{1}$, þá er $\frac{b}{a} \in K$ og

$$\frac{a}{b}\cdot\frac{b}{a} = \frac{ab}{ba} = \frac{ab}{ab} = \frac{1}{1}.$$

Þetta þýðir að K er *svið*. Nú höfum við vörpun $\varphi : R \to K, a \mapsto \frac{a}{1}$. Hún er eintæk baugamótun og við „samsömum R við mynd sína í K“ og skrifum a í stað $\frac{a}{1}$; þannig lítum við á R sem hlutmengi í K. Strangt tiltekið þýðir þetta eftirfarandi: Við tökum $\operatorname{Im}\varphi$ út úr K og setjum R inn í staðinn, þ.e.a.s. við myndum mengið

$$K' := R \cup (K \setminus \operatorname{Im}\varphi).$$

Við fáum gagntæka vörpun $\psi : K' \to K$ með því að setja

$$\psi(x) := \begin{cases}\varphi(x), & \text{ef } x \in R,\\ x, & \text{ef } x \in K \setminus \operatorname{Im}\varphi.\end{cases}$$

Við notum þessa vörpun til að flytja aðgerðirnar af K yfir á K', þannig að við setjum

$$\begin{aligned}x + y &:= \psi^{-1}(\psi(x) + \psi(y)),\\ xy &:= \psi^{-1}(\psi(x)\psi(y)).\end{aligned}$$

Þar eð ψ er baugamótun gefur þetta okkur aðgerðirnar á R fyrir $x, y \in R$; þannig verður R hlutbaugur í K'. Leyfum okkur svo að skrifa a jöfnum

höndum og $\frac{a}{1}$ lítum á K' og K sem sama hlutinn. Nú er ljóst: Stak $a \in R$ þ.a. $a \neq 0$, hefur margföldunarumhverfu í K, nefnilega $a^{-1} = \frac{1}{a}$. Fyrir $a, b \in R$, $b \neq 0$ er

$$\frac{a}{b} = \frac{a}{1} \cdot \frac{1}{b} = ab^{-1}.$$

Við höfum því sýnt:

Sérhver heilbaugur hefur brotasvið. ∎

Athugasemd. Ef $R = \mathbb{Z}$, þá er $K = \mathbb{Q}$.

Athugasemd. Einnig er hægt að smíða heilu tölurnar út frá $\mathbb{N}$ með því að sýna að $(a, b) \sim (c, d)$ þ.þ.a.a. $a + d = c + b$ myndi jafngildisvensl á $\mathbb{N} \times \mathbb{N}$.

Athugasemd. Látum R vera víxlinn einbaug. Hlutmengi S í R kallast *margfeldið*[1] ef $1 \in S$ og $ab \in S$ fyrir öll $a, b \in S$. Ef R er heilbaugur og S er margfeldið hlutmengi í R þ.a. $0 \neq S$ og K er brotasvið R, þá er

$$S^{-1}R := \left\{ \frac{a}{s} : a \in R, s \in S \right\}$$

hluteinbaugur í K sem inniheldur R, því að $0 = \frac{0}{1} \in S^{-1}R$; ef $x, y \in S^{-1}R$, þá má skrifa $x = \frac{a}{s}$ og $y = \frac{b}{t}$ með $s, t \in S$ og þá er

$$x + y = \frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st} \in S^{-1}R$$

og

$$xy = \frac{ab}{st} \in S^{-1}R.$$

Þetta gefur okkur ýmis dæmi um bauga, t.d. hlutbauga í $\mathbb{Q}$ með því að velja margfeldið hlutmengi í $\mathbb{Z}$.

Dæmi 9.3. (1) Ef a er stak í víxlnum einbaug R, þá er $\{a^n : n \in \mathbb{N}\}$ margfeldið hlutmengi í R; almennar ef $a_1, \ldots, a_n \in R$, þá er $\{a_1^{n_1} \cdots a_r^{n_r} : n_1, \ldots, n_r \in \mathbb{N}\}$ margfeldið hlutmengi í R.

(2) Ef p er frumtala, þá er $\mathbb{Z}/p\mathbb{Z} = \{n \in \mathbb{Z} : p \nmid n\}$ margfeldið hlutmengi í $\mathbb{Z}$. Almennar gildir: Látum R vera víxlinn einbaug. Íðal $\mathfrak{I}$ í R er frumíðal í R þ.þ.a.a. fyllimengið $R \setminus \mathfrak{I}$ sé margfeldið hlutmengi í R. □

[1] hér notað sem lýsingarorð

Kafli 10

Margliður

10.1 Margliður, margliðubaugar

Skilgreining 10.1. Látum R vera víxlbaug og athugum mengið $R[X]$ af öllum runum $(a_k)_{k\in\mathbb{N}}$ af stökum í R þannig að mengið $\{k \in \mathbb{N} : a_k \neq 0\}$ sé endanlegt; m.ö.o. þannig að til sé tala $n \in \mathbb{N}$ þ.a. $a_k = 0$ fyrir öll $k > n$. Skilgreinum samlagningu og margföldun á $R[X]$ sem hér segir:

$$(a_k)_{k\in\mathbb{N}} + (b_k)_{k\in\mathbb{N}} := (a_k + b_k)_{k\in\mathbb{N}},$$
$$(a_k)_{k\in\mathbb{N}} \cdot (b_k)_{k\in\mathbb{N}} := (c_k)_{k\in\mathbb{N}},$$

þar sem

$$c_k := \sum_{j=0}^{k} a_j b_{k-j}.$$

Til að sýna að þetta sé vel skilgreint athugum við: Ef $a_k = 0$ fyrir $k > n$ og $b_k = 0$ fyrir $k > m$, þá er $a_k + b_k = 0$ fyrir $k > \max\{n, m\}$ og $c_k = 0$ fyrir $k > n + m$, því þá gildir um öll $j \in \{0, \ldots, k\}$ að $j > n$ eða $k - j > m$ og þá $a_j b_{k-j} = 0$. Þar með er summan og margfeldið í $R[X]$ aftur í $R[X]$ og einfaldir (en langir) reikningar sýna að þessar aðgerðir gera $R[X]$ að baug, köllum hann ***margliðubauginn*** (í einni óákveðinni stærð) yfir R.

Gerum nú ávallt ráð fyrir að R sé víxlinn *einbaugur*. Þá hefur $R[X]$ einingarstak

$$1 = 1_{R[X]} = (\delta_{0k})_{k\in\mathbb{N}} = (1, 0, 0, \ldots).$$

Athugum nú stakið

$$x := (\delta_{1k})_{k\in\mathbb{N}} = (0, 1, 0, 0, \ldots).$$

Við höfum $x^2 = (c_k)_{k\in\mathbb{N}}$, þar sem $c_k = \sum_{j=0}^{k} \delta_{1j}\delta_{1,k-j} = \delta_{2k}$ svo

$$x^2 = (\delta_{2k})_{k\in\mathbb{N}} = (0, 0, 1, 0, 0, \dots).$$

Með sama hætti fæst með þrepun:

$$x^n = (\delta_{nk} n \in \mathbb{N}) = (0, 0, \dots, 0, 1, 0, 0, \dots),$$

þar sem stakið 1 er í n-ta sæti.

Táknuðum „óákveðnu stærðina“ með „x“, við skulum heldur nota upphafsstaf „X“. Þannig er

$$X = (\delta_{1k})_{k\in\mathbb{N}} = (0, 1, 0, 0, \dots).$$

Vörpunin $\varphi : R \to R[X], a \mapsto (a\delta_{0k})_{k\in\mathbb{N}} = (a, 0, 0, 0, \dots)$ er einbaugamótun og eintæk; við getum notað hana til að samsama R við mynd sína í $R[X]$; það þýðir að við skrifum „a“ í stað „$(a\delta_{0k})_{k\in\mathbb{N}}$“, við köllum margliður af þessu tagi *fastar* margliður. Nú sjáum við að fyrir $a \in R$ er

$$aX^n = (0, \dots, 0, a, 0, \dots)$$

með a í n-ta sæti. Látum nú $P = (a_n)_{n\in\mathbb{N}}$ vera einhverja margliðu í $R[X]$ og n vera þannig að $a_k = 0$ fyrir $k > n$. Þá er

$$\begin{aligned}\sum_{k=0}^{n} a_k X^k &= (a_0, 0, 0, \dots) + (0, a_1, 0, \dots) + \cdots + (0, \dots, 0, a_n, 0, \dots) \\ &= (a_0, a_1, a_2, \dots, a_n, 0, 0, \dots).\end{aligned}$$

M.ö.o. er

$$P = \sum_{k=0}^{n} a_k X^k.$$

Skrifum hér eftir margliður þannig. Þessi framsetning ákvarðast ótvírætt purtséð frá að sleppa má liðum $a_k X^k$ þannig að $a_k = 0$ (eða bæta þeim við). Látum nú $P = (a_k)_{k\in\mathbb{N}}$ vera margliðu og setjum

$$\operatorname{stig} P := \sup\{n \in \mathbb{N} : a_n \neq 0\}.$$

Þetta þýðir: Ef $P \neq 0$, þá er $\operatorname{stig} P$ stærsta tala k þannig að $a_k \neq 0$, en stig núllmargliðunnar er $-\infty$. Ef $n = \operatorname{stig} P \in \mathbb{N}$, þá kallast a_n *forystustuðull* margliðunnar P, en a_0 kallast *fastastuðull* hennar.

10.2 Deiling í margliðubaugum

Setning 10.1. Látum $P, Q \in R[X]$. Þá er

$$\operatorname{stig}(P+Q) \leq \max\{\operatorname{stig} P, \operatorname{stig} Q\}$$

og

$$\operatorname{stig}(P \cdot Q) \leq \operatorname{stig} P + \operatorname{stig} Q$$

og í seinni jöfnunni gildir jafnaðarmerki ef forystustuðlar P og Q eru ekki núlldeilar í R.

Sönnun. Höfðum séð að fyrir $P = (a_k)_{k\in\mathbb{N}}$, $Q = (b_k)_{k\in\mathbb{N}}$ gildir $a_k + b_k = 0$ fyrir $k > \max\{\operatorname{stig} P, \operatorname{stig} Q\}$ og $c_k := \sum_{j=0}^{k} a_j b_{k-j}$ er 0 fyrir $k > n+m$ ef $n = \operatorname{stig} P$ og $m = \operatorname{stig} Q$; þetta sýnir ójöfnurnar. Athugum nú að $c_{n+m} = a_n b_m$ þar sem a_n er forystustuðull P og b_m er forystuðull Q; þá er $a_n \neq 0$ og $b_m \neq 0$ og við fáum $c_{n+m} \neq 0$ nema a_n, b_m séu núlldeilar í R. ∎

Sér í lagi gildir jafnan

$$\operatorname{stig}(PQ) = \operatorname{stig} P + \operatorname{stig} Q$$

alltaf ef R er *heilbaugur* og þá sér í lagi ef R er svið. Fáum:

Fylgisetning 10.1. Ef R er heilbaugur þá er $R[X]$ líka heilbaugur.

Setning 10.2 (Um deilingu með afgangi í $R[X]$). Látum P vera margliðu í $R[X]$ þannig að $P \neq 0$ og P sé *eind* í R. Fyrir sérhverja margliðu F í $R[X]$ eru til margliður Q og G þannig að

$$F = PQ + G \qquad \text{og} \qquad \operatorname{stig} G < \operatorname{stig} P;$$

margliðurnar P, Q ákvarðast ótvírætt af þessum skilyrðum.

Sönnun. Fyrir tilvist notum við þrepun yfir $m := \operatorname{stig} F$. Látum $n := \operatorname{stig} P \geq 0$; ljóst ef $m < n$, því þá má taka $Q = 0$ og $G = F$. Gerum því ráð fyrir að $m \geq n$, skrifum $F = \sum_{k=0}^{m} a_k X^k$ og $P = \sum_{k=0}^{n} c_k X^k$; þá hafa F og $c_n^{-1} a_m X^{m-n} P$ bæði stig m og sama forystustuðul a_m, svo að $F_1 := F - c_n^{-1} a_m X^{m-n} P$ er af stigi $< m$. Skv. þrepunarforsendu má skrifa $F_1 = PQ_1 + G$, þar sem $\operatorname{stig} G < \operatorname{stig} P$, en þá er

$$F = F_1 + c_n^{-1} a_m X^{m-n} P = PQ + G,$$

þar sem $Q := Q_1 + c_n^{-1} a_m X^{m-n}$.

Ótvíræðni: Ef $F = PQ + G = PQ_1 + G_1$ þar sem G, G_1 hafa minna stig en P, en þá er

$$P(Q - Q_1) = G_1 - G$$

og þá

$$\operatorname{stig} P + \operatorname{stig}(Q - Q_1) = \operatorname{stig}(G_1 - G) < \operatorname{stig} P$$

því að forystustuðull P er eind og því ekki núlldeilir í R. Þetta stenst ekki nema $\operatorname{stig}(Q - Q_1) = \operatorname{stig}(G_1 - G) = -\infty$, þ.e. $Q = Q_1$ og $G = G_1$. ∎

Athugasemd. Héðan í frá verður **aðeins talað um einbauga**. Ef einhvers staðar stendur *baugur* í stað *einbaugur*, þá er óhætt að gera ráð fyrir að sá baugur sé samt sem áður einbaugur.

10.3 Margliðuföll

Skilgreining 10.2. Látum R vera hluteinbaug í einbaug S og látum $c \in S$. Fyrir margliðu $P = \sum_{k=0}^{n} a_k X^k$ í $R[X]$ setjum við

$$P(c) := \sum_{k=0}^{n} a_k c^k \in S.$$

Sér í lagi er $P(c)$ skilgreint fyrir öll $c \in R$, og við fáum vörpun

$$\tilde{P} : R \to R, c \mapsto P(c)$$

sem við köllum *margliðufallið* sem margliðan P skilgreinir.

Athugasemd. Almennt ákvarðast margliða *ekki* af margliðufallinu. T.d. hefur $\mathbb{Z}/2\mathbb{Z}[X]$ óendanlega mörg stök, en aðeins eru til fjórar varpanir $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$.

Setning 10.3 (Reiknireglur). Ef R er hluteinbaugur í S og $c \in S$, þá er

$$(P + Q)(c) = P(c) + Q(c)$$

$$(PQ)(c) = P(c) \cdot Q(c)$$

fyrir öll $P, Q \in R[X]$.

Fáum:

Setning 10.4. Látum R vera hluteinbaug í S og $c \in S$. Þá er til nákvæmlega ein baugamótun $\psi : R[X] \to S$ þannig að $\psi(r) = r$ fyrir öll $r \in R$ og $\psi(X) = c$; hún er gefin með

$$\psi(P) = P(c).$$

Sönnun. Ef ψ er slík baugamótun og $P = \sum_{k=0}^{n} a_k X^k \in R[X]$, þá er

$$\psi(P) = \Psi\left(\sum_{k=0}^{n} a_k X^k\right) = \sum_{k=0}^{n} \psi(a_k)\psi(X)^k = \sum_{k=0}^{n} a_k c^k.$$

Öfugt segja reiknireglurnar að ψ sé baugamótun. ∎

Skilgreining 10.3. Skrifum

$$R[c] := \operatorname{Im}\psi = \{P(c) : P \in R[X]\}.$$

Þá er $R[c]$ hlutbaugur í S, einsmóta $R[x]/\operatorname{Ker}\psi$.

10.4 Núllstöðvar margliða

Skilgreining 10.4. Látum R vera hluteinbaug í S og $P \in R[X]$. Segjum að stak $c \in S$ sé *núllstöð* margliðunnar P ef $P(c) = 0$.

Dæmi 10.1. Margliðan $X^2 + 1 \in \mathbb{R}[X]$ hefur ekki núllstöð í $\mathbb{R}$ en hún hefur núllstöð í stærri baugnum $\mathbb{C}$. □

Gerum nú ráð fyrir að R sé einbaugur og að $P \in R[X]$. Látum $a \in R$. Deilum $X - a$ upp í P með afgangi og skrifum

$$P = (X - a)Q + b$$

þar sem $\operatorname{stig}(b) < 1$, þ.e. b er föst margliða sem við höfum samsamað við stökin í R. Setjum nú a inn í margliðuna og fáum $P(a) = b$. Sjáum:

Setning 10.5. Ef R er einbaugur, $P \in R[X]$ og $a \in R$, þá gildir: Stakið a er núllstöð margliðunnar P þ.þ.a.a. skrifa megi

$$P = (X - a)Q$$

þar sem $Q \in R[X]$. Ef $P(a) = 0$ og $P \neq 0$, þá er $\operatorname{stig}(Q) = \operatorname{stig}(P) - 1$.

Athugum að stuðullinn við X í $X - a$ er 1, þ.e. eind, svo $\text{stig}(P) = \text{stig}(X - a) + \text{stig}(Q) = 1 + \text{stig}(Q)$. Með þrepun fæst:

Setning 10.6. Ef R er heilbaugur og $P \in R[X]$ hefur ólíkar núllstöðvar $a_1, \ldots, a_r \in R$, $P \neq 0$, þá má skrifa

$$P = (X - a_1) \cdots (X - a_r)Q$$

þar sem Q er margliða af stigi $\text{stig}(P) - r$.

Sönnun. Tilviki $r = 1$ er síðasta setning. Látum P hafa ólíkar núllstöðvar $a_1, \ldots, a_{r+1}$. Skv. þrepunarforsendu má skrifa

$$P = (x - a_1) \cdots (x - a_r)Q_q$$

þar sem Q_1 er margliða af stigi $\text{stig}(P) - r$. Nú er

$$0 = P(a_{r+1}) = (a_{r+1} - a_1) \cdots (a_{r+1} - a_r)Q_1(a_{r+1}).$$

Höfum $a_{r+1} - a_k \neq 0$ fyrir $k = 1, \ldots, r$; þar eð R er *heilbaugur* er $Q_1(a_r + 1) = 0$, svo að skrifa má $Q_1 = (X - a_{r+1})Q$, þar sem $\text{stig}(Q) = \text{stig}(Q_1) - 1 = \text{stig}(P) - \text{stig}(r + 1)$; og $P = (X - a_1) \cdots (X - a_{r+1})Q$. ∎

Fylgisetning 10.2. Látum R vera heilbaug og P vera margliðu í $R[X]$ af stigi n; þá hefur P í mesta lagi n ólíkar núllstöðvar í R.

Fylgisetning 10.3. Ef R er *óendanlegur heilbaugur*, þá ákvarðast margliða P af margliðufallinu $\tilde{P} : R \to R, a \mapsto P(a)$; m.ö.o. gildir: Ef $P, Q \in R[X]$ og $\tilde{P} = \tilde{Q}$, þá er $P = Q$.

Sönnun. $P - Q$ hefur óendanlega margar núllstöðvar, svo að $\text{stig}(P - Q) = -\infty$, þ.e. $P - Q = 0$. ∎

Athugasemd. Látum R vera heilbaug, $P \in R[X]$ og a vera núllstöð P; skrifum $P = (X - a)Q_1$. Ef a er líka núllstöð Q_1, þá má skrifa $Q_1 = (X - a)Q_2$, þ.e. $P = (X - a)^2 Q_2$. Þessu má halda áfram: Ef $P \neq 0$, þá tekur það enda og við fáum

$$P = (X - a)^r Q_r, \qquad Q_r(a) \neq 0.$$

Setjum þá að r sé *margfeldni* núllstöðvarinnar a (í margliðunni P).

Setning 10.7. Látum K vera svið. Þá er $K[X]$ höfuðíðalbaugur.

Sönnun. Látum $\mathfrak{A}$ vera íðal í $K[X]$ þ.a. $\mathfrak{A} \neq \{0\}$ (núllíðalið er alltaf höfuðíðal). Veljum margliðu $P \neq 0$ í $\mathfrak{A}$ af lægsta hugsanlega stigi. Látum nú $F \in \mathfrak{A}$, þar eð K er svið er forystustuðull margliðunnar P eind, svo að við getum skrifað $F = PQ + G$, þar sem $\operatorname{stig} G < \operatorname{stig}(P)$. En $G = F - PQ \in \mathfrak{A}$; svo að $G = 0$ skv. skilgreiningu á P. En það þýðir að $F \in P \cdot K[X]$. Ljóslega er $P \cdot K[X] \subset \mathfrak{A}$, svo að $\mathfrak{A} = PK[X]$. ∎

Athugasemd. Þetta gildir ekki ef K er bara heilbaugur; t.d. er $\mathbb{Z}[X]$ ekki höfuðíðalbaugur. Sýnum að $2\mathbb{Z}[X] + X\mathbb{Z}[X]$ er ekki höfuðíðal: Ef margliðurnar 2 og X eru ekki margfeldi af sömu margliðu í $\mathbb{Z}[X]$, þá verður sú margliða að vera föst, segjum fastinn a, en þá gengur a upp í forystustuðli X, sem er 1, svo $a = 1$ eða $a = -1$. En 1 er ekki í $2\mathbb{Z}[X] + X\mathbb{Z}[X]$; ef $1 = 2P_1 + XP_2$ með $P_1, P_2 \in \mathbb{Z}[X]$, þá gengur talan 2 upp í fastastuðli hægri hliðar jöfnunnar en ekki vinstri hliðar.

10.5 Evklíðskir baugar

Skilgreining 10.5. *Evklíðskur baugur* er heilbaugur R þannig að til sé vörpun $d : R \setminus \{0\} \to \mathbb{N}$ sem fullnægir eftirfarandi skilyrði:

> Ef $a, b \in R \setminus \{0\}$, þá eru til stök $q, r \in R$ þ.a. $a = bq + r$ og annaðhvort er $r = 0$ eða $d(r) < d(b)$.

Dæmi 10.2. (1) Baugurinn $\mathbb{Z}$ er evklíðskur með $d(x) := |x|$ fyrir $x \in \mathbb{Z}\setminus\{0\}$. Baugurinn $K[X]$, þar sem K er svið, er evklíðskur með $d(P) := \operatorname{stig}(P)$, $P \in K[X] \setminus \{0\}$.

(2) Baugurinn $\mathbb{Z}[i]$. Við höfum $i^2 = -1$, svo að i er tvinntala sem er núllstöð margliðunnar $X^2 + 1$, sem er í $\mathbb{Z}[i]$; sérhverja margliðu P í $\mathbb{Z}[X]$ má skrifa með nákvæmlega einum hætti sem $P = (X^2 + 1)Q + a + bX$, með $a, b \in \mathbb{Z}$ og það þýðir að sérhvert stak í $\mathbb{Z}[i]$ má skrifa með nákvæmlega einum hætti sem $a + bi$, þar sem $a, b \in \mathbb{Z}$, þ.e.

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}.$$

Þetta er hlutbaugur í $\mathbb{C}$ og kallast *Gauss-heiltalnabaugurinn* og stök hans *Gauss-heiltölur*. Þessi baugur er evklíðskur baugur með $d(z) := |z|^2 = z\overline{z}$ fyrir $z \in \mathbb{Z}[i] \setminus \{0\}$. Athugum að fyrir tvinntölur $z = x + iy$ með $x, y \in \mathbb{R}$ eru til heilar tölur m, n þ.a. $|x - n| \leq \frac{1}{2}$ og $|y - m| \leq \frac{1}{2}$; þá er

$$u := n + im \in \mathbb{Z}[i], \qquad |z - u|^2 = (x - u)^2 + (y - u)^2 \leq \frac{1}{4} + \frac{1}{4} < 1.$$

Látum nú $a, b \in \mathbb{Z}[i] \setminus \{0\}$. Finnum $q \in \mathbb{Z}[i]$ þannig að $|\frac{a}{b} - q|^2 < 1$; fyrir $r = a - bq$ er þá

$$|r|^2 = |a - bq|^2 = |b|^2 |\frac{a}{b} - q|^2 < |b|^2$$

og $a = bq + r$. □

Setning 10.8. Evklíðskur baugur er höfuðíðalbaugur.

Sönnun. Látum R vera evklíðskan baug með samsvarandi falli $d : R \setminus \{0\} \to \mathbb{N}$. Látum $\mathfrak{A}$ vera íðal í R, $\mathfrak{A} \neq 0$, látum b vera stak í $\mathfrak{A} \setminus \{0\}$ þ.a. $d(b)$ sé sem minnst. Fyrir $a \in \mathfrak{A}$ eru þá til $q, r \in R$ þannig að $a = bq + r$ og $r = 0$ eða $d(r) < d(b)$. En $r = a - bq \in \mathfrak{A}$, svo að $d(r) < d(b)$ kemur ekki til greina vegna skilgreiningar á b, svo að $r = 0$ og því $a = bq$; fáum $\mathfrak{A} = bR$. ■

Athugasemd. Í bók er þess krafist að d fullnægi líka öðru skilyrði, nefnilega

$$d(a) \leq d(ab)$$

fyrir öll $a, b \in R \setminus \{0\}$. Þetta er gagnlegur eiginleiki, hann leyfir að finna eindirnar í R; ef við höfum hann, þá er

$$R^* = \{a \in R \setminus \{0\} : d(a) = d(1)\}.$$

Kafli 11

Þáttun í heilbaugum

11.1 Tengd stök, þættanleiki og frumstök

Skilgreining 11.1. (1) Látum R vera heilbaug og $a, b \in R$. Við segjum að a *gangi upp í* b *í* R og skrifum

$$a \mid b$$

ef til er stak $c \in R$ þ.a. $b = ac$.

(2) Við segjum að stök $a, b \in R$ séu *tengd* ef

$$a \mid b \text{ og } b \mid a.$$

Athugasemd. Að stak $u \in R$ sé eind þýðir að $u \mid 1$.

Setning 11.1. Látum R vera heilbaug.

(1) Við höfum $a \mid b$ þ.þ.a.a. $bR \subset aR$.

(2) Stak u í R er eind þ.þ.a.a. það gangi upp í sérhverju staki í R.

(3) Fyrir öll a úr R er $a \mid 0$. Ef $0 \mid a$, þá er $a = 0$.

(4) Stök $a, b \in R$ eru tengd þ.þ.a.a. til sé eind u þ.a. $a = ub$.

(5) Fyrir öll a úr R er $a \mid a$.

(6) Ef $a, b, c \in R$ og $a \mid b$ og $b \mid c$, þá $a \mid c$.

Sönnun. Atriði (1), (2), (3) eru augljós.

(4) Ef $a = ub$, þar sem u er eind, þá gildir $b \mid a$; líka er $b = u^{-1}a$ svo að $a \mid b$. Ef hins vegar bæði $a \mid b$ og $b \mid a$, þá sjáum við fyrst að $a = 0$ þ.þ.a.a. $b = 0$ skv. (3). Gerum því ráð fyrir að $a, b \neq 0$. Nú er til u þannig að $b = ua$ og v þ.a. $a = vb$. En þá er $a = vb = vua$, og þar sem R er heilbaugur fæst $1 = vu$, þ.e. u er eind.

(5) Er ljóst: $a = 1a$.

(6) Ef $a \mid b$ og $b \mid c$, þá eru til x, y þ.a. $b = ax$ og $c = by$, og þá er $c = by = a(xy)$, svo að $a \mid c$. ∎

Skilgreining 11.2. (1) Við segjum að stak p í heilbaug R sé *óþættanlegt* ef það er hvorki núll né eind og ekki er hægt að skrifa p sem margfeldi $p = ab$ nema annaðhvort a eða b sé eind.

(2) Við segjum að stak p í heilbaug R sé *frumstak* ef það er hvorki núll né eind og fyrir öll $a, b \in R$ þ.a. $p \mid ab$ gildir annaðhvort $p \mid a$ eða $p \mid b$.

Athugasemd. (1) Ef p er frumstak í baug R og $a_1, \ldots, a_r \in R$ og $p \mid a_1 \cdots a_r$, þá er $r \geq 1$ og til er $k \in \{1, \ldots, r\}$ þannig að $p \mid a_k$. Þetta sjáum við með þrepun út frá skilgreiningunni.

(2) Sérhvert frumstak er óþættanlegt. Ef p er frumstak og til eru a, b í R þannig að $p = ab$, þá gengur p upp í a eða b; sejgum t.d. að $p \mid a$. Þá megum við skrifa $a = pu$, þar sem $u \in R$ og við fáum $p = ab = pub$; en $p \neq 0$ svo að $1 = ub$; en þá er b eind.

Hins vegar þarf óþættanlegt stak í baug ekki að vera frumstak!

Setning 11.2. Stak p í heilbaug R þannig að $p \neq 0$ er frumstak þ.þ.a.a. pR sé frumíðal.

Sönnun. Að pR sé frumíðal þýðir að $pR \neq R$ og

Ef $a, b \in pR$, þá er $a \in pR$ eða $b \in pR$.

Skilyrðið $pR \neq R$ þýðir að p er ekki eind; seinna skilyrðið segir: Ef $p \mid ab$, þá $p \mid a$ eða $p \mid b$. ∎

11.2 Þáttabaugar

Skilgreining 11.3. Baugur R kallast *þáttabaugur* ef hann er heilbaugur og sérhvert stak a í R þ.a. $a \neq 0$ má skrifa sem margfeldi

$$a = u \prod_{k=1}^{r} p_k$$

þar sem u er eind og $p_1, \ldots, p_r$ eru frumstök. Köllum þessa framsetningu *frumþáttun* staksins a og $p_1, \ldots, p_r$ *frumþætti* þess.

Athugasemd. (1) Við leyfum að $r = 0$ með því venjulega samkomulagi að $\prod_{k=1}^{r} = 1$ ef $r = 0$; stökin sem skrifa má þannig með $r = 0$ eru þá nákvæmlega eindirnar í R.

(2) Látum u vera eind í R. Ljóst er að stak p í R er frumstak í R þ.þ.a.a. up sé frumstak í R; ef nú $a \in R, a \neq 0$,

$$a = u \prod_{k=1}^{r} p_k,$$

og $u_1, \ldots, u_r$ eru eindir, þá má setja $q_k := up_k$ og $v := uu_1^{-1} \cdots u_r^{-1}$; og þá er líka

$$a = v \prod_{k=1}^{r} q_k.$$

Frumþáttunin ákvarðast almennt ekki ótvírætt. En við höfum:

Setning 11.3. Frumþáttun staks í þáttabaug ákvarðast ótvírætt burtséð frá röð og tengslum; þetta þýðir: Ef

$$a = u \prod_{k=1}^{r} p_k = v \prod_{j=1}^{s} q_j$$

þar sem u, v eru eindir í R og $p_1, \ldots, p_r, q_1, \ldots, q_s$ eru frumstök í R, þá er $r = s$ og til er gagntæk vörpun $\sigma : \{1, \ldots, r\} \to \{1, \ldots, r\}$ þ.a. p_k sé tengt $q_{\sigma(k)}$ fyrir öll $k = 1, \ldots, r$.

Sönnun. Þrepum yfir r. Ljóst ef $r = 0$ (eða $r = 1$). Látum þá $r \geq 1$. Höfum þá að $p_r \mid \prod_{j=1}^{s} q_j$ og þar sem p_r er frumstak er til j þ.a. $p_r \mid q_j$; með því að umraða $q_1, \ldots, q_s$ má g.r.f. að $p_r \mid q_s$. Skrifum $q_s = wp_r$. Þar sem q_s er frumstak er það óþættanlegt og p_r er ekki eind, svo w er eind. Nú fæst

$$u \prod_{k=1}^{r} p_k = uwp_k \prod_{j=1}^{s-1} q_j$$

og þá

$$u \prod_{k=1}^{r-1} p_k = uw \prod_{j=1}^{s-1} q_j.$$

Skv. þrepunarforsendu er $r - 1 = s - 1$, og við getum umraðað $q_1, \ldots, q_{r-1}$ þ.a. p_k sé tengt q_k fyrir $k = 1, \ldots, r - 1$. ∎

Fylgisetning 11.1. Í þáttabaug er sérhvert óþættanlegt stak frumstak.

Sönnun. Í frumþáttun óþættanlegs staks getur bara verið einn frumþáttur. ∎

Setning 11.4. Í höfuðíðalbaug er sérhvert frumíðal háíðal og sérhvert óþættanlegt stak frumstak.

Sönnun. Látum p vera óþættanlegt stak. Gerum ráð fyrir að $\mathfrak{A}$ sé eiginlegt íðal í R þ.a. $pR \subset \mathfrak{A}$. Skrifum $\mathfrak{A} = bR$ þar sem $b \in R$. Þá gildir $b \mid p$, svo að $p = bu$ þar sem $u \in R$; nú er b ekki eind, því að pR er eiginlegt íðal, svo að u verður að vera eind; en þá er ljóst að $bR = buR = pR$. Þar með er pR háíðal, og háíðal er frumíðal, svo að p er frumstak.

Ef svo $\mathfrak{P}$ er frumíðal, þá er $\mathfrak{P} = pR$, þar sem p er frumstak, þar með óþættanlegt, svo að $\mathfrak{P}$ er háíðal. ∎

Setning 11.5. Sérhver höfuðíðalbaugur er þáttabaugur.

Sönnun. Það nægir að sýna að sérhvert stak í höfuðíðalbaug R, sem er ekki eind, megi skrifa sem margfeldi af *óþættanlegum* stökum, því að þau eru frumstök skv. síðustu setningu. Látum því $a \in R$, a ekki eind. Ef a er óþættanlegt, þá þarf ekki að gera meira. Annars má skrifa $a = a_1 b_1$ þar sem hvorki a_1 né b_1 er eind. Þá er $a_1 \mid a$ og $Ra \subsetneq Ra_1$ (athugum að fyrir stök a, b í heilbaug R gildir $Ra = Rb$ þ.þ.a.a. $a \mid b$ og $b \mid a$, þ.e. a og b eru tengd). Ef a_1, b_1 eru óþættanleg, þá þarf ekki meira; annars má t.d. þátta $b_1 = a_2 b_2$ og skrifa $a = a_1 a_2 b_2$ þar sem $Ra_1 \subsetneq Ra_2$. Annaðhvort endar þetta á að við höfum skrifað a sem margfeldi af endanlega mörgum stökum, eða við fáum óendanlega runu $(a_k)_{k \in \mathbb{N}}$ af stökum í R þ.a.

$$Ra \subsetneq Ra_1 \subsetneq Ra_2 \subsetneq Ra_3 \subsetneq \cdots$$

En þá er $\mathfrak{A} = \bigcup_{k \in \mathbb{N}} Ra_k$ íðal í R. Nú er R höfuðíðalbaugur, svo að til er stak c úr $\mathfrak{A}$ þannig að $\mathfrak{A} = cR$. En þá er c stak í einhverju íðalanna Ra_k, svo að $Rc \subset Ra_k \subset Ra_j \subset Rc$, svo $Ra_k = Ra_j$, fyrir öll $j \geq k$, sem er *mótsögn.* ∎

11.3 Þáttun í margliðubaugum

Fylgisetning 11.2. (1) Ef K er svið, þá er $K[X]$ þáttabaugur.
(2) Gauss-talnabaugurinn $\mathbb{Z}[i]$ er þáttabaugur.

Athugasemd. (1) Sáum að í höfuðíðalbaug er sérhvert óþættanlegt stak frumstak. Þetta gildir almennar í öllum þáttabaugum: Ef p er óþættanlegt og hefur frumþáttun $p = up_1 \cdots p_r$, þar sem u er eind og $p_1, \ldots, p_r$ frumstök, þá er nauðsynlega $r = 1$ og $p = up_1$, svo að p er tengt frumstaki og því frumstak.

(2) Ef K er svið og P er óþættanleg margliða í $K[X]$, þá er P frumstak í $K[X]$ og $\langle P\rangle = PK[X]$ er háíðal, svo að $K[X]/PK[X]$ er svið. Athugum: Ef stig P er 2 eða 3, og P er þættanlegt, þá er annar þátturinn af stigi 1 og hefur því núllstöð, svo að P hefur núllstöð. Sjáum því að fyrir margliður af stigi 2 eða 3 gildir: $K[X]/PK[X]$ er svið þ.þ.a.a. P hafi enga núllstöð.

Fáum athyglisverða niðurstöðu:

Fylgisetning 11.3. Látum K vera svið og $P \in K[X]$, stig $P \geq 1$. Þá er til svið L þ.a. K er hlutsvið í L og P hafi núllstöð í L.

Sönnun. Látum P_1 vera einn frumþátt margliðunnar P í $K[X]$. Það nægir að sýna að P_1 hafi núllstöð í stærra sviði; hún er þá líka núllstöð fyrir P. Skv. athugasemd er $L_1 := K[X]/P_1K[X]$ svið. Látum $c := X + P_1K[X] \in L_1$. Þá er $P_1(c) = P_1(X) + P_1K[X] = 0$.[1] Nú er $\varphi : K \to L_1, \varphi(a) := a + P_1K[X]$ sviðamótun (þ.e. einbaugamótun milli sviða) og því eintæk, því $\operatorname{Ker}\varphi \neq K$ vegna $1 \notin \operatorname{Ker}\varphi$ og K hefur engin íðul nema $\{0\}$ og K, svo $\operatorname{Ker}\varphi = \{0\}$. Þá má nota φ til að samsama K við myndina $\operatorname{Im}\varphi$, sem er hlutsvið í L_1; fáum þannig svið L sem hefur K sem hlutsvið þ.a. P_1 hafi núllstöð í L. ∎

Dæmi 11.1. $X^2 + 1$ hefur ekki núllstöð í $\mathbb{R}$, svo að $\mathbb{R}[X]/(X^2+1)\mathbb{R}[X]$ er svið þar sem $X^2 + 1$ hefur núllstöð. Athugum: Höfum vörpun $\varphi : \mathbb{R}[X] \to \mathbb{C}, P \mapsto P(i)$, og mynd hennar er $\mathbb{R}[i] = \mathbb{C}$ og $\operatorname{Ker}\varphi = (X^2+1)\mathbb{R}[X]$: Ef $P \in \operatorname{Ker}\varphi$, þ.e. $P(i) = 0$, þá gengur $X - i$ upp í P í $\mathbb{C}[X]$; en þar sem P hefur rauntalnastuðla gengur $X + i$ líka upp í P, svo að $X^2 + 1 = (X - i)(X + i)$ gengur upp í P, þ.e. $P \in (X^2+1)\mathbb{R}[X]$. Því er

$$\mathbb{C} \cong \operatorname{Im}\varphi/\operatorname{Ker}\varphi = \mathbb{R}[X]/(X^2+1)\mathbb{R}[X].$$

Ef tvinntölurnar væru óþekktar, þá mætti nota þetta til að skilgreina þær út frá $\mathbb{R}$. □

[1] Að þessi jafna (nánar tiltekið fyrra jafnaðarmerkið) gildi er ekki alveg augljóst, sjá nánar tilsvarandi sönnun bls. 354-355 í kennslubók.

Athugasemd. Ef við skrifum $a \sim b$ til að tákna að a og b séu tengd, þá eru þetta jafngildisvensl; köllum jafngildisflokkana *tenglsaflokka*. Í baugnum $\mathbb{Z}$ er tengslaflokkur tölunnar a mengið $\{a, -a\}$; hann inniheldur nákvæmlega eina náttúrlega tölu. Láum R vera þáttabaug og P vera mengi sem inniheldur nákvæmlega eitt stak úr hverjum tengslaflokki *frumstaka* í R, og engin önnur stök. Þá getum við kallað P *fulltrúamengi fyrir frumstökin* í R. Mengi frumtalnanna er fulltrúamengi fyrir frumstökin í $\mathbb{Z}$.

Látum K vera svið; eindirnar í $K[X]$ eru margliður af stigi 0; það eru föstu margliðurnar nema núllmargliðan, m.ö.o. eindirnar í K (ef við samsömum stak í K við tilsvarandi fasta margliðu í $K[X]$). Nú er ljóst: Sérhver tengslaflokkur margliðu $P \neq 0$ inniheldur nákvæmlega eina margliðu þ.a. forystustuðullinn sé 1.

Skilgreining 11.4. Margliða er sögð vera *stöðluð* ef hún er ekki núllmargliðan og forystustuðull hennar er 1.

Óþættanlegar staðlaðar margliður mynda fulltrúamengi fyrir frumstökin í $K[X]$ ef K er svið.

Ef við höfum fulltrúamengi P fyrir frumstöki í þáttabaug R þá má þátta sérhvert stak $a \neq 0$ í R sem $a = up_1 \cdots p_r$ með $p_1, \ldots, p_r \in P$, u eind; þessi þáttun ákvarðast ótvírætt burtséð frá röð. Almennt er engin kerfisbundin aðferð til að búa til svona fulltrúamengi, þau eru alltaf til skv. frumsendu um val. Í $\mathbb{Z}[i]$ er fyrir $a \neq 0$ tengslaflokkurinn $\{a, -a, ia, -ia\}$ og allar aðferðir til að velja eitt stak framar öðrum eru ekki sjálfgefnar.

Skilgreining 11.5. Látum R vera heilbaug og $a_1, \ldots, a_n \in R$. Við segjum að stak $d \in R$ sé *stærsti samdeilir* stakanna $a_1, \ldots, a_n$ ef

(i) $d \mid a_k$ fyrir $k = 1, \ldots, n$ og

(ii) ef $c \in R$, $c \mid a_k$ fyrir $k = 1, \ldots, n$, þá $c \mid d$.

Segjum að stak $m \in R$ sé *minnsta samfeldi* $a_1, \ldots, a_n$ ef

(i') $a_k \mid m$ fyrir $k = 1, \ldots, n$ og

(ii') ef $c \in R$, $a_k \mid c$ fyrir $k = 1, \ldots, n$, þá $m \mid c$.

Athugasemd. Almennt þarf stærstur samdeilir ekki að vera til; en ef hann er til, þá ákvarðast tengslaflokkur hans ótvírætt; segjum að hann ákvarðist ótvírætt burtséð frá tengslum. Sama gildir um minnsta samfeldi. Í þáttabaug eru stærsti samdeilir og minnsta samfeldi alltaf til: Látum $a_1, \ldots, a_m \in$

$R \setminus \{0\}$, skrifum frumþáttun a_k sem

$$a_k = u_k p_1^{n(k,1)} \cdots p_r^{n(k,r)}$$

með $n(k,m) \geq 0$; getum valið sömu $p_1, \ldots, p_r$ með því að leyfa 0-ta veldi frumþáttar. Þá er

$$d := p_1^{i_1} \cdots p_r^{i_r}$$

þar sem $i_k = \min\{n(k,1), \ldots, n(k,r)\}$, stærsti samdeilir, og

$$m := p_1^{j_1} \cdots p_r^{j_r}$$

þar sem $j_k := \max\{n(k,1), \ldots, n(k,r)\}$ minnsta samfelldi.

Setning 11.6. Látum R vera höfuðíðalbaug og $a_1, \ldots, a_m \in R$. Stak d í R er stærstur samdeilir $a_1, \ldots, a_m$ þ.þ.a.a.

$$dR = a_1 R + \cdots + a_m R.$$

Stak g í R er minnsta samfeldi $a_1, \ldots, a_m$ þ.þ.a.a.

$$gR = a_1 R \cap \cdots \cap a_m.$$

Sönnun. Eins og fyrir heilar tölur! ∎

Athugasemd. Ef b er stærstur samdeilir a_1 og a_2 og d er stærstur samdeilir b og a_3, þá er d stærstur samdeilir a_1, a_2, a_3. Það dugar því að geta fundið stærstan samdeili *tveggja* staka. Í *evklíðskum* baug má finna stærstan samdeili tveggja staka með *reikniriti Evklíðs* alveg eins og fyrir heilar tölur.

Athugasemd. Sanna má: Ef U er svæði í $\mathbb{C}$ (þ.e. opið og samanhangandi hlutmengi), og $R = O(U)$ er baugur allra fágaðra falla á U, þá er R ekki þáttabaugur, en sérhver (endanleg) fjölskylda af stökum í R hefur stærstan samdeili.

Skilgreining 11.6. Látum R vera þáttabaug og $F = \sum_{k=0}^{n} a_k X^k \in R[X]$. Stærstur samdeilir stuðlanna $a_0, \ldots, a_n$ kallast *innihald* margliðunnar F. Margliðan F kallast *frumstæð* ef 1 er innihald hennar.

Athugasemd. (1) Innihald margliðu í $R[X]$ er skilgreint ótvírætt *burtséð frá tengslum.*

(2) Ef F er margliða í $R[X]$, R þáttabaugur, þá má skrifa $F = cF_1$ þar sem F_1 er frumstæð og c er innihald F; öfugt ef $F = cF_1$, þar sem $c \in R$ og F_1 er frumstæð, þá er c innihald F.

Athugasemd. Látum $\phi : R \to S$ vera baugamótun, þá fæst baugamótun

$$\hat{\phi} : R[X] \to S[X]$$

þannig að

$$\phi\left(\sum_{k=0}^{n} a_k X^k\right) := \sum_{k=0}^{n} \phi(a_k) X^k.$$

Sér í lagi ef $\mathfrak{A}$ er íðal í R, þá fæst baugamótun

$$R[X] \to R/\mathfrak{A}[X], \qquad \sum_{k=0}^{n} a_k X^k \mapsto \sum_{k=0}^{n} [a_k] X^k,$$

þar sem $[a_k] := a_k + \mathfrak{A}$ er náttúrlega ofanvarpið af a_k.

Hjálparsetning 11.1 (Gauss). Ef R er þáttabaugur og F, G eru frumstæðar margliður í $R[X]$, þá er margfeldið FG frumstæð margliða.

Fylgisetning 11.4. Ef $F, G \in R[X]$, R þáttabaugur, c er innihald F og d er innihald G, þá er cd innihald FG.

Sönnun (Sönnun á hjálparsetningu). Gerum ráð fyrir að FG sé ekki frumstæð; þá er til frumstak p í R sem gengur upp í öllum stuðlum FG. Táknum með $[P]$ mynd margliðu P í $R[X]$ í baugnum $R/pR[X]$. Við höfum þá $0 = [FG] = [F] \cdot [G]$; nú er R/pR svið svo að $R/pR[X]$ er heilbaugur og því er $[F] = 0$ eða $[G] = 0$; segjum að $[F] = 0$. En það þýðir að p gengur upp í öllum stuðlum F, og þá er hún ekki frumstæð! ∎

Sönnun (Sönnun á fylgisetningu). Skrifum $F = cF_1, G = dG_1$ þar sem F_1, G_1 eru frumstæðar, þá er $FG = cdF_1G_1$ og F_1G_1 er frumstæð, og þá er cd innihald FG. ∎

Hjálparsetning 11.2. Ef R er þáttabaugur, K er brotasvið hans og P er margliða í $R[X]$ sem er óþættanleg í $R[X]$, þá er hún óþættanleg í $K[X]$.

Sönnun. Sýnum: Ef P þáttast í $K[X], P = FG$ með $F, G \in K[X]$, stig $F \geq 1, \operatorname{stig} G \geq 1$, þá þáttast P í $R[X]$. Stuðlarnir í F og G eru brot $\frac{a}{b}$ þar sem $a, b \in R$; látum a vera margfeldi allra nefnaranna sem koma fyrir í öllum stuðlunum; þá er $a \neq 0$ og $aG \in R[X]$. Skrifum nú $aF = cF_1$ og $aG = dG_1$,

þar sem F_1 og G_1 eru frumstæðar margliður í $R[X]$. Þá er $a^2FG = cdF_1G_1$; skv. Gauss er F_1G_1 frumstæð. En nú er $FG = P = sP_1$ þar sem P_1 er frumstæð, $a^2sP_1 = cdF_1G_1$; og þá er a^2s tengt cd í R, þ.e. $cd = a^2r$, þar sem r er tengt s í R. Þ.e. $a^2P = a^2rF_1G_1$, svo að $P = (rF_1)G_1$, sem er þáttun í $R[X]$. ∎

Athugasemd. Margliða getur þáttast í $R[X]$, en verið óþættanleg í $K[X]$; t.d. er $2X + 2 = 2(X + 1) \in \mathbb{Z}[X]$, þá eru $2, X + 1$ ekki eindir í $\mathbb{Z}[X]$; svo að $2X + 2$ er þáttanlegt í $\mathbb{Z}[X]$, en ekki í $\mathbb{Q}[X]$, því 2 er eind í $\mathbb{Q}$ og því í $\mathbb{Q}[X]$. Hins vegar gildir

Setning 11.7. Látum R vera þáttabaug, P vera *frumstæða* margliðu í $R[X]$. Þá er jafngilt:

(i) P er óþáttanleg í $R[X]$,

(ii) P er óþáttanleg í $K[X]$,

(iii) P er frumstak í $K[X]$,

(iv) P er frumstak í $R[X]$.

Sönnun. (i)⇒(ii) er sértilfelli af síðustu hjálparsetningu. (ii)⇒(iii) er þekkt, því $K[X]$ er höfuðíðalbaugur. (iv)⇒(i) er líka þekkt. Eftir stendur (iii)⇒(iv): Gerum ráð fyrir að P sé frumstak í $K[X]$. Látum $F, G \in R[X]$ vera þ.a. $P \mid FG$ í $R[X]$. Þá er líka $P \mid FG$ í $K[X]$, svo að $P \mid F$ eða $P \mid G$, segjum $P \mid F$ í $K[X]$. Þá má skrifa $F = PQ$, þar sem $Q \in K[X]$. Nú er til stak a í R, $a \neq 0$, þ.a. $aQ \in R[X]$. Skrifum þá $aQ = cQ_1$, þar sem Q_1 er frumstæð margliða í $R[X]$. Höfum þá $aF = P \cdot aQ = cPQ_1$. En skv. Gauss er PQ_1 frumstæð, svo að $a \mid c$ (því að skrifa má $F = dF_1$, F_1 frumstæð, og þá $adF_1 = cPQ_1$, svo að c er tengt ad). Skrifum $c = ab$; höfum þá $aF = abPQ_1$ og vegna $a \neq 0$ er $F = P \cdot bQ_1$, $bQ_1 \in R[X]$ svo að P gengur upp í F í $R[X]$. ∎

Fylgisetning 11.5. Látum R vera þáttabaug. Frumstökin í $R[X]$ eru frumstökin í R (sem við lítum á sem fastar margliður) og óþættanlegu frumstæðu margliðurnar í $R[X]$.

Setning 11.8. Ef R er þáttabaugur, þá er $R[X]$ þáttabaugur.

Sönnun. Látum $F \in R[X]$, $F \neq 0$, skrifum $F = cF_1$ þar sem c er innihald F, við getum þáttað það í frumþætti í R; og það nægir að sýna að F_1 sé margfeldi af frumstæðum margliðum í $R[X]$. Þrepum yfir stig F; ljóst ef stig $F = 0$ eða 1. G.r.f. að stig $F \geq 2$. Ef F er óþættanlegt er ekkert að sýna; annars þáttum við $F = P_1Q_1$, þar sem P_1Q_1 eru ekki eindir; þær eru frumstæðar margliður skv. Gauss; og þær hafa þá minna stig en F; skv. þrepunarforsendu er hvor um sig margfeldi af óþættanlegum frumstæðum margliðum. ∎

Setning 11.9 (Eisenstein). Látum $F \in R[X]$, $F = \sum_{k=0}^{n} a_k X^k$ og gerum ráð fyrir að p sé frumstak í R þannig að $p \nmid a_n$, $p \mid a_j$ fyrir $j = 0, \ldots, n-1$ og $p^2 \nmid a_0$, þá er F óþættanleg í $R[X]$.

Sönnun bíður í bili.

Skilgreining 11.7. Látum R vera víxlinn (ein)baug og skrifum $R[X_1]$ í stað $R[X]$; þá getum við myndað margliðubauginn

$$R[X_1, X_2] := (R[X_1])[X_2] = R[X_1][X_2]$$

yfir $R[X_1]$; og almennar má skilgreina *margliðubauginn* $R[X_1, \ldots, X_n]$ *yfir* R *með* n *óákveðnum stærðum* með þrepun þannig að

$$R[X_1, \ldots, X_n, X_{n+1}] := R[X_1, \ldots, X_n][X_{n+1}].$$

Fáum nú:

Setning 11.10. Ef R er þáttabaugur þá er margliðubaugurinn $R[X_1, \ldots, X_n]$ líka þáttabaugur.

Sönnun. Augljóst með þrepun. ∎

Athugasemd. Sér í lagi er $\mathbb{Z}[X_1, \ldots, X_n]$ þáttabaugur og fyrir sérhvert svið K er $K[X_1, \ldots, X_n]$ þáttabaugur. Fyrir $n \geq 2$ eru þetta ekki höfuðíðalbaugar (ath. að svið er þáttabaugur sem hefur engin frumstök)!

Þessir þáttabaugar eru mikilvægir í algebru og algebrulegri rúmfræði.

Athugasemd. Notum stundum aðra bókstafi í stað $X_1, \ldots, X_n$, t.d. skrifum við oft $K[X, Y]$ í stað $K[X_1, X_2]$.

Eigum enn eftir að sanna setningu Eisensteins, til þess notum við hjálparsetningu:

Hjálparsetning 11.3. Látum R vera víxlinn einbaug, $\mathfrak{A}$ vera íðal í R. Ef $\pi : R \to R/\mathfrak{A}$ er ofanvarpið og

$$\hat{\pi} : R[X] \to R/\mathfrak{A}[X], \quad \sum a_k X^k \mapsto \sum \pi(a_k) X^k$$

er vörpunin sem π gefur af sér og P er margliða í $R[X]$ þ.a. $\hat{\pi}(P)$ sé ekki margfeldi af margliðum af minna stigi en P og forystustuðull P sé ekki í $\mathfrak{A}$, þá er P ekki margfeldi margliða af minna stigi.

Sönnun. Ef $P = Q_1 Q_2$ með $\operatorname{stig}(Q_1), \operatorname{stig}(Q_2) \leq \operatorname{stig}(P)$, þá er $\hat{\pi}(P) = \hat{\pi}(Q_1)\hat{\pi}(Q_2)$, $\operatorname{stig}(\hat{\pi}(Q_j)) < \operatorname{stig}(P) = \operatorname{stig}(\hat{\pi}(P))$ (þar sem forystustuðull P er ekki $\mathfrak{A}$ varpast hann ekki í núll, svo stigið er það sama). ∎

Sönnun (Sönnun á Eisenstein). Látum $\pi : R \to R/pR$ vera ofanvarpið og $\hat{\pi} : R[X] \to R/pR[X]$ vera samsvarandi vörpun. Vegna $p \nmid a_n$ er $\operatorname{stig}(\hat{\pi}(P)) = \operatorname{stig}(P) = n$. Vegna $p \mid a_j$ fyrir $j < n$ er $\hat{\pi}(P) = \pi(a_n)X^n$; ef P væri þættanlegt í $K[X]$, þá mætti skrifa $P = Q_1 Q_2$, þar sem Q_1, Q_2 hafa minna stig en P, segjum $Q_1 = \sum_{k=0}^{m} b_k X^k$, $Q_2 = \sum_{k=0}^{l} c_k X^k$, þar sem $m, l < n$ og $m + l = n$ (þetta er hægt því við gætum tekið innihald úr $P = cP_1$ og þáttað P_1). En þá er

$$\hat{\pi}(Q_1)\hat{\pi}(Q_2) = \hat{\pi}(P) = \pi(a_n)X^n,$$

og $R/pR[X]$ er þáttabaugur (því þetta er svið) þannig að $\hat{\pi}(Q_1) = d_1 X^m$, $\hat{\pi}(Q_2) = d_2 X^l$ fyrir einhver stök $d_1, d_2 \in R/pR$. En það þýðir að $p \mid b_0$ og $p \mid c_0$; en $a_0 = b_0 c_0$, svo að $p^2 \mid a_0$ í mótsögn við forsendu. ∎

Af hjálparsetningunni að ofan leiðir líka

Setning 11.11. Ef $P \in \mathbb{Z}[X]$ og p er frumtala, $\pi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ er náttúrlega ofanvarpið og $\hat{\pi}(P)$ er óþættanleg margliða í $\mathbb{Z}/p\mathbb{Z}[X]$, en af sama stigi og P, þá er P óþættanleg í $\mathbb{Q}[X]$.

Dæmi 11.2. (1) Látum p vera frumtölu. Þá er margliðan

$$F := X^{p-1} + X^{p-2} + \cdots + X + 1$$

óþættanleg í $\mathbb{Q}[X]$: Athugum að

$$X^p - 1 = (X - 1)(X^{p-1} + \cdots + X + 1).$$

Ef F væri þáttanleg, þá væri $F(X+1)$ það líka, en við höfum

$$\begin{aligned} XF(X+1) &= (X+1)^p - 1 \\ &= X^p + \binom{p}{1}X^{p-1} + \binom{p}{2}X^{p-2} + \cdots + \binom{p}{1}X \\ &= X\left(X^{p-1} + \sum_{k=1}^{p-1}\binom{p}{k}X^{p-k-1}\right) \end{aligned}$$

svo að

$$F(X+1) = X^{p-1}\sum_{k=1}^{p-1}\binom{p}{k}X^{p-k-1}.$$

En við vitum að fyrir frumtölu p gildir $p \mid \binom{p}{k}$ fyrir $k = 1, \ldots, p-1$ og $p^2 \nmid \binom{p}{1} = p$ (vitum að í baug með kennitölu p, sem er frumtala, gildir að $(x+y)^p = x^p + y^p$, sem var sannað á heimadæmi); svo skv. Eisenstein er $F(X+1)$ og þar með F óþættanleg í $\mathbb{Q}[X]$.

(2) Um Eisenstein: Sýnum að margliðan

$$P := X^2 + Y^2 + 1$$

er óþættanleg í $\mathbb{C}[X,Y]$: Lítum á $\mathbb{C}[X,Y]$ sem $\mathbb{C}[X][Y]$; getum skrifað

$$P = Y^2 + (X-i)(X+i).$$

Nú er (X_i) frumstak í $\mathbb{C}[X]$, gengur ekki upp í forystustuðul P (sem margliðu í Y), en það gengur upp í fastastuðulinn $(X-i)(X+i)$, en ekki tvisvar! Þar með er P óþættanleg skv. Eisenstein. □

Athugasemd. Undirstöðusetning algebrunnar segir að sérhver margliða í $\mathbb{C}[X]$ hafi núllstöð í $\mathbb{C}$ ef hún er ekki föst. Af því leiðir að frumþáttun í $\mathbb{C}[X]$ er af gerðinni

$$P = u(X-c_1)(X-c_2)\cdots(X-c_n)$$

þar sem $u \in \mathbb{C}\setminus\{0\}$ og $c_1, \ldots, c_n \in \mathbb{C}$. Stöðluðu margliðurnar $X - c$ með $c \in \mathbb{C}$ mynda fulltrúamengi fyrir frumstökin í $\mathbb{C}$.

Af þessu leiðir: Margliður í $\mathbb{R}[X]$ má þátta í línulegar margliður í $\mathbb{C}[X]$; ef núllstöð $c \in \mathbb{C}$ er ekki í $\mathbb{R}$, þá er $\bar{c}$ líka núllstöð, og við getum skrifað margliðu $(X-c)(X-\bar{c})P$, þar sem $P \in \mathbb{C}[X]$;

$$(X-c)(X-\bar{c}) = X^2 - 2\operatorname{Re} c + |c|^2 \in \mathbb{R}[X],$$

svo að P fæst með því að deila margliðu í $\mathbb{R}[X]$ upp í upphaflegu margliðuna, þar með er $P \in \mathbb{R}[X]$. Þrepun gefur að sérhverja margliðu í $\mathbb{R}[X]$ má skrifa sem

$$uP_1 \cdots P_r$$

þar sem $u \in \mathbb{R}^* = \mathbb{R} \setminus \{0\}$ og P_j er annaðhvort af gerðinni $X - c$ með $c \in \mathbb{R}$ eða margliða $X^2 + bX + c$ af öðru stigi án núllstöðva í $\mathbb{R}$, sem þýðir að $b^2 - 4c < 0$. Þessar margliður $X - c$ og $X^2 - bX + c, b^2 - 4c < 0$, mynda því fulltrúamengi fyrir frumstökin í $\mathbb{R}[X]$.

Chiroff-setningar í bókinni eru undirstöðusetningar grúpufræði, sem væri áhugavert að skoða, en vegna tímaskorts lítum við heldur á efni næsta kafla.

Kafli 12

Frumþáttun í Gauss-talnabaugnum $\mathbb{Z}[i]$

Höfum vörpun

$$N : \mathbb{Z}[i] \to \mathbb{N}, \quad z = x + iy \mapsto |z|^2 = z\bar{z} = x^2 + y^2,$$

um öll $z, w \in \mathbb{Z}[i]$ gildir

$$N(zw) = N(z)N(w)$$

og við vitum að N gerir $\mathbb{Z}[i]$ að evklíðskum baug, þar með er hann höfuðíðalbaugur og þáttabaugur. Við segjum að náttúrleg tala n sé *summa tveggja ferninga* ef til eru $x, y \in \mathbb{Z}$ þannig að $n = x^2 + y^2$; jafngilt er að til sé $z \in \mathbb{Z}[i]$ þannig að $n = N(z)$.

Ætlum að skoða þáttun í þessum baug og sjáum þá nákvæmlega hvaða heilar tölur eru summa tveggja ferninga!

Sjáum: Ef $z \mid w$ í $\mathbb{Z}[i]$, þá gildir $N(z) \mid N(w)$ í $\mathbb{N}$. Af því leiðir: Ef $N(z) = p$ er frumtala, þá er z frumstak í $\mathbb{Z}[i]$, annars mætti skrifa $z = uv$ þar sem $u, v \in \mathbb{Z}[i] \setminus \{0\}$ og $N(u) \neq 1$; og þá fengist $p = N(u)N(v)$ með $N(u), N(v) \geq 2$, sem fær ekki staðist.

Viljum ákvarða frumstökin í $\mathbb{Z}[i]$: Látum π vera frumstak í $\mathbb{Z}[i]$, þá höfum við $\pi \mid \pi\overline{\pi} = N(\pi) \geq 2$; nú má þætta $N(\pi)$ í frumþætti í $\mathbb{N}$; svo að π verður að ganga upp í einum frumþættinum svo að til er frumtala p þ.a. $\pi \mid p$ í $\mathbb{Z}[i]$. Það getur ekki verið til nema ein slík frumtala p, ef p, q væru frumtölur þ.a. $p \neq q$ og $\pi \mid p$, $\pi \mid q$ í $\mathbb{Z}[i]$, þá mætti finna heilar tölur k, j sem leysa Bézout-jöfnuna $1 = pq + qj$; og við fengjum þá að $\pi \mid 1$ í $\mathbb{Z}[i]$, sem er fráleitt. Við fáum þá öll frumstök í $\mathbb{Z}[i]$ með því að finna frumþætti venjulegra frumtalna í baugnum $\mathbb{Z}[i]$. Athugum þrjú tilvik:

1. tilvik, $p = 2$: Við höfum

$$2 = (-i)(1 + i)^2$$

og þetta er frumþáttun í $\mathbb{Z}[i]$, því að $-i$ er eind, og $N(1+i) = 2$ er frumtala, svo að $1+i$ er frumstak í $\mathbb{Z}[i]$.

2. tilvik, $p \equiv 3 \pmod 4$: Gerum ráð fyrir að π sé frumstak í $\mathbb{Z}[i]$ þ.a. $\pi \mid p$. Þá fæst $N(\pi) \mid N(p) = p^2$; nú er $N(\pi) \neq 1$, svo að $N(\pi)$ er annaðhvort p eða p^2. Skrifum $\pi = x + iy$, þá er $N(\pi) = x^2 + y^2$ og þetta getur aldrei verið jafnt p, því að $x^2 \equiv 0 \pmod 4$ ef $x^2 \equiv 1 \pmod 4$ ef x er oddatala, svo að $x^2 + y^2 \equiv 0, 1$ eða $2 \pmod 4$, og því er $x^2 + y^2 \neq p$. Þar með er $N(\pi) = p^2 = N(p)$. En þá eru π og p tengd í $\mathbb{Z}[i]$: Ef við skrifum $p = u\pi$, þá fæst $N(p) = N(u)N(\pi)$, svo að $N(u) = 1$ og því er u eind í $\mathbb{Z}[i]$. Þetta þýðir að p er frumstak í $\mathbb{Z}[i]$.

Athugasemd. Sýndum: Frumtala p þ.a. $p \equiv 3 \pmod 4$ er ekki summa tveggja ferninga.

3. tilvik, $p \equiv 1 \pmod 4$: Skrifum þá $p = 2n + 1$, þar sem n er *jöfn* tala. Þá er

$$\begin{aligned}(p-1)! &= (2n)! \\ &= n!(p-1)(p-2)\cdots(p-n) \\ &\equiv n!(-1)(-2)\cdots(-n) \\ &\equiv n!(-1)^n \cdot n! \\ &\equiv (n!)^2 \pmod p.\end{aligned}$$

Nú segir setning Wilsons að $(p-1)! \equiv -1 \pmod p$. Því er fyrir $x := n!$

$$p \mid x^2 + 1 = (x-i)(x+i).$$

Þá fæst líka $\pi \mid (x-i)(x+i)$ svo $\pi \mid x-i$ eða $\pi \mid x+i$ fyrir frumstak $\pi \in \mathbb{Z}[i]$ sem gengur upp í p. Hins vegar er ljóst að p gengur hvorki upp í $x+i$ né $x-i$ í $\mathbb{Z}[i]$. Ef $x+i = p(u+vi) = pu+pvi$ með $u, v \in \mathbb{Z}$ þá fengist $p \mid 1$ í $\mathbb{N}$, sem er fráleitt! Það þýðir að fyrir frumstak π í $\mathbb{Z}[i]$ sem gengur uppí p í $\mathbb{Z}[i]$ geta π og p ekki verið tengd í $\mathbb{Z}[i]$; þá er $N(\pi) \neq N(p) = p^2$, en $N(\pi) \mid p^2$, svo að $N(\pi) = p$. En þá er líka $N(\overline{\pi}) = p$, svo að $\overline{\pi}$ er frumstak í $\mathbb{Z}[i]$ og

$$p = N(\pi) = \pi\overline{\pi},$$

og þetta er frumþáttun í $\mathbb{Z}[i]$. Stökin π og $\overline{\pi}$ geta ekki verið tengd í $\mathbb{Z}[i]$: Skrifum $\pi = x + yi$; ef $\pi = \overline{\pi}$, þá væri $y = 0$ og $p = N(\pi) = x^2$, sem er fráleitt. Ef $\pi = -\overline{\pi}$, þá væri $x = 0$ og $p = N(\pi) = y^2$. Ef $\pi = i\overline{\pi} = -y + ix$, þá væri $p = N(\pi) = 2x^2$, sama fæst ef $\pi = -i\overline{\pi}$.

Athugasemd. Sjáum: Ef p er frumtala þ.a. $p \equiv 1 \pmod 4$, þá er p summa tveggja teninga.

Fáum:

Setning 12.1. Frumstökin í $\mathbb{Z}[i]$ eru (burstéð frá tengslum) eftirfarandi

(i) Talan $1+i$,

(ii) sérhver frumtala p þ.a. $p \equiv 3 \pmod 4$,

(iii) fyrir sérhverja frumtölu p þ.a. $p \equiv 1 \pmod 4$ tvö ótengd frumstök $\pi, \overline{\pi}$ þ.a. $\pi\overline{\pi} = p$.

Athugum að $2 = 1^2 + 1^2$, svo að 2 er summa tveggja ferninga. Sjáum:

Setning 12.2. Frumtala p er summa tveggja ferninga þ.þ.a.a $p = 2$ eða $p \equiv 1 \pmod 4$.

Setning 12.3. Náttúrleg tala n þ.a. $n \geq 1$ er summa tveggja ferninga þ.þ.a.a veldisvísir allra frumþátta p í frumþáttun tölunnar n (í $\mathbb{N}$) þannig að $p \equiv 3 \pmod 4$ sé jöfn tala.

Sönnun. Gerum ráð fyrir að $n = x^+y^2$ með $x, y \in \mathbb{Z}$. Þá má skrifa frumþáttun staksins $x+iy$ í $\mathbb{Z}[i]$ sem

$$x + iy = u(1+i)^h \pi_1^{j_1}\overline{\pi}_1^{k_1} \cdots \pi_r^{j_r}\overline{\pi}_r^{k_r} q_1^{l_1} \cdots q_s^{l_s}$$

þar sem u er eind í $\mathbb{Z}[i]$ þ.a. $u\overline{u} = 1$; fyrir $\rho = 1, \ldots, r$ er π_ρ frumstak í $\mathbb{Z}[i]$ þ.a. $\pi_\rho\overline{\pi}_\rho = p_\rho$ þar sem p_ρ er frumtala þ.a. $p_\rho \equiv 1 \pmod 4$ og fyrir $\sigma = 1, \ldots, s$ er q_σ frumtala þ.a. $q_\sigma \equiv 3 \pmod 4$. En þá er

$$\begin{aligned} n &= (x+iy)\overline{(x+iy)} \\ &= 2^h p_1^{j_1+k_1} \cdots p_r^{j_1+k_1} q_1^{2l_1} \cdots q_s^{2l_s}. \end{aligned}$$

Öfugt, ef skrifa má

$$n = 2^h p_1^{j_1} \cdots p_r^{j_r} \cdot q_1^{2l_1} \cdots q_s^{2l_s}$$

þar sem p_ρ eru frumtölur þ.a. $p_\rho \equiv 1 \pmod 4$ fyrir $p = 1, \ldots, r$ og $q_\sigma \equiv 3 \pmod 4$ fyrir $\sigma = 1, \ldots, s$, þá setjum við

$$z := (1+i)^2 \pi_1^{j_1} \cdots \pi_r^{j_r} q_1^{l_1} \cdots q_s^{l_s}$$

þar sem π_ρ er frumstak í $\mathbb{Z}[i]$ þ.a. $\pi_\rho\overline{\pi}_\rho = p_\rho$ fyrir $\rho = 1, \ldots, r$; fáum

$$\begin{aligned} N(z) &= N(1+i)^h N(\pi_1)^{j_1} \cdots N(\pi_r)^{j_r} N(q_1)^{l_1} \cdots N(q_s)^{l_s} \\ &= 2^h p_1^{j_1} \cdots p_r^{j_r} q_1^{2l_1} \cdots q_s^{2l_s}; \end{aligned}$$

svo að

$$n = N(z) = x^2 + y^2$$

ef $z = x + iy$ með $x, y \in \mathbb{Z}$. ∎

Atriðisorðaskrá