Jón Kristinn Arason

Tölur og mengi

1 Stök og mengi

Við munum leggja hugtökin „stak“, „mengi“ og „vera í“ til grundvallar þeirrar stærðfræði sem hér verður farið í. Það þýðir að þau verða ekki skilgreind út frá öðrum einfaldari hugtökum. Þau eru frumhugtök. Hinsvegar má reyna að gefa lýsingu á því hvað átt er við með þessum orðum, án þess að um skilgreiningu í stærðfræðilegum skilningi sé að ræða.

Stak er einstakur hlutur eða fyrirbæri. Hlutir þeir sem hér um ræðir geta verið hvort sem er, raunverulegir eða óhlutstæðir. En með því að þeir séu einstakir er átt við að þeir séu aðgreinanlegir, að hægt sé að fjalla um þá einn og einn. Það er augljóslega nauðsynleg forsenda þess að hægt sé að fjalla um þá á stærðfræðilegan hátt. Hugtakið „stak“ er því grundvallarhugtak í allri stærðfræði.

Þegar rætt er um stök þá er nauðsynlegt að gefa þeim nöfn, nota tákn fyrir þau. Til þess að unnt sé að aðgreina þau stök sem til umræðu eru má ekki nota sama táknið fyrir tvö eða fleiri mismunandi stök í sama samhengi. Aftur á móti má nota mismunandi tákn fyrir sama stakið. Það að tvö tákn, segjum a og b, séu nöfn á sama stakinu er gefið til kynna með því að skrifa

$$a = b$$

Að a og b séu tákn fyrir tvö mismunandi stök er hinsvegar ritað

$$a \neq b$$

Í samræmi við almenna málvenju við notkun nafna munum við segja einfaldlega „a sé stak“ í stað „a sé tákn fyrir stak“, tala um „stakið a“ í stað „stakið sem táknað er með a“, segja „stökin a og b eru söm“ í stað „a og b eru tákn fyrir sama stakið“ o.s.frv.

Þegar fjallað er um stökin þá er að sjálfsögðu oft fjallað um hópa eða söfn staka. En í mörgum greinum stærðfræðinnar er nauðsynlegt að fjalla um söfnin sjálf á stærðfræðilegan hátt. En þá þurfa söfnin að vera stök. *Mengi* er safn staka sem sjálft er stak, samantekt ákveðinna staka í eina heild, eitt stak. Þau stök sem mynda safnið, sem tekin eru saman í þessa heild, eru sögð *vera í* menginu eða liggja í menginu, og mengið er sagt hafa stökin eða innihalda stökin. Með því að stökin í heildinni séu ákveðin er átt við að fyrir sérhvert stak og sérhvert mengi sé víst að annaðhvort sé stakið í menginu eða ekki. Það að stak a sé í mengi M er táknað með

$$a \in M$$

Að stakið a sé ekki í menginu M er aftur á móti ritað

$$a \notin M$$

Þar sem lýsingar okkar á því hvað átt er við með frumhugtökunum geta ekki talist fullkomnar skilgreiningar, þá getum við ekki notað þær sem undirstöður sannana á setningum um stök og mengi. Við verðum að leggja ákveðnar reglur til grundvallar, reglur sem ekki verða sannaðar út frá öðrum augljósari, frumsetningar. En að sjálfsögðu má reyna að gefa skýringar á inntaki einstakra frumsetninga, án þess að um sannanir í stærðfræðilegum skilningi sé að ræða.

Við skiljum hugtakið „mengi“ þannig að sérhvert mengi sé ákvarðað af þeim stökum sem í því eru, að það sé aðeins háð því hvaða stök eru tekin saman í þessa heild, en ekki hvernig þau eru það. Við orðum þetta í frumsetningu á eftirfarandi hátt.

Frumsetning (um yfirgrip): Mengi M og N eru söm ef þau hafa sömu stökin.

Að mengi M og N séu söm þýðir þá tvennt. Annarsvegar að sérhvert stak í M sé líka í N og hinsvegar að sérhvert stak í N sé líka í M. Þetta gefur okkur tilefni til eftirfarandi skilgreiningar.

Skilgreining: M og N séu mengi. Ef sérhvert stak í M er líka í N þá er M sagt vera *hlutmengi* í N, táknað

$$M \subseteq N$$

Ef M er hlutmengi í N en $M \neq N$ þá er M sagt vera *eiginlegt hlutmengi* í N, táknað

$$M \subset N$$

Nú er eftirfarandi setning augljós af ofansögðu.

Setning 1.1: Fyrir sérhver mengi X, Y og Z gilda reglurnar:
(i) $X \subseteq X$
(ii) ef $X \subseteq Y$ og $Y \subseteq X$ þá $X = Y$
(iii) ef $X \subseteq Y$ og $Y \subseteq Z$ þá $X \subseteq Z$

Þar sem mengi er ákvarðað af þeim stökum sem það hefur, þá má lýsa mengi með fáum stökum með því að telja einfaldlega upp þau stök sem í því eru. Það hefur gefið tilefni til notkunar sérstakra tákna fyrir slík mengi. Ef mengið M hefur stakið a en ekkert annað stak þá er skrifað

$$M = \{a\}$$

Ef M hefur stökin a og b en engin önnur stök þá er ritað

$$M = \{a, b\}$$

o.s.frv.

Við munum að sjálfsögðu skilja hugtakið „mengi“ þannig að ef a er stak þá sé til mengi sem inniheldur a en ekkert annað stak, og ef a og b eru stök þá sé til mengi sem inniheldur a og b en engin önnur stök. Þetta þarf auðvitað að koma fram í frumsetningu. En við notum tækifærið til þess að koma því að að við lítum á tómt safn sem einstakan hlut, sem stak og þar með sem tómt mengi.

Frumsetning (um lítil mengi):
(i) Til er mengi sem hefur ekkert stak.
(ii) Ef a er stak þá er til mengi sem hefur a en ekkert annað stak.
(iii) Ef a og b eru stök þá er til mengi sem hefur a og b en engin önnur stök.

Í raun er liður (ii) í þessari frumsetningu óþarfur. Hann fæst nefnilega af lið (iii) með því að taka $b = a$. Á táknmáli: $\{a\} = \{a, a\}$.

Ef mengið M hefur ekkert stak og N er eitthvert mengi þá er M hlutmengi í N. Annars hlyti að vera til stak í M sem ekki væri í N. En slíkt stak er greinilega ekki til ef M er tómt. Ef N hefur nú heldur ekkert stak þá er af sömu ástæðu N líka hlutmengi í M. Samkvæmt Setningu 1.1 (ii) er þar með $M = N$. Við höfum því sannað eftirfarandi setningu.

Setning 1.2: Ekki er til nema eitt mengi sem hefur ekkert stak. Það er hlutmengi í sérhverju mengi.

Skilgreining: Mengið sem ekkert stak hefur heitir *tóma mengið*. Það er táknað með

$$\emptyset$$

Mengi með mjög mörgum stökum er ógerningur að lýsa með því að telja upp stökin í því. Í stað þess notfærum við okkur það að stökin í menginu geta haft einhvern sameiginlegan eiginleika sem önnur stök hafa ekki, að stökin í menginu geta uppfyllt eitthvert skilyrði sem önnur stök uppfylla ekki.

Við skulum segja að gefinn eiginleiki sé vel skilgreindur ef fyrir sérhvert stak er víst að annaðhvort hafi það þennan eiginleika eða ekki. Ef E táknar slíkan eiginleika þá verður það að stak x hafi hann táknað með $E(x)$. Gerum nú ráð fyrir að M sé mengi þannig að fyrir sérhvert stak x gildi að $x \in M$ þá og því aðeins að $E(x)$. Af frumsetningunni um yfirgrip leiðir þá að M

er algjörlega ákvarðað af E. Við segjum því að E sé skilgreinandi eiginleiki fyrir M og að M sé mengi þeirra staka x þannig að $E(x)$, táknað

$$M = \{\, x \mid E(x) \,\}$$

Við höfum til dæmis $\emptyset = \{\, x \mid x \neq x \,\}$ og $\{a, b\} = \{\, x \mid x = a \text{ eða } x = b \,\}$. (Bókstafurinn „$x$“ er hér aukaatriði. Í stað hans má nota má sérhvert það tákn sem ekki hefur þegar fengið fasta merkingu í samhenginu.)

Sérhverju mengi M má lýsa með skilgreinandi eiginleika — til dæmis er $M = \{\, x \mid x \in M \,\}$. En fyrir gefinn vel skilgreindan eiginleika E þarf ekki að vera til mengi M þannig að $M = \{\, x \mid E(x) \,\}$. Sem dæmi má taka eiginleikann að vera mengi sem ekki er stak í sjálfu sér. Ef þetta væri skilgreinandi eiginleiki fyrir mengi M þá gilti fyrir sérhvert stak x að $x \in M$ þá og því aðeins að x væri mengi og $x \notin x$. Þetta gilti þá sér í lagi fyrir $x = M$, svo að $M \in M$ þá og því aðeins að $M \notin M$, sem er greinilega mótsögn. Slíkt mengi M getur því ekki verið til. Í tilfellum sem þessum er stundum sagt að $\{\, x \mid E(x) \,\}$ sé ekki til.

Við gerum samt ráð fyrir að vel skilgreindur eiginleiki ákvarði hlutmengi í sérhverju fyrirfram gefnu mengi:

Frumsetning (um hlutmengi): U sé mengi. Ef E er vel skilgreindur eiginleiki þá er til mengi sem hefur öll þau stök í U sem hafa E en engin önnur stök.

Mengið í þessari frumsetningu, mengi allra þeirra staka $x \in U$ þannig að $E(x)$, er venjulega táknað með

$$\{\, x \in U \mid E(x) \,\}$$

En að sjálfsögðu má einnig nota $\{\, x \mid x \in U \text{ og } E(x) \,\}$.

Við skulum nú athuga hvað verður um dæmið hér að framan ef við takmörkum okkur við stökin í fyrirfram gefnu mengi U. Samkvæmt frumsetningunni um hlutmengi er til mengi

$$M = \{\, x \in U \mid x \text{ er mengi og } x \notin x \,\}$$

Ef nú $M \in U$ þá fengist á sama hátt og áður mótsögnin: $M \in M$ þá og því aðeins að $M \notin M$. Því hlýtur að gilda $M \notin U$. Þetta sýnir að til er mengi sem ekki er stak í U. Sér í lagi fæst eftirfarandi setning.

Setning 1.3: Ekki er til mengi sem hefur öll stök.

Því miður þekkja menn enga aðferð til þess að sjá það á gefnum vel skilgreindum eiginleika hvort hann skilgreini mengi eða ekki. Ekki heldur neinn einn flokk vel skilgreindra eiginleika sem ákvarða mengi, nógu víðtækan til þess að fullnægja þörfum nútíma stærðfræði. Því eru einstakir flokkar slíkra eiginleika taldir upp í frumsetningum. Síðustu tvær frumsetningar voru einmitt af þessu tagi og næstu tvær verða það líka.

Frumsetning (um veldismengi): U sé mengi. Þá er til mengi sem hefur öll þau stök sem eru hlutmengi í U en engin önnur stök.

Mengi þessu, mengi allra hlutmengja í U, má lýsa sem $\{\, X \mid X \subseteq U \,\}$.

Skilgreining: U sé mengi. Mengið $\{\, X \mid X \subseteq U \,\}$ heitir þá *veldismengi* U. Það er táknað með

$$\mathcal{P}(U)$$

Ef U er lítið þá er auðvelt að lýsa $\mathcal{P}(U)$. Til dæmis er $\mathcal{P}(\emptyset) = \{\emptyset\}$, $\mathcal{P}(\{a\}) = \{\emptyset, \{a\}\}$ og $\mathcal{P}(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$. Við vekjum athygli á því að $\mathcal{P}(U)$ er alltaf mengi mengja, þ.e. mengi þannig að sérhvert stak í því er líka mengi.

Frumsetning (um sammengi): $\mathcal{C}$ sé mengi mengja. Þá er til mengi sem hefur öll þau stök sem eru í að minnsta kosti einu mengjanna sem eru í $\mathcal{C}$, en engin önnur stök.

Mengið í þessari frumsetningu, mengi allra þeirra staka sem eru í einhverju mengjanna í $\mathcal{C}$, er $\{\, x \mid \text{til er } X \in \mathcal{C} \text{ með } x \in X \,\}$.

Skilgreining: $\mathcal{C}$ sé mengi mengja. Mengið $\{\, x \mid \text{til er } X \in \mathcal{C} \text{ með } x \in X \,\}$ heitir þá *sammengi* mengjanna í $\mathcal{C}$. Það er táknað

$$\bigcup_{X \in \mathcal{C}} X$$

Í frumsetningunni um sammengi má mengið $\mathcal{C}$ vera tómt. Við höfum einfaldlega $\bigcup_{X \in \emptyset} X = \emptyset$. Viljum við hinsvegar mynda mengi allra þeirra staka sem eru í öllum mengjunum í $\mathcal{C}$, þá verðum við að gera ráð fyrir að $\mathcal{C} \neq \emptyset$. Sérhvert stak er nefnilega í öllum mengjum sem eru í $\emptyset$. En samkvæmt setningu 1.3 er ekkert mengi til sem hefur öll stök. Aftur á móti þurfum við ekki sérstaka frumsetingu til þess að geta myndað þetta mengi.

Setning 1.4: $\mathcal{C}$ sé ekki tómt mengi mengja. Þá er til mengi sem hefur öll þau stök sem eru í öllum mengjunum sem eru í $\mathcal{C}$, en engin önnur stök.
Sönnun: Þar sem $\mathcal{C}$ er ekki tómt þá er til mengi $A \in \mathcal{C}$. Við setjum

$$M := \{\, x \in A \,|\, \text{fyrir öll } X \in \mathcal{C} \text{ gildir } x \in X \,\}$$

(Táknið „:=“ stendur fyrir „er skilgreint sem“.) Ljóst er að ef $x \in M$ þá er x í öllum mengjum $X \in \mathcal{C}$. En ef x er í öllum mengjum $X \in \mathcal{C}$ þá er sér í lagi $x \in A$, auk þess að $x \in X$ fyrir öll $X \in \mathcal{C}$, þar með $x \in M$. Þetta sýnir að M hefur öll þau stök sem eru í öllum mengunum í $\mathcal{C}$, en engin önnur.

Mengið í Setningu 1.4, mengi allra þeirra staka sem eru í öllum mengjunum í $\mathcal{C}$, má rita sem $\{\, x \,|\, \text{fyrir öll } X \in \mathcal{C} \text{ gildir } x \in X \,\}$.

Skilgreining: $\mathcal{C}$ sé ekki tómt mengi mengja. Mengið $\{\, x \,|\, \text{fyrir öll } X \in \mathcal{C} \text{ gildir } x \in X \,\}$ heitir þá *sniðmengi* mengjanna í $\mathcal{C}$. Það er táknað

$$\bigcap_{X \in \mathcal{C}} X$$

Við skulum nú athuga sammengi og sniðmengi mengja í litlum mengjum. Við höfum þegar séð að $\bigcup_{X \in \emptyset} X = \emptyset$ og að $\bigcap_{X \in \emptyset} X$ er ekki til. Ef nú A er mengi þá er greinilega $\bigcup_{X \in \{A\}} X = A$ og $\bigcap_{X \in \{A\}} X = A$.

Skilgreining: A og B séu mengi. Mengið $\bigcup_{X \in \{A,B\}} X$ heitir þá *sammengi* A og B. Það er einnig táknað

$$(A \cup B)$$

Mengið $\bigcap_{X \in \{A,B\}} X$ heitir hinsvegar *sniðmengi* A og B. Það er táknað með

$$(A \cap B)$$

Ef A og B eru mengi þá getum við greinilega skrifað $(A \cap B) = \{\, x \,|\, x \in A \text{ og } x \in B \,\}$. En áður en við lýsum $(A \cup B)$ með skilgreinandi eiginleika getum við þess að orðið „eða“ hefur tvær mismunandi merkingar í daglegu máli. Önnur þeirra útilokar að um báða möguleikana geti verið að ræða, hin ekki. Í stærðfræði er „eða“ aðeins notað í síðar nefndu merkingunni. Með það í huga sést að $(A \cup B) = \{\, x \,|\, x \in A \text{ eða } x \in B \,\}$.

Setning 1.5: Fyrir sérhver mengi X, Y og Z gilda reglurnar:
(i) $\quad (X \cup \emptyset) = X$

(ii) $(X \cap \emptyset) = \emptyset$
(iii) $(X \cup X) = X$
(iv) $(X \cap X) = X$
(v) $(X \cup Y) = (Y \cup X)$
(vi) $(X \cap Y) = (Y \cap X)$
(vii) $((X \cup Y) \cup Z) = (X \cup (Y \cup Z))$
(viii) $((X \cap Y) \cap Z) = (X \cap (Y \cap Z))$
(ix) $((X \cup Y) \cap Z) = ((X \cap Z) \cup (Y \cap Z))$
(x) $((X \cap Y) \cup Z) = ((X \cup Z) \cap (Y \cup Z))$
Ennfremur:
(xi) $X \subseteq (X \cup Y)$
(xii) $(X \cap Y) \subseteq X$
(xiii) ef $Y \subseteq Z$ þá $(X \cup Y) \subseteq (X \cup Z)$
(xiv) ef $Y \subseteq Z$ þá $(X \cap Y) \subseteq (X \cap Z)$
(xv) ef $X \subseteq Z$ og $Y \subseteq Z$ þá $(X \cup Y) \subseteq Z$
(xvi) ef $Z \subseteq X$ og $Z \subseteq Y$ þá $Z \subseteq (X \cap Y)$
Sönnun: Heimaverkefni.

Í samsetningum mengja með „$\cup$“ og „$\cap$“ er greinilega óhætt að sleppa yztu svigunum án þess að til misskilnings komi. Þar sem það einfaldar ritháttinn, þá munum við gera það og skrifa t.d. „$A \cup (B \cup C)$“ í stað „$(A \cup (B \cup C))$“ og „$A \cup (B \cap C)$“ í stað „$(A \cup (B \cap C))$“. Hinsvegar er yfirleitt ekki óhætt að sleppa innri svigum. Til dæmis er óljóst hvort „$A \cup B \cap C$“ ætti að þýða „$A \cup (B \cap C)$“ eða „$(A \cup B) \cap C$“. Samkvæmt reglu (vii) í setningunni hér að ofan getum við þó leyft okkur að nota ritháttinn „$A \cup B \cup C$“ fyrir hvort sem er, „$A \cup (B \cup C)$“ eða „$(A \cup B) \cup C$“. Eins veldur ritháttinn „$A \cap B \cap C$“ engum miskilningi vegna reglu (viii) í setningunni. Við munum á sama hátt spara okkur svigaskriftir við annarskonar samsetningar sem síðar munu koma fyrir.

Skilgreining: Ef A og B eru mengi þá heitir mengið

$$A \setminus B := \{\, x \mid x \in A \text{ og } x \notin B \,\}$$

mengjamismunur A og B. Ef M er mengi og A er hlutmengi í M þá heitir $M \setminus A$ einnig *fyllimengi* A í M.

Setning 1.6: Fyrir sérhver mengi X, Y og U gilda reglurnar
(i) $U \setminus \emptyset = U$
(ii) $U \setminus U = \emptyset$
(iii) $U \setminus (U \setminus X) = U \cap X$
(iv) $U \setminus (X \cup Y) = (U \setminus X) \cap (U \setminus Y)$

(v) $U \setminus (X \cap Y) = (U \setminus X) \cup (U \setminus Y)$
Sönnun: Heimaverkefni.

Við ljúkum þessum kafla með frumsetningu um mengi sem er af öðru tagi en fjórar síðustu frumsetningar. Fyrst kemur þó skilgreining.

Skilgreining: U sé mengi. Mengi $\mathcal{C}$ af hlutmengjum í U er sagt vera *deildamengi* af U ef eftirfarandi gildir:
(i) ef $X \in \mathcal{C}$ þá $X \neq \emptyset$
(ii) ef $X, Y \in \mathcal{C}$ og $X \neq Y$ þá $X \cap Y = \emptyset$
(iii) $\bigcup_{X \in \mathcal{C}} X = U$

Athugið að í lið (ii) í skilgreiningu þessari höfum við skrifað „$X, Y \in \mathcal{C}$“ í stað „$X \in \mathcal{C}$ og $Y \in \mathcal{C}$“. Við munum oft nota slíkar styttingar til einföldunar ritháttarins.

Af skilyrðunum í skilgreiningunni leiðir að fyrir gefið stak $a \in U$ er til eitt og aðeins eitt $X \in \mathcal{C}$ þannig að $a \in X$. Þetta X er kallað *deild* staksins a (með tilliti til $\mathcal{C}$).

Frumsetning (um val): $\mathcal{C}$ sé deildamengi af mengi U. Þá er til hlutmengi C í U sem inniheldur eitt og aðeins eitt stak úr sérhverju $X \in \mathcal{C}$.

Mengi C eins og í þessari frumsetningu er stundum kallað *fulltrúamengi* fyrir $\mathcal{C}$.

2 Varpanir

Skilgreining: Ef a og b eru stök þá heitir mengið

$$[a, b\rangle := \{\{a, b\}, \{a\}\}$$

örin frá a til b.

Setning 2.1: Fyrir sérhver stök x, y, u og v gildir reglan:
ef $[x, y\rangle = [u, v\rangle$ þá $x = u$ og $y = v$
Sönnun: Ef a og b eru stök þá er $[a, b\rangle$ mengi mengja og ljóst er að sniðmengi mengjanna í því er $\{a\}$ og sammengið $\{a, b\}$. Ef $[x, y\rangle = [u, v\rangle$ þá fæst því að $\{x\} = \{u\}$ og $\{x, y\} = \{u, v\}$. Af því fyrra sést að $x = u$. Það síðara segir þá að $\{x, y\} = \{x, v\}$. Ef $y \neq x$ þá fæst af $y \in \{x, v\}$ að $y = v$ og ef $v \neq x$ þá fæst af $v \in \{x, y\}$ að $v = y$. En ef $y = x$ og $v = x$ þá fæst líka $y = v$.

Skilgreining: A og B séu mengi. *Vörpun* f frá A til B er mengi f af örvum $[a, b\rangle$, þar sem $a \in A$ og $b \in B$, þannig að fyrir sérhvert $a \in A$ sé til eitt og aðeins eitt $b \in B$ með $[a, b\rangle \in f$.

Að f sé vörpun frá mengi A til mengis B er oft táknað $f : A \to B$. Ef $f : A \to B$ er vörpun og $[a, b\rangle \in f$ þá er sagt að f varpi a í b og stundum skrifað $f : a \mapsto b$.

Skilgreining: $f : A \to B$ sé vörpun. Ef $a \in A$ þá er stakið $b \in B$ þannig að $[a, b\rangle \in f$ nefnt *mynd* a við f og er táknað með

$$f(a)$$

Reyndar er stundum einfaldlega skrifað fa í stað $f(a)$.

Setning 2.2: Fyrir sérhverjar varpanir $f : X \to Y$ og $g : X \to Y$ gildir reglan:
$f = g$ þá og því aðeins að $f(x) = g(x)$ fyrir öll $x \in X$.
Sönnun: Af skilgreiningunum hér að ofan leiðir að $f = \{\, [x, f(x)\rangle \mid x \in X \,\}$ og $g = \{\, [x, g(x)\rangle \mid x \in X \,\}$. Setningin er augljós afleiðing af því.

Í reynd er einstökum vörpunum venjulega ekki lýst með því að gefa upp mengi af örvum. Til þess að lýsa vörpun f frá mengi A til mengis B er nefnilega samkvæmt Setningu 2.2 nóg að lýsa því fyrir sérhvert stak í A hvaða stak í B sé mynd þess við f. En gæta verður þess að sú lýsing eigi við eitt og aðeins eitt stak í B.

Skilgreining: $f : A \to B$ og $g : B \to C$ séu varpanir. Vörpunin frá A til C, sem varpar sérhverju staki $a \in A$ í stakið $g(f(a))$, er nefnd *samskeyting* f og g. Hún er táknuð með

$$g \circ f$$

Setning 2.3: Fyrir sérhverjar varpanir $f : X \to Y$, $g : Y \to Z$ og $h : Z \to W$ gildir reglan:

$(h \circ g) \circ f = h \circ (g \circ f)$

Sönnun: Fyrir öll $x \in X$ gildir $((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x))) = h((g \circ f)(x)) = (h \circ (g \circ f))(x)$.

Skilgreining: A sé mengi. Vörpunin frá A til A, sem varpar sérhverju staki $a \in A$ í a, er nefnd *hlutlausa* vörpunin á A. Hún er táknuð með

$$\mathrm{id}_A$$

Setning 2.4: Fyrir sérhverja vörpun $f : X \to Y$ gilda reglurnar:

(i) $f \circ \mathrm{id}_X = f$

(ii) $\mathrm{id}_Y \circ f = f$

Sönnun: Fyrir öll $x \in X$ gildir $(f \circ \mathrm{id}_X)(x) = f(\mathrm{id}_X(x)) = f(x)$ og $(\mathrm{id}_Y \circ f)(x) = \mathrm{id}_Y(f(x)) = f(x)$.

Skilgreining: Vörpun $f : A \to B$ er sögð vera *eintæk* ef fyrir sérhver $a_1, a_2 \in A$ þannig að $a_1 \neq a_2$ gildir $f(a_1) \neq f(a_2)$.

Til þess að sýna að gefin vörpun $f : A \to B$ sé eintæk nægir að sýna að fyrir sérhver $a_1, a_2 \in A$ gildi reglan:

ef $f(a_1) = f(a_2)$ þá $a_1 = a_2$

Setning 2.5: Gefin sé vörpun $f : X \to Y$. Ef til er vörpun $g : Y \to X$ þannig að $g \circ f = \mathrm{id}_X$, þá er vörpunin $f : X \to Y$ eintæk.

Sönnun: $g : Y \to X$ sé vörpun þannig að $g \circ f = \mathrm{id}_X$. Gefin séu $x_1, x_2 \in X$ þannig að $f(x_1) = f(x_2)$. Þá fæst $x_1 = \mathrm{id}_X(x_1) = (g \circ f)(x_1) = g(f(x_1)) = g(f(x_2)) = (g \circ f)(x_2) = \mathrm{id}_X(x_2) = x_2$.

Skilgreining: Vörpun $f : A \to B$ er sögð vera *átæk* ef fyrir sérhvert $b \in B$ er til $a \in A$ þannig að $f(a) = b$.

Setning 2.6: Gefin sé vörpun $f : X \to Y$. Ef til er vörpun $h : Y \to X$ þannig að $f \circ h = \mathrm{id}_Y$, þá er vörpunin $f : X \to Y$ átæk.

Sönnun: $h : Y \to X$ sé vörpun þannig að $f \circ h = \mathrm{id}_Y$. Gefið sé $y \in Y$. Látum $x = h(y)$. Þá fæst $f(x) = f(h(y)) = (f \circ h)(y) = \mathrm{id}_Y(y) = y$.

Skilgreining: Vörpun $f : A \to B$ er sögð vera *gagntæk* ef hún er bæði eintæk og átæk.

Ef $f : a \to B$ er gagntæk vörpun og $b \in B$ þá er samkvæmt skilgreiningunni til eitt og aðeins eitt $a \in A$ þannig að $f(a) = b$.

Skilgreining: $f : A \to B$ sé gagntæk vörpun. Vörpunin frá B til A, sem varpar sérhverju $b \in B$ í það stak $a \in A$ sem uppfyllir skilyrðið $f(a) = b$, heitir *andhverfa* f. Hún er táknuð með

$$f^{-1}$$

Setning 2.7: Fyrir sérhverja gagntæka vörpun $f : X \to Y$ gilda reglurnar:
(i) $f^{-1} \circ f = \mathrm{id}_X$
(ii) $f \circ f^{-1} = \mathrm{id}_Y$
Sönnun: (i): Ef $x \in X$ og $f(x) = y$ þá er $f^{-1}(y) = x$, svo að $(f^{-1} \circ f)(x) = f^{-1}(f(x)) = f^{-1}(y) = x = \mathrm{id}_X(x)$.
(ii): Ef $y \in Y$ og $x = f^{-1}(y)$ þá er $f(x) = y$, svo að $(f \circ f^{-1})(y) = f(f^{-1}(y)) = f(x) = y = \mathrm{id}_Y(y)$.

Setning 2.8: Gefin sé vörpun $f : X \to Y$. Ef til eru varpanir $g : Y \to X$ og $h : Y \to X$ þannig að $g \circ f = \mathrm{id}_X$ og $f \circ h = \mathrm{id}_Y$, þá er f gagntæk og $g = h = f^{-1}$.
Sönnun: Að f sé þá gagntæk leiðir strax af Setningum 2.5 og 2.6. Nú séu $g : Y \to X$ og $h : Y \to X$ varpanir þannig að $g \circ f = \mathrm{id}_X$ og $f \circ h = \mathrm{id}_Y$. Þá fæst $g = g \circ \mathrm{id}_Y = g \circ (f \circ f^{-1}) = (g \circ f) \circ f^{-1} = \mathrm{id}_X \circ f^{-1} = f^{-1}$ og $h = \mathrm{id}_X \circ h = (f^{-1} \circ f) \circ h = f^{-1} \circ (f \circ h) = f^{-1} \circ \mathrm{id}_Y = f^{-1}$.

Setning 2.9: Fyrir sérhverjar gagntækar varpanir $f : X \to Y$ og $g : Y \to Z$ gilda reglurnar:
(i) f^{-1} er gagntæk og $(f^{-1})^{-1} = f$
(ii) $g \circ f$ er gagntæk og $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$
Sönnun: Þetta eru afleiðingar af Setningu 2.8. (i) vegna þess að $f \circ f^{-1} = \mathrm{id}_Y$ og $f^{-1} \circ f = \mathrm{id}_X$ og (ii) vegna þess að $(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ (g \circ f)) = f^{-1} \circ ((g^{-1} \circ g) \circ f) = f^{-1} \circ (\mathrm{id}_Y \circ f) = f^{-1} \circ f = \mathrm{id}_X$ og $(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ (f^{-1} \circ g^{-1})) = g \circ ((f \circ f^{-1}) \circ g^{-1}) = g \circ (\mathrm{id}_Y \circ g^{-1}) = g \circ g^{-1} = \mathrm{id}_Z$.

Skilgreining: $f : A \to B$ sé vörpun. Ef $X \subseteq A$ þá heitir mengið

$$\{\, f(x) \,|\, x \in X \,\} := \{\, y \in B \,|\, \text{til er } x \in X \text{ með } f(x) = y \,\}$$

mynd X við f. Mengið $\{\, f(x) \,|\, x \in A \,\}$ heitir líka *myndmengi* f.

$f : A \to B$ sé vörpun. Ef $X \subseteq A$ þá er mynd X við f oftast táknuð með

$$f(X)$$

þótt það sé ekki nákvæmur ritháttur. Myndmengi f er oftast táknað með

$$\mathrm{Im}(f)$$

Setning 2.10: $f : A \to B$ sé vörpun. Fyrir sérhver hlutmengi X og Y í A gilda þá reglurnar:
(i) ef $X \subseteq Y$ þá $f(X) \subseteq f(Y)$
(ii) $f(X \cup Y) = f(X) \cup f(Y)$
(iii) $f(X \cap Y) \subseteq f(X) \cap f(Y)$
(iv) $f(X \setminus Y) \supseteq f(X) \setminus f(Y)$
Sönnun: Heimaverkefni.

Skilgreining: $f : A \to B$ sé vörpun. Ef $X \subseteq B$ þá heitir mengið

$$\{\, x \in A \mid f(x) \in X \,\}$$

frummynd X við f.

$f : A \to B$ sé vörpun. Ef $X \subseteq B$ þá er frummynd X við f oftast táknuð með

$$f^{-1}(X)$$

Athugið að ritháttur inn $f^{-1}(X)$ táknar ekki að f sé gagntæk. En ef $f : A \to B$ er gagntæk þá er frummynd X við f sama og mynd X við f^{-1}, svo að óhætt er að nota $f^{-1}(X)$ fyrir hvorttveggja.

Setning 2.11: $f : A \to B$ sé vörpun. Fyrir sérhver hlutmengi X og Y í B gilda þá reglurnar:
(i) ef $X \subseteq Y$ þá $f^{-1}(X) \subseteq f^{-1}(Y)$
(ii) $f^{-1}(X \cup Y) = f^{-1}(X) \cup f^{-1}(Y)$
(iii) $f^{-1}(X \cap Y) = f^{-1}(X) \cap f^{-1}(Y)$
(iv) $f^{-1}(X \setminus Y) = f^{-1}(X) \setminus f^{-1}(Y)$
Sönnun: Heimaverkefni.

Þegar við höfum rætt um varpanir þá höfum við yfirleitt talað um varpanir frá ákveðnum mengjum til ákveðinna mengja. Athugið þó að ef $f : A \to B$ er vörpun þá er mengið B ekki ákvarðað af f, samkvæmt þeirri skilgreiningu sem við höfum notað. Ef nefnilega C er eitthvert mengi þannig að $\mathrm{Im}(f) \subseteq C$, þá er f líka vörpun frá A til C. Þar af leiðir að þótt við höfum skilgreint

hvað það þýðir að vörpun $f : A \to B$ sé átæk, þá er ekki hægt að tala um það hvort vörpunin f sé átæk. En ef $f : A \to B$ er vörpun þá er mengið A ákvarðað af f.

Skilgreining: $f : A \to B$ sé vörpun og $C \subseteq A$. Þá er vörpunin frá C til B, sem varpar sérhverju $c \in C$ í $f(c)$, nefnd *einskorðun* f við C. Hún er táknuð með

$$f|_C$$

Setning 2.12: Ef A og B eru mengi þá er til mengi sem inniheldur allar varpanir frá A til B, en engin önnur stök.
Sönnun: Látum Ω vera mengi allra þeirra staka $\omega \in \mathcal{P}(\mathcal{P}(A \cup B))$ þannig að til séu $a \in A$ og $b \in B$ með $\omega = [a, b\rangle$. Þá er Ω greinilega mengi allra örva $[a, b\rangle$, þar sem $a \in A$ og $b \in B$. Við látum nú $\mathcal{F}$ vera mengi allra þeirra staka $f \in \mathcal{P}(\Omega)$ þannig að fyrir sérhvert $a \in A$ sé til eitt og aðeins eitt $b \in B$ með $[a, b\rangle \in f$. Þá er $\mathcal{F}$ greinilega mengi allra varpana frá A til B.

Mengi allra varpana frá mengi I til mengis A er oft táknað með

$$A^I$$

ekki sízt þegar stökin í I eru aðeins notuð til að auðkenna stökin í A. Þá er vörpun $x : I \to A$ einnig nefnd *fjölskylda* í A auðkennd með I, og fyrir $i \in I$ skrifað

$$x_i$$

í stað $x(i)$. Fjölskylda x auðkennd með I er líka táknuð með

$$(x_i)_{i \in I}$$

Ef $(X_i)_{i \in I}$ er fjölskylda af mengjum, þ.e. sérhvert X_i er mengi, þá er sammengi mengjanna í $\{ X_i \mid i \in I \}$ táknað með

$$\bigcup_{i \in I} X_i$$

Ef $I \neq \emptyset$ þá er sniðmengi mengjanna í $\{ X_i \mid i \in I \}$ táknað með

$$\bigcap_{i \in I} X_i$$

Skilgreining: $(X_i)_{i \in I}$ sé fjölskylda af mengjum. Mengi allra fjölskyldna $(x_i)_{i \in I}$ þannig að $x_i \in X_i$ fyrir sérhvert $i \in I$ er þá nefnt *kartesískt margfeldi* mengjanna X_i, $i \in I$.

Athugið að mengið í skilgreiningu þessari er til. Því er hægt að lýsa sem hlutmengi í mengi allra varpana frá I til sammengisins $\bigcup_{i\in I} X_i$.

Ef $(X_i)_{i\in I}$ er fjölskylda af mengjum þá er kartesískt margfeldi mengjanna X_i, $i \in I$, venjulega táknað með

$$\prod_{i\in I} X_i$$

Og að lokum fyrsta dæmið um notkun frumsetningarinnar um val:

Setning 2.13: $(X_i)_{i\in I}$ sé fjölskylda af mengjum þannig að $X_i \neq \emptyset$ fyrir sérhvert $i \in I$. Þá er líka $\prod_{i\in I} X_i \neq \emptyset$.
Sönnun: Við látum $M = \bigcup_{i\in I} X_i$ og látum R vera mengi allra örva $[i, m\rangle$, þar sem $i \in I$ og $m \in X_i$. (R er hlutmengi í mengi allra örva $[i, m\rangle$ þar sem $i \in I$ og $m \in M$.) Fyrir sérhvert $i \in I$ látum við svo R_i vera mengi allra örva $[i, m\rangle$ þar sem $m \in X_i$. Þá er R greinilega sammengi mengjanna R_i, $i \in I$. Auk þess er R_i ekki tómt, því að X_i er ekki tómt, en ef $i \neq j$ þá er sniðmengið $R_i \cap R_j$ augljóslega tómt. Svo að mengið $\{ R_i \mid i \in I \}$ er deildamengi af R. Samkvæmt frumsetningunni um val er því til hlutmengi x í R sem inniheldur eitt og aðeins eitt stak úr sérhverju R_i, $i \in I$. En það þýðir að x sé vörpun frá I til M þannig að $x(i) \in X_i$ fyrir sérhvert $i \in I$, þ.e.a.s. að x sé stak í $\prod_{i\in I} X_i$.

3 Náttúrlegar tölur

Frumsetning: Til er mengi N, stak $e \in N$ og vörpun $s : N \to N$ þannig að:
(1) $e \notin s(N)$
(2) s er eintæk
(3) ef $Q \subseteq N$ þannig að $e \in Q$ og $s(Q) \subseteq Q$ þá $Q = N$

Setning 3.1: Gefið sé mengi N, stak $e \in N$ og vörpun $s : N \to N$ þannig að:
(1) $e \notin s(N)$
(2) s er eintæk
(3) ef $Q \subseteq N$ þannig að $e \in Q$ og $s(Q) \subseteq Q$ þá $Q = N$
Fyrir sérhvert mengi X, stak $a \in X$ og vörpun $f : X \to X$ er þá til ein og aðeins ein vörpun $\varphi : N \to X$ þannig að $\varphi(e) = a$ og $\varphi(s(n)) = f(\varphi(n))$ fyrir öll $n \in N$.
Sönnun: R sé mengi allra örva $[n, x\rangle$ þar sem $n \in N$ og $x \in X$. Við skulum segja að hlutmengi α í R sé *lokað* ef
(i) $[e, a\rangle \in \alpha$
(ii) ef $[n, x\rangle \in \alpha$ þá $[s(n), f(x)\rangle \in \alpha$
Þar sem R sjálft er lokað þá er til lokað hlutmengi í R. Við getum því skilgreint mengið φ sem sniðmengi allra lokaðra hlutmengja í R. Auðvelt er að sjá að φ er þá lokað hlutmengi í R og samkvæmt skilgreiningu á φ þá er φ hlutmengi í sérhverju lokuðu hlutmengi í R. Sér í lagi fæst að ef $[m, y\rangle \in \varphi$ þá er $\varphi \setminus \{[m, y\rangle\}$ ekki lokað hlutmengi í R, sem þýðir að $[m, y\rangle = [e, a\rangle$ eða þá að til sé $[p, z\rangle \in \varphi$ með $s(p) = m$ og $f(z) = y$. Þar sem $e \notin s(N)$ þá getur ekki hvorttveggja gilt, svo að við fáum
(iii) ef $[e, y\rangle \in \varphi$ þá $y = a$
(iv_0) ef $[s(n), y\rangle \in \varphi$ þá er til $[p, z\rangle \in \varphi$ með $s(n) = s(p)$ og $y = f(z)$
En s er eintæk, svo að $n = p$ ef $s(n) = s(p)$. Því fæst
(iv) ef $[s(n), y\rangle \in \varphi$ þá er til $z \in X$ með $[n, z\rangle \in \varphi$ og $y = f(z)$
Við látum nú Q vera mengi allra þeirra $n \in N$ þannig að til sé eitt og aðeins eitt $x \in X$ með $[n, x\rangle \in \varphi$. Af (i) og (iii) leiðir þá að $e \in Q$. Nú sé $n \in Q$, segjum $[n, x\rangle \in \varphi$. Af (ii) leiðir þá að $[s(n), f(x)\rangle \in \varphi$. Ef $[s(n), y\rangle \in \varphi$ þá er samkvæmt (iv) til $z \in X$ með $[n, z\rangle \in \varphi$ og $y = f(z)$. En vegna $n \in Q$ þá hlýtur $z = x$, svo að $y = f(x)$. Við höfum því líka $s(n) \in Q$. Þetta sýnir að $s(Q) \subseteq Q$. Af (3) leiðir þar með að $Q = N$. Það þýðir að fyrir sérhvert $n \in N$ er til eitt og aðeins eitt $x \in X$ með $[n, x\rangle \in \varphi$. Því er φ vörpun frá N til X og af (i) og (ii) leiðir að $\varphi(e) = a$ og $\varphi(s(n)) = f(\varphi(n))$ fyrir öll $n \in N$.

Nú sé $\chi : N \to X$ einhver vörpun þannig að $\chi(e) = a$ og $\chi(s(n)) = f(\chi(n))$ fyrir öll $n \in N$. Við látum Q vera mengi allra þeirra $n \in N$ þannig

að $\chi(n) = \varphi(n)$. Vegna $\chi(e) = a = \varphi(e)$ er $e \in Q$. Ef $n \in Q$ þá fæst $\chi(s(n)) = f(\chi(n)) = f(\varphi(n)) = \varphi(s(n))$, svo að $s(n) \in Q$. Þetta sýnir að $s(Q) \subseteq Q$. Af (3) leiðir því að $Q = N$, þ.e.a.s. $\chi(n) = \varphi(n)$ fyrir öll $n \in N$. En það þýðir að $\chi = \varphi$.

Setning 3.2: Gefið sé mengi N, stak $e \in N$ og vörpun $s : N \to N$ þannig að:
(1) $e \notin s(N)$
(2) s er eintæk
(3) ef $Q \subseteq N$ þannig að $e \in Q$ og $s(Q) \subseteq Q$ þá $Q = N$
og mengi N', stak $e' \in N'$ og vörpun $s' : N' \to N'$ þannig að:
(1′) $e' \notin s'(N')$
(2′) s' er eintæk
(3′) ef $Q' \subseteq N'$ þannig að $e' \in Q'$ og $s'(Q') \subseteq Q'$ þá $Q' = N'$
Þá er til gagntæk vörpun $\varphi : N \to N'$ þannig að $\varphi(e) = e'$ og $\varphi(s(n)) = s'(\varphi(n))$ fyrir öll $n \in N$.
Sönnun: Samkvæmt Setningu 3.1 er til vörpun $\varphi : N \to N'$ þannig að $\varphi(e) = e'$ og $\varphi(s(n)) = s'(\varphi(n))$ fyrir öll $n \in N$, og sömuleiðis vörpun $\varphi' : N' \to N$ þannig að $\varphi'(e') = e$ og $\varphi'(s'(n')) = s(\varphi'(n'))$ fyrir öll $n' \in N'$. Þá fæst $(\varphi' \circ \varphi)(e) = \varphi'(\varphi(e)) = \varphi'(e') = e$ og $(\varphi' \circ \varphi)(s(n)) = \varphi'(\varphi(s(n))) = \varphi'(s'(\varphi(n))) = s(\varphi'(\varphi(n))) = s((\varphi' \circ \varphi)(n))$ fyrir öll $n \in N$. Einnig er $\mathrm{id}_N(e) = e$ og $\mathrm{id}_N(s(n)) = s(\mathrm{id}_N(n))$ fyrir öll $n \in N$. Af Setningu 3.1 leiðir því að $\varphi' \circ \varphi = \mathrm{id}_N$. Á sama hátt fæst að $\varphi \circ \varphi' = \mathrm{id}_{N'}$. Af þessu sést að φ er gagntæk.

Við veljum okkur nú eitthvert mengi N ásamt staki $e \in N$ og vörpun $s : N \to N$ þannig að
(1) $e \notin s(N)$
(2) s er eintæk
(3) ef $Q \subseteq N$ þannig að $e \in Q$ og $s(Q) \subseteq Q$ þá $Q = N$
Samkvæmt Setningu 3.2 er sama hvernig við veljum þetta mengi, stak og vörpun. Við nefnum stökin í N *náttúrulegar tölur* og notum hér eftir táknið $\mathbf{N}$ í stað N. Ef $n \in \mathbf{N}$ þá skrifum við (í bili) n^+ í stað $s(n)$ og köllum n^+ *næstu* náttúrulegu tölu *á eftir* n. Við segjum líka að n sé *næst á undan* n^+. Stakið e táknum við með 1 (og stakið 1^+ með 2, stakið 2^+ með 3, o.s.frv.). Eiginleikum náttúrulegu talnanna er þá lýst með eftirfarandi:
(P1:) 1 er náttúruleg tala.
(P2:) Næst á eftir sérhverri náttúrulegri tölu n kemur ákveðin náttúruleg tala n^+.
(P3:) Engin náttúruleg tala er næst á undan 1.

(P4:) Næst á undan sérhverri náttúrulegri tölu er í mesta lagi ein náttúruleg tala.

(P5:) Ef Q er mengi af náttúrulegum tölum þannig að
(i) Q inniheldur 1
(ii) ef Q inniheldur k þá líka k^+
þá inniheldur Q sérhverja náttúrulega tölu.

Það má líta á P1 - P5 sem kerfi frumsetninga fyrir náttúrulegu tölurnar. (Það er kennt við ítalska stærðfræðinginn G. Peano.) Eiginleikinn P5 er nefndur þrepunarlögmálið. Notkun þess byggist aðallega á tveim setningum, setningunni um sönnun með þrepun og setningunni um skilgreiningu með þrepun.

Sönnun með þrepun: Fyrir sérhverja náttúrulega tölu n sé gefin fullyrðing $p(n)$ þannig að:
(i) $p(1)$ er sönn
(ii) ef $k \in \mathbf{N}$ og $p(k)$ er sönn þá er $p(k^+)$ líka sönn
Þá er $p(n)$ sönn fyrir sérhverja náttúrulega tölu n.
Sönnun: Þetta sést með því að setja $Q = \{\, n \in \mathbf{N} \mid p(n) \,\}$ og nota P5.

Sem dæmi um sönnun með þrepun skulum við taka setninguna:

Setning 3.3: Fyrir sérhvert $n \in \mathbf{N}$ gildir $n^+ \neq n$.
Sönnun með þrepun (yfir n): Við athugum fullyrðinguna $n^+ \neq n$. Samkvæmt P3 gildir $1^+ \neq 1$, svo að hún er sönn fyrir $n = 1$. Ef hún er sönn fyrir $n = k$, þ.e.a.s. ef $k^+ \neq k$, þá leiðir af P4 að $(k^+)^+ \neq k^+$, sem sagt að fullyrðingin er líka sönn fyrir $n = k^+$. Samkvæmt setningunni um sönnun með þrepun er fullyrðingin þar með sönn fyrir sérhverja náttúrlega tölu n.

Við sjáum að sönnun setningar með þrepun yfir n skiptist í tvennt. Í fyrsta lagi þarf að sanna setninguna fyrir $n = 1$. Þessi hluti sönnunarinnar nefnist þrepunarbyrjun. Í öðru lagi þarf að sanna að ef setningin er rétt fyrir $n = k$, þá sé hún líka rétt fyrir $n = k^+$. Þessi hluti sönnunarinnar er nefndur þrepunarskref. Í þrepunarskrefinu er gefið að setningin sé rétt fyrir $n = k$. Þessi forsenda heitir þrepunarforsenda. Til einföldunar munum við hér venjulega einkenna þrepunarbyrjunina með „$n = 1$“ og þrepunarskrefið með „$n = k \to n = k^+$“.

Skilgreining með þrepun: Gefið sé mengi X, stak $a \in X$ og vörpun $f : X \to X$. Þá er til ein og aðeins ein vörpun $\varphi : \mathbf{N} \to X$ þannig að:
(i) $\varphi(1) = a$
(ii) ef $k \in \mathbf{N}$ þá $\varphi(k^+) = f(\varphi(k))$
Sönnun: Þetta er Setning 3.1.

Til eru almennari útgáfur af setningunni um skilgreiningu með þrepun. Hér kemur ein:

Setning 3.4: Gefið sé mengi X, stak $a \in X$ og fjölskylda $(f_n)_{n\in\mathbf{N}}$ af vörpunum $f_n : X \to X$. Þá er til ein og aðeins ein vörpun $\varphi : \mathbf{N} \to X$ þannig að:
(i) $\varphi(1) = a$
(ii) ef $k \in \mathbf{N}$ þá $\varphi(k^+) = f_k(\varphi(k))$
Sönnun: Látum Y vera mengi allra örva $[n, x\rangle$ þar sem $n \in \mathbf{N}$ og $x \in X$ og skilgreinum vörpunina $g : Y \to Y$ með því að setja $g([n, x\rangle) = [n^+, f_n(x)\rangle$ fyrir sérhver $x \in \mathbf{N}$ og $x \in X$. Samkvæmt setningunni um skilgreiningu með þrepun er til vörpun $\chi : \mathbf{N} \to Y$ þannig að $\chi(1) = [1, a\rangle$ og $\chi(k^+) = g(\chi(k))$ fyrir öll $k \in \mathbf{N}$. Fyrir sérhvert $n \in \mathbf{N}$ skrifum við $\chi(n) = [\sigma(n), \varphi(n)\rangle$. Skilyrðið $\chi(1) = [1, a\rangle$ þýðir þá að $\sigma(1) = 1$ og $\varphi(1) = a$ og skilyrðið $\chi(k^+) = g(\chi(k))$ að $\sigma(k^+) = \sigma(k)^+$ og $\varphi(k^+) = f_{\sigma(k)}(\varphi(k))$. Af þessu leiðir fyrst að σ er hlutlausa vörpunin á $\mathbf{N}$ og svo að vörpunin φ uppfyllir skilyrðin í setningunni.

Að φ er ótvírætt ákvörðuð fæst með einfaldri þrepun.

Af Setningu 3.4 leiðir að til er ein og aðeins ein vörpun $\varphi : \mathbf{N} \to \mathcal{P}(\mathbf{N})$ þannig að $\varphi(1) = \emptyset$ og $\varphi(n^+) = \varphi(n) \cup \{n\}$ fyrir öll $n \in \mathbf{N}$. Þetta sést með því að skilgreina fyrir sérhvert $n \in \mathbf{N}$ vörpunina $f_n : \mathcal{P}(\mathbf{N}) \to \mathcal{P}(\mathbf{N})$ með því að setja $f_n(A) = A \cup \{n\}$ fyrir sérhvert $A \subseteq \mathbf{N}$.

Skilgreining: $\varphi : \mathbf{N} \to \mathcal{P}(\mathbf{N})$ sé vörpunin þannig að $\varphi(1) = \emptyset$ og $\varphi(n^+) = \varphi(n) \cup \{n\}$ fyrir öll $n \in \mathbf{N}$. Fyrir sérhver $m, n \in \mathbf{N}$ segjum við þá að m sé *minna en* n (og að n sé *stærra en* m) ef $m \in \varphi(n)$. Að m sé minna en n er táknað með

$$m < n$$

Þessa skilgreiningu á „$<$“ má orða þannig að fyrir öll $m, n \in \mathbf{N}$ gildi:
R1: ekki $m < 1$
R2: $m < n^+$ þá og því aðeins að $m < n$ eða $m = n$

Setning 3.5: Fyrir öll $m, n, p \in \mathbf{N}$ gildir reglan
ef $m < n$ og $n < p$ þá $m < p$
Sönnun með þrepun yfir p: „$p = 1$“: Augljóst, því að samkvæmt R1 getur forsendan aldrei staðist. „$p = k \to p = k^+$“: Gefið sé $m < n$ og $n < k^+$. Að $n < k^+$ þýðir samkvæmt R2 að $n < k$ eða $n = k$. Ef $n < k$ þá leiðir af þrepunarforsendunni að $m < k$. Ef $n = k$ þá leiðir af $m < n$ að $m < k$. Í báðum tilfellum fæst því að $m < k$ og samkvæmt R2 þar með líka $m < k^+$.

Setning 3.6: Fyrir öll $m, n \in \mathbf{N}$ gildir reglan
ef $m < n$ þá ekki $n < m$
Sönnun með þrepun yfir m: „$m = 1$“: Augljóst samkvæmt R1. „$m = k \to m = k^+$“: Gefið sé $k^+ < n$. Samkvæmt R2 gildir $k < k^+$. Af Setningu 3.5 leiðir því að $k < n$. Samkvæmt þrepunarforsendu gildir því ekki $n < k$. Ennfremur fæst af $k < n$ að $n \neq k$, því að samkvæmt þrepunarforsendu myndi af $k < k$ leiða að ekki $k < k$. Því gildir hvorki $n < k$ né $n = k$. En það þýðir samkvæmt R2 að ekki $n < k^+$.

Ef $m, n \in \mathbf{N}$ þá táknum við það að $m < n$ eða $m = n$ með

$$m \leq n$$

Ekki getur gilt að bæði $m < n$ og $m = n$, því að þá fengist $m < m$, sem er í mótsögn við Setningu 3.6. Af þessu leiðir að fyrir sérhver $m, n \in \mathbf{N}$ gildir $m < n$ þá og því aðeins að $m \leq n$ og $m \neq n$.

Setning 3.7: Fyrir öll $m, n, p \in \mathbf{N}$ gilda reglurnar:
(i) $m \leq m$
(ii) ef $m \leq n$ og $n \leq m$ þá $m = n$
(iii) ef $m \leq n$ og $n \leq p$ þá $m \leq p$
Sönnun: (i) er augljóst.

(ii): Gefið sé $m \leq n$ og $n \leq m$. Ef $m \neq n$ þá væri $m < n$ og $n < m$. En það er ómögulegt samkvæmt Setningu 3.6.

(iii): Gefið sé $m \leq n$ og $n \leq p$. Ef $m = n$ þá leiðir af $n \leq p$ að $m \leq p$. Ef $n = p$ þá leiðir af $m \leq n$ að $m \leq p$. En ef $m \neq n$ og $n \neq p$ þá hlýtur $m < n$ og $n < p$. Af Setningu 3.5 leiðir þá $m < p$ og þar með $m \leq p$.

Vegna R1 og R2 má orða skilgreiningu okkar á „$\leq$“ þannig að fyrir öll $m, n \in \mathbf{N}$ gildi:
R1′: $m \leq 1$ þá og því aðeins að $m = 1$
R2′: $m \leq n^+$ þá og því aðeins að $m \leq n$ eða $m = n^+$
Eftirfarandi setning segir að hægt hefði verið að skilgreina „$\leq$“ á annan hátt.

Setning 3.8: Fyrir öll $m, n, \in \mathbf{N}$ gildir:
(i) $1 \leq n$
(ii) $m^+ \leq n$ þá og því aðeins að $m \leq n$ og $m \neq n$
Sönnun: (i) með þrepun yfir n: „$n = 1$“: Augljóst. „$n = k \to n = k^+$“: Samkvæmt þrepunarforsendu er $1 \leq k$. Samkvæmt R2′ er $k \leq k^+$. Af Setningu 3.7 (iii) leiðir því að $1 \leq k^+$.

(ii) með þrepun yfir n: „$n = 1$“: Vegna R1′ og P3 getur aldrei gilt $m^+ \leq 1$ og vegna R1′ getur heldur ekki gilt $m \leq 1$ og $m \neq 1$. „$n = k \to n = k^+$“:

Samkvæmt R2′ er $m^+ \leq k^+$ þá og því aðeins að $m^+ \leq k$ eða $m^+ = k^+$. Samkvæmt þrepunarforsendu er $m^+ \leq k$ þá og því aðeins að $m \leq k$ og $m \neq k$. Ennfremur leiðir af P4 að $m^+ = k^+$ þá og því aðeins að $m = k$. Af þessu sést að $m^+ \leq k^+$ þá og því aðeins að $m \leq k$. Samkvæmt R2 gildir hinsvegar að $m \leq k$ þá og því aðeins að $m < k^+$. En samkvæmt athugasemd á undan setningu 3.7 gildir $m < k^+$ þá og því aðeins að $m \leq k^+$ og $m \neq k^+$.

Skilgreining: Q sé hlutmengi í $\mathbf{N}$. Stak $m \in Q$ er þá sagt vera *minnsta stak* í Q ef fyrir öll $x \in Q$ gildir $m \leq x$.

Af Setningu 3.7 (ii) leiðir augljóslega að hlutmengi Q í $\mathbf{N}$ getur í mesta lagi haft eitt minnsta stak. Tóma mengið er hinsvegar dæmi um hlutmengi í $\mathbf{N}$ sem hefur ekkert minnsta stak. En það er líka eina dæmið:

Setning 3.9: Sérhvert ekki tómt hlutmengi í $\mathbf{N}$ hefur minnsta stak.
Sönnun: Það nægir greinilega að sanna að fyrir öll $n \in \mathbf{N}$ gildi:
Ef $Q \subseteq \mathbf{N}$ og $n \in Q$ þá hefur Q minnsta stak.
Þetta sönnum við með þrepun yfir n. „$n = 1$“ leiðir af Setningu 3.8 (i). „$n = k \rightarrow n = k^+$“: Gefið sé $Q \subseteq \mathbf{N}$ þannig að $k^+ \in Q$. Við setjum $R = Q \cup \{k\}$. Þá er $k \in R$, svo að R hefur minnsta stak m samkvæmt þrepunarforsendu. Ef $m \in Q$ þá er m greinilega líka minnsta stak í Q. Ef $m \notin Q$ þá hlýtur $m = k$ og $k \notin Q$. Því fæst að fyrir öll $x \in Q$ gildir $k \leq x$ og $k \neq x$. En samkvæmt Setningu 3.8 (ii) þá þýðir það að fyrir öll $x \in Q$ gildir $k^+ \leq x$. Vegna $k^+ \in Q$ þá er k^+ þar með minnsta stak í Q.

Setning 3.10: Fyrir öll $m, n \in \mathbf{N}$ gildir reglan
$m \leq n$ eða $n \leq m$
Sönnun: Setjum $Q = \{m, n\}$. Samkvæmt Setningu 3.9 hefur Q þá minnsta stak p. Ef $p = m$ þá fæst $m \leq n$. Ef $p = n$ þá fæst $n \leq m$.

Setning 3.11: Ef $m, n \in \mathbf{N}$ þá gildir eitt og aðeins eitt af þrennu:
(i) $m < n$
(ii) $m = n$
(iii) $n < m$
Sönnun: Af Setningu 3.10 leiðir að $m < n$, $m = n$ eða $n < m$. Samkvæmt Setningu 3.6 getur ekki gilt $m < n$ og $n < m$. En af $m < n$ og $m = n$ leiddi að $m < m$ og samkvæmt Setningu 3.6 þá einnig að ekki $m < m$, þ.e. mótsögn. Á sama hátt fengist mótsögn af $n < m$ og $m = n$.

Ef $n \in \mathbf{N}$ þá setjum við

$$[\![1, n]\!] = \{\, k \in \mathbf{N} \mid k \leq n \,\}$$

Mengin $[\![1,n]\!]$ eru mikið notuð sem auðkennamengi. Þegar það er gert þá er táknmálið oftast einfaldað. Til dæmis er fjölskylda $(x_i)_{i\in[\![1,n]\!]}$ oftast táknuð með $(x_i)_{i=1,\ldots,n}$ eða $(x_1,\ldots,x_n)$. Fjölskylda $(x_i)_{i\in[\![1,2]\!]}$ er því t.d. táknuð með (x_1,x_2) og er gjarnan nefnd *(röðuð) tvennd*.

Ef X er mengi þá er skrifað X^n í stað $X^{[\![1,n]\!]}$. Og ef $(X_i)_{i\in[\![1,n]\!]}$ er fjölskylda af mengjum þá er oftast skrifað $\prod_{i=1}^{n} X_i$ í stað $\prod_{i\in[\![1,n]\!]} X_i$. Svipað er gert fyrir sammengi og sniðmengi. Auk þess er í stað $\prod_{i=1}^{2} X_i$ gjarnan skrifað $X_1\times X_2$, í stað $\prod_{i=1}^{3} X_i$ gjarnan skrifað $X_1\times X_2\times X_3$, o.s.frv. Athugið að með þessum rithætti er til dæmis

$$X_1\times X_2=\{\,(x_1,x_2)\,|\,x_1\in X_1 \text{ og } x_2\in X_2\,\}$$

Setning 3.12: Gefin séu $m,n\in\mathbf{N}$. Ef til er gagntæk vörpun $f:[\![1,m]\!]\to[\![1,n]\!]$ þá er $m=n$.
Sönnun: Heimaverkefni.

M sé mengi. Gerum ráð fyrir að $m,n\in\mathbf{N}$ þannig að til séu gagntækar varpanir $f:[\![1,m]\!]\to M$ og $g:[\![1,n]\!]\to M$. Þá er $g^{-1}\circ f:[\![1,m]\!]\to[\![1,n]\!]$ gagntæk vörpun, svo að $m=n$ samkvæmt Setningu 3.12. Við sjáum því að til er í mesta lagi eitt $m\in\mathbf{N}$ þannig að til sé gagntæk vörpun $f:[\![1,m]\!]\to M$.

Skilgreining: M sé mengi. Ef til er $m\in\mathbf{N}$ og gagntæk vörpun $f:[\![1,m]\!]\to M$ þá er sagt að M sé *endanlegt* og talan m er nefnd *fjöldi* stakanna í M. Tóma mengið er einnig sagt vera endanlegt.

4 Venzl

Skilgreining: *Venzl* í mengi M er mengi af örvum $[a, b\rangle$, þar sem $a, b \in M$. Ef $\propto$ eru venzl í M þá er í stað $[a, b\rangle \in \propto$ skrifað

$$a \propto b$$

Í reynd er einstökum venzlum ekki lýst með því að gefa upp mengi af örvum. Til þess að lýsa venzlum $\propto$ í mengi M er nefnilega greinilega nóg að skilgreina vel fyrir hvaða stök a og b í M gildi að $a \propto b$.

Skilgreining: Venzl $\prec$ í mengi M eru sögð vera *ströng röðun* í M ef eftirfarandi reglur gilda fyrir sérhver $x, y, z \in M$

ef $x \prec y$ þá ekki $y \prec x$
ef $x \prec y$ og $y \prec z$ þá $x \prec z$

Fyrri reglan í skilgreiningunni segir að venzlin $\prec$ séu *andsamhverf* en sú seinni að þau séu *gegnvirk*.

Setning 4.1: Ef $\prec$ er ströng röðun í mengi M þá gildir fyrir sérhvert $x \in M$ reglan

ekki $x \prec x$

Sönnun: Ef $x \prec x$ þá ekki $x \prec x$ vegna andsamhverfninnar. En það er mótsögn.

Setningin segir að venzlin $\prec$ séu *andspegilvirk*.

Skilgreining: Venzl $\preceq$ í mengi M eru sögð vera *röðun* í M ef eftirfarandi reglur gilda fyrir sérhver $x, y, z \in M$

$x \preceq x$
ef $x \preceq y$ og $y \preceq x$ þá $x = y$
ef $x \preceq y$ og $y \preceq z$ þá $x \preceq z$

Fyrsta reglan í þessari skilgreiningu segir að venzlin $\preceq$ séu *spegilvirk*, sú næsta að þau séu *veikt andsamhverf*. Þriðja reglan er svo gegnvirknin.

Ef $\prec$ er ströng röðun í mengi M þá getum við skilgreint venzl $\preceq$ í M með því að setja

$x \preceq y$ þá og því aðeins að $x \prec y$ eða $x = y$

fyrir sérhver $x, y \in M$. Eins og í sönnun Setningar 3.7 sést að $\preceq$ er þá röðun í M. Ef hinsvegar er gefin röðun $\preceq$ í M þá má skilgreina stranga röðun $\prec$ í M með því að setja

$x \prec y$ þá og því aðeins að $x \preceq y$ og $x \neq y$
fyrir sérhver $x, y \in M$. Auðvelt er að sjá að þetta gefur gagnkvæma samsvörun á milli strangra raðana í M og raðana í M.

Skilgreining: Röðun $\preceq$ í mengi M er sögð vera *línuleg* ef fyrir sérhver $x, y \in M$ gildir
$x \preceq y$ eða $y \preceq x$

Ef $\prec$ er ströng röðun í mengi M þá er tilheyrandi röðun í M línuleg þá og því aðeins að fyrir sérhver $x, y \in M$ gildi
$x \prec y$ eða $x = y$ eða $y \prec x$
Auk þess er, eins og í sönnun Setningar 3.11, auðvelt að sjá að af þessu þrennu gildir í mesta lagi eitt.

Skilgreining: $\preceq$ sé röðun í mengi M og $\prec$ sé tilheyrandi ströng röðun í M. Stak $a \in M$ heitir þá *lágstak* í M með tilliti til $\preceq$ ef ekki er til $x \in M$ með $x \prec a$. Stakið a heitir minnsta stak í M með tilliti til $\preceq$ ef meira að segja $a \preceq x$ fyrir öll $x \in M$.

Ljóst er að mengi M getur í mesta lagi haft eitt minnsta stak með tilliti til röðunar $\preceq$ í M. Hinsvegar gæti M haft mörg lágstök tilliti til $\preceq$.

Ef $\preceq$ er röðun í mengi M og Q er hlutmengi í M þá fáum við röðun í Q með því að einskorða okkur við stökin í Q. Við getum því talað um lágstak í Q með tilliti til $\preceq$ og minnsta stak í Q með tilliti til $\preceq$. En hér kemur afstætt hugtak:

Skilgreining: $\preceq$ sé röðun í mengi M. Hlutmengi Q í M er þá sagt vera *takmarkað að neðan* í M með tilliti til $\preceq$ ef til er $c \in M$ þannig að $c \preceq x$ fyrir sérhvert $x \in Q$. Sérhvert slíkt c er þá kallað *neðri mörk* fyrir Q í M með tilliti til $\preceq$.

Eftirfarandi setning um raðanir í mengjum er mikilvægt hjálpartæki í mörgum greinum stærðfræðinnar.

Lemma Zorns: $\preceq$ sé röðun í mengi M þannig að sérhvert hlutmengi í M, sem er línulega raðað með tilliti til $\preceq$, sé takmarkað að neðan í M með tilliti til $\preceq$. Þá er til lágstak í M með tilliti til $\preceq$.
Sönnun sleppum við hér.

Samsvarandi hugtökunum „lágstak“, „minnsta stak“, „neðri mörk“ og „takmarkað að neðan“ má að sjálfsögðu skilgreina hugtökin „*hástak*“, „*stærsta*

stak“, „*efri mörk*“ og „*takmarkað að ofan*“. Reyndar er lemma Zorns venjulega orðað með síðar nefndu hugtökunum.

Skilgreining: Venzl $\sim$ í mengi M eru sögð vera *jafngildisvenzl* í M ef eftirfarandi reglur gilda fyrir sérhver $x, y, z \in M$

$x \sim x$
ef $x \sim y$ þá $y \sim x$
ef $x \sim y$ og $y \sim z$ þá $x \sim z$

Önnur reglan í skilgreiningu þessari segir að venzlin $\sim$ séu *samhverf*. Hinar tvær eru spegilvirknin og gegnvirknin.

Skilgreining: $\sim$ séu jafngildisvenzl í mengi M. Ef $a \in M$ þá er mengið $\{\, x \in M \,|\, x \sim a \,\}$ kallað *jafngildisflokkur* a með tilliti til $\sim$. Ef $\widetilde{a}$ táknar jafngildisflokk $a \in M$ með tilliti til $\sim$ þá er mengið $\{\, \widetilde{a} \,|\, a \in M \,\}$ táknað með

$$M/\!\sim$$

Vörpunin frá M yfir í $M/\!\sim$, sem varpar sérhverju $a \in M$ í $\widetilde{a}$, heitir *náttúrulega ofanvarpið* frá M á $M/\!\sim$.

Ljóst er að ef $\sim$ eru jafngildisvenzl í mengi M þá er náttúrulega ofanvarpið frá M á $M/\!\sim$ átækt.

Setning 4.2: Ef $\sim$ eru jafngildisvenzl í mengi M og $\widetilde{a}$ táknar jafngildisflokk $a \in M$ með tilliti til $\sim$ þá gilda fyrir sérhver $a, b \in M$ reglurnar

(i) $a \in \widetilde{a}$
(ii) $a \sim b$ þá og því aðeins að $\widetilde{a} = \widetilde{b}$
(iii) ef $\widetilde{a} \neq \widetilde{b}$ þá $\widetilde{a} \cap \widetilde{b} = \emptyset$

Sönnun: (i) er augljós afleiðing af spegilvirkninni.

(ii): Gerum fyrst ráð fyrir að $a \sim b$. Gefið sé $x \in \widetilde{a}$, svo að $x \sim a$. Af gegnvirkninni leiðir þá að $x \sim b$, svo að $x \in \widetilde{b}$. Þetta sýnir að $\widetilde{a} \subseteq \widetilde{b}$. Vegna spegilvirkninnar er líka $b \sim a$ og því fæst $\widetilde{a} \subseteq \widetilde{b}$ á sama hátt. Svo að $\widetilde{a} = \widetilde{b}$. Gerum þá ráð fyrir að $\widetilde{a} = \widetilde{b}$. Samkvæmt lið (i) fæst þá að $a \in \widetilde{b}$, það er að $a \sim b$.

(iii): Gerum ráð fyrir að $\widetilde{a} \cap \widetilde{b} \neq \emptyset$. Þá er til $c \in \widetilde{a} \cap \widetilde{b}$, þ.e.a.s. $c \in M$ þannig að $c \sim a$ og $c \sim b$. Af lið (ii) fæst þá að $\widetilde{c} = \widetilde{a}$ og $\widetilde{c} = \widetilde{b}$, þar af leiðandi $\widetilde{a} = \widetilde{b}$.

Ef $\sim$ eru jafngildisvenzl í mengi M þá leiðir af liðum (i) og (iii) í Setningu 4.2 að $M/\!\sim$ er deildamengi af M. Auðvelt er að sjá að þetta gefur gagnkvæma samsvörun á milli jafngildisvenzla í M og deildamengja af M.

Ef $f : M \to N$ er vörpun þá fást jafngildisvenzl $\sim$ í M með því að setja

$x \sim y$ þá og því aðeins að $f(x) = f(y)$

fyrir sérhver $x, y \in M$. En það má líka lýsa sérhverjum jafngildisvenzlum í M á þennan hátt. Ef nefnilega $\sim$ eru jafngildisvenzl í M og $\pi : M \to M/\!\sim$ er náttúrulega ofanvarpið þá segir liður (ii) í Setningu 4.2 að $x \sim y$ þá og því aðeins að $\pi(x) = \pi(y)$.

Setning 4.3: $\sim$ séu jafngildisvenzl í mengi M og $f : M \to N$ vörpun þannig að fyrir sérhver $x, y \in M$ gildi

ef $x \sim y$ þá $f(x) = f(y)$

Þá er til ein og aðeins ein vörpun $\widetilde{f} : M/\!\sim \to N$ þannig að fyrir sérhvert $x \in M$ gildi

$\widetilde{f}(\widetilde{x}) = f(x)$

þar sem $\widetilde{x}$ táknar jafngildisflokk x með tilliti til $\sim$.

Sönnun: Ef $\xi \in M/\!\sim$ þá er, samkvæmt skilgreiningu á $M/\!\sim$, til $x \in M$ með $\xi = \widetilde{x}$. Af þessu sést að ekki getur verið til nema ein slík vörpun $\widetilde{f}$. Að hægt sé að skilgreina vörpun $\widetilde{f} : M/\!\sim \to N$ með því að setja $\widetilde{f}(\xi) = f(x)$ ef $\xi = \widetilde{x}$ sést af því að til er slíkt x og af því að ef bæði $\xi = \widetilde{x_1}$ og $\xi = \widetilde{x_2}$ þá fæst af Setningu 4.2 (ii) að $x_1 \sim x_2$ og þar með $f(x_1) = f(x_2)$ samkvæmt forsendu.

$\sim$ séu jafngildisvenzl í mengi M og $f : M \to N$ vörpun. Ef $\pi : M \to M/\!\sim$ er náttúrulega ofanvarpið þá segir Setning 4.3 að skilyrðið „ef $x \sim y$ þá $f(x) = f(y)$“ sé nægilegt til að til sé vörpun $\widetilde{f} : M/\!\sim \to N$ þannig að $f = \widetilde{f} \circ \pi$. Það er hinsvegar augljóst að þetta skilyrði er nauðsynlegt.

Setning 4.4: $f : M \to N$ sé vörpun. Látum $\sim$ vera jafngildisvenzlin í M sem gefin eru með

$x \sim y$ þá og því aðeins að $f(x) = f(y)$

Þá gefur f af sér gagntæka vörpun $M/\!\sim \to \mathrm{Im}(f)$.

Sönnun: Látum $\widetilde{f}$ vera eins og í Setningu 4.3. Þá er greinilega $\mathrm{Im}(\widetilde{f}) = \mathrm{Im}(f)$. Ef nú $x, y \in M$ þannig að $\widetilde{f}(\widetilde{x}) = \widetilde{f}(\widetilde{y})$, þ.e. $f(x) = f(y)$, þá er $x \sim y$, svo að $\widetilde{x} = \widetilde{y}$. Þetta sýnir að $\widetilde{f}$ er eintæk.

Deildamengið $M/\!\sim$ í Setningu 4.4 er stundum táknað $\mathrm{Coim}(f)$. Svo að setningin segir að vörpun f gefi af sér gagntæka vörpun $\mathrm{Coim}(f) \to \mathrm{Im}(f)$.

5 Hálfgrúpur

Samkvæmt setningunni um skilgreiningu með þrepun þá er fyrir sérhvert $m \in \mathbf{N}$ til ein og aðeins ein vörpun $f_m : \mathbf{N} \to \mathbf{N}$ þannig að $f_m(1) = m^+$ og $f_m(k^+) = f_m(k)^+$ fyrir sérhvert $k \in \mathbf{N}$.

Skilgreining: Ef $m \in \mathbf{N}$ og $f_m : \mathbf{N} \to \mathbf{N}$ er vörpunin þannig að $f_m(1) = m^+$ og $f_m(k^+) = f_m(k)^+$ fyrir sérhvert $k \in \mathbf{N}$, þá er fyrir sérhvert $n \in \mathbf{N}$ náttúrulega talan $f_m(n)$ nefnd *summa* m og n. Summa m og n er táknuð með

$$m + n$$

Þessa skilgreiningu á „+“ má orða þannig að fyrir sérhver $m, n \in \mathbf{N}$ gildi
S1: $m + 1 = m^+$
S2: $m + n^+ = (m + n)^+$

Setning 5.1: Fyrir sérhver $m, n, p \in \mathbf{N}$ gildir reglan
$(m + n) + p = m + (n + p)$
Sönnun með þrepun yfir p:
„$p = 1$“: $(m + n) + 1 = (m + n)^+ = m + n^+ = m + (n + 1)$.
„$p = k \to p = k^+$“: $(m + n) + k^+ = ((m + n) + k)^+ = (m + (n + k))^+ = m + (n + k)^+ = m + (n + k^+)$.

Setning 5.2: Fyrir sérhver $m, n \in \mathbf{N}$ gildir reglan
$m + n = n + m$
Sönnun með þrepun yfir m:
„$m = 1$“ með þrepun yfir n:
„$n = 1$“: Augljóst.
„$n = l \to n = l^+$“: $1 + l^+ = (1 + l)^+ = (l + 1)^+ = (l^+)^+ = l^+ + 1$.
„$m = k \to m = k^+$“: $k^+ + n = (k + 1) + n = k + (1 + n) = k + (n + 1) = (k + n) + 1 = (n + k) + 1 = (n + k)^+ = n + k^+$.

Setning 5.3: Fyrir sérhver $m, n \in \mathbf{N}$ gildir
til er $x \in \mathbf{N}$ með $m + x = n$ þá og því aðeins að $m < n$
Sönnun: Við sönnum fyrst með þrepun yfir x að $m < m + x$:
„$x = 1$“: $m < m^+ = m + 1$.
„$x = k \to x = k^+$“: $m < m + k < (m + k)^+ = m + k^+$.
Síðan sönnum við með þrepun yfir n að ef $m < n$ þá sé til $x \in \mathbf{N}$ með $m + x = n$:
„$n = 1$“: Augljóst vegna R1.

„$n = l \to n = l^+$“: Gefið sé $m < l^+$. Samkvæmt R2 þýðir það að $m < l$ eða $m = l$. Ef $m < l$ þá er samkvæmt þrepunarforsendu til $x \in \mathbf{N}$ með $m + x = l$. En þá fæst samkvæmt S2 að $m + x^+ = (m + x)^+ = l^+$. Ef $m = l$ þá fæst samkvæmt S1 að $m + 1 = m^+ = l^+$.

Setning 5.4: Fyrir sérhver $m, n, p \in \mathbf{N}$ gildir
ef $n < p$ þá $m + n < m + p$
Sönnun: Gefið sé $n < p$. Samkvæmt Setningu 5.3 er þá til $x \in \mathbf{N}$ með $n + x = p$. Með Setningu 5.1 fæst að $(m + n) + x = m + (n + x) = m + p$. Samkvæmt Setningu 5.3 er þá $m + n < m + p$.

Setning 5.5: Fyrir sérhver $m, n, p \in \mathbf{N}$ gildir
ef $m + n = m + p$ þá $n = p$
Sönnun: Ef $n < p$ þá væri $m + n < m + p$ samkvæmt Setningu 5.4. Eins sést að ef $p < n$ þá væri $m + p < m + n$. Samkvæmt Setningu 3.11 hlýtur því $n = p$ ef $m + n = m + p$.

Skilgreining: *Samsetning* í mengi M er vörpun $\vee : M \times M \to M$. Ef $\vee$ er samsetning í M og $x, y \in M$ þá er í stað $\vee(x, y)$ venjulega skrifað

$$x \vee y$$

Skilgreining: *Hálfgrúpa* er mengi G ásamt samsetningu $\vee$ í G þannig að fyrir sérhver $x, y, z \in G$ gildi reglan
$(x \vee y) \vee z = x \vee (y \vee z)$

Reglan í skilgreiningunni heitir *tengiregla*. Í skilgreiningunni er talað um „mengi G ásamt samsetningu $\vee$“. Þetta er ekki alveg nákvæmt orðalag en það má gera það nákvæmt með því að tala í staðinn um tvenndina $(G, \vee)$.

Með summunni er skilgreind samsetning $+$ í $\mathbf{N}$. Setning 5.1 segir nú að $(\mathbf{N}, +)$ sé hálfgrúpa.

Skilgreining: Hálfgrúpa $(H, \wedge)$ er sögð vera *hluthálfgrúpa* í hálfgrúpu $(G, \vee)$ ef H er hlutmengi í G og $x \wedge y = x \vee y$ fyrir sérhver $x, y \in H$.

Ef $(H, \wedge)$ er hluthálfgrúpa í hálfgrúpunni $(G, \vee)$ þá ákvarðast samsetningin $\wedge$ í H af samsetningunni $\vee$ í G. Það er því óhætt að segja einfaldlega að H sé hluthálfgrúpa í $(G, \vee)$ og nota sama táknið fyrir samsetninguna í H og samsetninguna í G.

Setning 5.6: $(G, \vee)$ sé hálfgrúpa og H hlutmengi í G. Þá og því aðeins er H hluthálfgrúpa í $(G, \vee)$ að fyrir sérhver x og y gildi

ef $x \in H$ og $y \in H$ þá $x \vee y \in H$

Sönnun: Augljóst.

Skilyrðið í Setningu 5.6 er oft orðað þannig að H sé *lokað* með tilliti til $\vee$.

Skilgreining: $(G, \vee)$ og $(H, \wedge)$ séu hálfgrúpur. Vörpun $f : G \to H$ er sögð vera *mótun* hálfgrúpna (eða *hálfgrúpumótun*) frá $(G, \vee)$ yfir í $(H, \wedge)$ ef fyrir sérhver $x_1, x_2 \in G$ gildir

$$f(x_1 \vee x_2) = f(x_1) \wedge f(x_2)$$

Í stað þess að segja að $(G, \vee)$ og $(H, \wedge)$ séu hálfgrúpur og $f : G \to H$ sé mótun hálfgrúpna munum við yfirleitt segja einfaldlega að $f : (G, \vee) \to (H, \wedge)$ sé mótun hálfgrúpna.

Setning 5.7: Ef $f : (G, \vee) \to (H, \wedge)$ og $g : (H, \wedge) \to (K, \diamond)$ eru mótanir hálfgrúpna þá er $g \circ f : (G, \vee) \to (K, \diamond)$ líka mótun hálfgrúpna.
Sönnun: Fyrir sérhver $x_1, x_2 \in G$ gildir $(g \circ f)(x_1 \vee x_2) = g(f(x_1 \vee x_2)) = g(f(x_1) \wedge f(x_2)) = g(f(x_1)) \diamond g(f(x_2)) = (g \circ f)(x_1) \diamond (g \circ f)(x_2)$.

Setning 5.8: Ef $f : (G, \vee) \to (H, \wedge)$ er gagntæk mótun hálfgrúpna þá er $f^{-1} : (H, \wedge) \to (G, \vee)$ líka mótun hálfgrúpna.
Sönnun: Gefin séu $y_1, y_2 \in H$. Skrifum $x_1 = f^{-1}(y_1)$ og $x_2 = f^{-1}(y_2)$. Þá er $f(x_1) = y_1$ og $f(x_2) = y_2$. Því fæst $f^{-1}(y_1 \wedge y_2) = f^{-1}(f(x_1) \wedge f(x_2)) = f^{-1}(f(x_1 \vee x_2)) = x_1 \vee x_2 = f^{-1}(y_1) \vee f^{-1}(y_2)$.

Skilgreining: Gagntæk mótun hálfgrúpna $(G, \vee) \to (H, \wedge)$ er einnig nefnd *einsmótun* hálfgrúpna $(G, \vee) \to (H, \wedge)$. Ef til er einsmótun hálfgrúpna $(G, \vee) \to (H, \wedge)$ þá er sagt að hálfgrúpurnar $(G, \vee)$ og $(H, \wedge)$ séu *einsmóta*.

Ef $(G, \vee)$ er hálfgrúpa þá er $\mathrm{id}_G : (G, \vee) \to (G, \vee)$ greinilega einsmótun hálfgrúpna. Ef $f : (G, \vee) \to (H, \wedge)$ er einsmótun hálfgrúpna þá er, samkvæmt Setningum 5.8 og 2.9, $f^{-1} : (H, \wedge) \to (G, \vee)$ líka einsmótun hálfgrúpna. Og ef $f : (G, \vee) \to (H, \wedge)$ og $g : (H, \wedge) \to (K, \diamond)$ eru einsmótanir hálfgrúpna þá er, samkvæmt Setningum 5.7 og 2.9, $g \circ f : (G, \vee) \to (K, \diamond)$ líka einsmótun hálfgrúpna.

Skilgreining: Hálfgrúpa $(K, \diamond)$ er sögð vera *deildahálfgrúpa* af hálfgrúpu $(G, \vee)$ ef K er deildamengi af G og $[x] \diamond [y] = [x \vee y]$ fyrir sérhver $x, y \in G$. Hér táknar $[z] \in K$ deild staksins $z \in G$.

Athugið að skilyrðið „$[x] \diamond [y] = [x \vee y]$ fyrir sérhver $x, y \in G$“ í skilgreiningunni má orða þannig að náttúrulega ofanvarpið $(G, \vee) \to (K, \diamond)$ sé mótun hálfgrúpna.

Ef $(K, \diamond)$ er deildahálfgrúpa af hálfgrúpunni $(G, \vee)$ þá ákvarðast samsetningin $\diamond$ í K af samsetningunni $\vee$ í G. Það er því óhætt að segja að K sé deildahálfgrúpa af $(G, \vee)$.

Setning 5.9: $(G, \vee)$ sé hálfgrúpa og $\sim$ jafngildisvenzl í G. Þá og því aðeins er $G/\!\sim$ deildahálfgrúpa af $(G, \vee)$ að fyrir sérhver $x, y, x', y' \in G$ gildi

ef $x \sim x'$ og $y \sim y'$ þá $x \vee y \sim x' \vee y'$

Sönnun: Við skrifum $K = G/\!\sim$. Ef $z \in G$ þá táknar $[z] \in K$ deild z, þ.e. jafngildisflokk z með tilliti til $\sim$.

Gerum fyrst ráð fyrir að K sé deildahálfgrúpa af $(G, \vee)$ og táknum samsetninguna í K með $\diamond$. Ef þá $x, y, x', y' \in G$ þannig að $x \sim x'$ og $y \sim y'$ þá fæst $[x] = [x']$ og $[y] = [y']$, svo að $[x \vee y] = [x] \diamond [y] = [x'] \diamond [y'] = [x' \vee y']$ og þar með $x \vee y \sim x' \vee y'$.

Gerum þá ráð fyrir að fyrir sérhver $x, y, x', y' \in G$ þannig að $x \sim x'$ og $y \sim y'$ gildi $x \vee y \sim x' \vee y'$. Á sama hátt og í sönnun Setningar 4.3 sést að við getum skilgreint samsetningu $\diamond$ í K með því að setja $\xi \diamond \eta = [x \vee y]$ ef $\xi = [x]$ og $\eta = [y]$ með $x, y \in G$. Þá er $[x] \diamond [y] = [x \vee y]$ fyrir sérhver $x, y \in G$. Ef $\xi, \eta, \zeta \in K$, $\xi = [x]$, $\eta = [y]$ og $\zeta = [z]$ með $x, y, z \in G$, þá fæst $(\xi \diamond \eta) \diamond \zeta = ([x] \diamond [y]) \diamond [z] = [x \vee y] \diamond [z] = [(x \vee y) \vee z] = [x \vee (y \vee z)] = [x] \diamond [y \vee z] = [x] \diamond ([y] \diamond [z]) = \xi \diamond (\eta \diamond \zeta)$. Þetta sýnir að $(K, \diamond)$ er hálfgrúpa, deildahálfgrúpa af $(G, \vee)$.

Setning 5.10: $f : (G, \vee) \to (H, \wedge)$ sé mótun hálfgrúpna. Látum $\sim$ vera jafngildisvenzlin í G sem gefin eru með

$x \sim y$ þá og því aðeins að $f(x) = f(y)$

Þá er $G/\!\sim$ deildahálfgrúpa af $(G, \vee)$ og $\mathrm{Im}(f)$ hluthálfgrúpa í $(H, \wedge)$. Auk þess gefur f af sér einsmótun hálfgrúpna $(G/\!\sim, \widetilde{\vee}) \to (\mathrm{Im}(f), \wedge)$. Hér táknar $\widetilde{\vee}$ samsetninguna í deildahálfgrúpunni $G/\!\sim$ af $(G, \vee)$.

Sönnun: Ef $x, y, x', y' \in G$ þannig að $f(x) = f(x')$ og $f(y) = f(y')$ þá er $f(x \vee y) = f(x) \wedge f(y) = f(x') \wedge f(y') = f(x' \vee y')$. Af þessu sést að $G/\!\sim$ er deildahálfgrúpa af $(G, \vee)$.

Ef $u, v \in \mathrm{Im}(f)$, segjum $u = f(x)$ og $v = f(y)$, þá er $u \wedge v = f(x) \wedge f(y) = f(x \vee y) \in \mathrm{Im}(f)$. Af þessu sést að $\mathrm{Im}(f)$ er hluthálfgrúpa í $(H, \wedge)$.

Samkvæmt Setningu 4.4 gefur f af sér gagntæka vörpun $\widetilde{f} : G/\!\sim \to \mathrm{Im}(f)$. Ef $x \in G$ þá er $\widetilde{f}([x]) = f(x)$. Hér táknar $[x] \in G/\!\sim$ deild staksins $x \in G$. Fyrir sérhver $x, y \in G$ fæst því $\widetilde{f}([x] \widetilde{\vee} [y]) = \widetilde{f}([x \vee y]) = f(x \vee y) = f(x) \wedge f(y) = \widetilde{f}([x]) \wedge \widetilde{f}([y])$. Þetta sýnir að $\widetilde{f} : (G/\!\sim, \widetilde{\vee}) \to (\mathrm{Im}(f), \wedge)$ er mótun hálfgrúpna.

Skilgreining: Hálfgrúpa $(G, \vee)$ er sögð vera *víxlin* ef fyrir sérhver $x, y \in G$ gildir reglan

$$x \vee y = y \vee x$$

Reglan í skilgreiningunni heitir að sjálfsögðu *víxlregla*. Athugið að hluthálfgrúpa í víxlinni hálfgrúpu er augljóslega víxlin. Sömuleiðis deildahálfgrúpa af víxlinni hálfgrúpu.

Skilgreining: Hálfgrúpa $(G, \vee)$ er sögð vera *styttin* ef fyrir sérhver $x, y, z \in G$ gilda reglurnar

Ef $z \vee x = z \vee y$ þá $x = y$
Ef $x \vee z = y \vee z$ þá $x = y$

Reglurnar í þessari skilgreiningu heita *styttireglur*.

Setningar 5.2 og 5.5 segja nú að hálfgrúpan $(\mathbf{N}, +)$ sé bæði víxlin og styttin.

Setning 5.11: Ef $(G, \vee)$ er hálfgrúpa og $a \in G$ þá er til ein og aðeins ein mótun hálfgrúpna $f : (\mathbf{N}, +) \to (G, \vee)$ þannig að $f(1) = a$.
Sönnun: Samkvæmt setningunni um skilgreiningu með þrepun er til ein og aðeins ein vörpun $f : \mathbf{N} \to G$ þannig að $f(1) = a$ og $f(k+1) = f(k) \vee a$ fyrir sérhvert $k \in \mathbf{N}$. Til þess að sanna að f sé mótun hálfgrúpna þá sönnum við með þrepun yfir n að $f(m+n) = f(m) \vee f(n)$ fyrir sérhver $m, n \in \mathbf{N}$:
„$n = 1$“: $f(m+1) = f(m) \vee a = f(m) \vee f(1)$.
„$n = k \to n = k+1$“: $f(m + (k+1)) = f((m+k)+1) = f(m+k) \vee a = (f(m) \vee f(k)) \vee a = f(m) \vee (f(k) \vee a)) = f(m) \vee f(k+1)$.

Ef $(G, \vee)$ er hálfgrúpa, $a \in G$ og $f : \mathbf{N} \to G$ vörpunin þannig að $f(1) = a$ og $f(k+1) = f(k) \vee a$ fyrir sérhvert $k \in \mathbf{N}$ þá má tákna stakið $f(n)$ með

$$\overset{n}{\vee} a$$

Skilgreiningin á $\overset{n}{\vee} a$ segir þá að

$$\overset{1}{\vee} a = a$$

og að fyrir sérhvert $k \in \mathbf{N}$ gildi

$$\overset{k+1}{\vee} a = (\overset{k}{\vee} a) \vee a$$

Setning 5.11 segir síðan að fyrir sérhver $m, n \in \mathbf{N}$ gildi

$$\overset{m+n}{\vee} a = (\overset{m}{\vee} a) \vee (\overset{n}{\vee} a)$$

Lítum nú á tilfellið $(G, \vee) = (\mathbf{N}, +)$:

Skilgreining: Ef $m, n \in \mathbf{N}$ þá er náttúrulega talan $\overset{m}{+}n$ nefnd *margfeldi* m og n. Margfeldi m og n er táknað með

$$m \cdot n$$

Skilgreiningin á margfeldi náttúrulegra talna segir þá að fyrir sérhver $m, n \in \mathbf{N}$ gildi
M1: $1 \cdot n = n$
M2: $(m + 1) \cdot n = (m \cdot n) + n$
Og Setning 5.11 segir:

Setning 5.12: Fyrir sérhver $m, n, p \in \mathbf{N}$ gildir reglan
$(m + n) \cdot p = (m \cdot p) + (n \cdot p)$

Setning 5.13: Ef $(G, \vee)$ er hálfgrúpa og $a \in G$ þá gildir fyrir sérhver $m, n \in \mathbf{N}$ reglan
$\overset{m \cdot n}{\vee} a = \overset{m}{\vee}(\overset{n}{\vee} a)$
Sönnun með þrepun yfir m: „$m = 1$“: $\overset{1 \cdot n}{\vee} a = \overset{n}{\vee} a = \overset{1}{\vee}(\overset{n}{\vee} a)$.
„$m = k \to m = k+1$“: $\overset{(k+1) \cdot n}{\vee} a = \overset{(k \cdot n)+n}{\vee} a = (\overset{k \cdot n}{\vee} a) \vee (\overset{n}{\vee} a) = \overset{k}{\vee}(\overset{n}{\vee} a) \vee (\overset{n}{\vee} a) = \overset{k+1}{\vee}(\overset{n}{\vee} a)$.

Með því að nota þessa setningu á $(\mathbf{N}, +)$ fáum við:

Setning 5.14: Fyrir sérhver $m, n, p \in \mathbf{N}$ gildir reglan
$(m \cdot n) \cdot p = m \cdot (n \cdot p)$

Þessi setning segir að $(\mathbf{N}, \cdot)$ sé hálfgrúpa.

Setning 5.15: Ef $(G, \vee)$ er víxlin hálfgrúpa og $a, b \in G$ þá gildir fyrir sérhvert $m \in \mathbf{N}$ reglan
$\overset{m}{\vee}(a \vee b) = (\overset{m}{\vee} a) \vee (\overset{m}{\vee} b)$
Sönnun með þrepun yfir m:
„$m = 1$“: $\overset{1}{\vee}(a \vee b) = a \vee b = (\overset{1}{\vee} a) \vee (\overset{1}{\vee} b)$.

„$m = k \to m = k{+}1$“: $\overset{k+1}{\vee}(a \vee b) = (\overset{k}{\vee}(a \vee b)) \vee (a \vee b) = ((\overset{k}{\vee} a) \vee (\overset{k}{\vee} b)) \vee (a \vee b) = (((\overset{k}{\vee} a) \vee (\overset{k}{\vee} b)) \vee a) \vee b = ((\overset{k}{\vee} a) \vee ((\overset{k}{\vee} b) \vee a)) \vee b = ((\overset{k}{\vee} a) \vee (a \vee (\overset{k}{\vee} b))) \vee b = (((\overset{k}{\vee} a) \vee a) \vee (\overset{k}{\vee} b)) \vee b = ((\overset{k}{\vee} a) \vee a) \vee ((\overset{k}{\vee} b) \vee b) = (\overset{k+1}{\vee} a) \vee (\overset{k+1}{\vee} b)$

Sértilfellið $(G, \vee) = (\mathbf{N}, +)$ gefur nú:

Setning 5.16: Fyrir sérhver $m, n, p \in \mathbf{N}$ gildir reglan
$m \cdot (n + p) = (m \cdot n) + (m \cdot p)$

Til þess að spara okkur svigaskriftir skulum við, eins og vanalegt er, koma okkur saman um að margföldun náttúrulegra talna skuli fara fram á undan samlagningu, nema annað sé gert ljóst með svigum. Við skrifum sem sagt til dæmis $m \cdot n + p$ fyrir $(m \cdot n) + p$ og $m \cdot n + p \cdot r$ fyrir $(m \cdot n) + (p \cdot r)$.

Setning 5.17: Fyrir sérhver $m, n \in \mathbf{N}$ gildir reglan
$m \cdot n = n \cdot m$
Sönnun með þrepun yfir n:
„$n = 1$“ með þrepun yfir m:
„$m = 1$“: Augljóst.
„$m = l \to m = l + 1$“: $(l+1) \cdot 1 = l \cdot 1 + 1 \cdot 1 = 1 \cdot l + 1 \cdot 1 = 1 \cdot (l+1)$.
„$n = k \to n = k + 1$“: $m \cdot (k+1) = m \cdot k + m \cdot 1 = k \cdot m + 1 \cdot m = (k+1) \cdot m$.

Setning 5.18: Fyrir sérhver $m, n, p \in \mathbf{N}$ gildir reglan
ef $m < n$ þá $p \cdot m < p \cdot n$
Sönnun: Ef $m < n$ þá er, samkvæmt Setningu 5.3, til $x \in \mathbf{N}$ með $m + x = n$. Þá fæst $p \cdot m + p \cdot x = p \cdot (m + x) = p \cdot n$. Af Setningu 5.3 leiðir því að $p \cdot m < p \cdot n$.

Setning 5.19: Fyrir sérhver $m, n, p \in \mathbf{N}$ gildir reglan
ef $p \cdot m = p \cdot n$ þá $m = n$
Sönnun: Þetta fæst á sama hátt af Setningu 5.18 og Setning 5.5 af Setningu 5.4.

Setningar 5.17 og 5.19 segja að hálfgrúpan $(\mathbf{N}, \cdot)$ sé bæði víxlin og styttin.

Fyrir náttúrulegar tölur n og m munum við, eins og vanalegt er, skrifa n^m í stað $\overset{m}{\cdot} n$.

6 Grúpur

Við skilgreinum venzl $\sim$ í $\mathbf{N} \times \mathbf{N}$ með því að setja

$(b, a) \sim (d, c)$ þá og því aðeins að $b + c = a + d$

fyrir sérhver $a, b, c, d \in \mathbf{N}$. Ef $a, b \in \mathbf{N}$ þá er $b + a = a + b$, svo að

$(b, a) \sim (b, a)$

Ef $a, b, c, d \in \mathbf{N}$ og $b + c = a + d$ þá er $d + a = c + b$, svo að við fáum

ef $(b, a) \sim (d, c)$ þá $(d, c) \sim (b, a)$

Nú séu $a, b, c, d, e, f \in \mathbf{N}$, $b + c = a + d$ og $d + e = c + f$. Þá fæst $b + e + c = b + c + e = a + d + e = a + c + f = a + f + c$ og þar með $b + e = a + f$. Þetta sýnir að

ef $(b, a) \sim (d, c)$ og $(d, c) \sim (f, e)$ þá $(b, a) \sim (f, e)$

Við höfum þar með sýnt að $\sim$ eru jafngildisvenzl í $\mathbf{N} \times \mathbf{N}$. Jafngildisflokkana nefnum við *heilar tölur* og mengi allra heilla talna, þ.e. deildamengið $(\mathbf{N} \times \mathbf{N})/\sim$, táknum við með $\mathbf{Z}$. Jafngildisflokk $(b, a) \in \mathbf{N} \times \mathbf{N}$ táknum við með $(b - a)$. Samkvæmt skilgreiningu gildir þá fyrir sérhver $a, b, c, d \in \mathbf{N}$ að

$(b - a) = (d - c)$ þá og því aðeins að $b + c = a + d$

Ef samsetningin $\uplus$ í $\mathbf{N} \times \mathbf{N}$ er skilgreind með því að setja

$(b, a) \uplus (d, c) = (b + d, a + c)$

fyrir sérhver $a, b, c, d \in \mathbf{N}$, þá er $(\mathbf{N} \times \mathbf{N}, \uplus)$ víxlin hálfgrúpa, eins og auðvelt er að sjá. Ef nú $a, b, c, d, a', b', c', d' \in \mathbf{N}$, $b + a' = a + b'$ og $d + c' = c + d'$ þá fæst $b + d + a' + c' = b + a' + d + c' = a + b' + c + d' = a + c + b' + d'$. Þetta sýnir að

ef $(b, a) \sim (b', a')$ og $(d, c) \sim (d', c')$ þá $(b, a) \uplus (d, c) \sim (b', a') \uplus (d', c')$

Af þessu fæst að $\mathbf{Z} = (\mathbf{N} \times \mathbf{N})/\sim$ er deildahálfgrúpa af $(\mathbf{N} \times \mathbf{N}, \uplus)$. Við táknum samsetninguna í þessari hálfgrúpu (í bili) með $\oplus$. Samkvæmt skilgreiningu gildir þá fyrir sérhver $a, b, c, d \in \mathbf{N}$ að

$(b - a) \oplus (d - c) = ((b + d) - (a + c))$

Hálfgrúpan $(\mathbf{Z}, \oplus)$ er víxlin, því að $(\mathbf{N} \times \mathbf{N}, \uplus)$ er víxlin.

Setning 6.1: Fyrir sérhver $\alpha, \beta \in \mathbf{Z}$ er til $\xi \in \mathbf{Z}$ með $\xi \oplus \alpha = \beta$.
Sönnun: Skrifum $\alpha = (b - a)$ og $\beta = (d - c)$ með $a, b, c, d \in \mathbf{N}$. Setjum $\xi = ((a + d) - (b + c))$. Þá fæst $\xi \oplus \alpha = ((a + d + b) - (b + c + a))$. Nú er $a + d + b + c = b + c + a + d$, svo að $((a + d + b) - (b + c + a)) = (d - c)$, þ.e.a.s. $\xi \oplus \alpha = \beta$.

Setning 6.2: Með því að setja

$j(a) = ((a + a) - a)$

fyrir sérhvert $a \in \mathbf{N}$ er skilgreind eintæk mótun hálfgrúpna $j : (\mathbf{N}, +) \to (\mathbf{Z}, \oplus)$.

Sönnun: Ef $a, b \in \mathbf{N}$ þá er $j(a+b) = ((a+b+a+b)-(a+b)) = ((a+a+b+b)-(a+b)) = ((a+a)-a) \oplus ((b+b)-b) = j(a) \oplus j(b)$. Þetta sýnir að j er mótun.

Ef $a, b \in \mathbf{N}$ og $j(a) = j(b)$, þ.e. $((a+a)-a) = ((b+b)-b)$, þá er $a+a+b = a+b+b$, þar með $a+a = a+b$ og þar með líka $a = b$. Þetta sýnir að j er eintæk.

Ef við skrifum $\underline{x}$ fyrir stakið $((x+x)-x) \in \mathbf{Z}$ þá segir Setning 6.2 okkur að fyrir sérhver $a, b, c \in \mathbf{N}$ gildi

$\underline{a} = \underline{b}$ þá og því aðeins að $a = b$

og

$\underline{a} \oplus \underline{b} = \underline{c}$ þá og því aðeins að $a + b = c$

Við munum því hér eftir leyfa okkur að skrifa einfaldlega a í stað $\underline{a}$, líta á $\mathbf{N}$ sem hlutmengi í $\mathbf{Z}$ og nota táknið „$+$“ líka fyrir samsetninguna $\oplus$ í $\mathbf{Z}$. Þetta er að sjálfsögðu ekki hárnákvæmur ritháttur, en mun ekki koma að sök við venjulega notkun náttúrulegra og heilla talna.

Skilgreining: Hálfgrúpa $(G, \vee)$ er sögð vera *grúpa* ef $G \neq \emptyset$ og fyrir sérhver $a, b \in G$ eru til $x, y \in G$ með $x \vee a = b$ og $a \vee y = b$.

Þar sem hálfgrúpan $(\mathbf{Z}, +)$ er víxlin þá segir Setning 6.1 að $(\mathbf{Z}, +)$ sé grúpa.

Skilgreining: $(G, \vee)$ sé hálfgrúpa. Stak e í G er þá sagt vera *hlutleysa* í $(G, \vee)$ ef fyrir sérhvert $x \in G$ gildir

$e \vee x = x$ og $x \vee e = x$

Setning 6.3: Hálfgrúpa hefur í mesta lagi eina hlutleysu.
Sönnun: e_1 og e_2 séu hlutleysur í hálfgrúpunni $(G, \vee)$. Þá er $e_1 \vee e_2 = e_2$ þar sem e_1 er hlutleysa og $e_1 \vee e_2 = e_1$ þar sem e_2 er hlutleysa. Af þessu leiðir að $e_2 = e_1$.

Setning 6.4: Sérhver grúpa hefur hlutleysu.
Sönnun: $(G, \vee)$ sé grúpa og $a \in G$. Þá eru til stök $e_1, e_2 \in G$ með $e_1 \vee a = a$ og $a \vee e_2 = a$. Ef nú $b \in G$ þá er til $y \in G$ með $a \vee y = b$. Af því fæst að $e_1 \vee b = e_1 \vee a \vee y = a \vee y = b$. Á sama hátt fæst að $b \vee e_2 = b$ fyrir sérhvert $b \in G$. Eins og í sönnun Setningar 6.3 leiðir af þessu að $e_2 = e_1$. Svo að e_1 er hlutleysa í $(G, \vee)$.

Hlutleysan í $(\mathbf{Z}, +)$ er táknuð með 0.

Ef $c \in \mathbf{N}$ þá fæst fyrir sérhver $a, b \in \mathbf{N}$ að $(c-c)+(b-a) = ((c+b)-(c+a)) = (b-a)$, því að $c+b+a = c+a+b$. Þar sem $(\mathbf{Z}, +)$ er víxlin þá

þýðir þetta að $(c-c)$ er hlutleysa í $(\mathbf{Z},+)$. Fyrir sérhvert $c \in \mathbf{N}$ gildir því að $0=(c-c)$.

Skilgreining: $(G,\vee)$ sé hálfgrúpa með hlutleysu e og a sé stak í G. Stak a' í G er þá sagt vera *andhverfa* a í $(G,\vee)$ ef

$$a' \vee a = e \text{ og } a \vee a' = e$$

Setning 6.5: $(G,\vee)$ sé hálfgrúpa með hlutleysu. Stak a í G hefur þá í mesta lagi eina andhverfu í $(G,\vee)$.
Sönnun: e sé hlutleysan í $(G,\vee)$ og a_1', a_2' andhverfur a í $(G,\vee)$. Þar sem a_1' er andhverfa a þá fæst $a_1' \vee a \vee a_2' = e \vee a_2' = a_2'$, og þar sem a_2' er andhverfa a þá fæst $a_1' \vee a \vee a_2' = a_1' \vee e = a_1'$. Af þessu leiðir að $a_2' = a_1'$.

Setning 6.6: $(G,\vee)$ sé grúpa. Þá hefur sérhvert stak í G andhverfu í $(G,\vee)$.
Sönnun: e sé hlutleysan í $(G,\vee)$ og $a \in G$. Þar sem $(G,\vee)$ er grúpa þá eru til $a_1', a_2' \in G$ með $a_1' \vee a = e$ og $a \vee a_2' = e$. Eins og í sönnun Setningar 6.5 fæst að $a_2' = a_1'$, svo að a_1' er andhverfa a í $(G,\vee)$.

Ef $\alpha \in \mathbf{Z}$ þá er andhverfa α í $(\mathbf{Z},+)$ táknuð með $-\alpha$.

Ef $a,b \in \mathbf{N}$ þá fæst að $(a-b)+(b-a) = ((a+b)-(b+a)) = ((a+b)-(a+b)) = 0$. Þar sem $(\mathbf{Z},+)$ er víxlin þá þýðir þetta að $(a-b)$ er andhverfa $(b-a)$ í $(\mathbf{Z},+)$. Fyrir sérhver $a,b \in \mathbf{N}$ gildir því að $-(b-a) = (a-b)$.

Setning 6.7: $(G,\vee)$ sé hálfgrúpa með hlutleysu. Stakið a í G hafi andhverfu a' í $(G,\vee)$. Fyrir sérhver $b,x,y \in G$ gildir þá

$x \vee a = b$ þá og því aðeins að $x = b \vee a'$

$a \vee y = b$ þá og því aðeins að $y = a' \vee b$

Sönnun: e sé hlutleysan í $(G,\vee)$. Ef $x \vee a = b$ þá $x = x \vee e = x \vee a \vee a' = b \vee a'$. Ef $x = b \vee a'$ þá $x \vee a = b \vee a' \vee a = b \vee e = b$. Á sama hátt fæst að $a \vee y = b$ þá og því aðeins að $y = a' \vee b$.

Af Setningum 6.4, 6.6 og 6.7 leiðir að ef $(G,\vee)$ er grúpa þá er fyrir sérhver $a,b \in G$ til aðeins eitt $x \in G$ með $x \vee a = b$ og aðeins eitt $y \in G$ með $a \vee y = b$. Sér í lagi fæst að sérhver grúpa er styttin.

Ef $\alpha,\beta \in \mathbf{Z}$ þá fæst að til er eitt og aðeins eitt $\xi \in \mathbf{Z}$ með $\xi + \alpha = \beta$, nefnilega $\xi = \beta + (-\alpha)$. Nú séu $a,b \in \mathbf{N}$. Þá er $((b+b)-b) = ((b+a+a)-(a+a)) = (b-a)+((a+a)-a)$, þ.e. $b = (b-a)+a$. Þetta sýnir að fyrir $\xi = (b-a)$ gildir $\xi + a = b$, svo að $(b-a) = b+(-a)$. Við munum því hér eftir oftast skrifa $\beta - \alpha$ í stað $\beta + (-\alpha)$ fyrir hvaða heilar tölur α og β sem er.

Af Setningu 6.7 leiðir líka að sérhver hálfgrúpa með hlutleysu, sem hefur andhverfur fyrir öll sín stök, er grúpa. Við munum sanna almennari setningu.

En aðalatriðin í sönnun þeirrar setningar eru þess virði að skrifast sem sérstök setning:

Setning 6.8: $(G, \vee)$ sé hálfgrúpa með hlutleysu e. Stakið $a \in G$ hafi andhverfu a' í $(G, \vee)$ og stakið $b \in G$ hafi andhverfu b' í $(G, \vee)$. Þá gildir:
(i) e hefur andhverfu e í $(G, \vee)$.
(ii) a' hefur andhverfu a í $(G, \vee)$.
(iii) $a \vee b$ hefur andhverfu $b' \vee a'$ í $(G, \vee)$.
Sönnun: (i) og (ii) eru augljós. (iii) leiðir af því að $b' \vee a' \vee a \vee b = b' \vee e \vee b = b' \vee b = e$ og $a \vee b \vee b' \vee a' = a \vee e \vee a' = a \vee a' = e$.

Setning 6.9: $(G, \vee)$ sé hálfgrúpa með hlutleysu. H sé mengi allra þeirra staka í G sem hafa andhverfu í $(G, \vee)$. Þá er H hluthálfgrúpa í $(G, \vee)$ og $(H, \vee)$ er grúpa.
Sönnun: Að H sé hluthálfgrúpa í $(G, \vee)$ leiðir af Setningu 6.8 (iii). Að $H \neq \emptyset$ leiðir af Setningu 6.8 (i). Ef nú $a, b \in H$ þá er $(b \vee a') \vee a = b$ og $a \vee (a' \vee b) = b$, samkvæmt Setningu 6.7. Að $b \vee a' \in H$ og $a' \vee b \in H$ leiðir af Setningu 6.8 (ii) og (iii).

Setning 6.10: $(G, \vee)$ og $(H, \wedge)$ séu grúpur þannig að $(H, \wedge)$ sé hluthálfgrúpa í $(G, \vee)$. Þá er hlutleysan í $(H, \wedge)$ líka hlutleysan í $(G, \vee)$, og ef $a \in H$ þá er andhverfa a í $(H, \wedge)$ líka andhverfa a í $(G, \vee)$.
Sönnun: Ef e_H er hlutleysan í $(H, \wedge)$ og e_G hlutleysan í $(G, \vee)$ þá er $e_H \wedge e_H = e_H$ og $e_G \vee e_H = e_H$. Vegna $e_H \wedge e_H = e_H \vee e_H$ þá leiðir þar með af styttireglunni í $(G, \vee)$ að $e_H = e_G$. Við skrifum nú $e := e_H = e_G$.

Ef a'_H er andhverfa a í $(H, \wedge)$ og a'_G andhverfa a í $(G, \vee)$ þá er $a'_H \wedge a = e$ og $a'_G \vee a = e$. Eins og áður leiðir af þessu að $a'_H = a'_G$.

Ef $(G, \vee)$ og $(H, \wedge)$ eru eins og í Setningu 6.10 þá er að sjálfsögðu sagt að H sé *hlutgrúpa* í $(G, \vee)$.

$(G, \vee)$ sé hálfgrúpa. Ef ekki er talin hætta á misskilningi þá er oft einfaldlega sagt að G sé hálfgrúpa og í stað $a \vee b$ einfaldlega skrifað ab. Í stað $\overset{n}{\vee} a$ er þá ennfremur skrifað a^n. Að sjálfsögðu er þetta ekki nákvæmur ritháttur, en hann er þægilegur og ónákvæmnin kemur ekki að sök ef aðeins ein ákveðin samsetning í G er til umræðu. Ef $(G, \vee)$ er grúpa þá er eins sagt að G sé grúpa. Hlutleysan í G er þá gjarna táknuð með e_G, eða einfaldlega e, og andhverfa $a \in G$ táknuð með a^{-1}.

Ef grúpan $(G, \vee)$ er víxlin þá er stundum skrifað $a+b$ fyrir samsetninguna $a \vee b$, skrifað $n \cdot a$ í stað $\overset{n}{\vee} a$, hlutleysan táknuð með 0_G, eða einfaldlega 0, og andhverfa $a \in G$ með $-a$.

Setning 6.11: G sé grúpa og $H \subseteq G$. Þá og því aðeins er H hlutgrúpa í G að fyrir sérhver x og y gildi
(i) ef $x \in H$ og $y \in H$ þá $xy \in H$
(ii) $e_G \in H$
(iii) ef $x \in H$ þá $x^{-1} \in H$
Sönnun: Ef H er hlutgrúpa í G þá er H hluthálfgrúpa í G, svo að (i) gildir. Af Setningu 6.10 leiðir svo að (ii) og (iii) gilda líka. Gerum þá ráð fyrir að (i), (ii) og (iii) gildi. Vegna (i) er þá H hluthálfgrúpa í G. Af (ii) leiðir að H hefur hlutleysu e_G og af (iii) leiðir að sérhvert stak í H hefur andhverfu í H. Af Setningu 6.9 leiðir því að H er grúpa, þar með hlutgrúpa í G.

Setning 6.12: G og H séu grúpur og $f : G \to H$ mótun hálfgrúpna. Þá er $f(e_G) = e_H$ og $f(x^{-1}) = f(x)^{-1}$ fyrir sérhvert $x \in G$.
Sönnun: $f(e_G)f(e_G) = f(e_G e_G) = f(e_G) = e_H f(e_G)$. Af styttireglunni í H leiðir því að $f(e_G) = e_H$. Ef $x \in G$ þá er $f(x^{-1})f(x) = f(x^{-1}x) = f(e_G) = e_H = f(x)^{-1}f(x)$. Af styttireglunni í H leiðir því að $f(x^{-1}) = f(x)^{-1}$.

Ef G, H og f eru eins og í Setningu 6.12 þá er að sjálfsögðu sagt að $f : G \to H$ sé *mótun* grúpna (eða *grúpumótun*).

Setning 6.13: Deildahálfgrúpa af grúpu er grúpa.
Sönnun: G sé grúpa og K sé deildahálfgrúpa af G. Ef $x \in G$ þá sé $[x] \in K$ deild x. Fyrir sérhvert $x \in G$ gildir þá $[e_G][x] = [e_G x] = [x]$ og $[x][e_G] = [xe_G] = [x]$. Þetta sýnir að $[e_G]$ er hlutleysa í K. Ef $x \in G$ þá er $[x^{-1}][x] = [x^{-1}x] = [e_G]$ og $[x][x^{-1}] = [xx^{-1}] = [e_G]$, svo að $[x^{-1}]$ er andhverfa $[x]$ í K. Af Setningu 6.9 leiðir því að K er grúpa.

Athugið að í sönnun Setningar 6.13 kemur fram að deild hlutleysunnar í G er hlutleysan í K og að deild andhverfu staks í G er andhverfa deildar staksins í K. Þetta má líka leiða af Setningu 6.12, því að náttúrulega ofanvarpið $G \to K$ er augljóslega mótun grúpna.

Vegna Setningar 6.13 er deildahálfgrúpa af grúpu sögð vera *deildagrúpa* af grúpunni.

Setning 6.14: G sé grúpa og $\sim$ séu jafngildisvenzl í G þannig að $G/\sim$ sé deildagrúpa af G. Látum N vera jafngildisflokk hlutleysunnar í G. Þá gildir:
(i) N er hlutgrúpa í G
(ii) ef $x \in G$ og $u \in N$ þá $xux^{-1} \in N$
Ennfremur gildir fyrir sérhver $x, y \in G$ að:
(iii) $x \sim y$ þá og því aðeins að $y^{-1}x \in N$
Sönnun: e sé hlutleysan í G.

(i): Ef $u, v \in N$, þ.e. $u \sim e$ og $v \sim e$, þá er $uv \sim ee = e$. svo að $uv \in N$. Vegna $e \sim e$ er $e \in N$. Ef $u \in N$, þ.e. $u \sim e$, þá er $e = u^{-1}u \sim u^{-1}e = u^{-1}$, svo að $u^{-1} \sim e$, þ.e. $u^{-1} \in N$. Samkvæmt Setningu 6.11 er N þar með hlutgrúpa í G.
(ii): Ef $x \in G$ og $u \in N$, þ.e. $u \sim e$, þá $xu \sim xe = x$, þar með $xux^{-1} \sim xx^{-1} = e$, svo að $xux^{-1} \in N$.
(iii): Ef $x \sim y$ þá $y^{-1}x \sim y^{-1}y = e$, svo að $y^{-1}x \in N$. Ef $y^{-1}x \in N$, þ.e. $y^{-1}x \sim e$, þá $x = ex = yy^{-1}x \sim ye = y$.

Skilgreining: G sé grúpa og N hlutgrúpa í G. Þá er N sögð vera *normleg hlutgrúpa* í G ef fyrir sérhver x og u gildir

ef $x \in G$ og $u \in N$ þá $xux^{-1} \in N$

Liðir (i) og (ii) í Setningu 6.14 segja því að N sé normleg hlutgrúpa í G.

Setning 6.15: G sé grúpa og N sé normleg hlutgrúpa í G. Með því að setja

$x \sim y$ þá og því aðeins að $y^{-1}x \in N$

eru skilgreind jafngildisvenzl $\sim$ í G þannig að $G/\sim$ sé deildagrúpa af G. Ennfremur er N þá jafngildisflokkur hlutleysunnar í G.
Sönnun: Fyrst sönnum við að $\sim$ séu jafngildisvenzl í G:
$x \sim x$, því að $x^{-1}x = e \in N$.
Ef $x \sim y$, þ.e. $y^{-1}x \in N$, þá $x^{-1}y = x^{-1}(y^{-1})^{-1} = (y^{-1}x)^{-1} \in N$, svo að $y \sim x$.
Ef $x \sim y$ og $y \sim z$, þ.e. $y^{-1}x \in N$ og $z^{-1}y \in N$, þá $z^{-1}x = z^{-1}yy^{-1}x \in N$, svo að $x \sim z$.

Næst sýnum við að $G/\sim$ er deildagrúpa af G:
Gefin séu $x, y, x', y' \in G$ þannig að $x \sim x'$ og $y \sim y'$, þ.e. $x'^{-1}x \in N$ og $y'^{-1}y \in N$. Sanna þarf að $xy \sim x'y'$. Vegna $(xy')^{-1}(xy) = y'^{-1}x^{-1}xy = y'^{-1}y \in N$ þá er $xy \sim xy'$. Það nægir því að sanna að $xy' \sim x'y'$. Nú er $(x'y')^{-1}(xy') = y'^{-1}(x'^{-1}x)y' \in N$, því að $x'^{-1}x \in N$ og N er normleg hlutgrúpa í G. Þetta sýnir að $xy' \sim x'y'$.

Þá sýnum við að N sé jafngildisflokkur hlutleysunnar e í G:
Ef $x \in G$ þá $x \sim e$ þá og því aðeins að $e^{-1}x \in N$. En $e^{-1}x = ex = x$, svo að $x \sim e$ þá og því aðeins að $x \in N$.

Af Setningum 6.14 og 6.15 leiðir að gagnkvæm samsvörun er á milli normlegra hlutgrúpna N í grúpu G og jafngildisvenzla $\sim$ í G þannig að $G/\sim$ sé deildagrúpa af G. Ef nú N er normleg hlutgrúpa í G og $\sim$ eru tilheyrandi jafngildisvenzl í G þá er deildagrúpan $G/\sim$ venjulega táknuð með G/N. Jafngildisflokkur $x \in G$ er þá táknaður með xN, enda er jafngildisflokkur $x \in G$ einmitt mengið $\{\, xu \,|\, u \in N \,\}$. Ef notað er tákn, segjum $\vee$, fyrir

samsetninguna í G þá er jafngildisflokkur $x \in G$ þó venjulega táknaður með $x \vee N$.

Athugið að ef grúpan G er víxlin þá er sérhver hlutgrúpa í G normleg hlutgrúpa í G.

Skilgreining: $f : G \to H$ sé mótun grúpna. Hlutmengið

$$\mathrm{Ker}(f) := \{\, x \in G \mid f(x) = e_H \,\}$$

í G er þá kallað*kjarni* mótunarinnar f.

Setning 6.16: Ef $f : G \to H$ er mótun grúpna þá er $\mathrm{Ker}(f)$ normleg hlutgrúpa í G og $\mathrm{Im}(f)$ hlutgrúpa í H. Með því að setja

$$\widetilde{f}(x\mathrm{Ker}(f)) = f(x)$$

fyrir sérhvert $x \in G$ er skilgreind einsmótun grúpna

$$\widetilde{f} : G/\mathrm{Ker}(f) \to \mathrm{Im}(f)$$

Sönnun: $\sim$ séu jafngildisvenzlin í G þannig að fyrir sérhver $x, y \in G$ gildi
$x \sim y$ þá og því aðeins að $f(x) = f(y)$
Samkvæmt Setningu 5.10 þá er $G/\sim$ þá deildahálfgrúpa af G, $\mathrm{Im}(f)$ hlut-hálfgrúpa í H og með því að setja

$$\widetilde{f}(\widetilde{x}) = f(x)$$

fyrir sérhvert $x \in G$ er skilgreind einsmótun hálfgrúpna

$$\widetilde{f} : G/\sim \to \mathrm{Im}(f)$$

Hér er $\widetilde{x}$ jafngildisflokkur x. Samkvæmt Setningu 6.13 er $G/\sim$ deildagrúpa af G. Auk þess er $x \sim e_G$ þá og því aðeins að $f(x) = f(e_G) = e_H$, svo að jafngildisflokkur e_G er $\mathrm{Ker}(f)$. Af Setningu 6.14 leiðir því að $\mathrm{Ker}(f)$ er normleg hlutgrúpa í G og $G/\sim = G/\mathrm{Ker}(f)$, sér í lagi $\widetilde{x} = x\mathrm{Ker}(f)$ fyrir sérhvert $x \in G$. Að síðustu leiðir strax af Setningum 6.11 og 6.12 að $\mathrm{Im}(f)$ er hlutgrúpa í H.

Við lítum nú aftur á grúpuna $(\mathbf{Z}, +)$ og sönnum fyrst setningu um $(\mathbf{Z}, +)$ og almennar grúpur, sem samsvarar Setningu 5.11 um $(\mathbf{N}, +)$ og almennar hálfgrúpur.

Setning 6.17: Ef G er grúpa og $a \in G$ þá er til ein og aðeins ein mótun grúpna $f : (\mathbf{Z}, +) \to G$ þannig að $f(1) = a$.

Sönnun: Við sýnum fyrst að fyrir sérhver $m, n \in \mathbf{N}$ gildir $a^n(a^m)^{-1} = (a^m)^{-1}a^n$:
Við höfum $(a^m)^{-1}a^n a^m = (a^m)^{-1}a^{n+m} = (a^m)^{-1}a^{m+n} = (a^m)^{-1}a^m a^n = a^n$. Samkvæmt Setningu 6.7 er þar með $(a^m)^{-1}a^n = a^n(a^m)^{-1}$.

Næst sýnum við að ef $m, n, k, l \in \mathbf{N}$ þannig að $n + k = m + l$ þá sé $a^n(a^m)^{-1} = a^l(a^k)^{-1}$:
Vegna $n + k = m + l$ þá er $a^n a^k = a^{n+k} = a^{m+l} = a^m a^l$. Af því leiðir, með Setningu 6.7 og reglunni hér að ofan, að $a^n = a^l a^m (a^k)^{-1} = a^l (a^k)^{-1} a^m$. Samkvæmt Setningu 6.7 er þá $a^n(a^m)^{-1} = a^l(a^k)^{-1}$.

Af síðari reglunni sést að við getum skilgreint vörpun $f : \mathbf{Z} \to G$ með því að setja

$$f((n - m)) = a^n(a^m)^{-1}$$

fyrir sérhver $m, n \in \mathbf{N}$. Þá er greinilega $f(1) = f((1 + 1) - 1)) = aaa^{-1} = a$. Ef nú $m, n, k, l \in \mathbf{N}$ þá fæst $f((n - m) + (l - k)) = f(((n + l) - (m + k))) = a^{n+l}(a^{m+k})^{-1} = a^{n+l}(a^{k+m})^{-1} = a^n a^l (a^k a^m)^{-1} = a^n a^l (a^m)^{-1}(a^k)^{-1} = a^n(a^m)^{-1}a^l(a^k)^{-1} = f((n - m))f((l - k))$. Þetta sýnir að $f : (\mathbf{Z}, +) \to G$ er mótun grúpna.

Að lokum sýnum við að ef $g : (\mathbf{Z}, +) \to G$ er mótun grúpna þannig að $g(1) = a$ þá sé $g = f$:
Af Setningu 5.11 fæst að $g(n) = a^n$ fyrir sérhvert $n \in \mathbf{N}$. Vegna Setningar 6.12 er þá $g(-m) = (a^m)^{-1}$ fyrir sérhvert $m \in \mathbf{N}$. Því fæst að $g((n - m)) = g(n + (-m)) = g(n)g(-m) = a^n(a^m)^{-1} = f((n - m))$ fyrir sérhver $m, n \in \mathbf{N}$.

G sé grúpa, $a \in G$ og f eins og í Setningu 6.17. Ef notað er tákn, segjum $\vee$, fyrir samsetninguna í G þá má skrifa $\overset{n}{\vee} a$ fyrir $f(n)$. En ef ekkert tákn er notað þá er skrifað a^n fyrir $f(n)$. Að f sé mótun grúpna þýðir þá að fyrir sérhver $m, n \in \mathbf{Z}$ gildir

$$a^{m+n} = a^m a^n$$

Að $f(1) = a$ þýðir að $a^1 = a$. Athugið líka að samkvæmt Setningu 6.12 þá er $a^0 = e_G$ og $a^{-n} = (a^n)^{-1}$. Ef táknið „+“ er notað fyrir samsetninguna í G er þó vanalega skrifað $n \cdot a$ fyrir $f(n)$. Að f sé mótun grúpna þýðir þá að fyrir sérhver $m, n \in \mathbf{N}$ gildir

$$(m + n) \cdot a = (m \cdot a) + (n \cdot a)$$

Að $f(1) = a$ þýðir að $1 \cdot a = a$. Samkvæmt Setningu 6.12 þá er $0 \cdot a = 0_G$ og $(-n) \cdot a = -(n \cdot a)$.

Ef við notum þetta á grúpuna $(\mathbf{Z}, +)$ þá fáum við samsetningu $\cdot$ í $\mathbf{Z}$ sem nefnd er *margföldun*. Reglan hér að ofan gefur þá af sér eftirfarandi setningu.

Setning 6.18: Fyrir sérhver $m, n, p \in \mathbf{Z}$ gildir reglan

$$(m+n)\cdot p = m\cdot p + n\cdot p$$

Í þessari setningu höfum við sparað okkur svigaskriftir eins og við gerðum fyrir náttúrulegar tölur. Það munum við gera áfram.

Setning 6.19: Ef G er grúpa og $a \in G$ þá gildir fyrir sérhver $m, n \in \mathbf{Z}$ reglan

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

Sönnun: Gefið sé $n \in \mathbf{Z}$. Við skilgreinum vörpunina $g : \mathbf{Z} \to G$ með því að setja $g(m) = a^{m\cdot n}$ fyrir sérhvert $m \in \mathbf{Z}$. Ef $k, l \in \mathbf{Z}$ þá fæst $g(k+l) = a^{(k+l)\cdot n} = a^{k\cdot n + l\cdot n} = a^{k\cdot n}a^{l\cdot n} = g(k)g(l)$. Þetta sýnir að $g : (\mathbf{Z}, +) \to G$ er mótun grúpna. Auk þess er $g(1) = a^{1\cdot n} = a^n$. Af Setningu 6.17 leiðir því að $g(m) = (a^n)^m$ fyrir öll $m \in \mathbf{Z}$.

Ef táknið „+“ er notað fyrir samsetninguna í G þá segir setningin að fyrir sérhver $m, n \in \mathbf{Z}$ gildi

$$(m\cdot n)\cdot a = m\cdot(n\cdot a)$$

Sér í lagi fæst eftirfarandi setning.

Setning 6.20: Fyrir sérhver $m, n, p \in \mathbf{Z}$ gildir reglan

$$(m\cdot n)\cdot p = m\cdot(n\cdot p)$$

Þessi setning segir að $(\mathbf{Z}, \cdot)$ sé hálfgrúpa.

Setning 6.21: Ef G er víxlin grúpa og $a, b \in G$ þá gildir fyrir sérhvert $m \in \mathbf{Z}$ reglan

$$(ab)^m = a^m b^m$$

Sönnun: Við skilgreinum vörpunina $g : \mathbf{Z} \to G$ með því að setja $g(m) = a^m b^m$ fyrir sérhvert $m \in \mathbf{Z}$. Ef $k, l \in \mathbf{Z}$ þá fæst $g(k+l) = a^{k+l}b^{k+l} = a^k a^l b^k b^l = a^k b^k a^l b^l = g(k)g(l)$. Þetta sýnir að $g : (\mathbf{Z}, +) \to G$ er mótun grúpna. Auk þess er $g(1) = a^1 b^1 = ab$. Af Setningu 6.17 leiðir því að $g(m) = (ab)^m$ fyrir öll $m \in \mathbf{Z}$.

Ef táknið „+“ er notað fyrir samsetninguna í G þá segir setningin að fyrir sérhvert $m \in \mathbf{Z}$ gildi

$$m\cdot(a+b) = m\cdot a + m\cdot b$$

Sér í lagi fæst eftirfarandi setning.

Setning 6.22: Fyrir sérhver $m, n, p \in \mathbf{Z}$ gildir reglan

$$m\cdot(n+p) = m\cdot n + m\cdot p$$

Næsta setning segir að 1 sé hlutleysa í hálfgrúpunni $(\mathbf{Z}, \cdot)$.

Setning 6.23: Fyrir sérhvert $m \in \mathbf{Z}$ gildir

$1 \cdot m = m$ og $m \cdot 1 = m$

Sönnun: Þegar hafði komið fram að $1 \cdot m = m$. Ljóst er að $\mathrm{id}_{\mathbf{Z}} : (\mathbf{Z}, +) \to (\mathbf{Z}, +)$ er mótun grúpna og að $\mathrm{id}_{\mathbf{Z}}(1) = 1$. Af Setningu 6.17 leiðir því að $\mathrm{id}_{\mathbf{Z}}(m) = m \cdot 1$ fyrir öll $m \in \mathbf{Z}$.

Setning 6.24: Fyrir sérhver $m, n \in \mathbf{Z}$ gildir reglan

$m \cdot n = n \cdot m$

Sönnun: Gefið sé $n \in \mathbf{Z}$. Við skilgreinum vörpunina $g : \mathbf{Z} \to \mathbf{Z}$ með því að setja $g(m) = n \cdot m$ fyrir sérhvert $m \in \mathbf{Z}$. Ef $k, l \in \mathbf{Z}$ þá fæst $g(k + l) = n \cdot (k + l) = n \cdot k + n \cdot l = g(k) + g(l)$. Þetta sýnir að $g : (\mathbf{Z}, +) \to (\mathbf{Z}, +)$ er mótun grúpna. Auk þess er $g(1) = n \cdot 1 = n$ samkvæmt Setningu 6.23. Af Setningu 6.17 leiðir því að $g(m) = m \cdot n$ fyrir öll $m \in \mathbf{Z}$.

Þessi setning segir að hálfgrúpan $(\mathbf{Z}, \cdot)$ sé víxlin.

Setning 6.25: Ef $k \in \mathbf{Z}$ þá gildir eitt og aðeins eitt af þrennu:

(i) $k \in \mathbf{N}$

(ii) $k = 0$

(iii) $-k \in \mathbf{N}$

Sönnun: Skrifum $k = n - m$ með $m, n \in \mathbf{N}$. Ef $m < n$ þá er, samkvæmt Setningu 5.3, til $x \in \mathbf{N}$ með $x + m = n$. En þá fæst $k = x + m - m = x$, svo að $k \in \mathbf{N}$. Ef $m = n$ þá er $k = 0$. Og ef $n < m$ þá er til $y \in \mathbf{N}$ með $y + n = m$. Þá fæst $-k = m - n = y + n - n = y$, svo að $-k \in \mathbf{N}$. Þetta sýnir að eitt af (i), (ii) og (iii) gildir.

Nú er $0 \notin \mathbf{N}$, því að $0 + 1 = 1$ og við vitum að ekki er til $x \in \mathbf{N}$ með $x + 1 = 1$. Því geta (i) og (ii) ekki bæði gilt. Vegna $-0 = 0$ geta þá (iii) og (ii) heldur ekki bæði gilt. Og (i) og (iii) geta heldur ekki bæði gilt, því að ef $k \in \mathbf{N}$ og $-k \in \mathbf{N}$ þá fengist $0 = k + (-k) \in \mathbf{N}$.

Vegna Setningar 5.3 getum við útvíkkað venzlin $<$ og $\leq$ í $\mathbf{N}$ yfir í $\mathbf{Z}$ með eftirfarandi skilgreiningu.

Skilgreining: Ef $m, n \in \mathbf{Z}$ þá setjum við

$m < n$ þá og því aðeins að til sé $x \in \mathbf{N}$ með $x + m = n$

$m \leq n$ þá og því aðeins að $m < n$ eða $m = n$

Ef $m, n \in \mathbf{Z}$ þá er til eitt og aðeins eitt $x \in \mathbf{Z}$ með $x + m = n$, nefnilega $x = n - m$. Því gildir

$m < n$ þá og því aðeins að $n - m \in \mathbf{N}$

Sér í lagi fæst að

$0 < n$ þá og því aðeins að $n \in \mathbf{N}$

Nú séu $m, n \in \mathbf{Z}$. Samkvæmt Setningu 6.25 gildir þá eitt og aðeins eitt af þrennu:
(i) $n - m \in \mathbf{N}$, þ.e. $m < n$
(ii) $n - m = 0$, þ.e. $m = n$
(iii) $-(n - m) \in \mathbf{N}$, þ.e. $m - n \in \mathbf{N}$, þ.e. $n < m$
Ef nú $m, n, p \in \mathbf{Z}$, $m < n$ og $n < p$, þ.e. $n - m \in \mathbf{N}$ og $p - n \in \mathbf{N}$, þá fæst að $p - m = p - n + n - m \in \mathbf{N}$, þ.e. $m < p$.

Við höfum þar með sýnt að $<$ er ströng röðun í $\mathbf{Z}$ og að tilheyrandi röðun í $\mathbf{Z}$, þ.e. $\leq$, sé línuleg röðun í $\mathbf{Z}$. Við skrifum þetta upp sem setningu:

Setning 6.26: $\leq$ er línuleg röðun í $\mathbf{Z}$.

Setning 6.27: Fyrir sérhver $m, n, p \in \mathbf{Z}$ gilda reglurnar
(i) ef $m < n$ þá $m + p < n + p$
(ii) ef $m < n$ og $0 < p$ þá $m \cdot p < n \cdot p$
Sönnun: (i): Ef $m < n$, þ.e. $n - m \in \mathbf{N}$, þá er $(n + p) - (m + p) = n + p - p - m = n - m \in \mathbf{N}$, svo að $m + p < n + p$.
(ii): Ef $m < n$ og $0 < p$, þ.e. $n - m \in \mathbf{N}$ og $p \in \mathbf{N}$, þá er $n \cdot p - m \cdot p = n \cdot p + (-(m \cdot p)) = n \cdot p + ((-m) \cdot p) = (n + (-m)) \cdot p = (n - m) \cdot p \in \mathbf{N}$, svo að $m \cdot p < n \cdot p$.

Setning 6.28: Fyrir sérhver $m, n \in \mathbf{Z}$ gildir reglan
ef $m \cdot n = 0$ þá $m = 0$ eða $n = 0$
Sönnun: Gefið sé að $m \cdot n = 0$ og að $n \neq 0$. Gerum fyrst ráð fyrir að $0 < n$. Ef þá $0 < m$ þá fengist, samkvæmt Setningu 6.27 (ii), að $0 = 0 \cdot n < m \cdot n$. Og ef $m < 0$ þá fengist eins að $m \cdot n < 0 \cdot n = 0$. Því hlýtur $m = 0$. Þá sé $n < 0$. Þá er $0 = n + (-n) < 0 + (-n) = -n$ samkvæmt Setningu 6.27 (i) og $m \cdot (-n) = -(m \cdot n) = -0 = 0$. Því fæst eins og áður að $m = 0$.

Setning 6.29: Sérhvert ekki tómt hlutmengi í $\mathbf{Z}$, sem er takmarkað að neðan, hefur minnsta stak.
Sönnun: Gefið sé $Q \subseteq \mathbf{Z}$, $Q \neq \emptyset$, og $a \in \mathbf{Z}$ þannig að $a \leq x$ fyrir sérhvert $x \in Q$. Þá gildir $a < x + 1$, þ.e. $x + 1 - a \in \mathbf{N}$, fyrir sérhvert $x \in Q$. Við setjum $R := \{\, x + 1 - a \mid x \in Q \,\} \subseteq \mathbf{N}$. Þar sem $Q \neq \emptyset$ þá er $R \neq \emptyset$, svo að R hefur minnsta stak n samkvæmt Setningu 3.9. Skrifum $n = m + 1 - a$ með $m \in Q$. Ef $x \in Q$ þá fæst $n \leq x + 1 - a$, þ.e. $m + 1 - a \leq x + 1 - a$, þar með $m = m + 1 - a + (-(1 - a)) \leq x + 1 - a + (-(1 - a)) = x$ fyrir sérhvert $x \in Q$. Þetta sýnir að m er minnsta stak í Q.

7 Baugar

Skilgreining: *Baugur* er mengi R ásamt samsetningum $\oplus$ og $\odot$ í R þannig að:

(i) $(R, \oplus)$ er víxlin grúpa

(ii) $(R, \odot)$ er hálfgrúpa

(iii) Fyrir sérhver $x, y, z \in R$ gilda reglurnar

$$x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z)$$
$$(y \oplus z) \odot x = (y \odot x) \oplus (z \odot x)$$

Reglurnar í lið (iii) í skilgreiningu þessari heita *dreifireglur*.

Í skilgreiningunni er sagt að baugur sé „mengi R ásamt samsetningum $\oplus$ og $\odot$“ en nákvæmara er að tala um bauginn $(R, \oplus, \odot)$. Í reynd er þó oftast notaður enn ónákvæmari ritháttur en í skilgreingunni. Það er nefnilega einfaldlega sagt að R sé baugur og gert ráð fyrir að samsetningarnar í R séu gefnar. Sú fyrri er venjulega nefnd *samlagningin* í R og táknuð með $+$, og sú seinni er nefnd *margföldunin* í R og táknuð með $\cdot$ eða jafnvel skrifuð án tákns. Hlutleysan í $(R, +)$ er þá táknuð með 0_R, eða jafnvel aðeins 0, og andhverfa staks x í $(R, +)$ er táknuð með $-x$. Ef $x, y \in R$ þá er í stað $x + (-y)$ venjulega skrifað $x - y$. Þetta skilgreinir samsetningu í R sem kölluð er *frádráttur*. Auk þessa alls þá eru notaðar samskonar reglur og í $\mathbf{Z}$ til þess að spara svigaskriftir. Til dæmis er vinstri dreifireglan þá einfaldlega skrifuð á forminu $x(y + z) = xy + xz$.

Setningar 6.1, 6.20, 6.18 og 6.22 segja nú að $\mathbf{Z}$, ásamt venjulegri samlagningu og margföldun, sé baugur.

Setning 7.1: R sé baugur. Fyrir sérhver $x, y \in R$ gilda þá reglurnar

(i) $x0 = 0$ og $0x = 0$

(ii) $x(-y) = -(xy)$ og $(-y)x = -(yx)$

Sönnun: (i): Af $x0 = x(0 + 0) = x0 + x0$ leiðir að $x0 = 0$. Hér var vinstri dreifireglan notuð. Með notkun hægri dreifireglunnar fæst á sama hátt að $0x = 0$.

(ii): Af $xy + x(-y) = x(y + (-y)) = x0 = 0$ leiðir að $x(-y) = -(xy)$. Á sama hátt fæst að $(-y)x = -(yx)$.

Vegna liðs (ii) í Setningu 7.1 getum við leyft okkur að skrifa $-xy$ fyrir hvort sem er, $(-x)y$ eða $-(xy)$. Ennfremur fæst að $x(y-z) = x(y+(-z)) = xy+x(-z) = xy+(-(xz))$, þ.e. $x(y-z) = xy-xz$. Eins fæst að $(y-z)x = yx - zx$.

Skilgreining: R og S séu baugar. Vörpun $f : R \to S$ er sögð vera *mótun* bauga (eða *baugmótun*) ef $f : (R, +) \to (S, +)$ er mótun grúpna og $f : (R, \cdot) \to (S, \cdot)$ er mótun hálfgrúpna, þ.e. ef fyrir sérhver $x_1, x_2 \in R$ gildir

$$f(x_1 + x_2) = f(x_1) + f(x_2)$$
$$f(x_1 x_2) = f(x_1) f(x_2)$$

Setning 7.2: Ef $f : R \to S$ og $g : S \to T$ eru mótanir bauga þá er $g \circ f : R \to T$ líka mótun bauga.
Sönnun: Leiðir af Setningu 5.7.

Setning 7.3: Ef $f : R \to S$ er gagntæk mótun bauga þá er $f^{-1} : S \to R$ líka mótun bauga.
Sönnun: Leiðir af Setningu 5.8.

Skilgreining: Gagntæk mótun bauga $R \to S$ er einnig nefnd *einsmótun* bauga $R \to S$. Ef til er einsmótun bauga $R \to S$ þá er sagt að baugarnir R og S séu *einsmóta*.

Setning 7.4: R sé baugur og S sé hlutmengi í R þannig að S sé hlutgrúpa í $(R, +)$ og hluthálfgrúpa í $(R, \cdot)$. Þá er S baugur.
Sönnun: Augljóst.

Ef R og S eru eins og í Setningu 7.4 þá er að sjálfsögðu sagt að S sé *hlutbaugur* í R.

Setning 7.5: R sé baugur og T sé deildamengi af R þannig að T sé deildagrúpa af $(R, +)$ og deildahálfgrúpa af $(R, \cdot)$. Þá er T baugur.
Sönnun: Ef $w \in R$ þá sé $[w] \in T$ deild w. Fyrir sérhver $x, y, z \in R$ fæst þá að $[x]([y]+[z]) = [x][y+z] = [x(y+z)] = [xy+xz] = [xy]+[xz] = [x][y]+[x][z]$ og á sama hátt að $([y] + [z])[x] = [y][x] + [z][x]$. Þetta sýnir að T er baugur.

Ef R og T eru eins og í Setningu 7.5 þá segjum við að T sé *deildabaugur* af R.

Setning 7.6: R sé baugur og $\sim$ jafngildisvenzl í R þannig að $R/\!\sim$ sé deildabaugur af R. Látum I vera jafngildisflokk 0_R. Þá gildir:
(i) I er hlutgrúpa í $(R, +)$
(ii) ef $x \in R$ og $u \in I$ þá $xu \in I$ og $ux \in I$
Ennfremur gildir fyrir sérhver $x, y \in R$ að
(iii) $x \sim y$ þá og því aðeins að $x - y \in I$
Sönnun: Þar sem $R/\!\sim$ er sér í lagi deildagrúpa af $(R, +)$ þá leiða liðir (i) og (iii) af liðum (i) og (iii) í Setningu 6.14 (og af því að $(R, +)$ er víxlin, svo að $(-y) + x = x - y$).

(ii): Við táknum jafngildisflokk $w \in R$ með $[w] \in R/\sim$. Ef $u \in I$ þá $[u] = [0_R] = 0_{R/\sim}$. Fyrir $x \in R$ fæst því að $[xu] = [x][u] = [x]0_{R/\sim} = 0_{R/\sim} = [0_R]$, svo að $xu \in I$. Á sama hátt fæst að $ux \in I$.

Skilgreining: R sé baugur og I hlutgrúpa í $(R, +)$. Þá er I sagt vera *íðal* í R ef fyrir sérhver x og u gildir

ef $x \in R$ og $u \in I$ þá $xu \in I$ og $ux \in I$

Athugið að íðal í baugi er sér í lagi hlutbaugur.

Setning 7.7: R sé baugur og I sé íðal í R. Með því að setja

$x \sim y$ þá og því aðeins að $x - y \in I$

eru skilgreind jafngildisvenzl $\sim$ í R þannig að $R/\sim$ sé deildabaugur af R. Ennfremur er I þá jafngildisflokkur 0_R.

Sönnun: Þar sem $(R, +)$ er víxlin grúpa þá leiðir þetta allt af Setningu 6.15, nema það að $R/\sim$ sé deildahálfgrúpa af $(R, \cdot)$. Til þess að sanna það þarf að sýna að ef $x \sim x'$ og $y \sim y'$ þá sé $xy \sim x'y'$. En ef $x - x' \in I$ og $y - y' \in I$ þá eru $x(y - y') \in I$ og $(x - x')y' \in I$, svo að $xy - x'y' = xy - xy' + xy' - x'y' = x(y - y') + (x - x')y' \in I$.

Af þessum tveim síðustu setningum leiðir að gagnkvæm samsvörun er á milli íðala I í baugi R og jafngildisvenzla $\sim$ í R þannig að $R/\sim$ sé deildabaugur af R. Ef I er íðal í R þá er tilheyrandi deildabaugur af R því venjulega táknaður með R/I. Deild $x \in R$ í R/I er þá oft táknuð $x + I$.

Skilgreining: $f : R \to S$ sé mótun bauga. Hlutmengið

$$\mathrm{Ker}(f) := \{\, x \in R \mid f(x) = 0_S \,\}$$

í R er þá kallað *kjarni* mótunarinnar f.

Setning 7.8: Ef $f : R \to S$ er mótun bauga þá er $\mathrm{Ker}(f)$ íðal í R og $\mathrm{Im}(f)$ hlutbaugur í S. Með því að setja

$$\widetilde{f}(x + \mathrm{Ker}(f)) = f(x)$$

fyrir sérhvert $x \in R$ er skilgreind einsmótun bauga

$$\widetilde{f} : R/\mathrm{Ker}(f) \to \mathrm{Im}(f)$$

Sönnun: Samkvæmt Setningu 6.16 er $\mathrm{Ker}(f)$ hlutgrúpa í $(R, +)$, $\mathrm{Im}(f)$ hlutgrúpa í $(S, +)$ og $\widetilde{f} : (\mathrm{Ker}(f), +) \to (\mathrm{Im}(f), +)$ einsmótun grúpna. Samkvæmt sönnun Setningar 6.16 eru auk þess jafngildisvenzlin $\sim$ í R, sem gefa deildagrúpuna $(R/\mathrm{Ker}(f), +)$, skilgreind með

$x \sim y$ þá og því aðeins að $f(x) = f(y)$

Af Setningu 5.10 leiðir þar með að $(R/\mathrm{Ker}(f), \cdot)$ er deildahálfgrúpa af $(R, \cdot)$, að $(\mathrm{Im}(f), \cdot)$ er hluthálfgrúpa í $(S, \cdot)$ og að $\widetilde{f} : (R/\mathrm{Ker}(f), \cdot) \to (\mathrm{Im}(f), \cdot)$ er einsmótun hálfgrúpna. Af skilgreiningunum á deildabaugi, hlutbaugi og mótun bauga leiðir þá að $R/\mathrm{Ker}(f)$ er deildabaugur af bauginum R, að $\mathrm{Im}(f)$ er hlutbaugur í bauginum S og að $\widetilde{f} : R/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ er mótun bauga. Og af Setningu 7.6 leiðir nú að $\mathrm{Ker}(f)$ er íðal í R.

Skilgreining: Baugur R er sagður vera *einbaugur* ef hálfgrúpan $(R, \cdot)$ hefur hlutleysu.

Ef R er einbaugur þá er hlutleysan í $(R, \cdot)$ venjulega táknuð með 1_R, jafnvel aðeins með 1.

Deildabaugur af einbaug er greinilega einbaugur.

Setning 6.23 segir að $\mathbf{Z}$ sé einbaugur.

Skilgreining: R og S séu einbaugar og $f : R \to S$ sé mótun bauga. f er þá sögð vera *mótun einbauga* ef $f(1_R) = 1_S$.

Setning 7.9: Ef R er einbaugur þá er til ein og aðeins ein mótun einbauga $f : \mathbf{Z} \to R$.

Sönnun: Samkvæmt Setningu 6.17 er til ein og aðeins ein mótun grúpna $f : (\mathbf{Z}, +) \to (R, +)$ þannig að $f(1) = 1_R$. (Ef $m \in \mathbf{Z}$ þá höfum við skrifað $m \cdot 1_R$ fyrir $f(m)$.) Nú sé $n \in \mathbf{Z}$. Við skilgreinum varpanirnar $g : \mathbf{Z} \to R$ og $h : \mathbf{Z} \to R$ með því að setja

$$g(m) = f(mn) \text{ og } h(m) = f(m)f(n)$$

fyrir sérhvert $m \in \mathbf{Z}$. Fyrir sérhver $k, l \in \mathbf{Z}$ fæst þá $g(k+l) = f((k+l)n) = f(kn+ln) = f(kn)+f(ln) = g(k)+g(l)$ og $h(k+l) = f(k+l)f(n) = (f(k)+f(l))f(n) = f(k)f(n) + f(l)f(n) = h(k) + h(l)$. Þetta sýnir að g og h eru mótanir grúpna. Nú er $g(1) = f(1n) = f(n)$ og $h(1) = f(1)f(n) = 1_R f(n) = f(n)$. Samkvæmt Setningu 6.17 er því $g = h$, þ.e. $f(mn) = f(m)f(n)$ fyrir sérhvert $m \in \mathbf{Z}$. Þetta sýnir að f er mótun bauga.

Skilgreining: R sé einbaugur. Stak $u \in R$ er þá sagt vera *eining* í R ef u hefur andhverfu í $(R, \cdot)$.

Samkvæmt Setningu 6.9 er mengi allra eininga í einbaugi R grúpa með tilliti til margföldunarinnar í R. Þessi grúpa er gjarna táknuð með R^*.

Skilgreining: Einbaugur R er sagður vera *heilbaugur* ef $1_R \neq 0_R$ og fyrir sérhver $x, y \in R$ gildir

$$\text{ef } xy = 0_R \text{ þá } x = 0_R \text{ eða } y = 0_R$$

Samkvæmt þessari skilgreiningu þá er baugur R heilbaugur þá og því aðeins að $R\backslash\{0_R\}$ sé hálfgrúpa með hlutleysu með tilliti til margföldunarinnar í R.

Setning 6.28 segir nú að $\mathbf{Z}$ sé heilbaugur.

Setning 7.10: R sé heilbaugur. Fyrir sérhver $x, y, z \in R$ gilda þá reglurnar
ef $zx = zy$ og $z \neq 0_R$ þá $x = y$
ef $xz = yz$ og $z \neq 0_R$ þá $x = y$
Sönnun: Ef $zx = zy$ þá $zx - zy = 0_R$, svo að $z(x - y) = 0_R$. Vegna $z \neq 0_R$ þá hlýtur þar með $x - y = 0_R$, þ.e. $x = y$. Á sama hátt fæst að ef $xz = yz$ þá $x = y$.

Skilgreining: Einbaugur R er sagður vera *deilibaugur* ef $1_R \neq 0_R$ og sérhvert stak í $R \setminus \{0\}$ hefur andhverfu í $(R, \cdot)$, þ.e. $R^* = R \setminus \{0\}$.

Samkvæmt þessari skilgreiningu þá er baugur R deilibaugur þá og því aðeins að $R \setminus \{0\}$ sé grúpa með tilliti til margföldunarinnar í R. Sér í lagi er sérhver deilibaugur líka heilbaugur.

Skilgreining: Baugur R er sagður *víxlinn* ef hálfgrúpan $(R, \cdot)$ er víxlin.

Hlutbaugur í víxlnum baug er að sjálfsögðu víxlinn. Sömuleiðis deildabaugur af víxlnum baugi.

Setning 6.24 segir að $\mathbf{Z}$ sé víxlinn baugur.

Skilgreining: *Kroppur* er víxlinn deilibaugur.

R sé víxlinn heilbaugur. Við skilgreinum venzlin $\sim$ í $R \times (R \setminus \{0\}) = \{\, (b, a) \mid a, b \in R, a \neq 0 \,\}$ með því að setja
$(b, a) \sim (d, c)$ þá og því aðeins að $bc = ad$
fyrir sérhver $a, b, c, d \in R$, $a \neq 0$, $c \neq 0$. Fyrir sérhver $a, b, c, d, e, f \in R$, $a \neq 0$, $c \neq 0$, $e \neq 0$, fæst þá:
(i) $(b, a) \sim (b, a)$, því að $ba = ab$.
(ii) Ef $(b, a) \sim (d, c)$, þ.e. $bc = ad$, þá $da = cb$, þ.e. $(d, c) \sim (b, a)$.
(iii) Ef $(b, a) \sim (d, c)$ og $(d, c) \sim (f, e)$, þ.e. $bc = ad$ og $de = cf$, þá $bec = bce = ade = acf = afc$, vegna $c \neq 0$ þar með $be = af$, þ.e. $(b, a) \sim (f, e)$.
Þetta sýnir að $\sim$ eru jafngildisvenzl í $R \times (R \setminus \{0\})$. Við táknum jafngildisflokk $(b, a) \in R \times (R \setminus \{0\})$ með $\frac{b}{a}$ og deildamengið $(R \times (R \setminus \{0\}))/\sim$ með $\mathrm{Quot}(R)$. Við höfum þá

$$\mathrm{Quot}(R) = \{\, \frac{b}{a} \mid a, b \in R, a \neq 0 \,\}$$

og samkvæmt skilgreiningu gildir

$$\frac{b}{a} = \frac{d}{c} \text{ þá og því aðeins að } bc = ad$$

fyrir sérhver $a, b, c, d \in R$, $a \neq 0$, $c \neq 0$.

Nú séu $a, b, c, d, a', b', c', d' \in R$ þannig að $(b, a) \sim (b', a')$ og $(d, c) \sim (d', c')$, þ.e. $ba' = ab'$ og $dc' = cd'$. Þá fæst:

(i) $bca'c' = ba'cc' = ab'cc' = acb'c'$ og $ada'c' = adc'a' = acd'a' = aca'd'$, svo að $(bc + ad)a'c' = bca'c' + ada'c' = acb'c' + aca'd' = ac(b'c' + a'd')$, þ.e. $(bc + ad, ac) \sim (b'c' + a'd', a'c')$.

(ii) $bda'c' = ba'dc' = ab'cd' = acb'd'$, þ.e. $(bd, ac) \sim (b'd', a'c')$. Þetta sýnir að við getum skilgreint samlagningu og margföldun í $\mathrm{Quot}(R)$ með því að setja

$$\frac{b}{a} + \frac{d}{c} = \frac{bc + ad}{ac}$$

og

$$\frac{b}{a} \cdot \frac{d}{c} = \frac{bd}{ac}$$

fyrir sérhver $a, b, c, d \in R$, $a \neq 0$, $c \neq 0$.

Fyrir sérhver $a, b, c, d, e, f \in R$, $a \neq 0$, $c \neq 0$, $e \neq 0$, fæst nú:

(i) $(\frac{b}{a} + \frac{d}{c}) + \frac{f}{e} = \frac{bc+ad}{ac} + \frac{f}{e} = \frac{(bc+ad)e+acf}{ace} = \frac{bce+ade+acf}{ace} = \frac{bce+a(de+cf)}{ace} = \frac{b}{a} + \frac{de+cf}{ce} = \frac{b}{a} + (\frac{d}{c} + \frac{f}{e})$

(ii) $\frac{b}{a} + \frac{d}{c} = \frac{bc+ad}{ac} = \frac{ad+bc}{ac} = \frac{da+bc}{ca} = \frac{d}{c} + \frac{b}{a}$

(iii) $\frac{0}{1} + \frac{b}{a} = \frac{0a+1b}{1a} = \frac{0+b}{a} = \frac{b}{a}$

(iv) $\frac{-b}{a} + \frac{b}{a} = \frac{-ba+ab}{aa} = \frac{-ba+ba}{aa} = \frac{0}{aa} = \frac{0}{1}$, því að $0 \cdot 1 = 0 = aa \cdot 0$

(v) $(\frac{b}{a} \cdot \frac{d}{c}) \cdot \frac{f}{e} = \frac{bd}{ac} \cdot \frac{f}{e} = \frac{bdf}{ace} = \frac{b}{a} \cdot \frac{df}{ce} = \frac{b}{a} \cdot (\frac{d}{c} \cdot \frac{f}{e})$

(vi) $\frac{b}{a} \cdot \frac{d}{c} = \frac{bd}{ac} = \frac{db}{ca} = \frac{d}{c} \cdot \frac{b}{a}$

(vii) $\frac{1}{1} \cdot \frac{b}{a} = \frac{1 \cdot b}{1 \cdot a} = \frac{b}{a}$

(viii) $\frac{b}{a} \cdot (\frac{d}{c} + \frac{f}{e}) = \frac{b}{a} \cdot \frac{de+cf}{ce} = \frac{b(de+cf)}{ace} = \frac{b(de+cf)a}{acea}$, því að $b(de + cf)acea = aceb(de+cf)a$, þar með $\frac{b}{a} \cdot (\frac{d}{c} + \frac{f}{e}) = \frac{b(de+cf)a}{acea} = \frac{bdea+bcfa}{acea} = \frac{bdae+acbf}{acea} = \frac{bd}{ac} + \frac{bf}{ae} = \frac{b}{a} \cdot \frac{d}{c} + \frac{b}{a} \cdot \frac{f}{e}$

Þetta sýnir að $\mathrm{Quot}(R)$ er víxlinn einbaugur.

Fyrir $a, b \in R$, $a \neq 0$, fæst að $\frac{b}{a} = \frac{0}{1}$ þá og því aðeins að $b \cdot 1 = a \cdot 0$, þ.e. $b = 0$. Af því sést að ef $\frac{b}{a} \neq \frac{0}{1}$ þá $b \neq 0$, svo að $\frac{a}{b} \in \mathrm{Quot}(R)$. En þá gildir $\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{1}{1}$, því að $ab \cdot 1 = ba \cdot 1$. Þetta sýnir að $\mathrm{Quot}(R)$ er kroppur.

Við skilgreinum nú vörpunina $j : R \to \mathrm{Quot}(R)$ með því að setja

$$j(b) = \frac{b}{1}$$

fyrir sérhvert $b \in R$. Þá fæst $j(b + d) = \frac{b+d}{1} = \frac{b \cdot 1 + 1 \cdot d}{1 \cdot 1} = \frac{b}{1} + \frac{d}{1} = j(b) + j(d)$ og $j(bd) = \frac{bd}{1} = \frac{bd}{1 \cdot 1} = \frac{b}{1} \cdot \frac{d}{1} = j(b) \cdot j(d)$ fyrir sérhver $b, d \in R$. Ennfremur

er $j(1) = \frac{1}{1}$. Þetta sýnir að $j : R \to \mathrm{Quot}(R)$ er mótun einbauga. Ef nú $b, d \in R$ og $j(b) = j(d)$, þ.e. $\frac{b}{1} = \frac{d}{1}$, þá fæst $b \cdot 1 = 1 \cdot d$, þ.e. $b = d$. Þetta sýnir að j er eintæk.

Þótt ekki sé það alveg nákvæmur ritháttur þá er vanalega ekki gerður greinarmunur á $b \in R$ og $\frac{b}{1} \in \mathrm{Quot}(R)$ og því litið á R sem hlutbaug í $\mathrm{Quot}(R)$.

Skilgreining: R sé víxlinn heilbaugur. Kroppurinn $\mathrm{Quot}(R)$ er þá nefndur *brotakroppur* R.

Brotakroppur $\mathbf{Z}$ er táknaður með $\mathbf{Q}$. Stökin í $\mathbf{Q}$ eru nefnd *ræðar tölur*.

Ef $a, b \in \mathbf{Z}$, $a \neq 0$, þá er $\frac{-b}{-a} = \frac{b}{a}$, því að $-ba = -ab$. Af þessu leiðir að skrifa má sérhverja ræða tölu á forminu $\frac{b}{a}$ með $a, b \in \mathbf{Z}$, $0 < a$.

Skilgreining: Ræð tala α er sögð vera *jákvæð* ef skrifa má α á forminu $\alpha = \frac{b}{a}$ með $a, b \in \mathbf{Z}$, $0 < a$, $0 < b$.

Setning 7.11: Ef α og β eru jákvæðar ræðar tölur þá eru $\alpha + \beta$ og $\alpha\beta$ líka jákvæðar.
Sönnun: Skrifum $\alpha = \frac{b}{a}$ og $\beta = \frac{d}{c}$ með $a, b, c, d \in \mathbf{Z}$, $0 < a$, $0 < b$, $0 < c$, $0 < d$. Þá gildir $0 < ac$, $0 < bc + ad$ og $0 < bd$. Af því leiðir að $\alpha + \beta = \frac{bc+ad}{ac}$ og $\alpha\beta = \frac{bd}{ac}$ eru jákvæðar.

Setning 7.12: Ef $\alpha \in \mathbf{Q}$ þá gildir eitt og aðeins eitt af þrennu:
(i) α er jákvæð
(ii) $\alpha = 0$
(iii) $-\alpha$ er jákvæð
Sönnun: Skrifum $\alpha = \frac{b}{a}$ með $a, b \in \mathbf{Z}$, $0 < a$. Ef $0 < b$ þá er α jákvæð. Ef $b = 0$ þá er $\alpha = 0$. Og ef $b < 0$ þá $0 < -b$, svo að $-\alpha$ er jákvæð. Nú er 0 ekki jákvæð, því að $\frac{d}{c} = 0 = \frac{0}{1}$ þá og því aðeins að $d = 0$. Því geta (i) og (ii) ekki bæði gilt. Vegna $-0 = 0$ geta þá (iii) og (ii) heldur ekki bæði gilt. Og (i) og (iii) geta ekki bæði gilt, því að ef α og $-\alpha$ væru báðar jákvæðar þá fengist, samkvæmt Setningu 7.11, að $0 = \alpha + (-\alpha)$ væri jákvæð.

Fyrir $b = \frac{b}{1} \in \mathbf{Z}$ fáum við að b er jákvæð þá og því aðeins að $0 < b$, þ.e. $b \in \mathbf{N}$. Af þessu sést að fyrir sérhver $a, b \in \mathbf{Z}$ gildir

$a < b$ þá og því aðeins að $b - a$ sé jákvæð

Við getum því útvíkkað venzlin $<$ og $\leq$ í $\mathbf{Z}$ yfir í $\mathbf{Q}$ með eftirfarandi skilgreiningu.

Skilgreining: Ef $\alpha, \beta \in \mathbf{Q}$ þá setjum við

$\alpha < \beta$ þá og því aðeins að $\beta - \alpha$ sé jákvæð

og

$\alpha \leq \beta$ þá og því aðeins að $\alpha < \beta$ eða $\alpha = \beta$

Næstu tvær setningar sannast nú eins og Setningar 6.26 og 6.28.

Setning 7.13: $\leq$ er línuleg röðun í $\mathbf{Q}$ og $<$ er tilheyrandi ströng röðun í $\mathbf{Q}$.

Setning 7.14: Fyrir sérhver $\alpha, \beta, \gamma \in \mathbf{Q}$ gilda reglurnar
(i) ef $\alpha < \beta$ þá $\alpha + \gamma < \beta + \gamma$
(ii) ef $\alpha < \beta$ og $0 < \gamma$ þá $\alpha\gamma < \beta\gamma$

Nú séu $\alpha, \beta \in \mathbf{Q}$, $0 < \alpha$, $0 < \beta$. Við skrifum $\alpha = \frac{b}{a}$ og $\beta = \frac{d}{c}$ með $a, b, c, d \in \mathbf{N}$. Þá er $1 \leq c$ og $1 \leq b$, svo að $\frac{d}{c} \leq c\frac{d}{c} = d \leq db = da\frac{b}{a}$ samkvæmt Setningu7.14 (ii). Vegna $da \in \mathbf{N}$ höfum við því sannað eftirfarandi setningu.

Setning 7.15: Ef $\alpha, \beta \in \mathbf{Q}$, $0 < \alpha$ og $0 < \beta$, þá er til $m \in \mathbf{N}$ þannig að $\beta \leq m \cdot \alpha$.

Skilyrðið $0 < \beta$ í þessari setningu er að sjálfsögðu óþarft, því að ef $0 < \alpha$ og $\beta \leq 0$ þá $\beta \leq \alpha = 1 \cdot \alpha$.

8 Margfaldar samsetningar

Út frá gefinni samsetningu $\vee$ í mengi M má skilgreina varpanir $\vee_n : M^n \to M$, $n \in \mathbf{N}$, með þrepun á eftirfarandi hátt:

$$\vee_1(x_1) = x_1$$

fyrir öll $x_1 \in M$.

$$\vee_{k+1}(x_1, \ldots, x_{k+1}) = \vee_k(x_1, \ldots, x_k) \vee x_{k+1}$$

fyrir öll $x_1, \ldots, x_{k+1} \in M$.

Ef ekkert tákn er notað fyrir samsetninguna $\vee$ í M þá er venjulega skrifað

$$\prod_{i=1}^{n} x_i$$

í stað $\vee_n(x_1, \ldots, x_n)$. Sömuleiðis ef táknið „$\cdot$“ er notað fyrir samsetninguna. Við höfum þá samkvæmt skilgreiningu

$$\prod_{i=1}^{1} x_i = x_1$$

$$\prod_{i=1}^{k+1} x_i = \left(\prod_{i=1}^{k} x_i \right) x_{k+1}$$

Ef táknið „$+$“ er notað fyrir samsetninguna þá er hinsvegar skrifað

$$\sum_{i=1}^{n} x_i$$

í stað $\vee_n(x_1, \ldots, x_n)$. Við höfum þá

$$\sum_{i=1}^{1} x_i = x_1$$

$$\sum_{i=1}^{k+1} x_i = \left(\sum_{i=1}^{k} x_i \right) + x_{k+1}$$

samkvæmt skilgreiningu.

Ef $l \in \mathbf{Z}$, $n \in \mathbf{N}$ og $x_{l+1}, \ldots, x_{l+n} \in M$ þá er gjarna skrifað $\prod_{i=l+1}^{l+n} x_i$ í stað $\prod_{i=1}^{n} x_{l+i}$ og samsvarandi fyrir $\sum$.

Næsta setning er almenn tengiregla.

Setning 8.1: G sé hálfgrúpa. Fyrir sérhver $m, n \in \mathbf{N}$ og sérhver $x_1, \ldots, x_{m+n} \in G$ gildir þá reglan

$$\prod_{i=1}^{m+n} x_i = \left(\prod_{i=1}^{m} x_i\right)\left(\prod_{i=m+1}^{m+n} x_i\right)$$

Sönnun: Þetta fæst auðveldlega af tengireglunni í G með þrepun yfir n.

Þá kemur almenn víxlregla.

Setning 8.2: G sé víxlin hálfgrúpa. Fyrir sérhvert $n \in \mathbf{N}$, sérhver $x_1, \ldots, x_n \in G$ og sérhverja gagntæka vörpun $\sigma : [\![1, n]\!] \to [\![1, n]\!]$ gildir þá reglan

$$\prod_{i=1}^{n} x_i = \prod_{i=1}^{n} x_{\sigma(i)}$$

Sönnun: Þetta er sannað með þrepun yfir n. Þrepunarbyrjunin er augljós. Með því að nota eftirfarandi hjálparsetningu á tilfellið $n = k + 1$ og $j = \sigma^{-1}(k + 1)$ sést að í þrepunarskrefinu „$n = k \to n = k + 1$“ nægir að sanna fullyrðinguna í tilfellinu $\sigma(k + 1) = k + 1$. En það er auðvelt út frá þrepunarforsendunni.

Hjálparsetning: Ef $\sigma : [\![1, n]\!] \to [\![1, n]\!]$ er gagntæk vörpun og $j \in [\![1, n]\!]$ þá er með

$$\omega(i) = \begin{cases} i + j & \text{ef } 1 \leq i \leq n - j \\ i - (n - j) & \text{ef } n - j + 1 \leq i \leq n \end{cases}$$

skilgreind gagntæk vörpun $\omega : [\![1, n]\!] \to [\![1, n]\!]$ og

$$\prod_{i=1}^{n} x_{\sigma(i)} = \prod_{i=1}^{n} x_{(\sigma\circ\omega)(i)}$$

Sönnun: Ef $j = n$ þá er ω hlutlausa vörpunin og ekkert er að sanna. Gerum því ráð fyrir að $j < n$. Auðvelt er að sjá að ω er gagntæk. Og til þess að sjá að jafnan gildir er nóg að athuga að samkvæmt Setningu 8.1 gildir

$$\prod_{i=1}^{n} x_{\sigma(i)} = \left(\prod_{i=1}^{j} x_{\sigma(i)}\right)\left(\prod_{i=j+1}^{n} x_{\sigma(i)}\right)$$

og

$$\prod_{i=1}^{n} x_{(\sigma\circ\omega)(i)} = \left(\prod_{i=1}^{n-j} x_{(\sigma\circ\omega)(i)}\right)\left(\prod_{i=n-j+1}^{n} x_{(\sigma\circ\omega)(i)}\right)$$

og að samkvæmt skilgreiningu á ω gildir

$$\prod_{i=1}^{n-j} x_{(\sigma\circ\omega)(i)} = \prod_{i=1}^{n-j} x_{\sigma(i+j)} = \prod_{i=j+1}^{n} x_{\sigma(i)}$$

og

$$\prod_{i=n-j+1}^{n} x_{(\sigma\circ\omega)(i)} = \prod_{i=n-j+1}^{n} x_{\sigma(i-(n-j))} = \prod_{i=1}^{j} x_{\sigma(i)}$$

og að vegna víxlreglunnar í G gildir

$$\left(\prod_{i=1}^{j} x_{\sigma(i)}\right)\left(\prod_{i=j+1}^{n} x_{\sigma(i)}\right) = \left(\prod_{i=j+1}^{n} x_{\sigma(i)}\right)\left(\prod_{i=1}^{j} x_{\sigma(i)}\right)$$

G sé víxlin hálfgrúpa og J sé eitthvert endanlegt mengi, $J \neq \emptyset$. Gefin sé fjölskylda $(x_j)_{j\in J}$ af stökum x_j í G. Látum n vera fjölda stakanna í J. Ef $\varphi, \chi : [\![1, n]\!] \to J$ eru gagntækar varpanir þá er vörpunin $\sigma := \varphi^{-1} \circ \chi : [\![1, n]\!] \to [\![1, n]\!]$ líka gagntæk og $\varphi \circ \sigma = \chi$. Samkvæmt Setningu 8.2 gildir því

$$\prod_{i=1}^{n} x_{\varphi(i)} = \prod_{i=1}^{n} x_{\varphi(\sigma(i))} = \prod_{i=1}^{n} x_{\chi(i)}$$

Við getum því skilgreint samsetningu stakanna x_j, $j \in J$, með því að setja

$$\prod_{j\in J} x_j = \prod_{i=1}^{n} x_{\varphi(i)}$$

ef $\varphi : [\![1, n]\!] \to J$ er gagntæk vörpun.

Nú séu J_1 og J_2 sundurlæg endanleg mengi, hvorugt þeirra tómt, þannig að $J = J_1 \cup J_2$. Ef $\varphi_1 : [\![1, n_1]\!] \to J_1$ og $\varphi_2 : [\![1, n_2]\!] \to J_2$ eru gagntækar varpanir þá er með

$$\varphi(i) = \begin{cases} \varphi_1(i) & \text{ef } 1 \leq i \leq n_1 \\ \varphi_2(i - n_1) & \text{ef } n_1 + 1 \leq i \leq n_1 + n_2 \end{cases}$$

skilgreind gagntæk vörpun $\varphi : [\![1, n_1 + n_2]\!] \to J$. Af Setningu 8.1 leiðir því að

$$\prod_{j\in J} x_j = \left(\prod_{j\in J_1} x_j\right)\left(\prod_{j\in J_2} x_j\right)$$

Af þessari reglu fæst svo eftirfarandi setning með þrepun yfir fjölda stakanna í $\mathcal{C}$.

Setning 8.3: G sé víxlin hálfgrúpa. J sé endanlegt mengi, $J \neq \emptyset$, og $\mathcal{C}$ sé deildamengi af J. Fyrir sérhverja fjölskyldu $(x_j)_{j\in J}$ af stökum x_j í G gildir þá reglan

$$\prod_{j\in J} x_j = \prod_{C\in\mathcal{C}} \left(\prod_{j\in C} x_j \right)$$

Ef $m, n \in \mathbf{N}$ þá getum við skrifað $[\![1,n]\!]\times[\![1,m]\!]$ sem sammengi mengjanna $[\![1,n]\!] \times \{j\}$, $j \in [\![1,m]\!]$, en líka sem sammengi mengjanna $\{i\} \times [\![1,m]\!]$, $i \in [\![1,n]\!]$. Af Setningu 8.3 leiðir því að í víxlinni hálfgrúpu G gildir reglan

$$\prod_{i=1}^{n} \left(\prod_{j=1}^{m} x_{ij} \right) = \prod_{j=1}^{m} \left(\prod_{i=1}^{n} x_{ij} \right)$$

Að lokum koma svo almennar dreifireglur.

Setning 8.4: R sé baugur. J sé endanlegt mengi, $J \neq \emptyset$. Fyrir sérhverja fjölskyldu $(x_j)_{j\in J}$ af stökum x_j í R og sérhvert stak $y \in R$ gilda þá reglurnar

$$y \left(\sum_{j\in J} x_j \right) = \sum_{j\in J} y x_j$$

$$\left(\sum_{j\in J} x_j \right) y = \sum_{j\in J} x_j y$$

Sönnun með þrepun yfir fjölda stakanna í J.

9 Raðaðar grúpur

Í þessum kafla táknar $\mathcal{T}$ mengi allra þeirra hlutmengja í $\mathbf{Q}$ sem eru ekki tóm og eru takmörkuð að neðan í $\mathbf{Q}$. Ef $A \subseteq \mathbf{Q}$ þá táknum við mengi allra neðri marka fyrir A í $\mathbf{Q}$ með $U(A)$. Svo að $A \in \mathcal{T}$ þá og því aðeins að $A \neq \emptyset$ og $U(A) \neq \emptyset$.

Fyrir $A, B \in \mathcal{T}$ setjum við

$A \sim B$ þá og því aðeins að $U(A) = U(B)$

Með þessu eru augljóslega skilgreind jafngildisvenzl $\sim$ í $\mathcal{T}$. Jafngildisflokkarnir eru nefndir *rauntölur* og mengi allra rauntalna, þ.e. deildamengið $\mathcal{T}/\!\sim$, er táknað með $\mathbf{R}$. Jafngildisflokk $A \in \mathcal{T}$ táknum við með $\inf A$. Við höfum þá

$$\mathbf{R} = \{\, \inf A \mid A \in \mathcal{T} \,\}$$

og fyrir sérhver $A, B \in \mathcal{T}$ gildir

$\inf A = \inf B$ þá og því aðeins að $U(A) = U(B)$

Við getum nú greinilega skilgreint röðun $\leq$ í $\mathbf{R}$ með því að setja

$\inf A \leq \inf B$ þá og því aðeins að $U(A) \subseteq U(B)$

fyrir sérhver $A, B \in \mathcal{T}$.

Ef $A, B \in \mathcal{T}$ og ekki $\inf A \leq \inf B$ þá er til $x \in U(A)$ þannig að $x \notin U(B)$, þ.e. $x \leq a$ fyrir öll $a \in A$ en til $b \in B$ með $b < x$. En fyrir sérhvert $y \in U(B)$ fæst þá $y \leq b < x \leq a$ fyrir öll $a \in A$, svo að $y \in U(A)$. Þetta sýnir að $U(B) \subseteq U(A)$, þ.e. $\inf B \leq \inf A$. Við höfum þar með sannað eftirfarandi setningu.

Setning 9.1: $\leq$ er línuleg röðun í $\mathbf{R}$.

Þessa röðun í $\mathbf{R}$ mætti kalla venjulega röðun í $\mathbf{R}$ og þegar við ræðum um röðun í $\mathbf{R}$ eigum við við þessa röðun nema annað sé tekið fram. Tilheyrandi stranga röðun í $\mathbf{R}$ táknum við að sjálfsögðu með $<$.

Setning 9.2: Sérhvert hlutmengi í $\mathbf{R}$, sem er ekki tómt og er takmarkað að neðan í $\mathbf{R}$, hefur stærstu neðri mörk í $\mathbf{R}$.

Sönnun: Gefið sé hlutmengi $\mathcal{A}$ í $\mathbf{R}$ sem er ekki tómt og er takmarkað að neðan í $\mathbf{R}$. Fyrir sérhvert $\alpha \in \mathcal{A}$ veljum við okkur $A_\alpha \in \mathcal{T}$ þannig að $\alpha = \inf A_\alpha$ og setjum svo $B = \bigcup_{\alpha \in \mathcal{A}} A_\alpha$. Þar sem $\mathcal{A}$ er ekki tómt og sérhvert A_α, $\alpha \in \mathcal{A}$, er ekki tómt þá er B ekki tómt.

Ef $\xi \in \mathbf{R}$ eru neðri mörk fyrir $\mathcal{A}$, $\xi = \inf X$ með $X \in \mathcal{T}$, þá gildir $U(X) \subseteq U(A_\alpha)$ fyrir sérhvert $\alpha \in \mathcal{A}$, þar með $U(X) \subseteq U(B)$. Þar sem

$U(X) \neq \emptyset$ þá er þar með $U(B) \neq \emptyset$, svo að $B \in \mathcal{T}$. Við setjum $\beta = \inf B$. Af ofansögðu leiðir þá að fyrir sérhver neðri mörk ξ fyrir $\mathcal{A}$ í $\mathbf{R}$ gildir $\xi \leq \beta$.

Nú gildir greinilega $U(B) \subseteq U(A_\alpha)$ fyrir sérhvert $\alpha \in \mathcal{A}$, þ.e. $\beta \leq \alpha$ fyrir sérhvert $\alpha \in \mathcal{A}$, svo að β eru neðri mörk fyrir $\mathcal{A}$ í $\mathbf{R}$.

Ef $r \in \mathbf{Q}$ þá setjum við $\underline{r} = \inf\{r\} \in \mathbf{R}$. Með $i : r \mapsto \underline{r}$ er þá skilgreind vörpun $i : \mathbf{Q} \to \mathbf{R}$.

Ef nú $r, s \in \mathbf{Q}$, $r < s$, þá er greinilega $s \in U(\{s\})$ en $s \notin U(\{r\})$, svo að ekki gildir $\underline{s} \leq \underline{r}$. Þetta sýnir að fyrir sérhver $r, s \in \mathbf{Q}$ gildir

ef $r < s$ þá $\underline{r} < \underline{s}$

Sér í lagi er vörpunin i eintæk.

Nú sé $A \in \mathcal{T}$. Þá gildir greinilega $U(A) \subseteq U(\{a\})$ fyrir sérhvert $a \in A$, svo að $\inf A \leq \underline{a}$ fyrir sérhvert $a \in A$. $\inf A$ eru því neðri mörk fyrir hlutmengið $\{\, \underline{a} \,|\, a \in A \,\}$ í $\mathbf{R}$. En ef $\beta \in \mathbf{R}$, $\beta = \inf B$ með $B \in \mathcal{T}$, eru einhver neðri mörk fyrir þetta hlutmengi í $\mathbf{R}$ þá er $U(B) \subseteq U(\{a\})$ fyrir sérhvert $a \in A$, þar með $U(B) \subseteq U(A)$, svo að $\beta \leq \inf A$. Þetta sýnir að $\inf A$ eru stærstu neðri mörk fyrir hlutmengið $\{\, \underline{a} \,|\, a \in A \,\}$ í $\mathbf{R}$.

Fyrir sérhver $A, B \in \mathcal{T}$ setjum við nú

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

Þar sem A og B eru ekki tóm þá er $A + B$ ekki tómt. Og ef x eru neðri mörk fyrir A í $\mathbf{Q}$ og y eru neðri mörk fyrir B í $\mathbf{Q}$ þá eru $x + y$ greinilega neðri mörk fyrir $A + B$ í $\mathbf{Q}$. Því fæst að $A + B \in \mathcal{T}$. Nú er augljóslega $(A + B) + C = A + (B + C)$, $A + B = B + A$ og $A + \{0\} = A$ fyrir sérhver $A, B, C \in \mathcal{T}$, svo að $(\mathcal{T}, +)$ er víxlin hálfgrúpa með hlutleysu $\{0\}$.

Fyrir sérhver $A, B, C \in \mathcal{T}$ gildir nú reglan

ef $U(A) \subseteq U(B)$ þá $U(A + C) \subseteq U(B + C)$

Það sést af eftirfarandi: Ef til væri $x \in U(A+C)$ með $x \notin U(B+C)$ þá gilti $x \leq a + c$ fyrir sérhvert $a \in A$ og sérhvert $c \in C$ en til væru $b \in B$ og $c \in C$ með $b + c < x$. En þá fengist $b < x - c \leq a$ fyrir sérhvert $a \in A$, svo að $x - c \in U(A)$ en $x - c \notin U(B)$.

Nú séu gefin $A, B, A', B' \in \mathcal{T}$ þannig að $U(A) = U(A')$ og $U(B) = U(B')$. Af reglunni hér að ofan leiðir þá að $U(A + B) = U(A' + B)$ og $U(A' + B) = U(A' + B')$, svo að $U(A + B) = U(A' + B')$. Af þessu leiðir að $\mathbf{R}$ er deildahálfgrúpa af $(\mathcal{T}, +)$, þ.e. við getum skilgreint samlagningu $+$ í $\mathbf{R}$ með því að setja

$$\inf A + \inf B = \inf(A + B)$$

fyrir sérhver $A, B \in \mathcal{T}$, og $(\mathbf{R}, +)$ er þá hálfgrúpa. Þar sem $(\mathcal{T}, +)$ er víxlin með hlutleysu $\{0\}$ þá er $(\mathbf{R}, +)$ líka víxlin með hlutleysu $\inf\{0\}$.

Setning 9.3: $(\mathbf{R}, +)$ er víxlin grúpa.

Sönnun: Við eigum aðeins eftir að sýna að sérhvert $\alpha \in \mathbf{R}$ hafi andhverfu í $(\mathbf{R}, +)$. Skrifum $\alpha = \inf A$ með $A \in \mathcal{T}$ og setjum $B = \{ -x \,|\, x \in U(A) \}$. Þá er $B \neq \emptyset$, því að $U(A) \neq \emptyset$. Og ef $a \in A$ þá gildir $x \leq a$ fyrir sérhvert $x \in U(A)$, þar með $-a \leq -x$ fyrir sérhvert $x \in U(A)$, svo að $-a$ eru neðri mörk fyrir B. Við höfum því $B \in \mathcal{T}$ og setjum $= \inf B$. Við viljum sýna að β sé andhverfa fyrir α í $(\mathbf{R}, +)$, þ.e. að $U(A + B) = U(\{0\})$.

Ef $a \in A$ og $b \in B$ þá er $-b \in U(A)$, svo að $-b \leq a$, þ.e. $0 \leq a + b$. Þetta sýnir að $0 \in U(A + B)$ og af því leiðir augljóslega að $U(\{0\}) \subseteq U(A + B)$. Gerum nú ráð fyrir að til væri $y \in U(A + B)$ þannig að $y \notin U(\{0\})$, þ.e. þannig að $0 < y$. Af $y \in U(A + B)$ fengist að $y \leq a - x$, þ.e. $y + x \leq a$, fyrir sérvert $a \in A$ og sérhvert $x \in U(A)$. Það þýddi að ef $x \in U(A)$ þá líka $y + x \in U(A)$. Með þrepun yfir n fengist að ef $x \in U(A)$ og $n \in \mathbf{N}$ þá $ny + x \in U(A)$. En ef $a \in A$ og $x \in U(A)$ þá er, samkvæmt Setningu 7.15, til $m \in \mathbf{N}$ með $a - x \leq my$ og þar með $a - x < (m+1)y$, svo að $a < (m+1)y + x$ og því $(m + 1)y + x \notin U(A)$. Því hlýtur $U(A + B) \subseteq U(\{0\})$.

Ef $r, s \in \mathbf{Q}$ þá er $\{r\} + \{s\} = \{r + s\}$. Það sýnir að fyrir öll $r, s \in \mathbf{Q}$ gildir $\underline{r + s} = \underline{r} + \underline{s}$

Setning 9.4: Fyrir sérhver $\alpha, \beta, \gamma \in \mathbf{R}$ gildir reglan
ef $\alpha \leq \beta$ þá $\alpha + \gamma \leq \beta + \gamma$
Sönnun: Þetta er ekkert annað en reglan
ef $U(A) \subseteq U(B)$ þá $U(A + C) \subseteq U(B + C)$
sem var sönnuð hér að framan.

Skilgreining: *Röðuð grúpa* er víxlin grúpa $(M, +)$ ásamt línulegri röðun $\leq$ í M þannig að fyrir sérhver $x, y, z \in M$ gildi
ef $x \leq y$ þá $x + z \leq y + z$

Reyndar væri nákvæmara að skilgreina raðaða grúpu sem þrennd $(M, +, \leq)$. Við munum þó ekki vera svo nákvæm heldur munum við þvert á móti leyfa okkur að tala einfaldlega um „raðaða grúpu M“. Ströngu röðunina í M sem tilheyrir röðuninni $\leq$ í M munum við tákna með $<$. Í stað $x \leq y$ munum við stundum skrifa $y \geq x$ og $y > x$ í stað $x < y$.

Samkvæmt fyrri setningum þá eru $\mathbf{Z}$, $\mathbf{Q}$ og $\mathbf{R}$ raðaðar grúpur.

Setning 9.5: M sé röðuð grúpa. Fyrir sérhver $x, y, z, w \in M$ gilda þá reglurnar
(i) ef $x < y$ þá $x + z < y + z$
(ii) ef $x < y$ og $z < w$ þá $x + z < y + w$
(iii) ef $x < y$ þá $-y < -x$
(iv) ef $x < y$ og $n \in \mathbf{N}$ þá $n \cdot x < n \cdot y$

Sönnun: Heimaverkefni.

Þar sem röðunin í raðaðri grúpu er línuleg þá fæst af síðasta lið setningarinnar að fyrir sérhver $x, y \in M$ gildir

ef $n \in \mathbf{N}$ og $n \cdot x \leq n \cdot y$ þá $x \leq y$

Ennfremur fæst að ef $a \in M$, $a > 0$, þá gildir fyrir sérhver $m, n \in \mathbf{Z}$ að

$m \cdot a \leq n \cdot a$ þá og því aðeins að $m \leq n$

Skilgreining: M og N séu raðaðar grúpur og $f : M \to N$ sé grúpumótun. Við segjum að f sé *stefnd* ef fyrir sérhver $x_1, x_2 \in M$ gildir

ef $x_1 \leq x_2$ þá $f(x_1) \leq f(x_2)$

eða ef fyrir sérhver $x_1, x_2 \in M$ gildir

ef $x_1 \leq x_2$ þá $f(x_1) \geq f(x_2)$

Við segjum að f sé *strangt vaxandi* ef fyrir sérhver $x_1, x_2 \in M$ gildir

ef $x_1 < x_2$ þá $f(x_1) < f(x_2)$

Ef M er röðuð grúpa og $a \in M$ þá er vörpunin $f : \mathbf{Z} \to M$, $n \mapsto n \cdot a$, stefnd mótun raðaðra grúpna.

Vörpunin $i : \mathbf{Q} \to \mathbf{R}$, $r \mapsto \underline{r}$, er strangt vaxandi mótun raðaðra grúpna.

Skilgreining: Röðuð grúpa M er sögð vera *arkimedískt röðuð* ef fyrir sérhvert $a \in M$, $a > 0$, og sérhvert $x \in M$ er til $n \in \mathbf{N}$ þannig að $x \leq n \cdot a$.

Samkvæmt Setningu 7.15 er $\mathbf{Q}$ arkimedískt röðuð grúpa.

Setning 9.6: $\mathbf{R}$ er arkimedískt röðuð grúpa.
Sönnun: Gefið sé $\alpha \in \mathbf{R}$, $\alpha > \underline{0}$. Við setjum

$$\mathcal{A} = \{\, \xi \in \mathbf{R} \mid n \cdot \alpha < \xi \text{ fyrir öll } n \in \mathbf{N} \,\}$$

Þá er $\mathcal{A}$ greinilega takmarkað að neðan í $\mathbf{R}$. Gerum ráð fyrir að $\mathcal{A} \neq \emptyset$. Þá hefði $\mathcal{A}$ samkvæmt Setningu 9.2 stærstu neðri mörk η. Vegna $\eta - \alpha < \eta$ þá væri $\eta - \alpha \notin \mathcal{A}$. Það væri því til $m \in \mathbf{N}$ með $\eta - \alpha \leq m \cdot \alpha$, þ.e. $\eta \leq (m+1) \cdot \alpha$. Vegna $\eta < \eta + \alpha$ væru $\eta + \alpha$ ekki neðri mörk fyrir $\mathcal{A}$. Það væri því til $\xi \in \mathcal{A}$ með $\xi < \eta + \alpha$. En þá fengist $\xi < (m+1) \cdot \alpha + \alpha = (m+2) \cdot \alpha$ í mótsögn við skilgreinguna á $\mathcal{A}$. Því hlýtur $\mathcal{A} = \emptyset$. En það þýðir að fyrir sérhvert $\xi \in \mathbf{R}$ er til $n \in \mathbf{N}$ með $\xi \leq n \cdot \alpha$.

Ef M er arkimedískt röðuð grúpa, $a \in M$, $a > 0$, og $z \in M$ þá er samkvæmt skilgreiningu til $k \in \mathbf{N}$ með $z \leq k \cdot a$. Vegna $a > 0$ fæst þá að $z < (k+1) \cdot a$. Þetta sýnir að mengið $Q = \{\, h \in \mathbf{Z} \mid z < h \cdot a \,\}$ er ekki tómt. Nú er líka til $l \in \mathbf{N}$ með $-z \leq l \cdot a$. En þá er $-l \cdot a \leq z$. Og ef $h \leq -l$ þá fæst $h \cdot a \leq -l \cdot a \leq z$. Þetta sýnir að Q er takmarkað að neðan í $\mathbf{Z}$. Það er

því til minnsta stak n í Q, þ.e. $n \in \mathbf{Z}$ þannig að $z < n \cdot a$ en $(n-1) \cdot a < z$. Það þýðir að $z < n \cdot a \leq z + a$.

Setning 9.7: M sé arkimedískt röðuð grúpa og $a \in M$, $a > 0$. Gefin séu $x, y \in M$ með $x < y$. Þá eru til $m \in \mathbf{N}$ og $n \in \mathbf{Z}$ þannig að $m \cdot x < n \cdot a < m \cdot y$.
Sönnun: Af $x < y$ leiðir að $y - x > 0$, svo að til er $m \in \mathbf{N}$ með $a < m \cdot (y - x)$, þ.e. $m \cdot x + a < m \cdot y$. Og samkvæmt ofansögðu er til $n \in \mathbf{Z}$ með $m \cdot x < n \cdot a \leq m \cdot x + a$.

Nú séu $\xi, \eta \in \mathbf{R}$, $\xi < \eta$. Þar sem $\mathbf{R}$ er arkimedískt röðuð grúpa og $\underline{1} > \underline{0}$ þá leiðir af Setningu 9.7 að til eru $m \in \mathbf{N}$ og $n \in \mathbf{Z}$ með $m \cdot \xi < n \cdot \underline{1} < m \cdot \eta$. Ef við setjum nú $r = \frac{n}{m}$ þá er $m \cdot r = n$, svo að við fáum $m \cdot \xi < m \cdot \underline{r} < m \cdot \eta$. Þar sem $m \in \mathbf{N}$ þá fæst af þessu eftirfarandi setning.

Setning 9.8: Ef $\xi, \eta \in \mathbf{R}$, $\xi < \eta$, þá er til $r \in \mathbf{Q}$ þannig að $\xi < \underline{r} < \eta$.

M sé enn arkimedískt röðuð grúpa og $a \in M$, $a > 0$. Fyrir sérhvert $x \in M$ setjum við

$$F(x) = \{\, \frac{n}{m} \,|\, m \in \mathbf{N}, n \in \mathbf{Z} \text{ og } m \cdot x \leq n \cdot a \,\}$$

Þar sem til er $n \in \mathbf{N}$ með $x \leq n \cdot a$, þ.e. $\frac{n}{1} \in F(x)$, þá er $F(x) \neq \emptyset$. Nú séu gefin $k \in \mathbf{N}$ og $l \in \mathbf{Z}$.

Gerum fyrst ráð fyrir að $l \cdot a \leq k \cdot x$. Ef $m \in \mathbf{N}$ og $n \in \mathbf{Z}$ þannig að $m \cdot x \leq n \cdot a$ þá fæst að $ml \cdot a \leq mk \cdot x = km \cdot x \leq kn \cdot a$, þar með $ml \leq kn$, þ.e. $\frac{l}{k} \leq \frac{n}{m}$. Þetta þýðir að $\frac{l}{k} \in U(F(x))$.

Gerum þá ráð fyrir að $k \cdot x < l \cdot a$. Samkvæmt Setningu 9.7 eru þá til $m \in \mathbf{N}$ og $n \in \mathbf{Z}$ þannig að $mk \cdot x < n \cdot a < ml \cdot a$. En af því leiðir að $\frac{n}{mk} \in F(x)$ og að $n < ml$, þar með $\frac{n}{mk} < \frac{l}{k}$. Það sýnir að $\frac{l}{k} \notin U(F(x))$.

Við fáum að $\frac{l}{k} \in U(F(x))$ þá og því aðeins að $l \cdot a \leq k \cdot x$. En $l \cdot a \leq k \cdot x$ jafngildir $k \cdot (-x) \leq -l \cdot a$, þ.e.a.s. $-\frac{l}{k} \in F(-x)$. Við höfum því sýnt að

$$F(-x) = \{\, -r \,|\, r \in U(F(x)) \,\}$$

Þar sem $F(-x) \neq \emptyset$ þá fæst sér í lagi að $U(F(x)) \neq \emptyset$, þ.e. $F(x)$ er takmarkað að neðan í $\mathbf{Q}$.

Af þessu sést að við getum skilgreint vörpun $f : M \to \mathbf{R}$ með því að setja

$$f(x) = \inf F(x)$$

fyrir sérhvert $x \in M$.

Af ofansögðu fæst þá að fyrir sérhvert $x \in M$ gildir

$$f(-x) = -f(x)$$

Nú séu $x, y \in M$ og $x < y$. Samkvæmt Setningu 9.7 eru til $m \in \mathbf{N}$ og $n \in \mathbf{Z}$ þannig að $m \cdot x < n \cdot a < m \cdot y$. Af því leiðir að $\frac{n}{m} \notin U(F(x))$ en $\frac{n}{m} \in U(F(y))$, svo að ekki gildir $U(F(y)) \subseteq U(F(x))$, þ.e. ekki gildir $\inf F(y) \leq \inf F(x)$. Því fæst að fyrir sérhver $x, y \in M$ gildir

$$\text{ef } x < y \text{ þá } f(x) < f(y)$$

Þá séu aftur $x, y \in M$. Gefin séu $m, k \in \mathbf{N}$ og $n, l \in \mathbf{Z}$ þannig að $m \cdot x \leq n \cdot a$ og $k \cdot y \leq l \cdot a$. Þá fæst $mk \cdot x = km \cdot x \leq kn \cdot a = nk \cdot a$ og $mk \cdot y \leq ml \cdot a$, þar með $mk \cdot (x + y) = mk \cdot x + mk \cdot y \leq nk \cdot a + ml \cdot a = (nk + ml) \cdot a$. Það þýðir að $\frac{n}{m} + \frac{l}{k} = \frac{nk+ml}{mk} \in F(x+y)$. Þetta sýnir að $F(x) + F(y) \subseteq F(x+y)$. Af því leiðir svo að $U(F(x+y)) \subseteq U(F(x) + F(y))$, svo að $\inf F(x+y) \leq \inf(F(x)+F(y)) = \inf F(x) + \inf F(y)$. Við fáum því að fyrir sérhver $x, y \in M$ gildir

$$f(x + y) \leq f(x) + f(y)$$

En þá gildir líka $f(y) = f(-x+x+y) \leq f(-x)+f(x+y) = -f(x)+f(x+y)$ og þar með

$$f(x) + f(y) \leq f(x + y)$$

Við höfum því sýnt fram á að f er strangt vaxandi mótun grúpna. Fyrir $k \in \mathbf{N}$ og $l \in \mathbf{Z}$ gildir nú $l \cdot a \leq k \cdot a$ þá og því aðeins að $l \leq k$, þ.e. $\frac{l}{k} \leq 1$. Af því leiðir að $U(F(a)) = U(\{1\})$, svo að $\inf F(a) = \inf\{1\} = \underline{1}$, þ.e.

$$f(a) = \underline{1}$$

Nú sé $g : M \to \mathbf{R}$ einhver stefnd mótun grúpna þannig að $g(a) = 1$. Þar sem ekki gildir $\underline{1} \leq \underline{0}$ hlýtur þá að gilda $g(x) \leq g(y)$ ef $x \leq y$. Nú sé $x \in M$. Ef $m \in \mathbf{N}$ og $n \in \mathbf{Z}$ þannig að $m \cdot x \leq n \cdot a$ þá fæst að $m \cdot g(x) = g(m \cdot x) \leq g(n \cdot a) = n \cdot g(a) = n \cdot \underline{1}$, þar með $g(x) \leq \frac{n}{m}$. Þetta sýnir að $g(x)$ eru neðri mörk fyrir hlutmengið $\{\, \underline{r} \,|\, r \in F(x) \,\}$ í $\overline{\mathbf{R}}$, svo að $g(x) \leq \inf F(x)$. Við fáum því að fyrir sérhvert $x \in M$ gildir

$$g(x) \leq f(x)$$

En þá gildir líka $-g(x) = g(-x) \leq f(-x) = -f(x)$ og þar með

$$f(x) \leq g(x)$$

Við höfum því sýnt fram á að $g = f$.

Með þessu höfum við sannað eftirfarandi setningu.

Setning 9.9: *M sé arkimedískt röðuð grúpa og $a \in M$, $a > 0$. Þá er til ein og aðeins ein stefnd mótun grúpna $f : M \to \mathbf{R}$ þannig að $f(a) = \underline{1}$. Þessi mótun er strangt vaxandi, sér í lagi eintæk.*

Með því að nota Setningu 9.9 á $\mathbf{R}$ fáum við fyrir sérhvert $a \in \mathbf{R}$, $a > \underline{0}$, ótvírætt ákvarðaða stefnda mótun raðaðra grúpna $\delta_a : \mathbf{R} \to \mathbf{R}$ þannig að $\delta_a(a) = \underline{1}$. Greinilega hlýtur $\delta_{\underline{1}} = \mathrm{id}_{\mathbf{R}}$.

Nú sé $a \in \mathbf{R}$, $a > \underline{0}$. Setjum $b = \delta_a(\underline{1})$. Þar sem $\underline{1} > \underline{0}$ og δ_a er strangt vaxandi þá er $b > \underline{0}$. En þá er $\delta_b \circ \delta_a : \mathbf{R} \to \mathbf{R}$ stefnd mótun raðaðra grúpna og $(\delta_b \circ \delta_a)(\underline{1}) = \delta_b(b) = \underline{1}$. Því hlýtur $\delta_b \circ \delta_a = \delta_{\underline{1}} = \mathrm{id}_{\mathbf{R}}$. Af því leiðir að δ_b er átæk. Þar sem δ_b er strangt vaxandi þá er δ_b þar með gagntæk. Vegna $\delta_b \circ \delta_a = \mathrm{id}_{\mathbf{R}}$ hlýtur þá $\delta_a = {\delta_b}^{-1}$. Þar með er δ_a líka gagntæk og ${\delta_a}^{-1} = \delta_b$, sér í lagi $\delta_b(\underline{1}) = a$. Þá sé $\varepsilon : \mathbf{R} \to \mathbf{R}$ einhver stefnd mótun raðaðra grúpna þannig að $\varepsilon(\underline{1}) = a$. Grúpumótunin $\delta_a \circ \varepsilon : \mathbf{R} \to \mathbf{R}$ er þá líka stefnd og $(\delta_a \circ \varepsilon)(\underline{1}) = \delta_a(a) = \underline{1}$. Af því leiðir að $\delta_a \circ \varepsilon = \mathrm{id}_{\mathbf{R}}$ og þar með $\varepsilon = {\delta_a}^{-1} = \delta_b$.

Við höfum með þessu sýnt að fyrir sérhvert $a \in \mathbf{R}$, $a > \underline{0}$, er til ein og aðeins ein stefnd mótun raðaðra grúpna $\mu_a : \mathbf{R} \to \mathbf{R}$ þannig að $\mu_a(\underline{1}) = a$. Auk þess að μ_a er strangt vaxandi og gagntæk.

Setning 9.10: Fyrir sérhvert $a \in \mathbf{R}$ er til ein og aðeins ein stefnd mótun raðaðra grúpna $\mu_a : \mathbf{R} \to \mathbf{R}$ þannig að $\mu_a(\underline{1}) = a$. Ef $a \neq \underline{0}$ þá er μ_a gagntæk.
Sönnun: Samkvæmt ofansögðu þá er þetta rétt fyrir $a > \underline{0}$. Ef $\nu : \mathbf{R} \to \mathbf{R}$ er mótun grúpna þá er með $x \mapsto -\nu(x)$ skilgreind grúpumótun $-\nu : \mathbf{R} \to \mathbf{R}$. Bersýnilega er ν stefnd þá og því aðeins að $-\nu$ sé stefnd, $\nu(\underline{1}) = a$ þá og því aðeins að $(-\nu)(\underline{1}) = -a$, og ν gagntæk þá og því aðeins að $-\nu$ sé gagntæk. Af þessu sést að setningin er líka rétt fyrir $a < \underline{0}$ og að $\mu_{-a} = -\mu_a$.

Við skilgreinum nú $\mu_{\underline{0}} : \mathbf{R} \to \mathbf{R}$ með því að setja $\mu_{\underline{0}}(x) = \underline{0}$ fyrir öll $x \in \mathbf{R}$. Þá er $\mu_{\underline{0}}$ augljóslega stefnd mótun raðaðra grúpna og $\mu_{\underline{0}}(\underline{1}) = \underline{0}$. Þá sé $\nu : \mathbf{R} \to \mathbf{R}$ einhver stefnd mótun raðaðra grúpna þannig að $\nu(\underline{1}) = \underline{0}$. Gerum ráð fyrir að til væri $b \in \mathbf{R}$ með $\nu(b) \neq \underline{0}$ og setjum $c = \nu(b)$. Þá væri $\nu \circ \mu_b : \mathbf{R} \to \mathbf{R}$ stefnd mótun raðaðra grúpna og $(\nu \circ \mu_b)(\underline{1}) = \nu(b) = c$. Þar sem $c \neq \underline{0}$ þá hlyti því $\nu \circ \mu_b = \mu_c$ samkvæmt því sem þegar var sannað. En þar sem μ_b og μ_c eru gagntækar þá fengist þar með að ν væri gagntæk, í mótsögn við að $\nu(\underline{1}) = \underline{0}$. Því hlýtur $\nu = \mu_{\underline{0}}$.

Við skilgreinum nú margföldun í $\mathbf{R}$ með því að setja
$$ba = \mu_a(b)$$
fyrir sérhver $a, b \in \mathbf{R}$.

Þar sem μ_a er strangt vaxandi ef $a > \underline{0}$ þá gildir eftirfarandi setning.

Setning 9.11: Fyrir sérhver $a, b, c \in \mathbf{R}$ gildir reglan
ef $b < c$ og $a > \underline{0}$ þá $ba < ca$

Það að sérhvert μ_a, $a \in \mathbf{R}$, sé grúpumótun þýðir að fyrir sérhver $a, b, c \in \mathbf{R}$ gildir

$$(b+c)a = ba + ca$$

Ennfremur fæst að $\underline{0}a = \underline{0}$ og $(-b)a = -(ba)$. Og út frá skilgreiningu okkar á μ_a fyrir $a \leq \underline{0}$ fæst að $b(-a) = -(ba)$ og $b\underline{0} = \underline{0}$. Það að fyrir sérhvert $a \in \mathbf{R}$ gildir $\mu_a(\underline{1}) = a$ þýðir að

$$\underline{1}a = a$$

Og þar sem $\mathrm{id}_{\mathbf{R}} : \mathbf{R} \to \mathbf{R}$ er stefnd mótun raðaðra grúpna og $\mathrm{id}_{\mathbf{R}}(\underline{1}) = \underline{1}$ þá er $\mu_{\underline{1}} = \mathrm{id}_{\mathbf{R}}$. Það þýðir að fyrir sérhvert $a \in \mathbf{R}$ gildir

$$a\underline{1} = a$$

Ef nú $a, b \in \mathbf{R}$ þá er $\mu_a \circ \mu_b : \mathbf{R} \to \mathbf{R}$ stefnd mótun raðaðra grúpna og $(\mu_a \circ \mu_b)(\underline{1}) = \mu_a(b) = ba$. Af því leiðir að $\mu_a \circ \mu_b = \mu_{ba}$. En það þýðir að fyrir sérhvert $c \in \mathbf{R}$ gildir

$$(cb)a = c(ba)$$

Til að sanna að $\mathbf{R}$ sé einbaugur eigum við nú aðeins eftir að sýna að fyrir sérhver $a, b, c \in \mathbf{R}$ gildi

$$a(b+c) = ab + ac$$

Það gerum við nú:

(i) Ef $b \geq \underline{0}$ og $c \geq \underline{0}$ þá skoðum við grúpumótunina $\nu : \mathbf{R} \to \mathbf{R}$, sem skilgreind er með því að setja $\nu(x) = \mu_b(x) + \mu_c(x)$ fyrir öll $x \in \mathbf{R}$. Þar sem μ_b er strangt vaxandi ef $b > \underline{0}$ og $\mu_b(x) = \underline{0}$ fyrir öll $x \in \mathbf{R}$ ef $b = \underline{0}$ þá gildir að $\mu_b(x) \leq \mu_b(y)$ ef $x \leq y$. Sama regla gildir fyrir μ_c. En þá gildir hún líka fyrir ν, svo að ν er stefnd. Vegna $\nu(\underline{1}) = \mu_b(\underline{1}) + \mu_c(\underline{1}) = b + c$ þá hlýtur því $\nu = \mu_{b+c}$, sér í lagi $\nu(a) = \mu_{b+c}(a)$. En það þýðir að $ab + ac = a(b+c)$.

(ii) Ef $b \leq \underline{0}$ og $c \leq \underline{0}$ þá fæst af (i) að $a(-(b+c)) = a((-b)+(-c)) = a(-b) + a(-c)$. Af því leiðir að $a(b+c) = ab + ac$.

(iii) Þá sé $b \geq \underline{0}$ og $c \leq \underline{0}$. Ef $b+c \geq \underline{0}$ þá fæst af (i) að $ab = a((b+c)+(-c)) = a(b+c)+a(-c)$. Af því leiðir að $a(b+c) = ab+ac$. Ef $b+c \leq \underline{0}$ þá fæst af (ii) að $ac = a((-b)+(b+c)) = a(-b)+a(b+c)$. Af því leiðir að $a(b+c) = ab+ac$.

(iv) Með tilfellið $b \leq \underline{0}$ og $c \geq \underline{0}$ er farið á sama hátt og (iii).

Regluna, sem við vorum að sanna, má líka orða þannig að fyrir sérhvert $a \in \mathbf{R}$ sé vörpunin $\lambda_a : \mathbf{R} \to \mathbf{R}$, sem skilgreind er með því að setja

$$\lambda_a(x) = ax$$

fyrir öll $x \in \mathbf{R}$, mótun grúpna. Við viljum nú sýna að grúpumótanirnar λ_a, $a \in \mathbf{R}$, séu stefndar. Þar sem $\lambda_{-a}(x) = (-a)x = -(ax) = -\lambda_a(x)$ og $\lambda_{\underline{0}}(x) = \underline{0}x = \underline{0}$ fyrir öll $x \in \mathbf{R}$ þá nægir að sanna þetta fyrir $a > \underline{0}$. En það þýðir að við þurfum að sýna að

$$\text{ef } b < c \text{ og } a > \underline{0} \text{ þá } ab < ac$$

En samkvæmt ofansögðu þá er $ac - ab = a(b-c)$. Og þar sem $a > \underline{0}$ og $c - b > \underline{0}$ þá er, samkvæmt Setingu 9.11, $a(c-b) > \underline{0}(c-b) = \underline{0}$. Af því leiðir að $ac > ab$.

Þar sem sérhvert $\lambda_a : \mathbf{R} \to \mathbf{R}$, $a \in \mathbf{R}$, er stefnd mótun raðaðra grúpna og $\lambda_a(\underline{1}) = \underline{1}a = a$ þá hlýtur $\lambda_a = \mu_a$. Það þýðir að fyrir sérhver $a, b \in \mathbf{R}$ gildir

$ab = ba$

Með þessu höfum við sannað að $\mathbf{R}$ er víxlinn einbaugur. Þar sem $\underline{1} \neq \underline{0}$ og sérhvert $\mu_a : \mathbf{R} \to \mathbf{R}$, $a \neq \underline{0}$, er gagntæk vörpun þá fáum við eftirfarandi setningu.

Setning 9.12: $\mathbf{R}$ er kroppur.

Gefin séu $r, s \in \mathbf{Q}$. Skrifum $r = \frac{n}{m}$ með $m \in \mathbf{N}$ og $n \in \mathbf{Z}$. Þá fæst auðveldlega að $m \cdot \underline{r}\,\underline{s} = n \cdot \underline{s} = m \cdot \underline{rs}$. Af því leiðir að

$\underline{r}\,\underline{s} = \underline{rs}$

Þar með er sannað að vörpunin $i : \mathbf{Q} \to \mathbf{R}$ er eintæk mótun kroppa. Venjulega er ekki gerður greinarmunur á $r \in \mathbf{Q}$ og tilheyrandi staki $\underline{r} \in \mathbf{R}$ og því litið á $\mathbf{Q}$ sem hlutkropp í $\mathbf{R}$.

Skilgreining: *Raðaður kroppur* er kroppur K ásamt línulegri röðun $\leq$ í K þannig að fyrir sérhver $x, y, z \in K$ gildi

ef $x \leq y$ þá $x + z \leq y + z$

ef $x \leq y$ og $0 \leq z$ þá $xz \leq yz$

Sér í lagi eru $\mathbf{Q}$ og $\mathbf{R}$ raðaðir kroppar. Þeir eru reyndar báðir arkimedískt raðaðir, þ.e.a.s. arkimedískt raðaðar grúpur með tilliti til samlagningar.

Setning 9.13: K sé arkimedískt raðaður kroppur. Þá er til ein og aðeins ein stefnd mótun raðaðra kroppa $f : K \to \mathbf{R}$. Hún er strangt vaxandi, sér í lagi eintæk.

Sönnun: Í K hlýtur að gilda $1 > 0$. (Annars væri nefnilega $1 \leq 0$ og þá líka $-1 \geq 0$ en þetta tvennt gæfi mótsögn við seinna skilyrðið í skilgreiningunni á röðuðum kroppi.) Samkvæmt Setningu 9.9 er því til ein og aðeins ein stefnd mótun raðaðra grúpna $f : (K, +) \to (\mathbf{R}, +)$ þannig að $f(1) = 1$. Auk þess er f strangt vaxandi. Við þurfum því aðeins að sýna að $f(ab) = f(a)f(b)$ fyrir sérhver $a, b \in K$. Þar sem $f(0) = 0$ og $f(-x) = -f(x)$ þá nægir að sanna þetta fyrir $a > 0$.

Nú sé gefið $a \in K$, $a > 0$. Þá er $f(a) > 0$, sér í lagi $f(a) \neq 0$. Við skilgreinum vörpunina $g : K \to \mathbf{R}$ með því að setja $g(x) = f(a)^{-1} f(ax)$ fyrir sérhvert $x \in K$. Þá er auðvelt að sjá að $g : (K, +) \to (\mathbf{R}, +)$ er strangt vaxandi mótun raðaðra grúpna. Auk þess er augljóslega $g(1) = 1$. Samkvæmt Setningu 9.9 hlýtur því $g = f$. Það þýðir að $f(ax) = f(a)f(x)$ fyrir sérhvert $x \in K$.

Raðaði kroppurinn $\mathbf{R}$ hefur þann eiginleika að sérhvert hlutmengi í $\mathbf{R}$, sem er ekki tómt og er takmarkað að neðan í $\mathbf{R}$, hefur stærstu neðri mörk í $\mathbf{R}$. Næsta setning segir að þetta einkenni $\mathbf{R}$.

Setning 9.14: K sé raðaður kroppur þannig að sérhvert hlutmengi í K, sem er ekki tómt og er takmarkað að neðan í K, hefur stærstu neðri mörk í K. Þá er til ein og aðeins ein einsmótun raðaðra kroppa $f : K \to \mathbf{R}$.
Sönnun: Eins og í sönnun Setningar 9.6 sést að K er arkimedískt raðaður. Samkvæmt Setningu 9.13 er því til ein og aðeins ein stefnd mótun raðaðra kroppa $f : K \to \mathbf{R}$. Hún er auk þess strangt vaxandi, sér í lagi eintæk. Við megum því gera ráð fyrir að K sé hlutkroppur í $\mathbf{R}$ og þurfum aðeins að sýna að $K = \mathbf{R}$.

Við höfum $1 \in K$. Þar sem $(K, +)$ er hlutgrúpa í $(\mathbf{R}, +)$ þá leiðir af því að $\mathbf{Z} \subseteq K$. Þar sem $(K^*, \cdot)$ er hlutgrúpa í $(\mathbf{R}^*, \cdot)$ þá leiðir svo af þessu að $\mathbf{Q} \subseteq K$. Ef nú $a \in \mathbf{R}$, $a = \inf A$ með $A \in \mathcal{T}$, þá leiðir af forsendunni fyrir K að $\inf A \in K$, þ.e. $a \in K$.

10 Frumþáttun

Í þessum kafla er ákveðinn víxlinn heilbaugur R lagður til grundvallar.

Skilgreining: Ef $a, b \in R$ þá er sagt að a *gangi upp í* b, táknað $a|b$, ef til er $x \in R$ með $b = xa$.

Í stað þess að segja að a gangi upp í b þá er líka sagt að a sé þáttur í b eða að b sé margfeldi af a.

Fyrir sérhvert $a \in R$ gildir augljóslega

$1|a$

$a|a$

$a|0$

Auk þess er ljóst að

ef $0|a$ þá $a = 0$

Ennfremur sést auðveldlega að fyrir sérhver $a, b, c \in R$ gildir

ef $a|b$ og $b|c$ þá $a|c$

Skilgreining: Ef $a, b \in R$ þá er sagt að a sé *tengt* b ef $a|b$ og $b|a$.

Auðséð er að venzlin „tengt“ eru jafngildisvenzl í R. Auk þess er greinilegt að ef a er tengt a' og b er tengt b' þá gildir $a|b$ þá og því aðeins að $a'|b'$.

Setning 10.1: Ef $a, b \in R$ þá er a tengt b þá og því aðeins að til sé eining u í R með $b = ua$.

Sönnun: Ef u er eining í R þannig að $b = ua$ þá gildir líka $a = u^{-1}b$. Af því leiðir að a er tengt b.

Ef a er tengt b, segjum $b = xa$ og $a = yb$ með $x, y \in R$, þá er $a = yxa$. Ef $a = 0$ þá $b = x0 = 0$ og því $b = 1a$. Ef $a \neq 0$ þá leiðir af $a = yxa$ að $yx = 1$, svo að x er eining í R.

Sér í lagi fæst að 1 er tengt a þá og því aðeins að a sé eining í R.

Skilgreining: Ef $p \in R$, $p \neq 0$, þá er p sagt vera *óþáttanlegt* (í R) ef p er ekki eining í R og einu stökin í R sem ganga upp í p eru 1 og p og stök tengd þeim.

Augljóst er að ef p er tengt q þá er p óþáttanlegt þá og því aðeins að q sé óþáttanlegt.

Ef $p \in R$, $p \neq 0$, og $a, b \in R$ þannig að $p = ab$ þá er a tengt p þá og því aðeins að b sé eining í R, þ.e. að b sé tengt 1. Af þessu sést að:

ef $p \in R$, $p \neq 0$, þá er p óþáttanlegt þá og því aðeins að p sé ekki eining í R og að fyrir sérhver $a, b \in R$ gildi
ef $p = ab$ þá er a tengt p eða b tengt p

Skilgreining: Ef $p \in R$, $p \neq 0$, þá er p sagt vera *frumstak* (í R) ef p er ekki eining í R og fyrir sérhver $a, b \in R$ gildir
ef $p|ab$ þá $p|a$ eða $p|b$

Augljóst er að ef p er tengt q þá er p frumstak þá og því aðeins að q sé frumstak.

Ef p er frumstak í R þá fæst strax með þrepun yfir n að fyrir sérhver $a_1, \ldots, a_n \in R$ gildir
ef $p| \prod_{i=1}^{n} a_i$ þá er til $i \in [\![1, n]\!]$ þannig að $p|a_i$

Setning 10.2: Sérhvert frumstak í R er óþáttanlegt.
Sönnun: p sé frumstak í R og $a, b \in R$ þannig að $p = ab$. Þá fæst $a|p$ og $b|p$. Ennfremur fæst $p|ab$, svo að $p|a$ eða $p|b$. Af þessu leiðir að a er tengt p eða b er tengt p.

Við skulum nú, til að einfalda framsetninguna á því sem á eftir fer, koma okkur saman um að setja $\prod_{i=1}^{0} a_i = 1$. Þá gilda reglurnar í kafla 8 líka í tilfellinu $n = 0$. Við skrifum líka $\mathbf{N}_0 = \mathbf{N} \cup \{0\}$.

Skilgreining: Ef $a \in R$, $a \neq 0$, þá er sagt að a sé *frumþáttanlegt* (í R) ef til er eining u í R, $n \in \mathbf{N}_0$ og frumstök $p_1, \ldots, p_n$ í R þannig að $a = u \prod_{i=1}^{n} p_i$.

Með því að taka $n = 0$ í skilgreiningu þessari þá fæst að sérhver eining í R er frumþáttanleg.

Skilgreining: Mengi P af frumstökum í R er sagt vera *fulltrúamengi* fyrir frumstökin í R ef fyrir sérhvert frumstak q í R er til eitt og aðeins eitt $p \in P$ þannig að q sé tengt p.

P sé fulltrúamengi fyrir frumstökin í R.
Gefið sé $a \in R$. Ef $a = v \prod_{i=1}^{n} q_i$ með einingu v í R, $n \in \mathbf{N}_0$ og frumstökum $q_1, \ldots, q_n$ þá er fyrir sérhvert $i \in [\![1, n]\!]$ til $p_i \in P$ þannig að q_i sé tengt p_i, segjum $q_i = u_i p_i$ með einingu u_i í R. En þá er $a = v \prod_{i=1}^{n} (u_i p_i) = v(\prod_{i=1}^{n} u_i)(\prod_{i=1}^{n} p_i) = u \prod_{i=1}^{n} p_i$ með einingunni $u = v \prod_{i=1}^{n} u_i$ í R.
Þetta sýnir að í skilgreiningu okkar á frumþáttanlegum stökum hefðum við mátt einskorða okkur við frumstökin í P.

Næsta setning segir að frumþáttanlegt stak í R sé, í aðalatriðum, ekki frumþáttanlegt nema á einn hátt.

Setning 10.3: P sé fulltrúamengi fyrir frumstökin í R. Ef u og v eru einingar í R, $n, m \in \mathbf{N}_0$ og $p_1, \ldots, p_n, q_1, \ldots, q_m \in P$ þannig að

$$u \prod_{i=1}^{n} p_i = v \prod_{i=1}^{m} q_i$$

þá er $u = v$, $n = m$ og til er gagntæk vörpun $\sigma : [\![1, n]\!] \to [\![1, n]\!]$ þannig að $p_{\sigma(i)} = q_i$ fyrir sérhvert $i \in [\![1, n]\!]$.
Sönnun með þrepun yfir m:
„$m = 0$“: Gefið er að $u \prod_{i=1}^{n} p_i = v1 = v$, svo að $\prod_{i=1}^{n} p_i$ er eining í R. Það gengur greinilega ekki nema $n = 0$ og þar með $u = v$.
„$m = k \to m = k + 1$“: Gefið er að $u \prod_{i=1}^{n} p_i = v \prod_{i=1}^{k+1} q_i$. Þá gengur q_{k+1} upp í $u \prod_{i=1}^{n} p_i$, þar með líka upp í $\prod_{i=1}^{n} p_i$. Það er því til $j \in [\![1, n]\!]$ þannig að $q_{k+1} | p_j$. En þar sem p_j er óþáttanlegt og q_{k+1} er ekki eining í R þá hlýtur q_{k+1} þar með að vera tengt p_j. Og þar sem q_{k+1} og p_j eru bæði í P þá þýðir það að $q_{k+1} = p_j$. Nú er ljóst að röðin á $p_1, \ldots, p_n$ skiptir ekki máli, svo að við megum gera ráð fyrir að $j = n$, þ.e. að $q_{k+1} = p_n$. En þá fæst að $u \prod_{i=1}^{n-1} p_i = v \prod_{i=1}^{k} q_i$, svo að við getum notað þrepunarforsenduna.

Ef $a \in R$ þá er $Ra := \{\, xa \mid x \in R \,\}$ greinilega íðal í R. Og ef I er íðal í R þá er augljóst að $a \in I$ þá og því aðeins að $Ra \subseteq I$.

Nú séu $a, b \in R$. Samkvæmt skilgreiningu gildir $a|b$ þá og því aðeins að $b \in Ra$. Við fáum því að

$a|b$ þá og því aðeins að $Rb \subseteq Ra$

og þar með

a er tengt b þá og því aðeins að $Ra = Rb$

sér í lagi

a er eining í R þá og því aðeins að $Ra = R$

Setning 10.4: Ef $p \in R$, $p \neq 0$, þá gildir

p er frumstak þá og því aðeins að R/Rp sé heilbaugur

Sönnun ($\overline{a} \in R/Rp$ tákni deild staksins $a \in R$.): Að $\overline{1} \neq \overline{0}$ þýðir einmitt að $1 \notin Rp$, þ.e. að p sé ekki eining í R. Að $\overline{x}\,\overline{y} = \overline{0}$ leiði af sér $\overline{x} = \overline{0}$ eða $\overline{y} = \overline{0}$ þýðir að $xy \in Rp$ leiði af sér að $x \in Rp$ eða $y \in Rp$. En það þýðir einmitt að $p|xy$ leiði af sér að $p|x$ eða $p|y$.

Skilgreining: Íðul af taginu Ra með $a \in R$ eru kölluð *höfuðíðul* í R. R er sagður vera *höfuðíðalabaugur* ef sérhvert íðal í R er höfuðíðal.

Setning 10.5: Ef R er höfuðíðalabaugur og p er óþáttanlegt stak í R þá er R/Rp kroppur.

Sönnun ($\overline{a} \in R/Rp$ tákni deild staksins $a \in R$.): Þar sem p er ekki eining í R þá er $1 \notin Rp$, svo að $\overline{1} \neq \overline{0}$. Nú sé gefið $a \in R$ þannig að $\overline{a} \neq \overline{0}$, þ.e. $a \notin Rp$. Auðvelt er að sjá að mengið $Ra + Rp := \{\, xa + yp \mid x, y \in R \,\}$ er íðal í R. Þar sem R er höfuðíðalabaugur þá er til $b \in R$ þannig að $Ra + Rp = Rb$. Þá er $Rp \subseteq Rb$, svo að $b|p$. En þar sem $a \in Ra + Rp$ en $a \notin Rp$ þá er $Rb \neq Rp$, svo að b er ekki tengt p. Þar sem p er óþáttanlegt þá leiðir af þessu að b er eining í R, þar með $Ra + Rp = R$. Það eru því til $x, y \in R$ með $xa + yp = 1$. En vegna $\overline{y}\,\overline{p} = \overline{y}\,\overline{0} = \overline{0}$ þá leiðir af þessu að $\overline{x}\,\overline{a} = \overline{1}$, svo að $\overline{a}$ er eining í R/Rp. Þetta sýnir að R/Rp er kroppur.

Þar sem kroppur er sér í lagi heilbaugur þá er næsta setning afleiðing af Setningum 10.4 og 10.5.

Setning 10.6: Ef R er höfuðíðalabaugur þá er sérhvert óþáttanlegt stak í R frumstak.

Og þá er komið að höfuðsetningu þessa kafla:

Setning 10.7: Ef R er höfuðíðalabaugur þá er sérhvert stak í R frumþáttanlegt — nema 0.
Sönnun: Ef $a \in R$, $a \neq 0$, væri ekki frumþáttanlegt þá væri a sér í lagi ekki eining í R og ekki frumstak, samkvæmt Setningu 10.6 þar með ekki óþáttanlegt. Það væru því til stök b og c í R, hvorugt tengt a, þannig að $a = bc$. Stökin b og c gætu þá ekki bæði verið frumþáttanleg, því að margfeldi frumþáttanlegra staka er greinilega frumþáttanlegt.

Með þrepun yfir n fengist fjölskylda $(a_n)_{n\in\mathbf{N}}$ af stökum a_n í R, $a_1 = a$, þannig að fyrir sérhvert $n \in \mathbf{N}$ gilti $a_{n+1}|a_n$, en a_{n+1} ekki tengt a_n, þ.e. $Ra_n \subset Ra_{n+1}$.

Þá væri $I := \bigcup_{n\in\mathbf{N}} Ra_n$ greinilega íðal í R, svo að til væri $d \in R$ með $I = Rd$. Vegna $d \in Rd$ væri til $m \in \mathbf{N}$ þannig að $d \in Ra_m$, þar með $Rd \subseteq Ra_m$. En þar sem $Ra_{m+1} \subseteq I$ fengist þá að $Ra_{m+1} \subseteq Ra_m$, í mótsögn við að $Ra_m \subset Ra_{m+1}$.

Næsta setning gefur okkur grunndæmið um baug sem hægt er að nota Setningu 10.7 á.

Setning 10.8: $\mathbf{Z}$ er höfuðíðalabaugur.
Sönnun: Heimaverkefni.

Mengi allra jákvæðra frumstaka (frumtalna) í $\mathbf{Z}$ er oftast valið sem fulltrúamengi fyrir frumstökin í $\mathbf{Z}$.

Bent skal á að af Setningu 10.5 leiðir nú að $\mathbf{Z}/\mathbf{Z}p$ er kroppur ef p er frumtala.