5. Kvaziuspořádání a dělitelnost v komutativních monoidech

Buď $S = S(\cdot, \mathbf{1})$ monoid a ať $a \in S$. Definujeme $a^0 = \mathbf{1}$ a $a^n = a^{n-1}a$, je-li $n \in \mathbb{N}$.

5.1 Lemma. *Budiž $S = S(\cdot, \mathbf{1})$ monoid, $a \in S$ a $n, m \in \mathbb{N}_0$. Potom*

(i) $a^n a^m = a^{n+m}$,
(ii) $(a^n)^m = a^{nm}$.

Důkaz. Indukcí dle m. Dokažme nejprve (i), a pak (ii). Pro $m = 0$ oba vztahy zjevně platí. Ať $m > 0$:

(i) $a^n a^m = a^n a^{m-1} a = a^{n+m-1} a = a^{n+m}$,
(ii) $(a^n)^m = (a^n)^{m-1} a^n = a^{n(m-1)} a^n = a^{nm}$.

$\square$

Reflexivní a tranzitivní relace na množině A se nazývá *kvaziuspořádání* A.

Buď $\leq$ kvaziuspořádání množiny A. Pro $a, b \in A$ pišme $a \sim b$, jestliže současně platí $a \leq b$ a $b \leq a$.

5.2 Lemma. *Relace $\sim$ je ekvivalence.*

Důkaz. $\sim$ je zjevně symetrická a tranzitivní. Je-li $a \sim b$ a $b \sim c$, je $a \leq b \leq c$ a $c \leq b \leq a$, takže $a \sim c$. $\square$

Relaci $\sim$ nazýváme *jádrem* kvaziuspořádání $\leq$.

5.3 Lemma. *Buď $\sim$ jádro kvaziuspořádání $\leq$ množiny A a ať $\beta, \gamma \in A/\!\sim$. Jestliže $b_0 \in \beta$, $c_0 \in \gamma$ jsou takové, že $b_0 \leq c_0$, tak $b \leq c$ pro libovolná $b \in \beta$, $c \in \gamma$.*

Důkaz. Je $b \leq b_0 \leq c_0 \leq c$. $\square$

Na $A/\!\sim$ definujeme relaci $\preccurlyeq$ tak, že $\beta \preccurlyeq \gamma$ platí právě když existují $b \in \beta$ a $c \in \gamma$ taková, že je $b \leq c$. Z 5.3 vyplývá, že v takovém případě je $b \leq c$ pro všechna $b \in \beta$ a $c \in \gamma$. Můžeme tedy vyslovit následující lemma.

5.4 Lemma. *Buď $b, c \in A$. Pak $[b]_\sim \preccurlyeq [c]_\sim$ právě když $b \leq c$.*

5.5 Tvrzení. *Relace $\preccurlyeq$ je na $A/\!\sim$ uspořádáním.*

Důkaz. Důkaz reflexivity a tranzitivity je okamžitý. Ať $\beta, \gamma \in A/\!\sim$ a $\beta \preccurlyeq \gamma$, $\gamma \preccurlyeq \beta$. Potom pro $b \in \beta$, $c \in \gamma$ máme $b \leq c$, $c \leq b$, takže $b \sim c$ a $\beta = \gamma$. $\square$

Buď $\leq$ kvaziuspořádání A, $\sim$ jeho jádro a $\preccurlyeq$ uspořádání $A/\!\sim$. Kvaziuspořádání $\leq$ si můžeme představit tak, jakoby vzniklo z uspořádání $\preccurlyeq$ rozpadem jeho prvků do více exemplářů (prvek $\beta \in A/\!\sim$ se tedy jakoby rozpadá na všechna b obsažená v β, přičemž vztahy dané uspořádáním nijak narušeny nejsou). Pojmy definované pro uspořádání budeme používat i pro kvaziuspořádání, a to tímto způsobem:

Je-li $\mathcal{V}$ nějaká vlastnost prvků svazu, tak řekneme, že prvky $a_1, a_2, \dots$ z A mají vlastnost $\mathcal{V}$ právě když ji mají prvky $[a_1]_\sim, [a_2]_\sim, \dots$ svazu $(A/\!\sim, \preccurlyeq)$.

Tak například $a, b \in A$ jsou porovnatelné v $(A, \leq)$, jsou-li $[a]_\sim$ a $[b]_\sim$ porovnatelné v $(A/\!\sim, \preccurlyeq)$. Podobně definujeme v $(A, \leq)$ dolní a horní závory, infima a suprema. Zápis $b = \inf_{\leq} B$ ovšem v kvaziuspořádání prvek b neurčuje jednoznačně, jednoznačně je určena pouze třída $[b]_\sim$ (je totiž $[b]_\sim = \inf_{\preccurlyeq}\{[c]_\sim;\ c \in B\}$).

Prvek $a \in A$ nazveme *atomem*, jestliže jsou splněny tyto podmínky:

(i) A má (alespoň jeden) nejmenší prvek,
(ii) a není nejmenší prvek A,
(iii) je-li $c \in A$ a $c \leq a$, tak buď $c \sim a$, nebo je c nejmenší prvek A.

Podle 5.4 a 5.5 můžeme tedy říci, že $a \in A$ je atomem, právě když $\mathrm{nat}_\sim(a)$ pokrývá (jednoznačně určený) nejmenší prvek $A/\!\sim$.

Kvaziuspořádání $\leq$ množiny A nazveme *noetherovské*, jestliže neexistuje nekonečná posloupnost $a_1, a_2, a_3, \ldots$ prvků z A taková, že pro každé $i \in \mathbb{N}$ je $a_i \geq a_{i+1}$, a současně neplatí $a_i \sim a_{i+1}$.

5.6 Tvrzení. *Buď $\leq$ noetherovské kvaziuspořádání množiny A a ať a je nejmenší prvek A. Potom pro každé $c \in A$ platí, že je buď $c \sim a$, nebo existuje atom $b \in A$ takový, že $b \leq c$.*

Důkaz. Předpokládejme, že není $c \sim a$. Položme $c_1 = c$ a ať $c_1, \ldots, c_n$ jsou takové prvky A, že pro $1 \leq i \leq n$ není $c_i \sim a$, a že pro $1 \leq i \leq n-1$ je $c_i \geq c_{i+1}$ a neplatí $c_i \sim c_{i+1}$. Jestliže c_n není atomem, existuje $c_{n+1} \in A$ takové, že $c_n \geq c_{n+1} \geq a$ a není ani $c_{n+1} \sim c_n$, ani $c_{n+1} \sim a$. Protože $\leq$ je noetherovské, lze takto zkonstruovat jen konečně mnoho členů posloupnosti $c_1, c_2, c_3, \ldots$. Proto musí existovat $n \in \mathbb{N}$, že c_n je atomem. $\square$

Buď nyní $S = S(\cdot, \mathbf{1})$ monoid. Řekneme, že $a \in S$ *dělí* (zleva) $b \in S$, jestliže existuje $c \in S$ takové, že $b = a \cdot c$. Symbolicky píšeme $a|b$ a a nazýváme *dělitelem* b.

5.7 Tvrzení. *Relace dělitelnosti $|$ v monoidu $S = S(\cdot, \mathbf{1})$ je kvaziuspořádáním, přičemž $\mathbf{1}$ je jeho nejmenší prvek.*

Důkaz. Buď $a, b \in S$. Pak $\mathbf{1}|a$, $a|a$, a z $a|b$ a $b|c$ plyne $a|c$. $\square$

Jádro kvaziuspořádání $|$ budeme, jak je obvyklé, značit $||$. Je-li $a||b$, říkáme, že a a b jsou *asociovány*.

Uvědomte si, že z pouhého faktu, že $|$ je kvaziuspořádání, plyne podle 5.3 několik důsledků. Jsou-li $a, b \in S$ asociovány, tak pro každé $c \in S$ například dostáváme $a|c \Leftrightarrow b|c$ a $c|a \Leftrightarrow c|b$.

Buď $B = \{b_1, \ldots, b_k\} \subseteq A$, $k \geq 1$. Místo $b = \inf_{|} B$ píšeme $b = NSD(b_1, \ldots, b_k)$ a místo $b = \sup_{|} B$ píšeme $b = NSN(b_1, \ldots, b_k)$. Přitom NSD znamená *největší společný dělitel* a NSN *nejmenší společný násobek*.

V každém kvaziuspořádání je $b \leq c$ právě když $b = \inf_{\leq}\{b, c\}$. Proto platí:

5.8 Lemma. *Buď $b, c \in S$. Pak $b = NSD(b, c)$ právě když $b|c$.*

Z 4.1, 5.4 a 5.5 okamžitě dostáváme:

5.9 Lemma. *Ať $b_1, \ldots, b_{n+1}$, kde $n \in \mathbb{N}$, jsou prvky monoidu S, a ať $c \in S$ je takové, že $c = NSD(b_1, \ldots, b_n)$. Potom $NSD(b_1, \ldots, b_{n+1})$ existuje právě když existuje $NSD(c, b_{n+1})$. Pokud tyto největší společní dělitelé existují, jsou asociovány.*

V S tedy existují největší společní dělitelé, existuje-li $NSD(b,c)$ pro libovolná $b,c \in S$. Totéž lze říci o největších společných násobcích. Z 5.5 plyne, že v S existují největší společní dělitelé a nejmenší společné násobky právě když uspořádaná množina $(S/||, |)$ je svaz.

Prvky $a,b \in S$ se nazývají *nesoudělné*, jestliže $\mathbf{1} = NSD(a,b)$. Dělitel a prvku b se nazývá *vlastní*, jestliže neplatí ani $a||\mathbf{1}$ ani $a||b$.

Budeme se zabývat především komutativními monoidy s krácením. Monoid S je *komutativní*, jestliže $b \cdot c = c \cdot b$ pro libovolná $b,c \in S$. Monoid S je *s krácením*, jestliže pro libovolná $a,b,c \in S$ z $a \cdot b = a \cdot c$ plyne $b = c$ a z $b \cdot a = c \cdot a$ rovněž plyne $b = c$.

Všimněte si, že prvek $a \in S$ je asociován s $\mathbf{1}$ (tedy je v kvaziuspořádání dělením nejmenší) právě když existuje $b \in S$ splňující $ab = \mathbf{1}$ (tedy právě když je a zprava invertibilní). V komutativním případě proto platí, že prvek je asociován s $\mathbf{1}$ právě tehdy, když je invertibilní, a že prvky asociované s $\mathbf{1}$ tvoří podmonoid monoidu $S(\cdot, \mathbf{1})$ (viz 2.17).

5.10 Lemma. *Buď S komutativní monoid s krácením, a ať $a,b \in S$. Potom $a||b$ platí právě když existuje $u \in S$ invertibilní takové, že $b = a \cdot u$.*

Jestliže $a = bc$ pro nějaké $c \in S$, tak nastane jedna z následujících možností:

(i) *b i c jsou vlastní dělitelé a,*
(ii) *b je invertibilní a $a||c$,*
(iii) *c je invertibilní a $a||b$.*

Důkaz. Je-li $a||b$, existují $u,v \in S$ takové, že $a = bu$ a $b = av$. Tudíž $a = avu$, takže $vu = \mathbf{1}$. Jestliže $a = bu$ a u je invertibilní, lze nalézt $v \in S$ takové, že $uv = \mathbf{1}$, takže $b = buv = av$.

Je-li b (nebo c) invertibilní, tak $a||c$ (nebo $a||b$) platí podle prvé části lemmatu. Je-li $a||c$, tak existuje $u \in S$ takové, že $c = au$. Tudíž $a = bc = bau = abu$, a krácením dostáváme $\mathbf{1} = bu$, takže b je invertibilní. Podobně z $a||b$ plyne invertibilita c. $\square$

Ve zbytku této kapitoly bude $S = S(\cdot, \mathbf{1})$ vždy značit komutativní monoid s krácením, $|$ kvaziuspořádání S dělitelností, a $||$ jádro $|$.

Atomy kvaziuspořádání $|$ budeme nazývat *ireducibilními* prvky.

5.11 Tvrzení. *Ať kvaziuspořádání $|$ je noetherovské. Potom každý prvek S, který není invertibilní, lze vyjádřit jako součin ireducibilních prvků.*

Důkaz. Podle 5.6 má každý prvek S, který není invertibilní, ireducibilního dělitele. Ať $a = a_0$ není invertibilní. Budeme konstruovat posloupnost neinvertibilních prvků $a_0, a_1, \dots$ a posloupnost ireducibilních prvků $p_1, p_2, \dots$. Pokud a_i není ireducibilní, položíme $a_i = p_{i+1}a_{i+1}$ tak, aby p_{i+1} byl ireducibilní dělitel a_i. Potom je p_{i+1} vlastní dělitel a_i, takže podle 5.10 je i a_{i+1} vlastní dělitel a_i. Kdyby a_i nebyl ireducibilní pro žádné $i \in \mathbb{N}$, vznikla by nekonečná posloupnost $a_0, a_1, \dots$, ve které by pro každé $i \in \mathbb{N}$ byl a_i vlastní dělitel a_{i-1}. Protože předpokládáme, že $|$ je noetherovské, existuje $n \in \mathbb{N}$ takové, že a_n je ireducibilní, takže $a = p_1 \dots p_{n-1}a_n$. $\square$

5.12 Lemma. *Buď $a, b, c \in S$ a ať $d = NSD(a, b)$ a $e = NSD(ac, bc)$. Potom $e||dc$.*

Důkaz. $dc|ac$ a $dc|bc$, takže $dc|e$ a $e = dcu$ pro nějaké $u \in S$. Ať $x, y \in S$ jsou takové, že $ac = ex$ a $bc = ey$. Pak $a = dux$, $b = duy$, a vidíme, že du je společný dělitel a a b. Proto $du|d$, takže $du||d$ a u je invertibilní podle 5.10. Proto $e||dc$. □

5.13 Lemma. *Buď $a, b, c \in S$ a ať a a b jsou nesoudělné. Jestliže $NSD(ac, bc)$ existuje, tak z $a|bc$ plyne $a|c$.*

Důkaz. Podle 5.12 je $c = NSD(a, b)c = NSD(ac, bc)$. Odsud dostáváme $NSD(a, c) = NSD(a, ac, bc) = NSD(a, bc) = a$, takže $a|c$. □

Prvek $p \in S$ se nazývá *prvočinitel*, jestliže není invertibilní, a pro každé $a, b \in S$ z $p|ab$ plyne, že $p|a$ nebo $p|b$.

5.14 Tvrzení. *Každý prvočinitel S je ireducibilní. Jestliže v S existují největší společní dělitelé, tak je každý ireducibilní prvek prvočinitel.*

Důkaz. Buď p prvočinitel, a ať $p = ab$. Z faktu, že p je prvočinitel, plyne $p|a$ (a pak $p||a$) nebo $p|b$ (a pak $p||b$). Ať naopak $p \in S$ je ireducibilní, $p|ab$, p nedělí a a $d = NSD(p, a)$. Protože p nedělí a, není $d||p$. Protože p je ireducibilní a $d|p$, je $d||\mathbf{1}$. Prvky p a a jsou tedy nesoudělné, a podle 5.13 z existence $NSD(pb, ab)$ plyne $p|b$. □

5.15 Lemma. *Ať p je prvočinitel v S. Potom z $p|a_1 \dots a_n$, kde $a_i \in S$, $1 \leq i \leq n$, plyne, že $p|a_j$ pro některé $1 \leq j \leq n$.*

Důkaz. Postupujme indukcí dle n. Pro $n = 2$ tvrzení vyplývá z definice prvočinitele. Položme $b = a_2 \dots a_n$. Pak p dělí $a_1 b$, čili p dělí a_1 nebo p dělí $a_2 \dots a_n$. V druhém případě podle indukčního předpokladu existuje $2 \leq j \leq n$ takové, že $p|a_j$. □

Řekneme, že prvek $a \in S$ má *jednoznačný ireducibilní rozklad*, jestliže:

(i) existují $p_1, \dots, p_r \in S$ ireducibilní a takové, že $a = p_1 \dots p_r$,
(ii) kdykoliv $a = q_1 \dots q_s \in S$, kdy $q_1, \dots, q_s \in S$ jsou ireducibilní, tak $r = s$ a existuje permutace $\sigma \in S_r$, že $p_i||q_{\sigma(i)}$ pro $1 \leq i \leq r$.

(Jinými slovy ireducibilní rozklad je jednoznačný až na pořadí a $||$ ekvivalenci).

5.16 Tvrzení. *Jestliže v S je každý ireducibilní prvek prvočinitelem, tak jsou ireducibilní rozklady v S jednoznačné.*

Důkaz. Ať $p_1 \dots p_n = q_1 \dots q_m$, kde p_i, $1 \leq i \leq n$ a q_j, $1 \leq j \leq m$ jsou ireducibilní, a ať $n \leq m$. Z $q_1|p_1 \dots p_n$ plyne podle 5.15, že můžeme předpokládat, že $q_1 = p_1 u$ pro u invertibilní. Je-li $n = 1$, dostáváme krácením $\mathbf{1} = uq_2 \dots q_m$. Ovšem ireducibilní prvky nedělí $\mathbf{1}$, takže v tomto případě $m = 1$ a $p_1 = q_1$. Postupujme dále indukcí dle $n \geq 2$. Položme $q'_i = q_i$ pro $1 \leq i \leq n$, $i \neq 2$ a $q'_2 = up_2$. Pak $p_2 \dots p_n = q'_2 \dots q'_m$, a podle indukčního předpokladu $n = m$ a existuje $\sigma \in S_n$ takové, že $\sigma(1) = 1$ a $p_i||q'_{\sigma(i)}$. □

5.17 Tvrzení. *Ať každý neinvertibilní prvek má v S jednoznačný ireducibilní rozklad. Potom je každý ireducibilní prvek prvočinitel.*

Důkaz. Buď p ireducibilní prvek a ať $p|ab$. Buď $ab = pc$ a ať $c = c_1 \dots c_t$ je ireducibilní rozklad c (je-li c invertibilní, položme $c_1 = c$). Ať $a = a_1 \dots a_r$ a $b = b_1 \dots b_s$ jsou ireducibilní rozklady a a b. Potom $pc_1 \dots c_t = a_1 \dots a_r b_1 \dots b_s$ a z jednoznačnosti ireducibilních rozkladů plyne, že $p||a_i$ pro některé $1 \le i \le r$ (pak $p|a$) nebo $p||b_j$ pro některé $1 \le j \le s$ (pak $p|b$). $\square$

5.18 Věta. *Buď $S = S(\cdot, \mathbf{1})$ komutativní monoid s krácením, ve kterém každý neinvertibilní prvek má jednoznačný ireducibilní rozklad. Ať $P \subseteq S$ je taková množina ireducibilních prvků, že*

(a) *kdykoliv $r \in S$ je ireducibilní, tak existuje $p \in P$, že $p||r$,*
(b) *jsou-li $p_1, p_2 \in P$, tak $p_1||p_2$ právě pro $p_1 = p_2$.*

Označme ještě I množinu všech invertibilních prvků. Potom platí:

(i) *Každý prvek $a \in S$ lze (až na pořadí) jednoznačně vyjádřit ve tvaru $a = up_1^{k_1} \dots p_r^{k_r}$, kde $p_i \in P$, $k_i \in \mathbb{N}$ a $u \in I$ (přitom předpokládáme, že $p_i \ne p_j$ pro $1 \le i < j \le r$).*
(ii) *Je-li $a = up_1^{k_1} \dots p_r^{k_r}$ a $b = vp_1^{h_1} \dots p_r^{h_r}$, kde pro $1 \le i \le r$ je $p_i \in P$, $k_i \in \mathbb{N}_0$ a $h_i \in \mathbb{N}_0$, přičemž $u, v \in I$ a $p_i \ne p_j$ pro $1 \le i < j \le r$, tak $p_1^{\min(k_1,h_1)} \dots p_r^{\min(k_r,h_r)} = NSD(a,b)$. Dále platí, že b dělí a právě když $h_i \le k_i$ pro $1 \le i \le r$, přičemž b je vlastním dělitelem a, jestliže navíc existují $1 \le s, t \le r$ taková, že $h_s < k_s$ a $1 \le h_t$.*

Důkaz. (i) Jestliže a je invertibilní, tak nutně $u = a$, $r = 0$. Pokud a není invertibilní, existuje vyjádření $a = q_1 \dots q_s$, kde q_i, $1 \le i \le s$ jsou ireducibilní. Ovšem $q_i = u_i p_i$, kde $p_i \in P$ a $u_i \in I$, takže každý prvek lze jistě zapsat v požadovaném tvaru. Ať $a = up_1^{k_1} \dots p_r^{k_r} = vp_1^{h_1} \dots p_r^{h_r}$, kde $u, v \in I$, $p_i \in P$ a $k_i, h_i \in \mathbb{N}_0$. Ať přitom $p_i \ne p_j$ pro $1 \le i < j \le r$. Kdyby bylo například $k_1 < h_1$, tak $up_2^{k_2} \dots p_r^{k_r} = vp_1^{h_1-k_1} p_2^{h_2} \dots p_r^{h_r}$, takže podle 5.7 a 5.15 $p_1||p_j$ pro některé $2 \le j \le r$. To však odporuje předpokládaným vlastnostem množiny P, a proto $k_i = h_i$ pro $1 \le i \le r$. Krácením dostáváme $u = v$, čímž je důkaz jednoznačnosti vyjádření uzavřen.
(ii) Ať $vp_1^{h_1} \dots p_r^{h_r} = b$ dělí $a = up_1^{k_1} \dots p_r^{k_r}$ a ať je například $h_1 \ge k_1$. Potom $vp_1^{h_1-k_1} p_2^{h_2} \dots p_r^{h_r}$ dělí $up_2^{k_2} \dots p_r^{k_r}$ a z 5.7 a 5.15 plyne, že $h_1 - k_1 = 0$, čili $h_1 = k_1$. Proto $h_i \le k_i$ pro $1 \le i \le r$. Hledejme nyní $NSD(a,b)$, kde $a = up_1^{k_1} \dots p_r^{k_r}$ a $b = vp_1^{h_1} \dots p_r^{h_r}$. Buď $m_i = \min(k_i, h_i)$ pro $1 \le i \le r$. Z předchozího plyne, že $d = p_1^{m_1} \dots p_r^{m_r}$ dělí a i b. Ať c dělí rovněž a i b. Pak $c = wp_1^{c_1} \dots p_r^{c_r}$, kde $w \in I$ a $c_i \le k_i$ a $c_i \le h_i$ pro $1 \le i \le r$. Proto c dělí d, takže $d = NSD(a,b)$.

Zkoumejme ještě, kdy $b = vp_1^{h_1} \dots p_r^{h_r}$ je vlastní dělitel $a = up_1^{k_1} \dots p_r^{k_r}$. Víme, že pak $h_i \le k_i$ pro $1 \le i \le r$. Je-li $h_i = k_i$ pro všechna $1 \le i \le r$, je $a = uv^{-1}b$, takže $a||b$. Naopak, z $a||b$ plyne $h_i = k_i$ pro $1 \le i \le r$. Dále platí, že b je invertibilní právě když $h_1 = \dots = h_r = 0$. Proto je b vlastní dělitel a jedině tehdy, jestliže existují $1 \le s, t \le r$ taková, že $h_s < k_s$ a $1 \le h_t$. $\square$

5.19 Věta. *Buď $S = S(\cdot, \mathbf{1})$ komutativní monoid s krácením. Pak následující podmínky jsou ekvivalentní.*

(i) *V S má každý neinvertibilní prvek jednoznačný ireducibilní rozklad.*

(ii) *V S existují největší společní dělitelé a současně platí, že kvaziuspořádání dělitelností je noetherovské.*
(iii) *Každý ireducibilní prvek S je prvočinitelem a současně platí, že kvaziuspořádání dělitelností je noetherovské.*

Důkaz. (ii) plyne z (i) podle 5.18.
(iii) plyne z (ii) podle 5.15.
(i) plyne z (iii) podle 5.11 a 5.16. $\square$

5.20 Tvrzení. *Ať $S = S(\cdot, \mathbf{1})$ je komutativní monoid s krácením, ve kterém existují největší společné dělitele. Potom existují i nejmenší společné násobky, přičemž jsou-li $b, c, e, f \in S$ takové, že $e = NSD(b, c)$ a $ef = bc$, je $f = NSN(b, c)$. Uspořádání $S/||$ indukované dělitelností je v takovém případě svaz.*

Důkaz. Je-li $e = NSD(b, c)$, tak $e|bc$, takže jistě existuje f takové, že $bc = ef$. Buď nejprve $e = \mathbf{1}$. Pak je třeba ukázat, že $bc = NSN(b, c)$. Ať $b|h$, $c|h$ a $h = bg$. Potom $c|bg$, a podle 5.13 c dělí g. Tudíž $g = cx$, $h = bcx$, $bc|h$. Ať nyní $e \neq \mathbf{1}$, $b = eu$, $c = ev$. Pak $f = euv$ a pro $d = NSD(u, v)$ platí, že $ed|e$. Proto $ed||e$ a $\mathbf{1} = NSD(u, v)$. Ať $b|h$ a $c|h$. Pak $e|h$, a $h = ey$ pro nějaké $y \in S$. Krácením e dostáváme $u|y$, $v|y$, a podle prvé části důkazu platí $uv|y$. Tudíž $f = euv|ey = h$. $\square$