0.1 Faktorizacija: ID, ED, PID, ND, FD, UFD

Definicija. *Najava pojmova: [ID], [ED], [PID], [ND], [FD] i [UFD].*

ID: *Komutativan prsten $\mathbb{P}$, sa jedinicom $1 \neq 0$, je **integralni domen [ID]** (oblast celih), ili samo **domen**, akko $\mathbb{P}$ nema prave delitelje nule (akko $(\forall x, y \in P)\ (\ xy = 0 \Rightarrow x = 0 \vee y = 0)$).*

ED: *Domen $\mathbb{P}$ je **euklidski [ED]** akko postoji funkcija $\varphi : P \setminus \{0\} \to \mathbb{N}_0 = \{0, 1, 2, \dots\}$ tako da $(\forall a, b \in P)\,(\ b \neq 0\ \Rightarrow\ (\exists c, d \in P)\,(\ a = bc + d\ \wedge\ (\ d \neq 0\ \Rightarrow\ \varphi(d) < \varphi(b)\ )\ )\ )$.*

PID: *Domen $\mathbb{P}$ je **glavnoidealski [PID]** akko svaki ideal u $\mathbb{P}$ je glavni (generisan jednim elementom; oblika $aP := \{ab \mid b \in P\}$, za neko $a \in P$).*

ND: *Domen $\mathbb{P}$ je **Neterin [ND]** akko svaki rastući niz ideala u $\mathbb{P}$ je stacionaran (to jest, akko u $\mathbb{P}$ ne postoji strogo rastući beskonačan niz ideala). Preciznije, $\mathbb{P}$ je **ND** akko za svaki rastući niz ideala $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ postoji $n \in \mathbb{N}$ tako da je $(\forall k > n)\ I_n = I_k$.*

FD: *Domen $\mathbb{P}$ je **faktorizacijski [FD]** akko svaki nenula nejedinični element $a \in P$ ima atomičnu faktorizaciju, faktoriše se na (konačan) proizvod nekih atoma. Preciznije, $\mathbb{P}$ je **FD** akko $(\forall a \in P \setminus P_0^*)\ (\exists k \in \mathbb{N})\ (\exists a_1, a_2, \dots, a_k \in \mathrm{Atom}(\mathbb{P})\,)\ a = a_1 a_2 \cdots a_k$, gde je $P_0^* = \{0\} \cup P^*$.*

UFD: *Domen $\mathbb{P}$ **ima jedinstvenu faktorizaciju [je UFD]** akko $\mathbb{P}$ je FD i svake dve atomične faktorizacije elementa $a \in P$ su jednake do na redosled i asociranost faktora. $\mathbb{P}$ je **UFD** akko*
FD: $(\forall a \in P \setminus P_0^*)\ (\exists k \in \mathbb{N})\ (\exists a_1, a_2, \dots, a_k \in \mathrm{Atom}(\mathbb{P})\,)\ a = a_1 a_2 \cdots a_k$, i
UF: ako su $a = a_1 a_2 \cdots a_k$ i $a = b_1 b_2 \cdots b_l$ dve atomične faktorizacije, onda je $k = l$ i postoji permutacija σ skupa $\{1, 2, \dots, k\}$ tako da je $a_i \sim b_{\sigma(i)},\ 1 \leq i \leq k$. Ekvivalentno,
*$\mathbb{P}$ je **UFD** akko je FD i važi UF: $(\forall k, l \in \mathbb{N})\ (\forall a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_l \in \mathrm{Atom}(\mathbb{P})\,)$*
$\big(\ a_1 a_2 \cdots a_k \sim b_1 b_2 \cdots b_l\ \Rightarrow\ k = l,\ (\exists \sigma \in S_k)\ (a_1 \sim b_{\sigma(1)}, a_2 \sim b_{\sigma(2)}, \dots, a_k \sim b_{\sigma(k)})\ \big)$.

$$Fields \subseteq ED \subseteq PID \subseteq UFD \subseteq FD \subseteq ID \subseteq CommRings$$

$$Fields \subseteq ED \subseteq PID \subseteq ND \subseteq FD \subseteq ID \subseteq CommRings$$

$$F \subseteq ED \subseteq PID \begin{matrix} \subseteq ND \subseteq \\ \subseteq UFD \subseteq \end{matrix} FD \subseteq ID \subseteq CR$$

0.2 Euklidski domeni [ED]

Definicija. *Neka je $\mathbb{P}$ (integralni) domen.*

EF: ***Euklidska funkcija*** *domena $\mathbb{P}$ je funkcija $\varphi : P \setminus \{0\} \to \mathbb{N}_0 = \{0, 1, 2, \dots\}$ takva da*
(EF1:) $(\forall a, b \in P)\,(\ b \neq 0 \ \Rightarrow\ (\exists c, d \in P)\,(\ a = bc + d\ \wedge\ (\ d \neq 0 \ \Rightarrow\ \varphi(d) < \varphi(b)\ )\ )\ )$.

ED: $\mathbb{P}$ *je* ***euklidski domen [ED]*** *akko postoji (bar jedna) euklidska funkcija domena $\mathbb{P}$.*

Stav (ED je PID). Ako je $\mathbb{P}$ euklidski domen, onda je svaki njegov ideal glavni.

Δ. Neka je I proizvoljan ideal prstena. Ako je $I = \{0\}$, onda je $I = (0)$ glavni.
Ako je $I \neq \{0\}$, neka je φ euklidska funkcija domena $\mathbb{P}$.
Tada neprazan skup $I_\varphi := \{\varphi(i) \mid i \in I \setminus \{0\}\} \subseteq \mathbb{N}_0$ ima minimum.
Neka je $b \in I \setminus \{0\}$ takav da je $\varphi(b) = \min I_\varphi$. Onda je $(b) \subseteq I$.
Obrat? Neka je $a \in I$. Tada postoje $c, d \in P$ tako da je $a = bc + d$ i $d \neq 0 \ \Rightarrow\ \varphi(d) < \varphi(b)$.
Takođe, $d = a - bc \in I$ jer $a \in I,\ bc \in (b) \subseteq I$. Zato je $d = 0$ ili $\varphi(d) \geq \varphi(b)$.
I ovo drugo povlači $d = 0$, zbog gornje implikacije, kontrapozicijom.
Konačno $a = bc \in (b)$, pa je $I \subseteq (b)$. $\square$

Napomena. Ako je data euklidska funkcija $\varphi : P \setminus \{0\} \to \mathbb{N}_0$, onda se može definisati $\varphi_\circ : P \to \mathbb{N}_0$ tako da je $\varphi_\circ(a) := \varphi(a) + 1$, za $a \neq 0$, i $\varphi_\circ(0) := 0$, koja je takođe euklidska (važi EF1$_\circ$), gde je EF1$_\circ$: $(\forall a, b \in P)\,(\ b \neq 0 \ \Rightarrow\ (\exists c, d \in P)\,(\ a = bc + d\ \wedge\ \varphi_\circ(d) < \varphi_\circ(b)\ )\ )$.

Definicija. *Domen $\mathbb{P}$ je* ***euklidski [ED]*** *akko postoji funkcija $\varphi : P \to \mathbb{N}_0 = \{0, 1, 2, \dots\}$ tako da*
EF1$_\circ$: $(\forall a, b \in P)\,(\ b \neq 0 \ \Rightarrow\ (\exists c, d \in P)\,(\ a = bc + d\ \wedge\ \varphi(d) < \varphi(b)\ )\ )$.

Napomena. Ponekad za kodomen euklidske funkcije domena $\mathbb{P}$ (funkcije za koju važi EF1 ili EF1$_\circ$) uzimamo dobro uređen skup, umesto $\mathbb{N}_0$. Na primer, prsten polinoma $F[X]$ nad poljem F je ED, stepen polinoma $\deg : F[x] \to \mathbb{N}_0 \cup \{-\infty\}$ je euklidska funkcija (važi EF1$_\circ$).

Napomena. Ako je $\varphi : P \setminus \{0\} \to \mathbb{N}_0$ euklidska funkcija, onda je i $\overline{\varphi} : P \setminus \{0\} \to \mathbb{N}_0$, data sa $\overline{\varphi}(b) := \min\limits_{\beta \in P \setminus \{0\}} \varphi(\beta b)$, euklidska funkcija koja ima i osobinu (EF2:) $(\forall a, b \in P \setminus \{0\})\ \overline{\varphi}(a) \leq \overline{\varphi}(ab)$.

Δ. (DDT) Funkcija $\overline{\varphi}$ je dobro definisana, jer $\mathbb{P}$ nema prave delitelje nule i jer je $\mathbb{N}_0$ dobro uređen.
Proveravamo da važi EF1. Neka su $a, b \in P,\ b \neq 0$. Ako $a \in bP$, onda EF1 važi za $d = 0$. Neka sada $a \notin bP$. Kako je $b \neq 0$, postoji $\beta \neq 0$ tako da je $\overline{\varphi}(b) = \varphi(\beta b)$. Primenom EF1 na $a \in P$, $\beta b \neq 0$ i funkciju φ, dobijamo $(\exists c, d \in P)\ (\ a = \beta bc + d\ \wedge\ \varphi(d) < \varphi(\beta b)\ )$; jer je $d \neq 0$ zbog $a \notin bP$. Neka je $\overline{c} \in P$ takav da $\overline{\varphi}(a - \beta b\overline{c}) = \min\limits_{u \in P} \overline{\varphi}(a - \beta bu)$ i $\overline{d} := a - \beta b\overline{c}$. Tada je $a = b\beta\overline{c} + \overline{d}$. Dokazujemo da je $\overline{\varphi}(\overline{d}) < \overline{\varphi}(b)$.

$$\text{Zaista } \overline{\varphi}(\overline{d}) \leq \overline{\varphi}(a - \beta bc) = \overline{\varphi}(d) \leq \varphi(d) < \varphi(\beta b) = \overline{\varphi}(b).$$

Osobina EF2 sledi iz definicije funkcije $\overline{\varphi}$, jer je $\overline{\varphi}(b) := \min\limits_{u \in (b) \setminus \{0\}} \varphi(u)$, i iz $(ab) \subseteq (a)$. $\square$

0.3 Glavnoidealski domeni [PID]

Definicija. *Domen $\mathbb{P}$ je* ***glavnoidealski [PID]*** *akko svaki ideal u $\mathbb{P}$ je glavni (generisan jednim elementom; oblika $aP := \{ab \mid b \in P\}$, za neko $a \in P$).*

Stav (ED je PID). Ako je $\mathbb{P}$ ED, onda je $\mathbb{P}$ PID.

Definicija. *Neka je $\mathbb{P}$ domen. Element $d \in P$ je* ***najveći zajednički delilac (n.z.d.)*** *elemenata $a, b \in P$ akko $d \mid a,\ d \mid b,\ i\ (\forall d' \in P)\ (d' \mid a,\ d' \mid b \ \Rightarrow\ d' \mid d)$. Tada, ipak$^{\circledast}$, pišemo $d = (a, b)$.*

$\circledast$: $d, d' \in P$ su oba n.z.d. elemenata $a, b \in P$ akko d i d' su asocirani ($d \sim d'$) akko $(d) = (d')$.

Lema (NZD). Ako je $\mathbb{P}$ glavnoidealski, onda za svako $a, b \in P$ postoji njihov najveći zajednički delilac $d \in P$ i pri tom važi $(a) + (b) = (d)$.

Δ. Zbir ideala $(a) + (b)$ je glavni ideal u $\mathbb{P}$. Zato postoji $d \in P$ tako da je $(a) + (b) = (d)$.
Dokazujemo da je $d = (a, b)$.
$(a) \subseteq (a) + (b) = (d) \ \Rightarrow\ (a) \subseteq (d) \ \Rightarrow\ d \mid a$,
$(b) \subseteq (a) + (b) = (d) \ \Rightarrow\ (b) \subseteq (d) \ \Rightarrow\ d \mid b$,
$d' \mid a,\ d' \mid b \ \Rightarrow\ (a) \subseteq (d'),\ (b) \subseteq (d') \ \Rightarrow\ (a) + (b) \subseteq (d') \ \Rightarrow\ (d) \subseteq (d') \ \Rightarrow\ d' \mid d.$ $\square$

Stav (atom=prost). Neka je $\mathbb{P}$ PID, i $a \in P$. Tada: ako je a atom, onda je a prost.

Δ. Neka je $a \in P$ atom. Tada je a prost akko $(\forall b, c \in P)\ (a \mid bc \ \Rightarrow\ a \mid b \ \vee\ a \mid c)$.
Pretpostavimo: a je atom; $b, c \in P$, $a \mid bc$, $a \nmid b$. Dokazujemo: $a \mid c$.
a je atom, $a \nmid b \ \Rightarrow\ a$ je atom, $b \nsim a$
$\Rightarrow\ (a, b) = 1 \ \Rightarrow\ (a) + (b) = (1) = P$, zbog Leme,
$\Rightarrow\ (\exists s, t \in P)\ as + bt = 1 \ \Rightarrow\ (\exists s, t \in P)\ asc + btc = c$
$\Rightarrow\ (\exists s, t \in P)\ a \mid asc + bct = c$, jer $a \mid bc$,
$\Rightarrow\ a \mid c$. $\square$

Primer. $\mathbb{Z}[i\sqrt{5}] := \{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}\}$ nije PID, jer je 2 atom, ali nije prost.

Δ. Ako je $\mathrm{N} : \mathbb{Z}[i\sqrt{5}] \to \mathbb{N}_0 : a + bi\sqrt{5} \mapsto a^2 + 5b^2$, onda je N multiplikativna, $\mathrm{N}(2) = 4$ i $\mathrm{N}(1 \pm i\sqrt{5}) = 6$. Zato je 2 atom, a iz $2 \cdot 3 = 6 = (1 - i\sqrt{5}) \cdot (1 + i\sqrt{5})$ i $4 \nmid 6$ sledi da 2 nije prost. $\square$

Stav (PID je ND). Neka je $\mathbb{P}$ glavnoidealski. Ako je $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ rastući niz ideala u $\mathbb{P}$, onda postoji $n \in \mathbb{N}$ tako da je $(\forall k > n)\ I_n = I_k$.

Δ. Neka je $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ rastući niz ideala, i neka je $I := \bigcup_{s \geq 1} I_s$. Tada je I ideal (Zašto?).
$\mathbb{P}$ je glavnoidealski, pa postoji $a \in P$ tako da je $I = (a)$. Tada $a \in I = \bigcup_{s \geq 1} I_s$, pa $a \in I_n$, za neko $n \geq 1$.
Ako je $k > n$, onda $a \in I_n \subseteq I_k \subseteq I = (a)$. Otuda $I = (a) \subseteq I_n \subseteq I_k \subseteq I$, pa je $I_n = I_k$, za $k > n$. $\square$

0.4 Neterini domeni [ND]

Definicija. *Domen $\mathbb{P}$ je **Neterin [ND]** akko svaki rastući niz ideala u $\mathbb{P}$ je stacionaran (to jest, akko u $\mathbb{P}$ ne postoji strogo rastući beskonačan niz ideala). Preciznije, $\mathbb{P}$ je **ND** akko za svaki rastući niz ideala $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ postoji $n \in \mathbb{N}$ tako da je $(\forall k > n)\ I_n = I_k$.*

Stav (PID je ND). Ako je $\mathbb{P}$ PID, onda je $\mathbb{P}$ ND.

Lema. Ako je $\mathbb{P}$ Neterin domen, onda za svako $a \in P \setminus P_0^*$ postoji bar jedan atom koji ga deli.

Δ. Trebalo bi da dokažemo: Ako je $\mathbb{P}$ Neterin domen, onda $(\forall a \in P \setminus P_0^*)\ (\exists b \in P)\ (b \mid a\ \wedge\ b$ je atom).

Dokazujemo: Ako $(\exists a \in P)\ (a \notin P_0^*\ \wedge\ (\forall b \in P)\ (b \mid a\ \Rightarrow\ b$ nije atom)), onda $\mathbb{P}$ nije ND.

Neka je $\Psi(a) := (a \notin P_0^*\ \wedge\ (\forall b \in P)\ (b \mid a\ \Rightarrow\ b$ nije atom)), i pretpostavimo da $(\exists a \in P)\ \Psi(a)$.

$\Psi(a)\ \Rightarrow\ a \notin P_0^*,\ a$ nije atom, $\Psi(a)$

$\Rightarrow\ (\exists a_1 \in P)\ (a_1 \mid a,\ a_1 \notin P_0^*,\ a_1 \nsim a),\ \Psi(a)$

$\Rightarrow\ (\exists a_1 \in P)\ (a_1 \notin P_0^*,\ (\forall b \in P)\ (b \mid a_1\ \Rightarrow\ b \mid a),\ a_1 \mid a,\ a_1 \nsim a),\ \Psi(a)$

$\Rightarrow\ (\exists a_1 \in P)\ (a_1 \notin P_0^*,\ (\forall b \in P)\ (b \mid a_1\ \Rightarrow\ b$ nije atom$),\ a_1 \mid a,\ a_1 \nsim a)$

$\Rightarrow\ (\exists a_1 \in P)\ (\Psi(a_1),\ (a) \subsetneq (a_1))$.

Zato $\exists\ a, a_1, a_2, \ldots \in P$ tako da $\Psi(a),\ \Psi(a_1),\ (a) \subsetneq (a_1),\ \Psi(a_2),\ (a_1) \subsetneq (a_2),\ \ldots$. Sledi da

$\exists\ a, a_1, a_2, \ldots \in P$ tako da je $(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots$ strogo rastući niz ideala. Znači da $\mathbb{P}$ nije ND. $\square$

0.5 Faktorizacijski domeni [FD]

Definicija. *Domen $\mathbb{P}$ je **faktorizacijski [FD]** akko svaki nenula nejedinični element $a \in P$ ima atomičnu faktorizaciju, faktoriše se na (konačan) proizvod nekih atoma. Preciznije, $\mathbb{P}$ je **FD** akko $(\forall a \in P \setminus P_0^*)\ (\exists k \in \mathbb{N})\ (\exists a_1, a_2, \ldots, a_k \in \mathrm{Atom}(\mathbb{P}))\ a = a_1 a_2 \cdots a_k$, gde je $P_0^* = \{0\} \cup P^*$.*

Stav (ND je FD). Ako je $\mathbb{P}$ ND, onda je $\mathbb{P}$ FD.

Δ. Pretpostavimo suprotno: $\mathbb{P}$ je Neterin, a nije faktorizaciski domen.

Neka je $\Phi(a) := (a \notin P_0^*\ \wedge\ a$ nema atomičnu faktorizaciju). $\mathbb{P}$ nije FD, pa $(\exists a \in P)\ \Phi(a)$.

$\mathbb{P}$ je ND, pa, prema prethodnoj Lemi, $a \notin P_0^*\ \Rightarrow\ (\exists a_1, b_1 \in P)\ (a = a_1 b_1\ \wedge\ a_1$ je atom).

$\Phi(a)\ \Rightarrow\ a \notin P_0^*,\ \Phi(a)$

$\Rightarrow\ (\exists a_1, b_1 \in P)\ (a = a_1 b_1,\ a_1$ je atom, $b_1 \notin P_0^*\ ),\ \Phi(a)$

$\Rightarrow\ (\exists b_1 \in P)\ (b_1 \mid a \nmid b_1,\ \Phi(b_1))$

$\Rightarrow\ (\exists b_1 \in P)\ (\Phi(b_1),\ (a) \subsetneq (b_1))$.

Zato $\exists\ a, b_1, b_2, \ldots \in P$ tako da $\Phi(a),\ \Phi(b_1),\ (a) \subsetneq (b_1),\ \Phi(b_2),\ (b_1) \subsetneq (b_2),\ \ldots$. Sledi da

$\exists\ a, b_1, b_2, \ldots \in P$ tako da je $(a) \subsetneq (b_1) \subsetneq (b_2) \subsetneq \cdots$ strogo rastući niz ideala.

Ovo je u kontradikciji sa pretpostavkom da je $\mathbb{P}$ ND. $\square$

0.6 Domeni sa jedinstvenom faktorizacijom [UFD]

Definicija. *Domen* $\mathbb{P}$ ***ima jedinstvenu faktorizaciju [je UFD]*** *akko* $\mathbb{P}$ *je FD i svake dve atomične faktorizacije elementa* $a \in P$ *su jednake do na redosled i asociranost faktora. Detaljnije,* $\mathbb{P}$ *je* ***UFD*** *akko* $(\forall a \in P \setminus P_0^*)\ (\exists k \in \mathbb{N})\ (\exists a_1, a_2, \ldots, a_k \in \mathrm{Atom}(\mathbb{P}))\ a = a_1 a_2 \cdots a_k$*, i: ako su* $a = a_1 a_2 \cdots a_k$ *i* $a = b_1 b_2 \cdots b_l$ *dve atomične faktorizacije, onda je* $k = l$ *i postoji permutacija* σ *skupa* $\{1, 2, \ldots, k\}$ *tako da je* $a_i \sim b_{\sigma(i)},\ 1 \le i \le k.$ Ekvivalentno,
$\mathbb{P}$ je **UFD** akko $\mathbb{P}$ je FD i važi UF: $(\forall k, l \in \mathbb{N})\ (\forall a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_l \in \mathrm{Atom}(\mathbb{P}))$
$\big(\ a_1 a_2 \cdots a_k \sim b_1 b_2 \cdots b_l \ \Rightarrow\ k = l,\ (\exists \sigma \in S_k)\ (a_1 \sim b_{\sigma(1)}, a_2 \sim b_{\sigma(2)}, \ldots, a_k \sim b_{\sigma(k)})\ \big)$.

Stav (o UFD). Neka je $\mathbb{P}$ FD. Tada: $\mathbb{P}$ je UFD akko svi atomi su prosti.

Δ. $\Rightarrow$: Neka je $\mathbb{P}$ UFD, $a \in P$ atom.
Neka su $b, c \in P$ i neka $a \mid bc$.
Ako $b \in P_0^*$, onda $a \mid c$; ako $c \in P_0^*$, onda $a \mid b$; ako je $b = 0$ ili $c = 0$, onda $a \mid b$ ili $a \mid c$, jer $a \mid 0$.
Znači, ako $b \in P_0^*$ ili $c \in P_0^*$, onda $a \mid b$ ili $a \mid c$.
Ako $b \notin P_0^*$, $c \notin P_0^*$, onda $(\exists d \in P)\ (ad = bc,\ d \notin P_0^*)$, ovo drugo zbog UF.
$\mathbb{P}$ je FD, $b, c, d \notin P_0^*$, pa $(\exists k, l, j \in \mathbb{N})\ (\exists b_1, \ldots, b_k, c_1, \ldots, c_l, d_1, \ldots, d_j \in \mathrm{Atom}(\mathbb{P}))$
$(\ d = d_1 \cdots d_j,\ b = b_1 \cdots b_k,\ c = c_1 \cdots c_l,\ ad_1 \cdots d_j = b_1 \cdots b_k c_1 \cdots c_l\ )$.
Iz poslednje jednakosti sledi, na osnovu UF, $a \sim b_s$ ili $a \sim c_t$, za neke $s, t, 1 \le s \le k, 1 \le t \le l$.
Znači, ako $b \notin P_0^*$, $c \notin P_0^*$, onda $a \mid b$ ili $a \mid c$.
$\Leftarrow$: Neka su svi atomi u $\mathbb{P}$ prosti.
Indukcijom po k, dokazujemo UF: $(\forall k, l \in \mathbb{N})\ (\forall a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_l \in \mathrm{Atom}(\mathbb{P}))$
$\big(\ a_1 a_2 \cdots a_k \sim b_1 b_2 \cdots b_l \ \Rightarrow\ k = l,\ (\exists \sigma \in S_k)\ (a_1 \sim b_{\sigma(1)}, a_2 \sim b_{\sigma(2)}, \ldots, a_k \sim b_{\sigma(k)})\ \big)$.
BI: $k = 1$. Uvodimo oznake: Φ_1 za $a_1, b_1, b_2, \ldots, b_l \in \mathrm{Atom}(\mathbb{P})$, Ψ_1 za $a_1 \sim b_1 b_2 \cdots b_l$. Tada:
$\Phi_1,\ \Psi_1\ \Rightarrow\ a_1$ je prost, $a_1 \mid b_1 b_2 \cdots b_l,\ \Psi_1,\ \Phi_1$
$\Rightarrow\ a_1 \mid b_1\ \vee\ \ldots\ \vee\ a_1 \mid b_l,\ \Psi_1,\ \Phi_1$
$\Rightarrow\ (\exists \sigma \in S_l)\ b_{\sigma(1)} \sim a_1 \sim b_1 b_2 \cdots b_l,\ \Phi_1$
$\Rightarrow\ (\exists \sigma \in S_l)\ (a_1 \sim b_{\sigma(1)},\ b_{\sigma(2)} \cdots b_{\sigma(l)} \mid 1),\ \Phi_1$
$\Rightarrow\ l = 1,\ a_1 \sim b_1$.
KI: Neka je $k > 1$, i pretpostavimo da (IH:) tvrđenje važi za $k - 1$. Uvodimo oznake:
Φ_k za $a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_l \in \mathrm{Atom}(\mathbb{P})$, Ψ_k za $a_1 a_2 \cdots a_k \sim b_1 b_2 \cdots b_l$. Tada:
$\Phi_k,\ \Psi_k\ \Rightarrow\ a_1$ je prost, $a_1 \mid b_1 b_2 \cdots b_l,\ \Psi_k,\ \Phi_k$
$\Rightarrow\ a_1 \mid b_1\ \vee\ \ldots\ \vee\ a_1 \mid b_l,\ \Psi_k,\ \Phi_k$
$\Rightarrow\ (\exists \rho \in S_l)\ a_1 \mid b_{\rho(1)},\ \Psi_k,\ \Phi_k$
$\Rightarrow\ (\exists \rho \in S_l)\ (a_1 \sim b_{\rho(1)},\ a_2 \cdots a_k \sim b_{\rho(2)} \cdots b_{\rho(l)}),\ \Phi_k$
$\Rightarrow\ k - 1 = l - 1,\ (\exists \sigma \in S_k)\ (a_1 \sim b_{\sigma(1)},\ a_2 \sim b_{\sigma(2)},\ \ldots,\ a_k \sim b_{\sigma(k)}),$ po IH,
$\Rightarrow\ k = l,\ (\exists \sigma \in S_k)\ (a_1 \sim b_{\sigma(1)},\ a_2 \sim b_{\sigma(2)},\ \ldots,\ a_k \sim b_{\sigma(k)})$. $\square$

Stav (PID je UFD). Ako je $\mathbb{P}$ PID, onda je $\mathbb{P}$ UFD.

Δ. PID je ND, ND je FD, u PID su svi atomi prosti. Sledi: PID je UFD. $\square$