

Dziedzinę, której każdy ideał jest główny, określamy akronimem PID (od *principal ideal domain*). Takimi są np. $\mathbf{Z}$ i $K[X]$: w ideale I wybieramy najmniejszy (co do wartości bezwzględnej / stopnia) element a i sprawdzamy, że $I = (a)$; istotnie, gdyby $x \in I$ nie był podzielny przez a , to reszta z dzielenia x przez a też leżałaby w I , co przeczyłoby minimalności a . Ten argument stosuje się do dziedzin, w których można dzielić z resztą (w pewnym sensie mniejszą od tego, przez co dzielimy).

Def. Dziedzinę R nazywamy dziedziną euklidesową, jeśli istnieje funkcja $N: R \setminus \{0\} \rightarrow \mathbf{N} \cup \{0\}$ (zwana *normą*), taka że

$$(\forall b \in R)(\forall a \in R \setminus \{0\})(\exists q, r \in R)(b = qa + r \wedge (r = 0 \vee N(r) < N(a))).$$

Wniosek. Dziedzina euklidesowa jest PID.

Używa się tego wniosku np. by uzasadnić własność PID dla kilkunastu pierścieni podobnych do pierścienia Gaussa $\mathbf{Z}[i]$. A PID implikuje UFD, jak zaraz pokażemy.

Istnienie rozkładu.

Pokażemy najpierw, że niezerowy i nieodwracalny element x pierścienia R spełniającego PID daje się przedstawić jako iloczyn czynników nierozkładalnych.

Gdyby tak nie było, moglibyśmy nietrywialnie napisać $x = aa_1 = aba_2 = abca_3 = \dots$. Wtedy $(x) \subset (a_1) \subset (a_2) \subset \dots$ (wszystkie zawierania właściwe). Ale wówczas $I = \bigcup (a_i)$ jest ideałem R , właściwym (gdyż $1 \notin I$); zatem $I = (A)$ dla pewnego A należącego do pewnego (a_j) . Stąd wynika, że ciąg ideałów (a_i) stabilizuje się od miejsca j , sprzeczność.

Jednoznaczność rozkładu.

Pokażemy, że w pierścieniu PID elementy nierozkładalne są pierwsze. Schemat dowodu jest taki:

$$\begin{array}{ccccc} a \text{ nierozkładalny} & \Rightarrow & (a) \text{ maksymalny} & \Leftrightarrow & R/(a) \text{ jest ciałem} \\ & & & & \Downarrow \\ a \text{ pierwszy} & \Leftarrow & (a) \text{ pierwszy} & \Leftrightarrow & R/(a) \text{ jest dziedziną} \end{array}$$

Uwagi: równoważności nie wymagają założenia PID, ani główności ideału; podobnie strzałka $\Downarrow$, która jest oczywista. Ideał I jest *pierwszy*, jeśli $ab \in I \Rightarrow a \in I \vee b \in I$. (Ćw. poziome strzałki są odwracalne.)

($\Rightarrow$) Gdyby $(a) \subset (b) \subset R$, to $b \in (a)$, zatem $a = bc$ dla pewnego c .

($\Leftarrow$) $a|xy \iff xy \in (a) \Rightarrow x \in (a) \vee y \in (a) \iff a|x \vee a|y$.

Przejdźmy teraz do uzasadniania równoważności. Odrzucamy więc założenie PID, a zamiast (a) rozpatrujemy dowolny ideał I .

($\iff$ dolna) R/I jest dziedziną, o ile spełnia: jeśli $xy + I = 0$ w R/I , to $x + I = 0$ w R/I lub $y + I = 0$ w R/I . Ale $z + I = 0$ w $R/I \iff z \in I$. Ta równoważność tłumaczy powyższy warunek na pierwszość ideału I .

Fakt. I pierwszy $\iff R/I$ jest dziedziną.

($\iff$ górna) Potrzebny jest

Lemat. Pierścień R jest ciałem $\iff R$ ma dwa ideały: (0) i R .

Dowód. ($\Rightarrow$) Niezerowy ideał I ma niezerowy element a . Ale wtedy każdy inny element $b = (ba^{-1})a$ należy do I , więc $I = R$. ($\Leftarrow$) Jeśli $a \neq 0$, to $(a) = R$. Zatem $1 \in (a)$, a stąd a odwracalny. $\diamond$

Teraz rozważmy homomorfizm ilorazowy $q: R \rightarrow R/I$. Przypisanie $J \mapsto q^{-1}J$ zadaje bijekcję między zbiorem ideałów R/I a zbiorem tych ideałów R , które zawierają I . Stąd

Fakt. I maksymalny $\iff R/I$ jest ciałem.

W ten sposób uzasadniliśmy wszystkie implikacje.

Tw. PID $\Rightarrow$ UFD.

Inne wnioski:

- Ideał maksymalny jest pierwszy.
- Niezerowy homomorfizm z ciała w pierścień jest monomorfizmem (bo jądro jest zerowym ideałem).