

Pierścień.

Pierścień to zbiór R z dwoma działaniami: dodawaniem $+$ i mnożeniem $\cdot$, oraz z wyróżnionym elementem 0 – spełniający warunki: (a) $(R, +, 0)$ jest grupą abelową, (b) rozdzielnosc mnożenia względem dodawania: $a(b+c) = ab+ac$, $(a+b)c = ac+bc$. Dla nas pierścień będzie zawsze dodatkowo *przemienny* (tzn. $ab = ba$) i z *jedynką* (tzn. z elementem $1 \in R$ spełniającym $a \cdot 1 = 1 \cdot a = a$).

Przykłady: ciała, $\mathbf{Z}$, pierścienie wielomianów $R[X]$, pierścień szeregów formalnych $R[[X]]$, pierścień szeregów Laurenta $R((X))$, pierścień funkcji ciągłych $C(X)$, $\mathbf{Z}_{(p)}$.

Rozkład na czynniki.

Rozkład liczby całkowitej na czynniki pierwsze nazywamy jednoznaczny, choć ściśle rzecz biorąc mamy z tym kłopoty: $-6 = (-2) \cdot 3 = 2 \cdot (-3)$. Dla $\mathbf{R}[X]$: $x^2 - 1 = (x-1)(x+1) = (2x-2)(\frac{1}{2}x + \frac{1}{2})$. Aby sprawę dobrze wyrazić wprowadzamy kilka pojęć. Elementem *odwracalnym* (inaczej *jednostką*) nazywamy każdy taki element $u \in R$, dla którego istnieje $u' \in R$ spełniające $uu' = 1$. Zbiór $\mathcal{U}(R)$ (piszemy też: $R^\times$) wszystkich jednostek pierścienia R tworzy grupę moltiplikatywną. Elementy $r, r' \in R$ nazywamy *stowarzyszonymi* (i piszemy $r \sim r'$), jeśli $r' = ur$ dla pewnej jednostki u (z tą dokładnością czynniki rozkładu mają szansę być jednoznaczne). Element r (niezerowy i nieodwracalny) nazywamy *nierozkładalnym*, jeśli w każdym rozkładzie $r = r'r''$ albo r' , albo r'' jest jednostką.

Przykłady. $\mathbf{Z}$: jednostki to $\{\pm 1\}$, stowarzyszenie to równość co do znaku, elementami nierozkładalnymi są $\pm 2, \pm 3, \pm 5, \dots$. $\mathbf{C}[X]$: jednostki to niezerowe stałe, stowarzyszenie to proporcjonalność, elementy nierozkładalne to jednomiany $X - z$ (i ich skalarnie krotności).

Pierścień nazywamy *UFD* (od *unique factorization domain*), jeśli

- (a) jest *dziedzina*: $(rr' = 0) \Rightarrow (r = 0 \vee r' = 0)$, oraz
- (b) każdy element – niezerowy i niebędący jednostką – rozkłada się na iloczyn czynników nierozkładalnych, jednoznacznie (z dokładnością do kolejności i stowarzyszenia).

Pierścienie $\mathbf{Z}$ oraz $K[X]$ są UFD. Istnienie rozkładu bierze się stąd, że przy rozkładaniu wartość bezwzględna / stopień maleje. Jednoznaczność sprawdza się tak: jeśli $r = r_1 \cdot \dots \cdot r_n = r'_1 \cdot \dots \cdot r'_k$ są dwoma rozkładami na czynniki nierozkładalne, to r_1 dzieli iloczyn po prawej, więc dzieli pewien jego czynnik, więc jest z owym czynnikiem stowarzyszony. Kluczowym krokiem tego argumentu jest następująca własność elementów nierozkładalnych (zachodząca w $\mathbf{Z}$ i w $K[X]$, ale nie w każdym pierścieniu): $p|ab \Rightarrow p|a \vee p|b$ (piszemy $x|y$ i czytamy “ x dzieli y ”, jeśli $y = xz$ dla pewnego z). Elementy p (niezerowe i nieodwracalne) mające tę własność nazywamy *pierwszymi*. W pierścieniach $\mathbf{Z}$ i $K[X]$ elementy nierozkładalne są pierwsze: (rozszerzony) algorytm Euklidesa pozwala wyrazić największy (co do wartości bezwzględnej / stopnia) wspólny dzielnik (a, b) elementów a, b w postaci $xa + yb$; jeśli teraz $p|ab$ ale $p \nmid a$, to $1 = (p, a) = xp + ya$; stąd $b = xpb + yab$, i p dzieli oba składniki sumy, więc $p|b$.

Ideały.

W pierścieniu $\mathbf{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbf{Z}\}$ rozkład na czynniki nie jest jednoznaczny: $6 = 2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5})$, i wszystkie czynniki są nierozkładalne. (Tę nierozkładalność stwierdzamy z użyciem normy: $N(a + b\sqrt{-5}) = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2$. Norma jest moltiplikatywna, oraz nie ma w $\mathbf{Z}[\sqrt{-5}]$ elementów o normie 2 ani 3.) Kummer postanowił ratować własność UFD wprowadzając czynniki idealne: czynniki A, A', B, B' niebędące elementami $\mathbf{Z}[\sqrt{-5}]$, takie że $2 = AA'$, $3 = BB'$, $1 + \sqrt{-5} = AB$, $1 - \sqrt{-5} = A'B'$. Dla Kummera nie było istotne, *czym jest B*; chciał umieć poznać, kiedy $B|r$. Jeśli chcemy ratować UFD, to $B|r \iff BB'|rB' \iff BB'|rA'B' \iff 3|r(1 - \sqrt{-5})$. Stąd wychodzi, że $B|a + b\sqrt{-5} \iff 3|a - b$.

Dedekind (zgodnie z ideami Jocelyna de Soissons) *zdefiniował* czynnik B jako zbiór wszystkich $r \in \mathbf{Z}[\sqrt{-5}]$ “podzielnych przez B ”, tzn. jako $\{a + b\sqrt{-5} \in \mathbf{Z}[\sqrt{-5}] \mid 3|a - b\}$. Nazwał też tego typu zbiory *ideałami*.

Def. *Ideałem* pierścienia nazywamy jego niepusty podzbiór zamknięty na dodawanie i odejmowanie oraz na mnożenie przez dowolne elementy pierścienia. (Notacja: $I \triangleleft R$.)

Zauważmy, że zbiór elementów podzielnych przez ustalone $a \in R$ jest ideałem R . Ideał taki nazywamy *głównym* i oznaczamy (a) lub Ra . Definiujące własności ideału to podstawowe cechy zbioru tej postaci; można by powiedzieć, że ideał to zbiór elementów pierścienia poszukujących wspólnego dzielnika. Nie zawsze taki

dzielnik istnieje (w pierścieniu), jak pokazuje przykład powyżej. W języku ideałów łatwo wyrazić podzielność i stowarzyszenie: $a|b \iff (a) \supseteq (b)$; $a \sim b \iff (a) = (b)$.

Inne motywacje dla pojęcia ideału:

- 1) Jądro homomorfizmu pierścieni jest ideałem.
- 2) Jeśli $I \triangleleft R$, to na ilorazie (grup addytywnych) R/I można dobrze określić mnożenie: $(r + I)(r' + I) = rr' + I$. Powstaje w ten sposób pierścień ilorazowy.
- 3) Jeśli $V \subseteq X \subseteq \mathbf{R}^n$, to $I(V) = \{f \in C(X) \mid f|_V = 0\} \triangleleft C(X)$.