Algebra ISIM 2. Wykład 10: R UFD $\Rightarrow R[X]$ UFD

Ciało ułamków.

Niech R będzie dziedziną. Na zbiorze $R \times (R \setminus \{0\})$ par zapisywanych w postaci $\frac{p}{q}$ (gdzie $q \neq 0$) wprowadzamy relację równoważności (zwaną relacją równości): $\frac{p}{q} = \frac{p'}{q'} \iff pq' = p'q$. Na zbiorze klas abstrakcji definiujemy działania dodawania i mnożenia wzorami takimi jak dla zwykłych ułamków. Otrzymujemy w ten sposób ciało R_0 zwane ciałem ułamków dziedziny R. Odwzorowanie $R \ni r \mapsto \frac{r}{1} \in R_0$ jest monomorfizmem.

Przykłady: $\mathbf{Z}_0 = \mathbf{Q}$, $K[X]_0 = K(X)$.

Zawartość.

Niech R będzie UFD. Dla $r \in R$ i elementu pierwszego $p \in R$ określamy $v_p(r)$ jako wykładnik najwyższej potęgi p dzielącej r. Dla $r/s \in R_0$ kładziemy $v_p(r/s) = v_p(r) - v_p(s)$. Dla wielomianu $A = \sum_{i=0}^n a_i X^i \in R_0[X]$ definiujemy $v_p(A) = \min\{v_p(a_i) \mid 0 \leq i \leq n\}$. Wreszcie, wybieramy po jednym elemencie z każdej klasy stowarzyszenia elementów pierwszych pierścienia R otrzymując pewien zbiór $\mathcal{P}$. Definiujemy *zawartość* (ang. content) niezerowego wielomianu $A \in R_0[X]$ jako $c(A) = \prod_{p \in \mathcal{P}} p^{v_p(A)}$. Formalnie jest to element R_0, ale wygodnie jest o nim myśleć, że jest określony z dokładnością do mnożenia przez jednostki pierścienia R – wówczas zawartość staje się niezależna od wyboru zbioru $\mathcal{P}$. Będziemy pisać $a \sim b$, gdy $a/b \in R^\times$.

Wielomian A nazywamy *prymitywnym,* jeśli $c(A) \sim 1$.

Proste własności zawartości:

- Jeśli $\deg A = 0$, tzn. $A \in R_0$, to $A \sim c(A)$.
- Wielomian prymitywny leży w $R[X]$. (Inaczej pewien jego współczynnik miałby pewne v_p ujemne, ale wtedy v_p wielomianu też byłoby ujemne.)
- Każdy wielomian A jest postaci $A = c(A)A_1$, gdzie A_1 jest wielomianem prymitywnym. (Zwykłe czyszczenie mianowników.)
- Jeśli $q \in R_0$ i $A \in R_0[X]$, to $c(qA) \sim qc(A)$. (v_p każdego a_i zmienia się o $v_p(q)$.)
- Wielomian nierozkładalny w $R[X]$ jest prymitywny. (Inaczej $A = c(A)A_1$ jest rozkładem.)

Lemat Gaussa.

Iloczyn wielomianów prymitywnych jest prymitywny.

Dowód. Gdyby $A, B \in R[X]$ były prymitywne, a AB nie, to moglibyśmy znaleźć p z $v_p(AB) > 0$. Wtedy obrazy A i B w dziedzinie $(R/(p))[X]$ byłyby niezerowe, a ich iloczyn – obraz AB –zerowy, sprzeczność.

Wniosek. Dla $A, B \in R_0[X]$ zachodzi $c(AB) \sim c(A)c(B)$.

Mamy bowiem $c(AB)(AB)_1 = AB = c(A)c(B)A_1B_1$; licząc zawartości obu stron otrzymujemy tezę.

R **UFD** $\Rightarrow R[X]$ **UFD.**

Istnienie rozkładu: najpierw rozkładamy ściśle zmniejszając stopień czynników, potem wyciągamy zawartości (czynniki prymitywne pozostają nierozkładalne) i rozkładamy je w R.

Jednoznaczność rozkładu wymaga lematu:

Lemat. *Jeśli $A \in R[X]$ jest nierozkładalny w $R[X]$, to jest też nierozkładalny w $R_0[X]$.*

Gdyby $A = PQ$, $P, Q \in R_0[X]$, to $c(P)c(Q) = c(A) \sim 1$; wtedy $A = c(P)P_1c(Q)Q_1 = uP_1Q_1$ ($u \in R^\times$).

Niech teraz $A = \prod a_i \prod A_i = \prod b_j \prod B_j$ będą dwoma rozkładami A w $R[X]$, gdzie a_i, b_j są stopnia 0, zaś A_i, B_j stopnia dodatniego. Z jednoznaczności rozkładu w $R_0[X]$ wynika, że można połączyć A_i, B_j w stowarzyszone pary. Ale w takiej parze oba wielomiany są prymitywne, więc czynnik stowarzyszający jest jednostką R. Porównując teraz zawartości widzimy, że $\prod a_i \sim \prod b_j$, więc i te produkty muszą być równoważne na mocy warunku UFD dla R.

Wnioski.

$\mathbf{Z}[X]$ jest UFD, mimo że nie jest PID (np. $(2, X)$ nie jest główny).

$\mathbf{Z}[X, Y] = (\mathbf{Z}[X])[Y]$ jest UFD; przez indukcję: $\mathbf{Z}[X_1, \ldots, X_n]$ jest UFD.

Podobnie $K[X_1, \ldots, X_n]$ jest UFD.