12. Jednoznaczność rozkładu w pierścieniach wielomianów.

Celem tego rozdziału jest udowodnienie twierdzenia Gaussa, które mówi, że pierścień wielomianów nad dziedziną z jednoznacznoćią rozkładu jest także dziedziną z jednoznacznością rozkładu.

Rozważania poprzedzimy opisem konstrukcji, która danej dziedzinie całkowitości przyorz'adkowuje ciało, tę dziedzinę całkowitości zawierające jako podpierścień.

Ciało ułamków.

Załóżmy, że R jest dziedziną całkowitości. Obowiązuje wówczas, tak jak w ciele, prawo skracania (przez elementy niezerowe) dla mnożenia:

$$\forall_{x\neq 0}\forall_{y,z}\ xy = xz \Leftrightarrow y = z.$$

Jednak, inaczej niż w ciele, niektóre niezerowe elementy mogą nie mieć odwrotności. Okazuje się, że dziedzina R, choć sama nie musi być ciałem, jest zawsze *zawarta* w pewnym ciele. Istnieje prosta konstrukcja, która to gwarantuje, tzw. konstrukcja ciała ułamków $Q(R)$ dziedziny R. W szczególnym przypadku, gdy $R = \mathbb{Z}$ otrzymujemy dobrze znane ciało liczb wymiernych: $Q(\mathbb{Z}) = \mathbb{Q}$.

Niech R będzie dziedziną całkowitości. Na zbiorze par uporządkowanych $R \times (R \setminus \{0\})$ określamy relację równoważności $\sim$ wzorem
$(x, y) \sim (z, v) \Leftrightarrow xv = yz$. Klasę równoważności tej relacji nazywamy ułamkiem i oznaczamy symbolem $\frac{x}{y}$ (tak więc $\frac{x}{y} = \frac{z}{v} \Leftrightarrow xv = yz$). Zbiór wszystkich ułamków oznaczamy symbolem $Q(R)$.

12.1. Definicja. **Ciałem ułamków** *dziedziny całkowitości R nazywamy zbiór $Q(R)$ z ułamkiem $\frac{0}{1}$ jako zerem, ułamkiem $\frac{1}{1}$ jako jedynką i działaniami określonymi wzorami:*

$$\frac{x}{y} + \frac{p}{q} = \frac{xq + py}{yq}$$
$$\frac{x}{y} \cdot \frac{p}{q} = \frac{xp}{yq}$$
$$-\frac{p}{q} = \frac{-p}{q}$$

Łatwo sprawdzić, że takie działania są dobrze określone i że definiują ciało. Odwzorowanie $i : R \hookrightarrow Q(R)$ zadane wzorem $i(x) = \frac{x}{1}$ jest monomorfizmem pierścieni. Zatem istotnie, każda dziedzina całkowitości jest podpierścieniem pewnego ciała.

12.2. Przykład. Niech $R = k[X]$ będzie pierścieniem wielomianów ciała k. Ciało ułamków $Q(k[X])$ oznaczamy symbolem $k(X)$ i nazywamy **ciałem funkcji wymiernych nad** k. Dla $k = \mathbb{Z}_p$ konstrukcja ta dostarcza przykładu ciała nieskończonego charakterystyki p.

Konstrukcję ciała ułamków rozumiemy jako operację dodania do dziedziny całkowitości pewnych brakujących elementów. Zauważmy, że oczywiście

12.3. Uwaga. Jeżeli dziedzina całkowitości R jest ciałem, to $Q(R) \cong R$.

Ciało ułamków jest scharakteryzowane przez następujące stwierdzenie.

12.4. Stwierdzenie. *Jeżeli R jest dziedziną całkowitości, a $j : R \hookrightarrow F$ włożeniem w ciało F, to istnieje dokładnie jedno włożenie $k : Q(R) \hookrightarrow F$ dla którego $ki = j$, gdzie $i : R \hookrightarrow Q(R)$.*

Dowód tego twierdzenia jest oczywisty.

Twierdzenie Gaussa.

12.5. Twierdzenie Gaussa. *Jeżeli R jest dziedziną z jednoznacznością rozkładu, to pierścień wielomianów $R[X]$ jest także dziedziną z jednoznacznością rozkładu.*

W dalszych rozważaniach zakładamy, że R jest dziedziną z jednoznacznością rozkładu. Pierścień R jest zawarty w $R[X]$ jako wielomiany stopnia 0. Ponieważ R jest dziedziną całkowitości, to $\deg fg = \deg f + \deg g$. Ta prosta obserwacja pozwala na scharakteryzowanie odwracalnych i nierozkładalnych elementów dziedziny całkowitości $R[X]$.

12.6. Uwaga. *Element $R[X]$ jest odwracalny wtedy i tylko wtedy, gdy jest odwracalnym elementem R.*

12.7. Definicja. *Zawartością niezerowego wielomianu $f = a_0 + a_1X + \cdots + a_nX^n$ nazywamy $\mathrm{NWD}(a_0, a_1, \ldots, a_n)$ i oznaczamy ją symbolem $\mathrm{cont}(f)$. Zawartość wielomianu jest wyznaczona jednoznacznie z dokładnością do stowarzyszenia w R. Wielomian $f \in R[X] \setminus \{0\}$, nazywa się* **pierwotny** *jeżeli $\mathrm{cont}(f) = 1$.*

12.8. Stwierdzenie. *Każdy niezerowy wielomian możemy zapisać w postaci $f = \mathrm{cont}(f)f_1$, gdzie f_1 jest wielomianem pierwotnym.*

12.9. Stwierdzenie. *Elementami nierozkładalnymi dziedziny $R[X]$ są:*
nierozkładalne elementy pierścienia R
wielomiany pierwotne stopnia większego od zera, których nie można przedstawić w postaci iloczynu wielomianów mniejszego stopnia.

Dowód. Jest jasne, że nierozkładalne wielomiany stopnia 0, to dokładnie nierozkładalne elementy pierścienia R. Jeżeli $\deg f > 0$ i f nierozkładalny, to f musi być pierwotny i nie być iloczynem wielomianów mniejszego stopnia. W przeciwnym bowiem razie $f = \mathrm{cont}(f)f_1$ lub $f = gh$, $\deg g > 0$ i $\deg h > 0$ byłyby przedstawieniem f w postaci iloczynu elementów nieodwracalnych. Odwrotnie, przypuśćmy że f , $\deg f > 0$ jest wielomianem pierwotnym którego nie można przedstawić w postaci iloczynu wielomianów mniejszego stopnia. Jeżeli $f = gh$, to stopień jednego z wielomianów np. g jest równy 0. Zatem $g = a \in R$ i $a \mid \mathrm{cont}(f)$. Ponieważ $cont(f) = 1$, to a jest elementem odracalnym, a więc f jest nierozkładalny. □

Łatwo widać, że każdy wielomian można przedstawić w postaci iloczynu nierozkładalnych elementów $R[X]$.

12.10. Stwierdzenie. *Każdy element dziedziny $R[X]$ może być przedstawiony w postaci iloczynu elementów nierozkładalnych.*

Dowód. Wielomian $f \in R[X]$ przedstawiamy w postaci $f = \mathrm{cont}(f)f_1$, gdzie f_1 jest wielomianem pierwotnym. Element $\mathrm{cont}(f) \in R$ przedstawiamy w postaci iloczunu nierozkładalnych elementów R, gdyż R jest DJR - elementy nierozkładalne R są też elementami nierozkładalnymi $R[X]$. Wielomian pierwotny f_1 jeśli nie jest nierozkładalny, to $f_1 = g_1h_1$, przy czym $\deg g_1 < \deg f_1$ i $\deg h_1 < \deg f_1$ i

oczywiście oba wielomiany g_1 i h_1 są pierwotne. Powtarzamy procedurę w odniesieniu do wielomianów g_1 i h_1. Po skończonej liczbie kroków otrzymamy iloczyn pierwotnych wielomianów nierozkładalnych dodatniego stopnia, gdyż za każdym krokiem stopień wielomianu zmniejsza się. □

W celu zakończenia dowodu należy wykazać jednoznaczność rozkładu dowodząc (Stwierdzenie 10.7), że elementy nierozkładalne dziedziny $R[X]$ są pierwsze.

12.11. Stwierdzenie. *Jeżeli $a \in R$ jest elementem nierozkładalnym, to a jest elementem pierwszym dziedziny $R[X]$.*

Dowód. Jeżeli a jest elementem nierozkładalnym dziedziny z jednoznacznością rozkładu R, to a jest elementem pierwszym, czyli ideał (a) jest pierwszy i $R/(a)$ jest dziedziną całkowitości. Homomorfizm $\pi : R \to R/(a)$ wyznacza homomorfizm $\pi_*: R[X] \to R/(a)[X]$. Niech $a \mid fg$ w $R[X]$. Zatem $fg = ah$ w $R[X]$ i $\pi_*(f)\pi_*(g) = \pi_*(a)\pi_*(h)$ w pierścieniu $R/(a)[X]$. Ale $\pi_*(a) = 0$, więc w dziedzinie całkowitości $R/(a)[X]$, $\pi_*(f)\pi_*(g) = 0$, co oznacza. że $\pi_*(f) = 0$ lub $\pi_*(g) = 0$, co jest równoważne $a \mid f$ lub $a \mid g$. □

Pokazanie, że nierozkładalny wielomian pierwotny f dodatniego stopnia w $R[X]$ jest elementem pierwszym w $R[X]$ jest bardziej skomplikowane i stanowi główną trudność dowodu twierdzenia Gaussa. Pierścień $R[X]$ rozpatrujemy jako podpierścień pierścienia wielomianów $Q(R)[X]$ nad ciałem ułamków R. Wnioskowanie jest następujące:

1. nierozkładalny wielomian pierwotny f dodatniego stopnia w $R[X]$ jest elementem nierozkładalnym w $Q(R)[X]$,
2. ponieważ $Q(R)[X]$ jest DJR jako dziedzina euklidesowa, to wielomian f jest elementem pierwszym w $Q(R)[X]$,
3. jeżeli f jest elementem pierwszym w $Q(R)[X]$, to jest też elementem pierwszym w $R[X]$.

Do udowodnienia punktu 1. potrzebny jest:

12.12. Lemat Gaussa. *Dla wielomianów $f, g \in R[X] \setminus \{0\}$,*

$$\operatorname{cont}(fg) = \operatorname{cont}(f)\operatorname{cont}(g)$$

Dowód. Wystarczy pokazać, że iloczyn wielomianów pierwotnych jest wielomianem pierwotnym. Załóżmy nie wprost, że $f, g \in R[X] \setminus \{0\}$ są wielomianami pierwotnymi, a fg nie jest pierwotny. Ponieważ R jest DJR, to istnieje element pierwszy p, taki że $p \mid \operatorname{cont}(fg)$. Niech $f = a_0 + a_1X + \cdots + a_nX^n$, $g = b_0 + b_1X + \cdots + b_mX^m$ i niech a_r i b_s będą najniższymi współczynnikami, których nie dzieli p. Element p dzieli współczynnik c_{r+s} iloczynu fg, który jest równy

$$c_{r+s} = \underbrace{a_0b_{r+s} + \cdots + a_{r-1}b_{s+1}} + a_rb_s + \underbrace{a_{r+1}b_{s-1} + \cdots + a_{r+s}b_0}$$

Element p dzieli te składniki sumy, które są ujęte w klamry, a więc dzieli także a_rb_s. Ponieważ p jest elementem pierwszym, to $p \mid a_r$ lub $p \mid b_s$ - sprzeczność. □

12.13. Uwaga Niech teraz $Q(R)$ będzie ciałem ułamków dziedziny R z jednoznacznością rozkładu. Jest jasne, że wielomian $f \in Q(R)[X] \setminus \{0\}$ można przedstawić w postaci

$$f = \frac{a}{b}\tilde{f},$$

gdzie $\tilde{f} \in R[X]$, $\deg \tilde{f} = \deg f$ jest wielomianem pierwotnym (o współczynnikach z R), zaś $\frac{a}{b} \in Q(R)$. Ponieważ zawartość wielomianu jest wyznaczona jednoznacznie z dokładnością do stowarzyszenia w R, to wielomian $\tilde{f}$ jest wyznaczony jednoznacznie z dokładnością do mnożenia przez element odwracalny pierścienia R, czyli do stowarzyszenia w $R[X]$.

Możemy teraz podać dowód punktu 1.

12.14. Lemat. *Niech $f \in R[X]$ będzie wielomianem nierozkładalnym w $R[X]$, $\deg f > 0$. Wówczas f jest wielomianem nierozkładalnym w $Q(R)[X]$.*

Dowód. Z założenia wynika, że wielomian f jest pierwotny. Przypuśćmy, ze f jest rozkładalny w $Q(R)[X]$. Wynika z tego, że $f = gh$, gdzie $g, h \in Q(R)[X]$ nieodwracalne, a zatem $\deg g > 0$ i $\deg h > 0$. Przedstawiając wielomiany g i h zgodnie z uwagą poprzedzającą lemat, otrzymujemy

$$f = \frac{a}{b}\,\tilde{g}\,\tilde{h} \quad a, b \in R,$$

przy czym wielomiany $\tilde{g}, \tilde{h} \in R[X]$ są pierwotne dodatniego stopnia. Z lematu Gaussa wynika, że $\tilde{g}\tilde{h}$ jest także wielomianem pierwotnym, więc poprzedniego lematu wnioskujemy, że f i $\tilde{g}\tilde{h}$ są stowarzyszone w pierścieniu $R[X]$, co przeczy nierozkładalności f. □

12.15. Stwierdzenie. *Niech $f \in R[X]$ będzie wielomianem pierwotnym nierozkładalnym w $R[X]$, $\deg f > 0$. Wówczas f jest elementem pierwszym dziedziny $R[X]$.*

Dowód. Musimy pokazać, że ideał generowany przez wielomian f w pierścieniu $R[X]$ jest pierwszy. Oznaczmy go przez $(f)_{R[X]}$. Z poprzedniego lematu wynika, że wielomian f rozpatrywany jako element $Q(R)[X]$ jest nierozkładalny, a więc pierwszy. Oznaczmy przez $(f)_{Q(R)[X]}$ ideał generowany przez wielomian f w pierścieniu $Q(R)[X]$ – jest on ideałem pierwszym. Mamy $(f)_{R[X]} = i_*^{-1}((f)_{Q(R)[X]})$, gdzie $i_* : R[X] \to Q(R)[X]$ jest włożeniem. Zatem $(f)_{R[X]}$ jest pierwszy jako przeciwobraz ideału pierwszego. □

Możemy teraz zrekapitulować dowód twierdzenia Gaussa.

Dowód Twierdzenia Gaussa Ze stwierdzenia 12.10 wynika, że każdy element jest iloczynem elementów nierozkładalnych. Ze stwierdzeń 12.11 i 12.15 wynika, że rozkład ten jest jednoznaczny. □

12.16. Wniosek. *Jeżeli R jest dziedziną z jednoznacznością rozkładu, to dla każdej liczby naturalnej n , $R[X_1, X_2, \ldots, X_n]$ jest dziedziną z jednoznacznością rozkładu.*

Kryterium Eisensteina

Wiedząc, że pierścienie wielomianów skończonej liczby zmiennych nad ciałem są dziedzinami z jednoznacznością rozkładu, naturalnym jest pytanie o kryterium rozkładalności wielomianu. Odpowiedź na to pytanie jest trudna i nie dysponujemy warunkiem koniecznym i dostatecznym, który by te kwestie rozstrzygał. Niekiedy pomocny jest następujący warunek dostateczny.

12.17. Twierdzenie Kryterium Eisensteina. *Niech R będzie dziedziną z jednoznacznością rozkładu i niech $f \in R[X]$.*

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

Jeżeli istnieje element pierwszy dziedziny R, taki że
$p \nmid a_n$
$p \mid a_i$ *dla* $0 \leq i \leq n-1$
$p^2 \nmid a_0$.
Wówczas f jest elementem nierozkładalnym w $Q(R)[X]$. Jeżli f jest wielomianem pierwotnym, to f jest elementem nierozkładalnym w $R[X]$.

Dowód. Przypuśćmy, że f jest rozkładalny w $Q(R)[X]$. Z lematu 2.14 wynika, że $f = gh$ w $R[X]$, $\deg g > 0$ i $\deg h > 0$. Niech $\pi : R \to R/(p)$ będzie epimorfizmem na dziedzinę całkowitości $R/(p)$, zaś $\pi_* : R[X] \to R/(p)[X]$ homomorfizmem indukowanym. Z warunków zadania wynika, że $\pi_*(g)\pi_*(h) = \pi_*(f) = \pi(a_n)X^n$, $\pi(a_n) \neq 0$. Jeśli popatrzymy na tę równość jak na mającą miejsce w pierścieniu $Q(R/(p))[X]$, to z jednoznaczności rozkładu w $Q(R/(p))[X]$, wynika że $\pi_*(g)$ jest stowarzyszone w nim z X^k a $\pi_*(h)$ z X^l dla pewnych $k, l \in \mathbb{N}$, $k + l = n$. Mamy $k = \deg \pi_*(g) \leq \deg g$ i podobnie $l = \deg \pi_*(h) \leq \deg h$. Ponieważ $n = k + l \leq \deg g + \deg h = \deg f = n$, to $k = \deg g > 0$ i $l = \deg h > 0$. Wynika z tego, że wyraz wolny wielomianu g i wielomianu h jest podzielny przez p, co z kolei pociąga $p^2 \mid a_0$. Sprzeczność. □