9 Pierścienie

Pierścieniem nazywamy zbiór z dwoma łącznymi działaniami dodawaniem i mnożeniem. Dodawanie w pierścieniu jest przemienne, ma element neutralny 0 i przeciwny do każdego elementu pierścienia. Mnożenie jest rozdzielne względem dodawania. Dodatkowo będziemy zakładać, że w pierścieniu jest element neutralny dla mnożenia (jedność) i przemienność mnożenia. Takie pierścienie nazywa się zwykle przemiennymi z jednością.

Przykładami pierścieni są zbiór liczb całkowitych, pierścień wielonianów nad ciałem lub pierścieniem, pierścień macierzy o wyrazach należących do pierścienia (ten ostatni pierścień nie jest przemienny).

10 Moduły

Modułem nad pierścieniem R nazywamy algebrę z dodawaniem i (zewnętrznym) mnożeniem przez elementy R. Dodawanie w modułach jest łączne i przemienne, ma element neutralny i element przeciwny do każdego elementu modułu. Mnożenie jest rozdzielne względem dodawania, zachodzą prawa $1x = x$ oraz $(ab)x = a(bx)$. Moduły nad ciałami nazywamy przestrzeniami liniowymi.

Przykładami modułów są przestrzenie liniowe, zbiory wielomianów nad ciałem lub pierścieniem, zbiór Z^n z działaniami definiowanymi w zwykły sposób, jak dla wektorów. Każdy pierścień jest modułem nad samym sobą.

11 Ideały

Ideałem w pierścieniu R nazywamy zbiór $I \subseteq R$ zamknięty ze względu na odejmowanie i mnożenie (elementów I) przez dowolne elementy pierścienia.

Jeżeli pierścień R uważamy jako moduł nad R, to ideały w R są podmodułami modułu R.

Ideałem w pierścieniu R są zbiory

$$(a) = \{ax \in R : x \in R\}$$

(zbiór „wielokrotności” elementu a, takie ideały nazywamy głównymi) oraz

$$ker(f) = \{x \in R : f(x) = 0\},$$

gdzie f jest dowolnym homomorfizmem pierścienia R. Ten ostatni wzór ustala (z dokładnością do izomorfizmu) wzajemnie jednoznaczą odpowiedniość między ideałami w R i homomorfizmami R. Nazywa się on jądrem homomorfizmu f.

Lemat 11.1 *Niech R będzie pierścieniem i $A \subseteq R$. Wtedy zbiór*

$$(A) = \{\sum_{i=1}^{n} a_i x_i : n \in N \wedge a_1, \ldots, a_n \in A \wedge x_1, \ldots, x_n \in R\}$$

najmniejszy ideałem w R zawierającym A (jest ideałem generowanym przez A). $\square$

12 Ideały w pierścieniu liczb całkowitych

Twierdzenie 12.1 *Każdy ideał w pierścieniu liczb całkowitych jest główny.*

Dowód. Przypuśćmy, że $I \subseteq Z$ jest niezerowym (różnym od $\{0\}$) ideałem i a jest najmniejszą dodatnią liczbą należącą do I. Ideał (a) jest zawarty w I. Pokażemy, że jest równy I. W przeciwnym razie, istnieje $b \in I$ taki, że $b \notin (a)$. Podzielmy b przez a. Mamy więc $b = ka + r$ dla pewnego k i r takiego, że $0 < r < a$. Stąd $r = b - ka \in I$. W ten sposób uzyskaliśmy sprzeczność z definicją a. □

Wniosek 12.2 *Pierścień liczb całkowitych jest pierścieniem ideałów głównych.* □

Twierdzenie 12.3 *Pierścień wielomianów nad dowolnym ciałem jest pierścieniem ideałów głównych.*

Dowód. Twierdzenie to dowodzimy tak, jak poprzednie korzystając z możliwości dzielenia wielomianów przez siebie. □

Ideały mają związek z teorią podzielności. Dowodzi się np., że $(a) \cap (b) = (NWW(a,b))$, liczba a jest pierwsza wtedy i tylko wtedy, gdy ideał a jest maksymalny, różny od Z, itp. Element $a \neq 0$ jest nierozkładalny, jeżeli nie ma właściwego rozkładu, a więc nie daje się przedstawić w postaci iloczynu xy, gdzie x i y są nieodwracalne. Element a jest pierwszy, jeżeli jest różny od 0 i to, że a dzieli iloczyn xy implikuje, że a dzieli x lub dzieli y. W zbiorze liczb całkowitych definicje elementu nierozkładalnego i pierwszego są równoważne.

Lemat 12.4 *W pierścieniu przemiennym z jednością, bez dzielników zera elementy pierwsze są nierozkładalne.*

Dowód. Przypuśćmy, że a jest elementem pierwszym i jest rozkładalny Wtedy $a = xy$ i np. a dzieli x. Wtedy $a = (az)y$. Stąd $a(1 - zy) = 0$. Ponieważ element pierwszy jest różny od 0 więc $1 = zy$. Oznacza to, że rozkład nie jest właściwy. □

Lemat 12.5 *W pierścieniu ideałów głównych elementy nierozkładalne są pierwsze.*

Dowód. Przypuśćmy, że a jest nierozkładalny i dzieli xy. Weźmy ideał generowany przez a i x. Jest to ideał główny generowany przez b. Stąd $a = bz$ i jeden z elementów b lub z jest odwracalny. Jeżeli z jest odwracalny, to a (i b) dzielą x. Jeżeli b jest odwracalny, to z równości $b = ua + vx$ wynika, że $by = uay + vxy$ jest podzielny przez a. Więc także y jest podzielny przez a. □

Lemat 12.6 *Jeżeli elementy nierozkładalne są pierwsze i w pierścieniu każdy element $\neq 0$ można rozłożyć na iloczyn elementów nierozkładalnych, to jest to pierścień z jednoznacznością rozkładu (a więc rozkład każdego elementu jest jednoznaczny z dokładnością do kolejności czynników).*

13 Pierścień wielomianów nad Z

Rozważamy pierścień (formalnych) wielomianów $Z[x]$ zmiennej x nad pierścieniem liczb całkowitych.

Zbiór $\{w \in Z[x] : 2|w(0)\}$ jest ideałem, ale nie jest to ideał główny. Jako moduł jest generowany przez wielomian x i wielomian stały 2. Mamy

$$\{w \in Z[x] : 2|w(0)\} = \{x \cdot u(x) + 2 \cdot v(x) : u, v \in Z[x]\}.$$

14 Pierścienie noetherowskie

Lemat 14.1 *Rozważamy pierścień R. Następujące warunki są równoważne:*

1. *każdy ideał $I \subseteq R$ jest skończenie generowalny,*
2. *każdy (słabo) rosnący ciąg ideałów $\subseteq R$ stabilizuje się,*
3. *każdy niepusty zbiór ideałów ma element maksymalny.*

Pierścień R jest noetherowski (od nazwiska Noether, Amalie Emmy), jeżeli zachodzi jeden z trzech warunków z powyższego lematu.

Twierdzenie 14.2 *Pierścień przemienny z jednością i bez dzielników zera, noetherowski jest pierścieniem z rozkładem (niekoniecznie jednoznacznym).*

Dowód. Załóżmy, że istnieje element, który nie daje się przedstawić w postaci iloczynu elementów nierozkładalnych. Weźmy dowolny taki element a. Element a nie jest ani odwracalny, ani nie jest nierozkładalny. Daje się przedstawić w postaci iloczynu bc, b i c nie są odwracalne. Wtedy $(a) \subset (b), (c)$. Ponadto jeden z elementów b lub c nie może miec rozkładu. W ten sposób konstruujemy rosnący ciąg ideałow. □

Twierdzenie 14.3 (Hilbert?) *Jeżeli R jest pierścieniem noeterowskim, to $R[x]$ też jest pierścieniem noeterowskim.*

Dowód. Przypuśćmy, że I jest ideałem w $R[x]$. Niech A_n będzie zbiorem najstarszych współczynników wielomianów stopnia n z ideału I (możemy przyjąć, że $A_n = \{0\}$, jeżeli w I nie ma wielomianów stopnia n).

Zbiory A_n są ideałami w R, ciąg tych ideałów jest słabo rosnący, a więc $A_n \subseteq A_{n+1}$.

Przyjmijmy, że dla $a \in A_i$ symbolem w_a oznaczamy (wybrany) wielomian należący do I, stopnia i, o najstarszym współczynniku równym a.

Załóżmy, że ciąg A_n stabilizuje się od miejsca r. Ideały $A_1, \ldots, A_r$ są skończenie generowalne. Bierzemy generatory i wybieramy po jednym z odpowiadających im wielomianów z I. Pokażemy, że wybrane w ten sposób wielomiany generują I przedstawiając dowolny wielomian z I w postaci ich kombinacji. Zrobimy to przez indukcję ze względu na stopień rozkładanego wielomianu.

Przypuśćmy, że $W \in I$ ma stopień n i jego najstarszy współczynnik jest równy a. Zbiór A_n jest jednym z ideałów $A_1, \ldots, A_r$, przyjmijmy, że $n \geqslant r$ i $A_n = A_r$ (tak jest najczęściej, w pozostałych przypadkach trzeba minimalnie zmienić dalej podane wzory). Ideał A_r jest generowany przez $a_1, \ldots, a_m$. Wobec tego, $a = c_1 a_1 + \ldots + c_n a_m$ dla pewnych $c_i \in R$. Od wielomianu W najpierw odejmujemy stosowną kombinację wybranych wielomianów i otrzymujemy

$$V(x) = W(x) - c_1 w_{a_1}(x) x^{n-r} - \ldots - c_m w_{a_m} x^{n-r}.$$

Stopień V jest mniejszy od n i do wielomianu V możemy zastosować założenie indukcyjne. Stąd i z powyższego wzoru otrzymujemy potrzebne przedstawienie wielomianu W. □

Wniosek 14.4 (twierdzenie Hilberta o bazie) *Pierścień wielomianów $Z[x_1, \ldots, x_n]$ ze zmiennymi $x_1, \ldots, x_n$ jest noetherowski.* □

Wniosek 14.5 *Każdy nieskończony układ równań diofantycznych ze skończoną liczbą zmiennych jest równoważny układowi skończonemu.*

Dowód. Przypuśćmy, że rozważamy układ równań $w_i(\vec{x}) = 0$ dla $i \in K$. Weźmy najmniejszy ideał $I \subseteq Z[\vec{x}]$ zawierający wszystkie wielomiany w_i. Zauważmy, że

$$\{\vec{x} : w_i(\vec{x}) = 0 \text{ dla } i \in K\} = \{\vec{x} : w(\vec{x}) = 0 \text{ dla } w \in I\}.$$

Weźmy teraz wielomiany $v_1, \ldots, v_n$ generujące I. Każdy z tych wielomianów jest skończoną kombinacją wielomianów w_i dla $i \in K$. Niech K' będzie zbiorem indeksów wielomianów występujących w tych kombinacjach. Mamy też

$$\{\vec{x} : w(\vec{x}) = 0 \text{ dla } w \in I\} = \{\vec{x} : v_i(\vec{x}) = 0 \text{ dla } i = 1, \ldots, n\} = \{\vec{x} : w_i(\vec{x}) = 0 \text{ dla } i \in K'\}. \ \square$$