PIERŚCIENIE I CIAŁA

Wykład 7

Największy wspólny dzielnik i najmniejsza wspólna wielokrotność

Niech $a_1, a_2, ..., a_n$ będą niezerowymi elementami pierścienia całkowitego P. Element $d \in P$ jest ***największym wspólnym dzielnikiem*** $a_1, a_2, ..., a_n$, jeśli

(1) $\bigwedge\limits_{k=1,...,n} d \mid a_k$

(2) $\bigwedge\limits_{c \in P} \Big(\Big(\bigwedge\limits_{k=1,...,n} c \mid a_k \Big) \Rightarrow c \mid d \Big)$.

Warunek (1) oznacza, że d jest wspólnym dzielnikiem $a_1, a_2, ..., a_n$, zaś warunek (2), że każdy wspólny dzielnik $a_1, a_2, ..., a_n$ dzieli d. Największy wspólny dzielnik nie jest wyznaczony jednoznacznie, a jedynie z dokładnością do stowarzyszenia, tzn. jeżeli d_1, d_2 są największymi wspólnymi dzielnikami $a_1, a_2, ..., a_n$, to $d_2 = ud_1$ dla pewnego elementu odwracalnego $u \in P$. Dla największego wspólnego dzielnika d elementów $a_1, a_2, ..., a_n$ piszemy więc $d \sim \mathrm{NWD}(a_1, a_2, ..., a_n)$.

Mówimy, że elementy $a, b \in P$ są ***względnie pierwsze***, jeśli $1 \sim \mathrm{NWD}(a, b)$.

Dla $P = \mathbb{Z}$ za największy wspólny dzielnik niezerowych liczb $a_1, a_2, ..., a_n \in \mathbb{Z}$ uznajemy dodatni największy wspólny dzielnik d i piszemy $d = \mathrm{NWD}(a_1, a_2, ..., a_n)$. W tym przypadku mamy dokładną zgodność z nazwą, gdyż d jest największą liczbą wśród wszystkich wspólnych dzielników $a_1, a_2, ..., a_n$.

Podobnie definiujemy najmniejszą wspólną wielokrotność różnych od zera elementów $a_1, a_2, ..., a_n$ pierścienia całkowitego P. Element $w \in P$ jest ***najmniejszą wspólną wielokrotnością*** $a_1, a_2, ..., a_n$, jeśli

(1) $\bigwedge\limits_{k=1,...,n} a_k \mid w$

(2) $\bigwedge\limits_{c \in P} \Big(\Big(\bigwedge\limits_{k=1,...,n} a_k \mid c \Big) \Rightarrow w \mid c \Big)$.

Piszemy wtedy $w \sim \mathrm{NWW}(a_1, a_2, ..., a_n)$, gdyż najmniejsza wspólna wielokrotność nie jest wyznaczona jednoznacznie.

Dla $P = \mathbb{Z}$ za najmniejszą wspólną wielokrotność niezerowych liczb $a_1, a_2, ..., a_n \in \mathbb{Z}$ uznajemy dodatnią najmniejszą wspólną wielokrotność w i piszemy $w = \mathrm{NWD}(a_1, a_2, ..., a_n)$. Jest to najmniejsza liczba wśród wszystkich dodatnich wspólnych wielokrotności $a_1, a_2, ..., a_n$.

W pierścieniu Gaussa istnieje największy wspólny dzielnik i najmniejsza wspólna wielokrotność skończenie wielu niezerowych elementów. Korzystając z rozkładów na czynniki nierozkładalne otrzymujemy następujące wzory na $\mathrm{NWD}(a, b)$ i $\mathrm{NWW}(a, b)$ dla elementów a, b pierścienia Gaussa.

Twierdzenie 1. *Niech a, b będą elementami pierścienia Gaussa P, których rozkłady na czynniki nierozkładalne mają postać*

$$a = u \prod_{i=1}^{n} a_i^{p_i}, \quad b = v \prod_{i=1}^{n} a_i^{q_i}, \tag{1}$$

gdzie $u \sim 1$, $v \sim 1$, $p_1, ..., p_n, q_1, ..., q_n \in \mathbb{N} \cup \{0\}$. *Wtedy*

$$\prod_{i=1}^{n} a_i^{r_i} \sim \mathrm{NWD}(a,b), \quad \prod_{i=1}^{n} a_i^{s_i} \sim \mathrm{NWW}(a,b), \tag{2}$$

gdzie $r_i = \min\{p_i, q_i\}$, $s_i = \max\{p_i, q_i\}$ *dla* $i = 1, ..., n$. *Ponieważ* $r_i + s_i = p_i + q_i$, *więc w konsekwencji otrzymujemy wzór*

$$ab = uv \prod_{i=1}^{n} a_i^{p_i+q_i} \sim \mathrm{NWD}(a,b)\,\mathrm{NWW}(a,b). \tag{3}$$

Jeśli $1 \sim \mathrm{NWD}(a,b)$, *to wynika stąd, że*

$$ab \sim \mathrm{NWW}(a,b). \tag{4}$$

Przykład 1. Niech

$$a = 2 \cdot 3^2 \cdot 7^3 \cdot 13^4, \quad b = 2^5 \cdot 3^2 \cdot 5 \cdot 7^2 \cdot 11^3.$$

Wtedy

$$\mathrm{NWD}(a,b) = 2 \cdot 3^2 \cdot 7^2, \quad \mathrm{NWW}(a,b) = 2^5 \cdot 3^2 \cdot 5 \cdot 7^3 \cdot 11^3 \cdot 13^4.$$

Wzory (2) można uogólnić na przypadek, gdy wyznaczamy NWD i NWW dla więcej niż dwóch elementów pierścienia Gaussa. Mamy wtedy także wzory

$$\mathrm{NWD}(a_1, a_2, ..., a_n) \sim \mathrm{NWD}(\mathrm{NWD}(\mathrm{NWD}(a_1, a_2), a_3), ...), a_n)$$
$$\mathrm{NWW}(a_1, a_2, ..., a_n) \sim \mathrm{NWW}(\mathrm{NWW}(\mathrm{NWW}(a_1, a_2), a_3), ...), a_n),$$

które sprowadzają problem wyznaczania największego wspólnego dzielnika i najmniejszej wspólnej wielokrotności dla n elementów do wyznaczania największego wspólnego dzielnika i najmniejszej wspólnej wielokrotności dla dwóch elementów.

Wzór analogiczny do (3) nie jest prawdziwy dla więcej niż dwóch elementów, na przykład $\mathrm{NWD}(2,3,4) = 1$, $\mathrm{NWW}(2,3,4) = 12$, więc

$$\mathrm{NWD}(2,3,4)\,\mathrm{NWW}(2,3,4) = 12 \neq 2 \cdot 3 \cdot 4.$$

Jednak (4) ma swój odpowiednik dla n elementów.

Twierdzenie 2. *Niech* $a_1, a_2, \ldots, a_n$ *będą parami względnie pierwszymi elementami pierścienia Gaussa* P. *Wtedy*

$$a_1 a_2 \ldots a_n \sim \mathrm{NWW}(a_1, a_2, \ldots, a_n).$$

Zgodnie z definicją elementu pierwszego, jeśli taki element dzieli iloczyn, to dzieli któryś z czynników. W następnym twierdzeniu mamy uogólnienie tej własności.

Twierdzenie 3. *Jeżeli* a, b, c *są niezerowymi elementami pierścienia Gaussa* P, $a \mid bc$ *i* $1 \sim \mathrm{NWD}(a,b)$, *to* $a \mid c$.

Dowód. Ponieważ $a \mid bc$, więc bc jest wspólną wielokrotnością a i b. Zatem $\mathrm{NWW}(a,b) \mid bc$. Ale zgodnie z (4) mamy $ab \sim \mathrm{NWW}(a,b)$. Stąd $ab \mid bc$ i w konsekwencji $a \mid c$. □

Pierścienie euklidesowe

Definicja 1. Pierścień całkowity P jest ***pierścieniem euklidesowym*** jeśli istnieje funkcja $N : P \to \mathbb{N} \cup \{0\}$ taka, że

(1) $\bigwedge\limits_{a \in P} N(a) = 0 \Leftrightarrow a = 0$

(2) $\bigwedge\limits_{a,b \in P \setminus \{0\}} a \mid b \Rightarrow N(a) \leqslant N(b)$

(3) Jeżeli $a, b \in P$, $b \neq 0$, to istnieją $q, r \in P$ takie, że $N(r) < N(b)$ i

$$a = qb + r \quad \text{(wzór na dzielenie z resztą).} \tag{5}$$

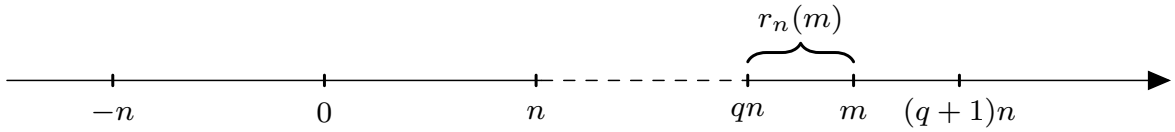
Uwaga 1. Jeśli $a, b \in P \setminus \{0\}$ i $a \mid b$, to z warunku (2) wiemy, że $N(a) \leqslant N(b)$. Przy dodatkowym założeniu, że a nie jest stowarzyszone z b mamy ostrą nierówność

$$N(a) < N(b).$$

Rzeczywiście, ponieważ $a \mid b$, więc $b = ac$ dla pewnego $c \in P$, przy czym jeśli a nie jest stowarzyszone z b, to c nie jest elementem odwracalnym. Dzieląc a przez b z resztą otrzymujemy $a = qb + r$, przy czym $N(r) < N(b)$. Mamy $a = qac + r$, czyli $a(1 - qc) = r$. Ponieważ c nie jest elementem odwracalnym, więc $qc \neq 1$. Stąd $r \neq 0$ i z warunku (2) otrzymujemy nierówność $N(a) \leqslant N(r) < N(b)$.

Element $r \in P$ ze wzoru (5) nazywamy resztą z dzielenia a przez b. Reszta ta nie musi być wyznaczona jednoznacznie.

Przykład 2.
1. Pierścień $\mathbb{Z}$ jest pierścieniem euklidesowym dla $N(a) = |a|$. Mamy tutaj dwie możliwe reszty z dzielenia: jedną nieujemną i drugą niedodatnią. Zwykle za resztę z dzielenia liczby $m \in \mathbb{Z}$ przez $n \in \mathbb{Z}$ przyjmuje się nieujemną resztę, którą oznaczmy przez $r_n(m)$.



2. Pierścień $\mathbb{Z}[i]$ jest pierścieniem euklidesowym dla $N(z) = |z|^2$. Tutaj $|z|$ oznacza moduł liczby zespolonej z.

Twierdzenie 4. *Każdy pierścień euklidesowy P jest pierścieniem ideałów głównych.*

Dowód. Niech I będzie ideałem w P. Jeśli $I = \{0\}$, to $I = (0)$. Jeśli $I \neq \{0\}$, to wybieramy $b \in I$ taki, że

$$N(b) = \min\{N(a) : a \in I,\ a \neq 0\}. \tag{6}$$

Dla $a \in I$ mamy $a = qb + r$, gdzie $q, r \in P$ i $N(r) < N(b)$. Ponieważ $b \in I$, więc $qb \in I$ i stąd także $r = a - qb \in I$. Ale $N(r) < N(b)$, co wobec wzoru (6) jest możliwe jedynie wtedy, gdy $r = 0$. Zatem $a = qb$ dla każdego $a \in I$, czyli $I = (b)$. □

W szczególności pierścień $\mathbb{Z}$ jest pierścieniem ideałów głównych, przy czym generatorem ideału $I \neq \{0\}$ w pierścieniu $\mathbb{Z}$ jest liczba

$$n = \min\{k > 0 : k \in I\}.$$

Twierdzenie 5. *Jeżeli P jest pierścieniem euklidesowym, to P jest pierścieniem Gaussa.*

Nie każdy pierścień Gaussa jest pierścieniem euklidesowym. Na przykład pierścień $\mathbb{Z}[x]$ wielomianów o współczynnikach całkowitych jest pierścieniem Gaussa, ale nie jest ideałów głównych (patrz wykład 6), a więc nie jest pierścieniem euklidesowym.

Algorytm Euklidesa

Ponieważ pierścień euklidesowy P jest pierścieniem Gaussa, więc dla dowolnych niezerowych elementów $a, b \in P$ istnieją $\mathrm{NWD}(a,b)$, $\mathrm{NWW}(a,b)$ i można je wyznaczyć korzystając z rozkładów na czynniki nierozkładalne. W tym przypadku $\mathrm{NWD}(a,b)$ można także wyznaczyć przy użyciu algorytmu Euklidesa. Jego podstawą jest następująca obserwacja.

Uwaga 2. Załóżmy, że w pierścieniu całkowitym P zachodzi równość $a = qb + r$. Wtedy zbiór wszystkich wspólnych dzielników elementów a, b jest taki sam, jak zbiór wszystkich wspólnych dzielników elementów b, r. Wynika stąd, że jeśli istnieją $\mathrm{NWD}(a,b)$ i $\mathrm{NWD}(b,r)$, to $\mathrm{NWD}(a,b) \sim \mathrm{NWD}(b,r)$.

Dowód. Załóżmy, że $d \mid a$ i $d \mid b$. Ponieważ $r = a - qb$, więc $d \mid r$. Zatem d jest wspólnym dzielnikiem b i r. Na odwrót, jeśli $d \mid b$ i $d \mid r$, to z równości $a = qb + r$ wynika, że $d \mid a$. Zatem r jest wspólnym dzielnikiem a i b. □

Niech a, b będą niezerowymi elementami pierścienia euklidesowego P. Wykonujemy kolejne dzielenia z resztą:

$$\begin{aligned}
a &= q_0 b + r_0, \quad && N(r_0) < N(b),\\
b &= q_1 r_0 + r_1, \quad && N(r_1) < N(r_0),\\
r_0 &= q_2 r_1 + r_2, \quad && N(r_2) < N(r_1),\\
&\vdots && \vdots\\
r_{n-2} &= q_n r_{n-1} + r_n, \quad && N(r_n) < N(r_{n-1}),\\
r_{n-1} &= q_{n+1} r_n. &&
\end{aligned}$$

Ze względu na to, że $N(b) > N(r_0) > ... > N(r_{n-1}) > N(r_n)$ są liczbami naturalnymi, nie może być to ciąg nieskończony, a więc po skończonej liczbie kroków dostajemy resztę 0.

Twierdzenie 6. *Ostatnia niezerowa reszta w* ***algorytmie Euklidesa*** *jest największym wspólny dzielnikiem a i b, czyli $r_n \sim \mathrm{NWD}(a,b)$.*

Dowód. Z ostatniego wzoru wynika, że $r_n \sim \mathrm{NWD}(r_n, r_{n-1})$. Stąd i z uwagi 2 otrzymujemy

$$\begin{aligned}
r_n \sim \mathrm{NWD}(r_n, r_{n-1}) \sim \mathrm{NWD}(r_{n-1}, r_{n-2}) \sim ...\\
... \sim \mathrm{NWD}(r_1, r_0) \sim \mathrm{NWD}(r_0, b) \sim \mathrm{NWD}(a,b).
\end{aligned}$$ □

Równania diofantyczne

Twierdzenie 7. *Dla dowolnych niezerowych elementów a, b pierścienia euklidesowego P istnieją elementy $x, y \in P$ takie że*

$$ax + by \sim \mathrm{NWD}(a, b). \tag{7}$$

Dowód. Stosując algorytm Euklidesa otrzymujemy $r_0 = a - q_0 b = ax_0 + by_0$, gdzie $x_0 = 1$, $y_0 = -q_0$. Następnie

$$r_1 = b - q_1 r_0 = b - q_1(ax_0 + by_0) = -ax_0 q_1 + b(1 - y_0) = ax_1 + by_1,$$

gdzie $x_1 = -x_0 q_1$, $y_1 = 1 - y_0$.

Postępując w ten sposób otrzymujemy kolejne równości $r_k = ax_k + by_k$ dla $k = 0, 1, ..., n$. Ostatnia z nich daje wzór $ax_n + by_n = r_n \sim \mathrm{NWD}(a, b)$. □

Obie strony przystawania (7) można pomnożyć przez dowolny element $c \in P$. Prowadzi to do następującej obserwacji.

Uwaga 3. Niech a, b, d będą niezerowymi elementami pierścienia euklidesowego P. Równanie

$$ax + by = d \tag{8}$$

ma rozwiązanie $x, y \in P$ wtedy i tylko wtedy, gdy $\mathrm{NWD}(a, b) \mid d$.

Twierdzenie 8. *Elementy a, b pierścienia euklidesowego P są względnie pierwsze wtedy i tylko wtedy, gdy istnieją $x, y \in P$ takie, że*

$$ax + by = 1 \tag{9}$$

Dowód. Jeżeli elementy a, b są względnie pierwsze, to równanie (8) ma rozwiązanie dla każdego $d \in P$, a więc w szczególności dla $d = 1$. Na odwrót, jeśli istnieją $x, y \in P$, dla których zachodzi równość (9) i $c \in P$ jest wspólnym dzielnikiem a i b, to c dzieli lewą stronę w (9). Stąd c dzieli prawą stronę, czyli 1, więc $c \sim 1$. □

Rozwiązując równanie (8) można zawsze przejść do postaci (9). Rzeczywiście, niech $d_0 \sim \mathrm{NWD}(a, b)$. Wtedy $d = d_0 d_1$, $a = d_0 a_1$ i $b = d_0 b_1$ dla pewnych $d_1, a_1, b_1 \in P$. Skracając obie strony równania (8) przez d_0 otrzymujemy

$$a_1 x + b_1 y = d_1,$$

przy czym elementy a_1, b_1 są względnie pierwsze. Stąd równanie

$$a_1 x + b_1 y = 1$$

ma rozwiązanie $x_1, y_1 \in P$. Zatem $a_1 x_1 d_1 + b_1 y_1 d_1 = d_1$ i dalej

$$d_0 a_1 x_1 d_1 + d_0 b_1 y_1 d_1 = d_0 d_1,$$

czyli $ax_1 d_1 + by_1 d_1 = d$, co oznacza, że rozwiązaniem równania (8) jest $x = x_1 d_1$, $y = y_1 d_1$.

Równanie (9) nie ma jednoznacznego rozwiązania i zbiór wszystkich rozwiązań opisuje następujące twierdzenie.

Twierdzenie 9. *Niech a, b będą względnie pierwszymi elementami pierścienia euklidesowego P. Jeśli $ax_0 + by_0 = 1$, gdzie $x_0, y_0 \in P$, to dowolne rozwiązanie równania*

$$ax + by = 1$$

ma postać $x = x_0 + cb$ i $y = y_0 - ca$, gdzie $c \in P$.

Dowód. Niech $ax + by = 1$, gdzie $x, y \in P$. Odejmując stronami od tej równości równość $ax_0 + by_0 = 1$ otrzymujemy $a(x - x_0) + b(y - y_0) = 0$. Zatem

$$a(x - x_0) = b(y_0 - y),$$

a ponieważ elementy a, b są względnie pierwsze, więc $a \mid (y_0 - y)$, czyli $y_0 - y = ca$ dla pewnego $c \in P$. Stąd $y = y_0 - ca$.

Ponadto $a(x - x_0) = bca$ i stąd $x - x_0 = bc$, czyli $x = x_0 + cb$. □

Równania postaci (8) otrzymujemy chcąc wyznaczyć element odwrotny do danego elementu pierścienia $\mathbb{Z}_n$.

Twierdzenie 10. *Niezerowy element k pierścienia $\mathbb{Z}_n$ jest odwracalny wtedy i tylko wtedy, gdy liczba k jest względnie pierwsza z n.*

Dowód. Fakt, że $l \in \mathbb{Z}_n$ jest elementem odwrotnym do k oznacza, że $k \odot_n l = 1$, czyli $r_n(kl) = 1$, więc $kl = qn + 1$ dla pewnego $q \in \mathbb{Z}$. Z twierdzenia 8 wynika więc, że aby istniał element odwrotny k^{-1} do k w $\mathbb{Z}_n$, liczby k i n muszą być względnie pierwsze.

Na odwrót, jeśli k i n są względnie pierwsze, to zgodnie z twierdzeniem 8 istnieją $x, y \in \mathbb{Z}$ takie, że $kx + ny = 1$, czyli $kx = n(-y) + 1$. Oznacza to, że

$$1 = r_n(kx) = r_n(r_n(k)r_n(x)) = r_n(kr_n(x)) = k \odot_n r_n(x).$$

Zatem k jest elementem odwracalnym i $k^{-1} = r_n(x)$. □

Pierścień wielomianów

Niech P będzie pierścieniem przemiennym z $1 \neq 0$. Przez $C(P)$ oznaczmy zbiór wszystkich ciągów $(a_0, a_1, ...)$ o wyrazach z P. W $C(P)$ definiujemy działania:

$$(a_n) + (b_n) = (a_n + b_n), \quad (a_n) \cdot (b_n) = (c_n), \tag{10}$$

gdzie

$$c_n = \sum_{i+j=n} a_i b_j,$$

czyli

$$c_0 = a_0 b_0,\ c_1 = a_0 b_1 + a_1 b_0,\ c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0, ...$$

Zbiór $C(P)$ z tymi działaniami jest pierścieniem przemiennym z $1 \neq 0$.

Wielomianem nazywamy ciąg $(a_n) \in C(P)$, który jest od pewnego miejsca zerowy, czyli istnieje $m \in \mathbb{N}$ takie, że $a_n = 0$ dla wszystkich $n > m$. Zbiór wszystkich wielomianów z działaniami (10) jest również pierścieniem przemiennym z $1 \neq 0$.

Oznaczamy $x = (0, 1, 0, ...)$. Wtedy

$$x^k = (0, 0, ..., 0, 1, 0, ...)$$

dla $k = 1, 2...$, gdzie 1 występuje na k-tym miejscu. Niech $f = (a_0, a_1, ..., a_n, 0, 0, 0, ...)$. Wtedy

$$\begin{aligned} f &= (a_0, 0, ...) + (0, a_1, 0, ...) + (0, 0, a_2, 0, ...) + ... + (0, 0, ..., 0, a_n, 0, 0, ...) = \\ &= (a_0, 0, ...) + (a_1, 0, 0, ...)x + (a_2, 0, 0, ...)x^2 + ... + (a_n, 0, 0, ...)x^n. \end{aligned} \tag{11}$$

Pierścień wszystkich wielomianów o współczynnikach z P oznaczmy przez $P[x]$.

Ponieważ

$$(a, 0, 0, ...) + (b, 0, 0, ...) = (a + b, 0, 0, ...), \quad (a, 0, 0, ...) \cdot (b, 0, 0, ...) = (ab, 0, 0, ...)$$

więc wielomian postaci $(a, 0, 0, 0, ...)$ możemy utożsamiać z elementem $a \in P$. Przy takim utożsamieniu wzór (11) przyjmuje postać

$$f = a_0 + a_1x + a_2x^2 + ... + a_nx^n = \sum_{k=0}^{n} a_kx^k.$$

Jeśli f jest wielomianem zerowym, czyli $a_i = 0$ dla każdego i, to za stopień wielomianu f przyjmujemy $-\infty$ i piszemy $\operatorname{st} f = -\infty$. Jeśli f nie jest wielomianem zerowym, to jego stopień definiujemy jako

$$\operatorname{st} f = \max\{k : a_k \neq 0\}.$$

Dla $f, g \in P[x]$ mamy

$$\operatorname{st}(f + g) \leqslant \max\{\operatorname{st} f, \operatorname{st} g\}, \quad \operatorname{st}(fg) \leqslant \operatorname{st} f + \operatorname{st} g.$$

We wzorach tych może pojawiać się $-\infty$. Przyjmujemy, że $-\infty < m$ i $-\infty + m = -\infty$ dla wszystkich $m \in \mathbb{N} \cup \{0\}$.

Jeśli współczynniki przy najwyższej potędze x w f i g nie są dzielnikami zera, to

$$\operatorname{st}(fg) = \operatorname{st} f + \operatorname{st} g.$$

W szczególności jeżeli P jest pierścieniem całkowitym, to wzór ten jest prawdziwy dla dowolnych niezerowych wielomianów $f, g \in P[x]$.

Niech $f = \sum_{k=0}^{n} a_kx^k \in P[x]$, gdzie $\operatorname{st} f > 0$. Wstawiając zamiast x element $c \in P$ otrzymujemy element pierścienia

$$f(c) = \sum_{k=0}^{n} a_kc^k$$

Funkcję która elementowi $c \in P$ przyporządkowuje $f(c)$ nazywamy funkcją wielomianową odpowiadającą wielomianowi f. Funkcję tę również oznaczmy przez f, chociaż dla pewnych pierścieni nie ma jednoznacznej odpowiedniości między wielomianami, a funkcjami wielomianowymi.

Przykład 3. Niech $P = \mathbb{Z}_2$ i $f = x + x^2$. Wtedy $f(0) = 0$ i $f(1) = 1 \oplus 1 = 0$, więc wielomianowi f odpowiada zerowa funkcja wielomianowa.

W tym przypadku nie jest więc prawdą, że jeśli funkcje wielomianowe dwóch wielomianów są identyczne, to wielomiany te są sobie równe, czyli mają takie same współczynniki.

Przykład ten pokazuje dlaczego definiujemy wielomian jako ciąg współczynników, a nie jako funkcję. Jeśli jednak P jest nieskończonym pierścieniem całkowitym, to dwie funkcje wielomianowe są identyczne wtedy i tylko wtedy, gdy wielomiany te są sobie równe. W tym

przypadku nie ma potrzeby rozróżniania wielomianów i funkcji wielomianowych. Jest tak np. dla wielomianów o współczynnikach w $\mathbb{R}$ albo $\mathbb{C}$.

Dzielenie wielomianów

Twierdzenie 11. *Niech P będzie pierścieniem przemiennym, $f, g \in P[x]$ i współczynnik przy najwyższej potędze x w wielomianie g jest odwracalny. Wtedy istnieją jednoznacznie wyznaczone wielomiany $q, r \in P[x]$ takie, że $\operatorname{st} r < \operatorname{st} g$ i*

$$f = qg + r. \tag{12}$$

W szczególności dzielenie jest wykonalne, jeśli g jest wielomianem unormowanym, czyli współczynnik w g przy najwyższej potędze x jest równy 1. Jeśli P jest ciałem, to współczynnik przy najwyższej potędze x w g jest niezerowy, a więc odwracalny i z twierdzenia 11 otrzymujemy następujący wniosek.

Wniosek 1. *Jeżeli P jest ciałem, to $P[x]$ jest pierścieniem euklidesowym dla funkcji $N : P \to \mathbb{N} \cup \{0\}$ określonej wzorem $N(f) = 2^{\operatorname{st} f}$, gdzie przyjmujemy $2^{-\infty} = 0$. Zatem $P[x]$ jest pierścieniem Gaussa.*