Maciej Grzesiak

Wielomiany

1. Pojęcia podstawowe

Wielomian definiuje się w szkole średniej jako funkcję postaci

$$f(x) = a_0 + a_1x + a_2x + \ldots + a_nx^n$$

Dogodniejsza z punktu widzenia algebry jest następująca definicja.

Definicja 1. Niech K będzie ciałem. *Wielomianem* jednej zmiennej o współczynnikach z K nazywamy każdy ciąg $f = (a_0, a_1, a_2, \ldots)$, gdzie wyrazy ciągu f są prawie wszystkie równe 0 (tzn. istnieje takie n, że $a_m = 0$ dla $m > n$).

W zbiorze wielomianów wprowadzamy działania:

$$f + g = (a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots)$$

$$fg = (a_0b_0, a_0b_1 + a_1b_0, a_0b_2 + a_1b_1 + a_2b_0, \ldots)$$

Po wprowadzeniu oznaczeń:

$$(0, 0, 0, \ldots) = 0,\ (1, 0, 0, \ldots) = 1,\ (0, 1, 0, \ldots) = X$$

widzimy, że

$$(0, 0, 1, 0, \ldots) = X^2\ ,\ (0, 0, 0, 1, 0, \ldots) = X^3 \text{ itd.}$$

Możemy wobec tego napisać:

$$f = (a_0, a_1, a_2, \ldots, a_n) = a_0 + a_1X + a_2X + \ldots + a_nX^n$$

i wtedy działania na wielomianach można wykonywać tak, jak to się robiło w szkole średniej. Jak widać, zmienna X, która pojawia się w zapisie, pełni rolę czysto formalną — ułatwia zapis wielomianu i wykonywanie działań na wielomianach.
Każdemu wielomianowi o współczynnikach z K można przyporządkować *funkcję wielomianową* $f : K \longrightarrow K$:

$$K \ni x \longrightarrow a_0 + a_1x + \ldots + a_nx^n \in K.$$

Element $a_0 + a_1x + \cdots + a_nx^n$ nazywać będziemy *wartością wielomianu* w punkcie $x \in K$.
Rozróżnienie między wielomianami a funkcjami wielomianowymi nie jest tylko formalizmem. Czasem dwa różne wielomiany określają tę samą funkcję. Np. wielomiany $1 + X$ oraz $1 + X^3$ wyznaczają tę samą funkcję w ciele $\mathbb{Z}_3$:

$$0 \to 1, \quad 1 \to 2, \quad 2 \to 0.$$

Jednak dla ciała $\mathbb{R}$ lub ciała $\mathbb{C}$ odpowiedniość:

$$\text{wielomian} \to \text{funkcja wielomianowa}$$

jest wzajemnie jednoznaczna.
Zbiór wszystkich wielomianów jednej zmiennej o współczynnikach z K oznaczamy przez $K[X]$.
Stopień wielomianu f, tzn. największą z liczb n, dla których $a_n \neq 0$, będziemy oznaczali przez $\deg f$. Przyjmujemy, że $\deg 0 = -\infty$. Łatwo zauważyć, że

$$\deg(f + g) \leqslant \max(\deg f, \deg g),$$

$$\deg(fg) = \deg f + \deg g.$$

2. Dzielenie wielomianów

Definicja 2. Niech $f, g \in K[X]$. Mówimy, że w $K[X]$ jest wykonalne *dzielenie z resztą* wielomianu g przez wielomian f, gdy istnieją takie wielomiany $q, r \in K[X]$, że $g = fq + r$, przy czym $\deg r < \deg f$.

Wielomian f nazywamy *unormowanym*, jeżeli $f \neq 0$ i jego najwyższy współczynnik jest równy 1.

Twierdzenie 1. *Jeżeli $f \in K[X]$ jest wielomianem unormowanym, a $g \in K[X]$ dowolnym wielomianem, to w $K[X]$ jest wykonalne dzielenie z resztą g przez f.*

D o w ó d. Twierdzenie jest prawdziwe gdy $\deg g < \deg f$ (wtedy $q = 0$, $r = g$). Niech $m = \deg g, m \geqslant n, n = \deg f$. Załóżmy, że twierdzenie jest prawdziwe dla wielomianu g stopnia mniejszego niż m. Niech teraz $\deg g = m$ i niech $g - b_m X^{m-n} f = h$. W wielomianie h współczynnik przy X^m jest równy 0. Stąd $\deg h < m$. Na mocy założenia indukcyjnego istnieją takie $q, r \in K[X]$, $\deg r < n$, że $h = fq + r$. Wobec tego $g = b_m X^{m-n} f + h = b_m X^{m-n} f + fq + r = (b_m X^{m-n} + q)f + r$, co należało wykazać. □

Przykład. Obliczyć ilorazy i reszty z dzielenia:
1. $(X^4 + 4X^3 + X^2 + aX + 1) : (X^2 + X - 1)$
2. $(3X^5 - X^4 + X^3 + 7X^2 - 6X + 8) : (X^3 - X + 2)$
3. $(2X^3 - X^2 + 2X - 3) : (X - 1)$
4. $(\mathrm{i}\, z^3 + 2z - 1 + 3\,\mathrm{i}) : (z - 2\,\mathrm{i})$

Definicja 3. Wielomian $d(X)$ nazywamy *największym wspólnym dzielnikiem* (nwd) wielomianów $f(X)$ i $g(X)$ jeśli
1. $d(X)$ dzieli zarówno $f(X)$ jak i $g(X)$,
2. każdy wielomian dzielący $f(X)$ i $g(X)$ jest dzielnikiem $d(X)$,
3. $d(X)$ jest unormowany.

Ostatni warunek jest po to, aby nwd był jednoznacznie określony.
Największy wspólny dzielnik można wyznaczyć stosując *algorytm Euklidesa.*

Opis algorytmu Euklidesa.
Niech $P = \mathbb{Z}$ lub $P = K[x]$ (K – ciało), i niech a, b będą dowolnymi elementami pierścienia P. Algorytm Euklidesa znajdowania największego wspólnego dzielnika $\mathrm{nwd}(a, b)$ polega na wykonywaniu kolejnych dzieleń:

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1 q_2 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ \dots &\quad \dots \quad \dots \\ r_{n-2} &= r_{n-1} q_n + r_n \\ r_{n-1} &= r_n q_{n+1} \end{aligned}$$

dopóki nie uzyskamy reszty 0.
Ostatnia niezerowa reszta to właśnie $\mathrm{nwd}(a, b)$.
Z algorytmu wynika dodatkowo, że istnieją elementy $s, t \in P$ takie, że

$$\mathrm{nwd}(a, b) = sa + tb.$$

Przykład. Wyznaczyć w pierścieniu $\mathbb{R}[X]$ największy wspólny dzielnik $d(X)$ wielomianów $f(X) = X^5 + X^4 + X^3 + X^2 + X + 1$ i $g(X) = X^4 + X^3 + 2X^2 + X + 1$ i przedstawić go w postaci $d(X) = a(X)f(X) + b(X)g(X)$.
(Odp. $d(X) = 2(X^2 + X + 1)$ i $d(X) = (X + 1)f(X) + (-X^2 - X + 1)g(X)$).

3. Obliczanie wartości wielomianów

Omówimy teraz problem obliczania wartości wielomianów. Niech $f \in K[X]$,

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

Aby obliczyć wartość $f(x_0)$ dla jakiegoś $x_0 \in K$, można obliczać każdy człon osobno i potem dodać. Wymaga to j mnożeń do obliczenia j–tego składnika, czyli $1+2+\cdots+n = n(n+1)/2$ mnożeń oraz n dodawań.
Poprawimy efektywność, jeśli będziemy wykorzystywać już obliczone wartości licząc $x_0^{j+1} = x_0 x_0^j$. Wtedy wymaga to $2n-1$ mnożeń oraz n dodawań.
Jednak najbardziej efektywny sposób znajdziemy pisząc wielomian w postaci zagnieżdżonej:

$$f(x_0) = (\cdots((a_n x_0 + a_{n-1})x_0 + a_{n-2})\, x_0 + \cdots)\, x_0 + a_0.$$

Ten schemat postępowania (*schemat Hornera*) wymaga tylko n mnożeń oraz n dodawań.
Schemat ten zapisujemy następująco:

	a_n	a_{n-1}	a_{n-2}	$\cdots$	a_1	a_0
		ab_n	ab_{n-1}	$\cdots$	ab_2	ab_1
x_0	$b_n = a_n$	b_{n-1}	b_{n-2}	$\cdots$	b_1	$b_0 = f(x_0)$

Liczby b_k pojawiające się po drodze są współczynnikami ilorazu z dzielenia $f(X)$ przez $X - x_0$:

$$f(X) = (b_n X^{n-1} + b_{n-1} X^{n-2} + \cdots + b_2 X + b_1)(X - x_0) + b_0,$$

gdyż porównując współczynniki po lewej i prawej stronie otrzymujemy układ równości:

$$\begin{aligned} b_n &= a_n \\ b_{n-1} - b_n x_0 &= a_{n-1} \\ &\vdots \quad \vdots \quad \vdots \\ b_2 - b_3 x_0 &= a_2 \\ b_1 - b_2 x_0 &= a_1 \\ b_0 - b_1 x_0 &= a_0, \end{aligned}$$

czyli:

$$\begin{aligned} b_n &= a_n \\ b_{n-1} &= b_n x_0 + a_{n-1} \\ &\vdots \quad \vdots \quad \vdots \\ b_2 &= b_3 x_0 + a_2 \\ b_1 &= b_2 x_0 + a_1 \\ b_0 &= b_1 x_0 + a_0. \end{aligned}$$

A więc wielomian $q = b_n X^{n-1} + b_{n-1} X^{n-2} + \cdots + b_2 X + b_1$ jest ilorazem z dzielenia $f(X)$ przez $X - x_0$.

Wniosek 1. (twierdzenie Bézout) *Reszta z dzielenia $f(X)$ przez $X - x_0$ wynosi $f(x_0)$.*

Przykład. Obliczymy $f(3)$ dla $f(X) = X^5 + 4X^4 + 3X^3 - 2X + 1$.

	1	4	3	0	−2	1
		3	21	72	216	642
3	1	7	24	72	214	643

Zatem $f(3) = 643$.

Jednocześnie widzimy, że dzieląc $f(X) = X^5 + 4X^4 + 3X^3 - 2X + 1$ przez $X - 3$ otrzymujemy $q(X) = X^4 + 7X^3 + 24X^2 + 72X + 214$ i resztę 643.

4. Pierwiastki wielomianów

Element $c \in K$ jest pierwiastkiem wielomianu $f \in K[X]$, jeśli $f(a) = 0$.

Twierdzenie 2. *Element $c \in K$ jest pierwiastkiem wielomianu $f \in K[X]$ wtedy i tylko wtedy, gdy f jest podzielny przez $(X - c)$.*

D o w ó d. ($\Rightarrow$) Na mocy twierdzenia 1 $f = (X-c)q+r$, $\deg r < 1$, czyli r jest stałą. Ponieważ $f(c) = 0$, więc $0 = f(c) = (c - c)q(c) + r$. Stąd $r = 0$. ($\Leftarrow$) Odwrotnie, jeśli $f = (X - c)q$, to $f(c) = (c - c)q(c) = 0$, co kończy dowód twierdzenia. □

Definicja 4. Jeżeli $f = (X - c)^k q$, gdzie $q(c) \neq 0$, to c nazywamy *k-krotnym pierwiastkiem* wielomianu f. Elementy ciała K nie będące pierwiastkami wielomianu f nazywamy 0-krotnymi pierwiastkami wielomianu.

Przykład. Każdy pierwiastek niezerowego wielomianu ma jakąś krotność nie większą niż $\deg f$, gdyż wielomian stopnia n nie może być podzielny przez $(X - c)^k$ dla $k > n$.

Twierdzenie 3. *Niech $f \in K[X]$, $f \neq 0$, i niech $c_1, c_2, \ldots, c_n$ będą różnymi pierwiastkami wielomianu f o krotnościach $m_1, m_2, \ldots, m_n$. Wielomian f można przedstawić w postaci*

$$f = (X - c_1)^{m_1}(X - c_2)^{m_2} \cdots (X - c_n)^{m_n} \cdot h, \tag{1}$$

gdzie h jest pewnym wielomianem.

Dowód można przeprowadzić przez indukcję względem n. Łatwe szczegóły pomijamy.

Wniosek 2. *Jeżeli $c_1, \ldots, c_n$ są różnymi pierwiastkami wielomianu $f \in K[X]$ o krotnościach odpowiednio $m_1, \ldots, m_n$, to*

$$m_1 + \cdots + m_n \leqslant m,$$

gdzie $m = \deg f$.

D o w ó d. Istotnie stopień wielomianu (1) jest równy $m_1 + \cdots + m_n + \deg h$, a $\deg f = m$, więc $m_1 + \ldots + m_n \neq m$. □

Twierdzenie 4. (wzory Viete'a) *Niech $f \in K[X]$, gdzie K jest ciałem. Jeżeli*

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

i $c_1, c_2, \ldots, c_n$ są różnymi pierwiastkami wielomianu f, to

$$\sum_{k=1}^{n} c_k = -\frac{a_{n-1}}{a_n},$$

$$\sum_{i,j=1, i\neq j}^{n} c_i c_j = \frac{a_{n-2}}{a_n},$$

$$\cdots$$

$$\prod_{k=1}^{n} c_k = (-1)^n \frac{a_0}{a_n}.$$

D o w ó d. Wystarczy przedstawić wielomian f w postaci

$$f = a_n(X - c_1)(X - c_2)\cdots(X - c_n)$$

wymnożyć i porównać z pierwotną postacią.

5. Pierwiastki z jedności

Definicja 5. *Pierwiastkiem stopnia n* z elementu $b \in K$ nazywamy każdy pierwiastek dwumianu $X^n - b$.

Kolejne twierdzenie pokazuje specjalną rolę pierwiastków z jedności.

Twierdzenie 5. *Niech element $a \in K$ będzie pierwiastkiem stopnia n z elementu $b \in K$, $b \neq 0$, i niech $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r$ będą wszystkimi pierwiastkami stopnia n z 1 w K. Wówczas elementy $\varepsilon_1 a, \varepsilon_2 a \ldots, \varepsilon_r a$ są wszystkimi pierwiastkami stopnia n z elementu b.*

D o w ó d. Przede wszystkim elementy $\varepsilon_i a$ dla $i = 1, \ldots, r$ są pierwiastkami stopnia n z elementu b ponieważ $(\varepsilon_i a)^n = \varepsilon_i^n a^n = 1 \cdot a^n = b$. Ponadto, jeśli a_1 jest dowolnym pierwiastkiem stopnia n z b, to $a_1 a^{-1}$ jest pierwiastkiem stopnia n z 1, gdyż $(a_1 a^{-1})^n = a_1^n (a^n)^{-1} = b b^{-1} = 1$. Wobec tego $a_1 a^{-1} = \varepsilon_i$ dla pewnego $i = 1, \ldots, r$, a stąd $a_1 = a\varepsilon_i$, co kończy dowód. □
Oczywiście, jeśli w powyższym twierdzeniu $\varepsilon_i \neq \varepsilon_j$ dla $i \neq j$, to $\varepsilon_i a \neq \varepsilon_j a$ dla $i \neq j$. Otrzymujemy więc poniższy wniosek.

Wniosek 3. *Jeżeli $0 \neq b \in K$ ma w K pierwiastek stopnia n, to liczba pierwiastków stopnia n z b w ciele K równa się liczbie pierwiastków stopnia n z 1 w K.*

Definicja 6. Pierwiastek ε stopnia n z 1 nazywamy *pierwiastkiem pierwotnym* stopnia n, jeżeli ε nie jest pierwiastkiem z 1 stopnia mniejszego niż n.

Twierdzenie 6. *Każdy pierwiastek z 1 w ciele K jest pierwiastkiem pierwotnym dokładnie jednego stopnia. Jeśli ε jest pierwiastkiem pierwotnym stopnia n, to w ciele tym istnieje dokładnie n różnych pierwiastków stopnia n z 1; są to potęgi $\varepsilon^0 = 1$, $\varepsilon^1 = \varepsilon, \ldots, \varepsilon^{n-1}$.*

Do wyznaczenia wszystkich pierwiastków z 1 stopnia n wystarczy więc znaleźć jakikolwiek pierwiastek pierwotny stopnia n.
Przykład. Łatwo uzasadnić, że wszystkie pierwiastki stopnia n z jedności w ciele liczb zespolonych są potęgami pierwiastka $\varepsilon_1 = \cos(2\pi/n) + i \sin(2\pi/n)$. Dodamy teraz (bez dowodu) następującą uwagę.
Na to, by liczba ε_k była n-tym pierwiastkiem pierwotnym z jedności, potrzeba i wystarcza, by liczby k i n były względnie pierwsze.
Na przykład, dla $n = 5$ pierwotne są $\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4$. Dla $n = 6$ pierwotne są tylko ε_1 i ε_5.
Łatwo uzasadnić, że pierwiastki $1, \varepsilon_1, \ldots, \varepsilon_1^{n-1}$ są wierzchołkami n-kąta wypukłego foremnego wpisanego w okrąg jednostkowy. Gdy weźmiemy zamiast ε_1 inny pierwiastek pierwotny ε_k i połączymy po kolei wierzchołki $1, \varepsilon_k, \varepsilon_k^2, \ldots, \varepsilon_k^{n-1}$, otrzymamy gwiaździsty n-bok foremny wpisany w koło jednostkowe.
Następujace twierdzenie nazywane jest tradycyjnie zasadniczym twierdzeniem algebry.

Twierdzenie 7. (zasadnicze twierdzenie algebry) *Każdy wielomian stopnia dodatniego o współczynnikach zespolonych posiada w ciele liczb zespolonych co najmniej jeden pierwiastek.*

Znanych jest kilkadziesiąt dowodów tego twierdzenia (pierwszy był Gaussa z 1799 r.). Wszystkie są dość trudne. Przy tym dowody czysto algebraiczne właściwie nie istnieją, zatem tradycyjna nazwa jest myląca — to twierdzenie należałoby właściwie zaliczyć do analizy zespolonej. W ciałach $\mathbb{Q}$ i $\mathbb{R}$ twierdzenie nie jest prawdziwe, bo wielomian $X^2 + 1$ nie ma pierwiastka w $\mathbb{R}$ (a tym bardziej w $\mathbb{Q}$).
Zauważmy, że z twierdzenia 7 wynika prosto poniższy wniosek.

Wniosek 4. *Dowolny wielomian stopnia n o współczynnikach zespolonych posiada w ciele liczb zespolonych dokładnie n pierwiastków (pierwiastki wielokrotne liczymy tyle razy, ile wynosi ich krotność).*

6. Pierścienie ilorazowe wielomianów

Niech P będzie pierścieniem, a I jego ideałem.

Jeżeli $I \lhd P$, to I jest dzielnikiem normalnym grupy $(P, +)$. Można więc utworzyć grupę ilorazową P/I. Jej elementami są warstwy względem podgrupy I. Warstwę zawierającą element a oznaczamy $a + I$. W grupie ilorazowej określimy mnożenie wzorem:

$$(a + I)(b + I) = ab + I.$$

Grupa P/I po wprowadzeniu w niej mnożenia uzyskuje strukturę pierścienia. Pierścień ten nazywamy *pierścieniem ilorazowym.*
Jeżeli ideał jest generowany przez zbiór jednoelementowy, to nazywamy go *głównym.* Pierścień całkowity, którego każdy ideał jest główny, nazywamy *pierścieniem ideałów głównych.*

Wniosek 5. *Ideał główny (a) generowany przez element $a \in P$ jest zbiorem elementów postaci ab, gdzie $b \in P$.*

Twierdzenie 8. *Każdy ideał pierścienia liczb całkowitych $\mathbb{Z}$ jest główny.*

Zastosujemy powyższe pojęcia do pierścienia wielomianów.

Opis pierścienia ilorazowego wielomianów.

Rozważmy pierścień $K[X]$ wielomianów nad ciałem K.

Twierdzenie 9. *Każdy ideał pierścienia $K[X]$ jest główny.*

Zatem każdy ideał P pierścienia $K[X]$ jest generowany przez pewien wielomian $p(X)$, tj. składa się ze wszystkich wielomianów podzielnych przez $p(X)$.
Wobec tego elementami pierścienia ilorazowego $K[X]/P$ są klasy równoważności relacji na $K[X]$ określonej warunkiem

$$f(X) = g(X) \bmod (p(X)) \text{ wtedy i tylko wtedy, gdy } f(X) - g(X) \in (p(X))$$

Lemat 1. *$f(X) = g(X) \bmod (p(X))$ wtedy i tylko wtedy, gdy $f(X)$ i $g(X)$ dają tę samą resztę przy dzieleniu przez $p(X)$.*

Zatem każda warstwa $[f(X)]$ zawiera resztę z dzielenia $f(X)$ przez $p(X)$. Z poniższego twierdzenia wynika, że ta reszta jest jednoznacznie określona.

Twierdzenie 10. *Niech $K[X]$ będzie pierścieniem wielomianów nad ciałem K i niech P oznacza ideał generowany przez wielomian $p(X)$ stopnia $n > 0$. Każdy element pierścienia ilorazowego $K[X]/P$ jest postaci*

$$P + a_0 + a_1 X + \cdots + a_{n-1} X^{n-1},$$

gdzie $a_0, a_1, \ldots, a_{n-1} \in K$, przy czym różnym ciągom $a_0, a_1, \ldots, a_{n-1}$ odpowiadają różne elementy.

Przykład. Napisać tabelki operacji w pierścieniu $\mathbb{Z}_2[X]/(X^2 + X + 1)$.
Możliwe reszty z dzielenia przez $X^2 + X + 1$ to $0, 1, X, X + 1$. Są więc 4 warstwy:

$$P, P + 1, P + X, P + X + 1.$$

Tabelka dodawania:

$+$	P	$P+1$	$P+X$	$P+X+1$
P	P	$P+1$	$P+X$	$P+X+1$
$P+1$	$P+1$	P	$P+X+1$	$P+X$
$P+X$	$P+X$	$P+X+1$	P	$P+1$
$P+X+1$	$P+X+1$	$P+X$	$P+1$	P

Tabelka mnożenia:

$\cdot$	P	$P+1$	$P+X$	$P+X+1$
P	P	P	P	P
$P+1$	P	$P+1$	$P+X$	$P+X+1$
$P+X$	P	$P+X$	$P+X+1$	$P+1$
$P+X+1$	P	$P+X+1$	$P+1$	$P+X$

Przy obliczaniu iloczynów uwzględniamy fakt, że $P + X^2 + X + 1 = P$ (czyli praktycznie $X^2 + X + 1 = 0$, bądź równoważnie $X^2 = X + 1$).
Elementy pierścienia ilorazowego można oznaczać: $[f(X)]$ lub $P + f(X)$, ale najpraktyczniej jest oznaczać je po prostu jako $a_0 + a_1X + \cdots + a_{n-1}X^{n-1}$, bo taki wielomian określa warstwę jednoznacznie.
Jeżeli $P = (p(X))$ oraz $\deg p(X) = n$, to elementami pierścienia ilorazowego są wszystkie wielomiany stopnia mniejszego od n. Ilość tych wielomianów zależy od ciała K.
Przykład. Niech $p(X) = X^2+1$. Wtedy pierścień ilorazowy składa się z wielomianów postaci $a_1X + a_0$, gdzie $a_0, a_1 \in K$. Zatem
1. jeśli $K = \mathbb{R}$, to jest nieskończenie wiele takich wielomianów;
2. jeśli $K = \mathbb{Z}_2$, to są 4 takie wielomiany;
3. jeśli $K = \mathbb{Z}_3$, to jest 9 takich wielomianów;
4. jeśli $K = \mathbb{Z}_5$, to jest 25 takich wielomianów;

Mnożenie warstw (czyli wielomianów) wykonujemy w tym pierścieniu modulo $X^2 + 1$, co praktycznie oznacza, że X^2 zastępujemy przez -1. Zatem
1. jeśli $K = \mathbb{R}$, to $(a + bX)(c + dX) = ac + (ad + bc)X + bdX^2 = (ac - bd) + (ad + bc)X$;
2. jeśli $K = \mathbb{Z}_2$, to np. $(X + 1)^2 = X^2 + 1 = 0$;
3. jeśli $K = \mathbb{Z}_3$, to np. $(X + 2)^2 = X^2 + X + 1 = X$;
4. jeśli $K = \mathbb{Z}_5$, to np. $(X + 2)^2 = X^2 + 4X + 4 = -1 + 4X + 4 = 4X$.

Należy pamiętać, że elementami pierścienia ilorazowego są warstwy względem ideału $(p(X))$, czyli zbiory wielomianów. Warstwa zawiera tylko jeden wielomian stopnia mniejszego niż $\deg p(X)$, i ten wielomian jest jej reprezentantem.