9. Wykład 9: Jednoznaczność rozkładu w pierścieniach wielomianów. Kryteria rozkładalności wielomianów.

9.1. Jednoznaczność rozkładu w pierścieniach wielomianów.

Uwaga 9.1. *Niech $(R,+,\cdot)$ będzie pierścieniem z jednoznacznym rozkładem. Niech $a \in R$ będzie elementem nierozkładalnym. Wówczas wielomian $f = \text{const}.a$ jest nierozkładalny w $R[x]$.*

Dowód. Niech $a = fg$, $f, g \in R[x]$. Wówczas $0 = \deg a = \deg f + \deg g$, zatem $\deg f = \deg g = 0$, a więc $f, g \in R$. Ponieważ a jest nierozkładalny, więc $f, g \in U(R) = U(R[x])$. □

Definicja 9.1. *Niech $(R,+,\cdot)$ będzie pierścieniem z jednoznacznym rozkładem, niech $f(x) = a_0 + a_1x + \ldots + a_nx^n \in R[x]$.*

(1) **Zawartością wielomianu** *f nazywamy element $z(f) \sim NWD(a_0, a_1, \ldots, a_n)$.*
(2) *Wielomian f nazywamy* **pierwotnym,** *jeżeli $z(f) \sim 1$.*

Uwaga 9.2. *Niech $(R,+,\cdot)$ będzie pierścieniem z jednoznacznym rozkładem, niech $f, g \in R[x]$, $a \in R$. Wówczas:*

(1) *jeżeli $\deg f = 0$, to $z(f) \sim f$;*
(2) *jeżeli $f \in U(R)$, to $z(f) \sim 1$;*
(3) *$z(af) \sim az(f)$;*
(4) *jeżeli $f = ag$, to $a|z(f)$.*

Proste dowody powyższych własności pozostawiamy jako ćwiczenie.

Lemat 9.1. *Niech $(R,+,\cdot)$ będzie pierścieniem z jednoznacznym rozkładem, niech $0 \neq f \in R[x]$. Wówczas istnieje wielomian pierwotny $f^* \in R[x]$ taki, że*

$$f \sim z(f)f^*.$$

Ponadto wielomian f^* jest wyznaczony jednoznacznie z dokładnością do stowarzyszenia.

Dowód. Niech $f(x) = a_0 + a_1x + \ldots + a_nx^n \in R[x]$. Wówczas $z(f) \sim NWD(a_0, a_1, \ldots, a_n)$. Wobec tego $a_0 = z(f)a_0'$, $a_1 = z(f)a_1'$, …, $a_n = z(f)a_n'$, gdzie $1 \sim NWD(a_0', a_1', \ldots, a_n')$. Niech $f^*(x) = a_0' + a_1'x + \ldots + a_n'x^n$. Wówczas f^* jest pierwotny i $f = z(f)f^*$.

Pokażemy jednoznaczność stosownego przedstawienia. Niech $f = z(f)f^* = cf_1$, gdzie $c \in R$ i $f_1 \in R[x]$ jest pierwotny. Wówczas $z(f) = z(cf_1) \sim cz(f_1) \sim c$, więc $z(f) \sim c$, czyli $z(f) = cu$, dla pewnego $u \in U(R)$. Zatem $z(f)f^* = cf_1$, czyli $cuf^* = cf_1$, skąd $uf^* = f_1$ i $f^* \sim f_1$. □

Lemat 9.2 (lemat Gaussa)**.** *Niech $(R,+,\cdot)$ będzie pierścieniem z jednoznacznym rozkładem. W pierścieniu $R[x]$ iloczyn dowolnej liczby wielomianów pierwotnych jest wielomianem pierwotnym.*

Dowód. Niech $f(x) = a_0 + a_1x + \ldots + a_nx^n, g(x) = b_0 + b_1x + \ldots + b_mx^m \in R[x]$, $a_n, b_m \neq 0$. Niech $fg(x) = c_0 + c_1x + \ldots + c_{n+m}x^{n+m}$, gdzie $c_k = \sum_{i=0}^{k} a_ib_{k-i}$, $k \in \{0, \ldots, n+m\}$. Przypuśćmy, że wielomian fg nie jest pierwotny, czyli $1 \nsim NWD(c_0, \ldots, c_{n+m})$. Wówczas istnieje element nierozkładalny $p \in R$ taki, że $p|c_0, p|c_1, \ldots, p|c_{n+m}$. Ponieważ $1 \sim NWD(a_0, \ldots, a_n)$ oraz $1 \sim NWD(b_0, \ldots, b_m)$, więc możemy określić

$$k = \min\{i \in \{0, \ldots, n\} : p \nmid a_i\} \text{ oraz } l = \min\{j \in \{0, \ldots, m\} : p \nmid b_j\}.$$

Wówczas $c_{k+l} = a_0b_{k+l} + \ldots + a_kb_l + \ldots + a_{k+l}b_0$, przy czym

$$p|a_0b_{k+l} + \ldots + a_{k-1}b_{l+1}, p|a_{k+1}b_{l-1} + \ldots + a_{k+l}b_0,$$

zatem, skoro $p|c_{k+l}$, zachodzi $p|a_k b_l$. Ale ponieważ p jest nierozkładalny w pierścieniu z jednoznacznym rozkładem, a więc pierwszy, więc $p|a_k$ lub $p|b_l$, co jest sprzecznością. Dla iloczynów większej liczby wielomianów pierwotnych stosujemy łatwą indukcję. □

Wniosek 9.1. *Niech $(R,+,\cdot)$ będzie pierścieniem z jednoznacznym rozkładem, niech $f,g \in R[x]$. Wówczas:*

(1) *$z(fg) \sim z(f)z(g)$;*
(2) *jeżeli $f = z(f)f^*$, gdzie f^* jest pierwotny, to $\deg f = \deg f^*$;*
(3) *jeżeli f jest pierwotny i rozkładalny, to $f = gh$, gdzie $\deg g > 0$ i $\deg h > 0$.*

Dowód. (1) Niech $f = z(f)f^*$, $g = z(g)g^*$, gdzie f^* i g^* są pierwotne. Wówczas $fg = (z(f)z(g))(f^*g^*)$. Wobec lematu Gaussa wielomian f^*g^* jest pierwotny. Ponadto, wobec Lematu 9.1, $fg = z(fg)h^*$, gdzie h^* jest wyznaczony jednoznacznie co do stowarzyszenia. Zatem $h^* \sim f^*g^*$ oraz $z(fg) \sim z(f)z(g)$.

(2) Oczywiste.

(3) Niech $f = gh$, gdzie g i h są wielomianami niezerowymi i nieodwracalnymi. Przypuśćmy, że $\deg g = 0$ lub $\deg h = 0$. Załóżmy, że $\deg g = 0$. Wówczas $1 \sim z(f) \sim z(gh) \sim z(g)z(h) = gz(h)$. Zatem $g|1$, co jest sprzecznością.

□

Lemat 9.3. *Niech $(R,+,\cdot)$ będzie pierścieniem z jednoznacznym rozkładem, niech $F = (R)$ będzie ciałem ułamków pierścienia R. Niech $0 \neq\in F[x]$. Wówczas istnieją $a,b \in R$, $b \neq 0$, oraz wielomian pierwotny $f^* \in R[x]$ takie, że*

$$f = \frac{a}{b} f^*.$$

Dowód. Niech $f(x) = a_0 + a_1 x + \ldots + a_n x^n$. Powiedzmy, że $a_0 = \frac{c_0}{d_0}, \ldots, a_n = \frac{c_n}{d_n}$, dla $c_0, \ldots, c_n, d_0, \ldots, d_n \in R$, przy czym $d_0 \neq 0, \ldots, d_n \neq 0$. Niech $d = d_0 \cdot \ldots \cdot d_n$ i niech $e_0 = c_0 \frac{d}{d_0}, \ldots, e_n = c_n \frac{d}{d_n}$. Wówczas:

$$\begin{aligned} f(x) &= a_0 + a_1 x + \ldots + a_n x^n = \frac{c_0}{d_0} + \frac{c_1}{d_1} x + \ldots + \frac{c_n}{d_n} x^n = \\ &= \frac{1}{d}(e_0 + e_1 x + \ldots + e_n x^n) = \frac{1}{d} g(x) \end{aligned}$$

gdzie $g(x) = e_0 + e_1 x + \ldots + e_n x^n \in R[x]$. Wobec Lematu 9.1, $g = z(g)g^*$, gdzie $g^* \in R[x]$ jest pierwotny. Wówczas

$$f = \frac{z(g)}{d} g^*.$$

Kładąc $a = z(g)$, $b = d$ i $f^* = g^*$ otrzymujemy tezę. □

Twierdzenie 9.1. *Niech $(R,+,\cdot)$ będzie pierścieniem z jednoznacznym rozkładem, niech $F = (R)$. Niech $f \in R[x]$ i niech $\deg f > 0$. Następujące warunki są równoważne:*

(1) *f jest nierozkładalny w $R[x]$,*
(2) *f jest pierwotny i nierozkładalny w $F[x]$.*

Dowód. (2) $\Rightarrow$ (1) : Załóżmy, że f jest pierwotny i nierozkładalny w $F[x]$ i przypuśćmy, że jest rozkładalny w $R[x]$. Wobec Wniosku 9.1 (3), $f = gh$, gdzie $\deg g > 0$ oraz $\deg h > 0$, $g,h \in R[x]$. Wówczas g i h są niezerowymi elementami nieodwracalnymi w $F[x]$, co daje sprzeczność z nierozkładalnością f w $F[x]$.

(1) $\Rightarrow$ (2) : Załóżmy, że f jest nierozkładalny w $R[x]$. Pokażemy najpierw, że f jest pierwotny. Wobec Lematu 9.1, $f \sim z(f)f^*$, gdzie $f^* \in R[x]$ jest pierwotny. Wobec Wniosku 9.1 (2), $\deg f^* = \deg f > 0$, a

zatem $f^* \notin U(R[x])$. Ponieważ f jest nierozkładalny, $z(f) \in U(R[x]) = U(R)$. Zatem $z(f) \sim 1$, czyli f jest pierwotny.

Pokażemy, że f jest nierozkładalny w $F[x]$. Przypuśćmy bowiem, że $f = gh$, gdzie $g, h \in F[x]$ i $\deg g > 0$, $\deg h > 0$. Wobec Lematu 9.3 istnieją $a, b, c, d \in R$, $b, d \neq 0$ i wielomiany pierwotne $g^*, h^* \in R[x]$ takie, że

$$g = \frac{a}{b} g^* \text{ oraz } h = \frac{c}{d} h^*.$$

Mamy więc, że $f = \frac{a}{b}\frac{c}{d} h^* g^*$, czyli $bdf = ach^* g^*$. Wobec lematu Gaussa $h^* g^*$ jest wielomianem pierwotnym, a więc wobec Lematu 9.1 $f = f^* \sim h^* g^*$, czyli f jest rozkładalny w $R[x]$, co jest niemożliwością. □

Przykład:

(1) Rozważmy pierścień $\mathbb{Z}$, ciało $\mathbb{Q}$ i wielomian $f(x) = 2x^2 + 6x + 10$. Wówczas $z(f) \sim 2$, więc f jest rozkładalny w $\mathbb{Z}[x]$, ale f jest nierozkładalny w $\mathbb{Q}[x]$, jako że jest wielomianem stopnia 2 bez wymiernych pierwiastków.

Lemat 9.4. *Niech $(R, +, \cdot)$ będzie pierścieniem z jednoznacznym rozkładem, niech $f \in R[x]$ będzie wielomianem pierwotnym i $\deg f > 0$. Wówczas f jest iloczynem elementów nierozkładalnych pierścienia $R[x]$.*

Dowód. Niech $\deg f = n > 0$. Dowód prowadzimy przez indukcję względem n. Załóżmy, że $n = 1$. Przypuśćmy, że w tym przypadku f jest rozkładalny, $f = gh$, gdzie $g, h \in R[x]$ są wielomianami niezerowymi i nieodwracalnymi. Wówczas $1 = \deg f = \deg g + \deg h$, więc $\deg g = 0$ lub $\deg h = 0$. Załóżmy, że $\deg g = 0$. Wobec Uwagi 9.2 (4), $g | z(f)$. Z drugiej strony $z(f) \sim 1$, więc $g \in U(R)$, czyli f jest nierozkładalny, co prowadzi do sprzeczności.

Załóżmy, że $n > 1$ i że dla $0 < k < n$ wielomian pierwotny stopnia k jest iloczynem elementów nierozkładalnych pierścienia $R[x]$. Jeżeli f jest nierozkładalny, to ma rozkład trywialny, załóżmy więc, że f jest rozkładalny. Wobec Wniosku 9.1 (3), $f = gh$, gdzie $g, h \in R[x]$ i $\deg g > 0$, $\deg h > 0$. Zatem $\deg g < n$ i $\deg h < n$. Ponadto $1 \sim z(f) \sim z(g)z(h)$, czyli $z(g) \sim 1$ i $z(h) \sim 1$, a więc g i h są pierwotne. Wobec założenia indukcyjnego g i h mają żądany rozkład, a więc i f go ma. □

Twierdzenie 9.2 (Gaussa)**.** *Niech $(R, +, \cdot)$ będzie pierścieniem z jednoznacznym rozkładem. Wówczas $R[x]$ jest pierścieniem z jednoznacznym rozkładem.*

Dowód. Pokażemy najpierw, że $R[x]$ jest pierścieniem z rozkładem. Ustalmy wielomian niezerowy i nieodwracalny $f \in R[x]$. Załóżmy, że $\deg f = 0$. Wówczas $0 \neq f \in R \setminus U(R)$ i skoro R jest pierścieniem z rozkładem, to $f = a_1 \cdot \ldots \cdot a_n$, gdzie $a_1, \ldots, a_n$ są elementami nierozkładalnymi w R. Wobec Uwagi 9.1 wielomiany $a_1, \ldots, a_n$ są nierozkładalne w $R[x]$.

Załóżmy teraz, że $\deg f > 0$. Wobec Lematu 9.1 istnieje wielomian pierwotny $f^* \in R[x]$ taki, że

$$f = z(f) f^*.$$

Wielomian const.$z(f)$ ma rozkład jako wielomian stopnia 0. Ponadto $\deg f^* = \deg f > 0$. Wobec Lematu 9.4 f^* ma rozkład, zatem i f ma rozkład.

Pokażemy teraz, że każdy element nierozkładalny w $R[x]$ jest pierwszy. Ustalmy wielomian nierozkładalny $f \in R[x]$ i niech $f | gh$, dla pewnych $g, h \in R[x]$. Załóżmy, że $\deg f = 0$. Wówczas $f f_1 = gh$, gdzie $f \in R$ i $f_1 \in R[x]$. Stąd, wobec Uwagi 9.2 (3):

$$z(gh) \sim z(g)z(h) \sim z(f f_1) \sim f z(f_1).$$

Zatem $f | z(g)z(h)$. Ponieważ $f \in R$ jest nierozkładalny, więc f jest pierwszy. Stąd $f | z(g)$ lub $f | z(h)$, a więc $f | g$ lub $f | h$, czyli $f \in R[x]$ jest pierwszy.

Załóżmy, że $\deg f > 0$. Niech $F = (R)$. Wobec Twierdzenia 9.1 $f \in R[x]$ jest pierwotny i nierozkładalny w $F[x]$. Pierścień $F[x]$ jest dziedziną ideałów głównych, a więc pierścieniem z jednoznacznym rozkładem. Zatem f jest pierwszy w $F[x]$. Stąd $f|g$ w $F[x]$ lub $f|h$ w $F[x]$. Załóżmy, że $f|g$ w $F[x]$. Wówczas $g = fw$, dla pewnego $w \in F[x]$. Wobec Lematu 9.3 istnieją $c, d \in R$, $d \neq 0$ oraz wielomian pierwotny $w^* \in R[x]$ takie, że

$$w = \frac{c}{d} w^*.$$

Stąd istnieje wielomian pierwotny $g^* \in R[x]$ taki, że

$$z(g)g^* = g = fw = \frac{c}{d} f w^*.$$

Zatem

$$z(g)dg^* = cfw^*.$$

Wobec lematu Gaussa fw^* jest wielomianem pierwotnym. Wobec Lematu 9.1 mamy $g^* \sim fw^*$, czyli $f|g^*$, a więc $f|g$. □

Przykład:

(2) Rozważmy pierścień z jednoznacznym rozkładem R. Wówczas $R[x_1, \ldots, x_n]$ jest pierścieniem z jednoznacznym rozkładem.

9.2. **Kryteria rozkładalności wielomianów.**

Twierdzenie 9.3. *Niech $(R, +, \cdot)$ będzie pierścieniem z jednoznacznym rozkładem, niech $F = (R)$. Niech $0 \neq f \in R[x]$, gdzie*

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n.$$

Jeżeli dla pewnego $\frac{a}{b} \in F$, takiego, że $NWD(a, b) \sim 1$, $a, b \in R$, zachodzi $f(\frac{a}{b}) = 0$, to $b|a_n$ oraz $a|a_0$. Ponadto, jeżeli f jest unormowany (tj. $a_n = 1$), to każdy jego pierwiastek z ciała F należy do R.

Dowód. Załóżmy, że dla pewnego $\frac{a}{b} \in F$ takiego, że $NWD(a, b) \sim 1$, $a, b \in R$, mamy

$$a_0 + a_1 \frac{a}{b} + \ldots + a_n \left(\frac{a}{b}\right)^n = 0.$$

Wówczas

$$a_0 b^n + a_1 a b^{n-1} + \ldots + a_n a^n = 0,$$

przy czym $b^n, ab^{n-1}, \ldots, a^n \in R$, skąd

$$a(a_1 b^{n-1} + \ldots + a_n a^{n-1}) = -a_0 b^n.$$

Ponieważ $NWD(a, b) \sim 1$, więc $NWD(a, b^n) \sim 1$. Zatem $a|a_0 b^n$ i stąd $a|a_0$. Analogicznie pokazujemy, że $b|a_n$. Dalej, jeśli założymy, że f jest unormowany, to skoro $b|a_n$, otrzymujemy, że $b \in U(R)$, a zatem $\frac{a}{b} = ab^{-1} \in R$. □

Przykład:

(1) Rozważmy pierścień $\mathbb{Z}[x]$ i wielomian $f(x) = x^3 - 3x^2 - 6x + 3$. Wówczas f jest nierozkładalny w $\mathbb{Z}[x]$.

Dowód. Pokażemy najpierw, że f nie ma pierwiastków w ciele $\mathbb{Q} = (\mathbb{Z})$. Istotnie, przypuśćmy bowiem, że $\frac{a}{b} \in \mathbb{Q}$ jest pierwiastkiem f. Wówczas $b|1$ oraz $a|3$ i $NWD(a, b) \sim 1$, więc $\frac{a}{b} \in \{\pm 1, \pm 3\}$. Ale, jak łatwo sprawdzamy, $f(\pm 1), f(\pm 3) \neq 0$, co daje sprzeczność.

Wobec tego f jest nierozkładalny w $\mathbb{Q}[x]$. Ponadto f jest pierwotny, więc wobec Twierdzenia 9.1 f jest nierozkładalny w $\mathbb{Z}[x]$. □

Twierdzenie 9.4 (kryterium Eisensteina[19])**.** *Niech $(R,+,\cdot)$ będzie pierścieniem z jednoznacznym rozkładem, niech $F=(R)$. Niech $0\neq f\in R[x]$, gdzie*

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

Jeżeli dla pewnego elementu nierozkładalnego $p\in R$ zachodzi

$$p|a_0, p|a_1,\ldots,p|a_{n-1}, p\nmid a_n, p^2\nmid a_0,$$

to f jest nierozkładalny w $F[x]$. Jeżeli ponadto f jest pierwotny, to f jest nierozkładalny w $R[x]$.

Dowód. Przypuśćmy, że f jest rozkładalny w $F[x]$, czyli że istnieją niezerowe i nieodwracalne wielomiany $g,h\in F[x]$ takie, że $f=gh$. Wobec Twierdzenia 9.1 istnieją niezerowe i nieodwracalne wielomiany $g_1,h_1\in R[x]$ takie, że $f=g_1h_1$. Rozważmy homomorfizm kanoniczny $\kappa: R\to R/(p)$ dany wzorem

$$\kappa(a)=a+(p)$$

i jego przedłużenie $\overline{\kappa}: R[x]\to R/(p)[x]$ dane wzorem

$$\overline{\kappa}(\sum_{i=0}^{m}b_ix^i)=\sum_{i=0}^{m}\kappa(b_i)x^i.$$

Zauważmy, że $\overline{\kappa}(f)=\kappa(a_n)x^n$. Z drugiej strony $\overline{\kappa}(f)=\overline{\kappa}(g_1)\overline{\kappa}(h_1)$ oraz $\deg\overline{\kappa}(g_1)<n$, $\deg\overline{\kappa}(h_1)<n$. Ponieważ element p jest nierozkładalny, więc, wobec Twierdzenia 7.1, jest pierwszy, a zatem, wobec Uwagi 7.11 (4), i ideał (p) jest pierwszy, a tym samym pierścień $R/(p)$ jest całkowity. Wobec tego wyrazy wolne $\overline{\kappa}(g_1)$ oraz $\overline{\kappa}(h_1)$ są równe 0 w pierścieniu $R/(p)$, a więc należą do ideału (p) w pierścieniu R, tj. są podzielne przez p. Tym samym wyraz wolny wielomianu f, czyli a_0, musi być podzielny przez p^2 wbrew założeniom. □

Przykłady:

(2) Rozważmy pierścień $\mathbb{Z}[x]$ i wielomian $f(x)=3x^3+6x^2+18$. Wówczas f jest nierozkładalny w $\mathbb{Q}[x]$, ale rozkładalny w $\mathbb{Z}[x]$.

Dowód. Zauważmy, że $2|18$, $2|0$, $2|0$, $2|6$, $2\nmid 3$, $4\nmid 18$. Wobec kryterium Eisensteina f jest nierozkładalny w $\mathbb{Q}[x]$. Ale nie jest pierwotny, więc nie musi być nierozkładalny w $\mathbb{Z}[x]$ – i nie jest:

$$f(x)=3(x^3+2x^2+6),\ \text{oraz } 3\notin U(\mathbb{Z}[x]).$$

□

Uwaga 9.3. *Niech $(R,+,\cdot)$ będzie pierścieniem z jednoznacznym rozkładem, niech $f\in R[x]$, niech $a\in R$. Wówczas*

f jest nierozkładalny w $R[x]$ wtedy i tylko wtedy, gdy $f(x+a)$ jest nierozkładalny w $R[x]$.

Dowód. ($\Rightarrow$) : Niech $\deg f=n$. Dowód prowadzimy przez indukcję względem n. Dla $n=0$ teza jest oczywista, ponieważ $f(x)=f(x+a)$, dla wszelkich $a\in R$. Ustalmy $n>0$ i załóżmy, że teza zachodzi dla wszystkich wielomianów stopnia k dla $k<n$ i przypuśćmy, że dla pewnego $a\in R$ wielomian $f(x+a)$ jest rozkładalny. Wobec twierdzenia Gaussa, $R[x]$ jest pierścieniem z jednoznacznym rozkładem, niech więc $f(x+a)=u\cdot g_1(x)\cdot\ldots\cdot g_k(x)$, dla $u\in U(R[x])$ oraz nierozkładalnych wielomianów $g_1,\ldots,g_k\in R[x]$. Wówczas $f(x)=u\cdot g_1(x-a)\cdot\ldots\cdot g_k(x-a)$. Jeżeli $\deg g_i=n$, dla pewnego $i\in\{1,\ldots,k\}$, powiedzmy $\deg g_1=n$, to wówczas $\deg g_2=\ldots=\deg g_k=0$. Ponieważ f jest nierozkładalny, więc, na przykład, $g_2\in U(R[x])$, co daje sprzeczność z nierozkładalnością g_2. Jeżeli $\deg g_i<n$ dla wszelkich $i\in\{1,\ldots,k\}$,

[19]F.G. Eisenstein (1823 – 1852) – matematyk niemiecki. Twierdzenie w istocie odkrył Schönemann w 1846 roku

to, wobec założenia, $g_i(x-a)$ są nierozkładalne, a więc $R[x]$ nie może być pierścieniem z jednoznaczym rozkładem, co znów daje sprzeczność.

($\Leftarrow$) : Wynika z udowodnionej już części twierdzenia i faktu, że $f(x) = f((x-a)+a)$. □

Przykłady:

(3) Rozważmy pierścień $\mathbb{Z}[x]$, liczbę pierwszą p i wielomian $f(x) = x^{p-1}+x^{p-2}+\ldots+x+1$. Wówczas f jest nierozkładalny w $\mathbb{Z}[x]$.

Dowód. Zauważmy, że $f(x) = \frac{x^p-1}{x-1}$. Zatem $f(x+1) = \frac{(x+1)^p-1}{x} = x^{p-1} + \binom{p}{1}x^{p-2} + \ldots + \binom{p}{p-2}x + \binom{p}{p-1}$. Dalej, $p|\binom{p}{p-1}$, ..., $p|\binom{p}{1}$, $p \nmid 1$, $p^2 \nmid \binom{p}{p-1}$ i wobec kryterium Eisensteina $f(x+1)$ jest nierozkładalny. □

Twierdzenie 9.5. *Niech $f \in \mathbb{Z}[x]$ i niech $\deg f = n$. Jeżeli w $n+1$ punktach całkowitych f przyjmuje wartości ± 1, to f jest nierozkładalny w $\mathbb{Z}[x]$.*

Dowód. Przypuśćmy, że f gh, dla pewnych $g, h \in \mathbb{Z}[x]$, przy czym $0 < \deg g \leq \deg h < n$. W szczególności $\deg g \leq \frac{n}{2}$. Pokażemy, że dla co najmniej $\frac{n+1}{2}$ wartości całkowitych g przybiera wartość 1 lub dla co najmniej $\frac{n+1}{2}$ wartości całkowitych g przybiera wartość -1. Istotnie, przypuśćmy bowiem, że dla mniej niż $\frac{n+1}{2}$ wartości całkowitych g przybiera wartość 1 oraz dla mniej niż $\frac{n+1}{2}$ wartości całkowitych g przybiera wartość -1. Zatem dla mniej niż $2\frac{n+1}{2} = n+1$ wartości całkowitych g przyjmuje wartość ± 1. W konsekwencji dla mniej niż $n+1$ wartości całkowitych f przybiera wartość ± 1, wbrew założeniom.

Przyjmijmy, dla ustalenia uwagi, że dla co najmniej $\frac{n+1}{2}$ wartości całkowitych g przybiera wartość 1. Wówczas $g(x)-1$ jest wielomianem stopnia mniejszego od $\frac{n+1}{2}$, który ma $\frac{n+1}{2}$ miejsc zerowych, co jest niemożliwością. □

Przykłady:

(4) Rozważmy pierścień $\mathbb{Z}[x]$ i wielomian $f(x) = x^2+x-1$. Wówczas f jest nierozkładalny.

Dowód. $\deg f = 2$ oraz $f(0) = -1$, $f(1) = 1$ i $f(-1) = -1$, co daje żądany rezultat. □

Uwaga 9.4. *Niech $f(x) = (x-a_1)(x-a_2)\cdot\ldots\cdot(x-a_n)-1 \in \mathbb{Z}[x]$, gdzie $a_1, \ldots, a_n \in \mathbb{Z}$ są parami różne. Wówczas f jest nierozkładalny.*

Dowód. Przypuśćmy, że $f = gh$, $g, h \in \mathbb{Z}[x]$ oraz $0 < \deg g \leq \deg h < n$. Dla wszelkich $i \in \{1, \ldots, n\}$, $g(a_i), h(a_i) \in \mathbb{Z}$ oraz $g(a_i)h(a_i) = -1$. Zatem $g(a_i)+h(a_i) = 0$, dla $i \in \{1, \ldots, n\}$. Zatem wielomian $g+h$ stopnia mniejszego od n ma n miejsc zerowych. Stąd $g+h \equiv 0$, więc $g = -h$ i tym samym $f = -g^2$, co daje sprzeczność. □

Definicja 9.2. *Niech $m, n \in \mathbb{N}$ i niech $f \in \mathbb{Z}[x_1, \ldots, x_n]$.* **Redukcją wielomianu f według modułu** *m nazywamy wielomian $\tilde{f} \in \mathbb{Z}_m[x_1, \ldots, x_n]$, którego współczynniki są współczynnikami wielomianu f w obrazie poprzez odwzorowanie $\phi : \mathbb{Z} \to \mathbb{Z}_m$ dane wzorem $\phi(a) =$ reszta z dzielenia a przez m.*

Uwaga 9.5. *Niech $m, n \in \mathbb{N}$ i niech $f \in \mathbb{Z}[x_1, \ldots, x_n]$. Jeżeli równanie $f(x_1, \ldots, x_n) = 0$ ma rozwiązanie w $\mathbb{Z}$ oraz $\tilde{f} \in \mathbb{Z}_m[x_1, \ldots, x_n]$ jest redukcją wielomianu f według modułu m, to równanie $\tilde{f}(x_1, \ldots, x_n) = 0$ ma rozwiązanie w $\mathbb{Z}_m$.*

Prosty dowód pozostawiamy jako ćwiczenie.

Wniosek 9.2. *Niech $m, n \in \mathbb{N}$ i niech $f \in \mathbb{Z}[x_1, \ldots, x_n]$. Jeżeli równanie $\tilde{f}(x_1, \ldots, x_n) = 0$ nie ma rozwiązania w $\mathbb{Z}_m$, gdzie $\tilde{f} \in \mathbb{Z}_m[x_1, \ldots, x_n]$ jest redukcją wielomianu f według modułu m, to równanie $f(x_1, \ldots, x_n) = 0$ ma rozwiązanie w $\mathbb{Z}$.*

Przykłady:

(5) Pokazać, że równanie $x^2 + y^2 = 31z^2 + 15$ nie ma rozwiązań w $\mathbb{Z}$.

Dowód. Rozważmy redukcję tego równania według modułu 8:

$$x^2 + y^2 = 7z^2 + 7.$$

Wszystkimi kwadratami w $\mathbb{Z}_8$ są 0, 1 i 4. Zatem wszystkimi wartościami wyrażenia $7z^2 + 7$ są 7, 6 i 3. Ponadto żadna z liczb 7, 6 i 3 nie jest sumą liczb 0, 1 i 4 modulo 8. □

Twierdzenie 9.6 (kryterium redukcyjne)**.** *Niech P i R będą pierścieniami całkowitymi, niech $\phi : P \to R$ będzie homomorfizmem, niech $f \in P[x]$. Niech $\overline{\phi} : P[x] \to R[x]$ będzie przedłużeniem homomorfizmu ϕ na pierścienie wielomianowe dane wzorem:*

$$\overline{\phi}(a_0 + a_1x + \ldots + a_nx^n) = \phi(a_0) + \phi(a_1)x + \ldots + \phi(a_n)x^n.$$

Jeżeli $\deg f = \deg \overline{\phi}(f)$ oraz $\overline{\phi}(f) \in R[x]$ jest wielomianem nierozkładalnym, to f jest wielomianem nierozkładalnym.

Dowód. Załóżmy, że $\overline{\phi}(f) \in R[x]$ jest wielomianem nierozkładalnym. Przypuśćmy, że $f = gh$, dla pewnych $g, h \in P[x]$ takich, że $0 < \deg g \leq \deg h < \deg f$. Wówczas $\overline{\phi}(f) = \overline{\phi}(g)\overline{\phi}(h)$ oraz $\deg \overline{\phi}(g) = \deg g > 0$, $\overline{\phi}(h) = \deg h > 0$, co daje sprzeczność. □

Przykłady:

(6) Rozważmy pierścień $\mathbb{Z}[x]$ i liczbę pierwszą p wraz z wielomianem $f(x) = x^p - x - 1$. Wówczas f jest nierozkładalny w $\mathbb{Z}[x]$.

Dowód. Rozważmy redukcję wielomianu f według modułu p:

$$-x - 1.$$

Jest to wielomian nierozkładalny w $\mathbb{Z}_p[x]$, zatem f jest nierozkładalny w $\mathbb{Z}[x]$. □

Twierdzenie 9.7 (kryterium Kroneckera)**.** *Niech $f \in \mathbb{Z}[x]$, $\deg f = n$. Niech $c_0 = f(0), c_1 = f(1), \ldots, c_n = f(n)$. Niech $q \in \{0, 1, \ldots, n-1\}$, niech $e_0, e_1, \ldots, e_q$ będą dowolnymi dzielnikami liczb $c_0, c_1, \ldots, c_q$ i niech $g_{e_0e_1\ldots e_q} \in \mathbb{Z}[x]$ będzie wielomianem takim, że*

$$g_{e_0e_1\ldots e_q}(0) = e_0, g_{e_0e_1\ldots e_q}(1) = e_1, \ldots, g_{e_0e_1\ldots e_q}(q) = e_q.$$

Wówczas f jest nierozkładalny w $\mathbb{Q}[x]$ wtedy i tylko wtedy, gdy

(1) *$c_0 \neq 0, c_1 \neq 0, \ldots, c_n \neq 0$;*
(2) *wielomian f nie jest podzielny przez żaden z wielomianów $g_{e_0e_1\ldots e_q}$.*

Lemat 9.5. *Niech $f \in \mathbb{Z}[x]$, $\deg f = n$. Niech $c_0 = f(0), c_1 = f(1), \ldots, c_n = f(n)$. Niech $q \in \{0, 1, \ldots, n-1\}$, niech $e_0, e_1, \ldots, e_q$ będą dowolnymi dzielnikami liczb $c_0, c_1, \ldots, c_q$ i niech $g_{e_0e_1\ldots e_q} \in \mathbb{Z}[x]$ będzie wielomianem takim, że*

$$g_{e_0e_1\ldots e_q}(0) = e_0, g_{e_0e_1\ldots e_q}(1) = e_1, \ldots, g_{e_0e_1\ldots e_q}(q) = e_q.$$

Wówczas jeżeli $g \in \mathbb{Q}[x]$ jest dzielnikiem $f \in \mathbb{Z}[x]$, to dla pewnych $e_0, e_1, \ldots, e_q$ zachodzi

$$g_{e_0e_1\ldots e_q} | g.$$

Dowód. Niech $g \in \mathbb{Q}[x]$ będzie taki, że $g|f$, $\deg g = q$. Wobec Twierdzenia 9.1 istnieją wielomiany $g_1, h_1 \in \mathbb{Z}[x]$ takie, że $f = g_1h_1$ oraz $\deg g_1 = q$. Ponieważ $c_j = f(j) = g(j)h(j)$ dla $j \in \{0, \ldots, q\}$, więc $g_1(j)|c_j$ dla $j \in \{0, \ldots, q\}$. Wobec tego $g_1 = g_{g_1(0)g_1(1)\ldots g_1(q)}$. □

Przechodzimy do dowodu Twierdzenia 9.7.

Dowód. ($\Rightarrow$) : Załóżmy, że $c_0 = 0$ lub $c_1 = 0$ lub $\ldots$ lub $c_n = 0$ lub wielomian f jest podzielny przez jeden z wielomianów $g_{e_0e_1\ldots e_q}$. Jeżeli dla pewnego i_0 zachodzi $c_{i_0} = 0$, to $x - i_0 | f$, więc f jest rozkładalny. Jeżeli dla pewnych $e_0, e_1, \ldots, e_q$ zachodzi $g_{e_0e_1\ldots e_q} | f$, to f jest rozkładalny.

($\Leftarrow$) : Załóżmy, że f jest rozkładalny w $\mathbb{Q}[x]$. Załóżmy, że $c_0 \neq 0, c_1 \neq 0, \ldots, c_n \neq 0$. Wobec Lematu, dla pewnych $e_0, e_1, \ldots, e_q$ zachodzi wtedy $g_{e_0e_1\ldots e_q} | f$. $\square$