ROZDZIAŁ VIII

WIELOMIANY

§ 1. Dzielenie wielomianu przez wielomian. Reszta. *Wielomianem zmiennej* rzeczywistej lub zespolonej x nazywamy wyrażenie

$$(1)\qquad W(x) = a_0x^m + a_1x^{m-1} + \ldots + a_{m-1}x + a_m,$$

gdzie $a_0, a_1, \ldots, a_m$ oznaczają liczby dane, rzeczywiste lub zespolone.

W Rozdziale tym zamiast „wielomian zmiennej x“ będziemy mówili poprostu „wielomian“.

Przez *wielomian stopnia* 0 rozumiemy stałą (mogącą być w szczególności zerem).

Wielomianem stopnia $m>0$ nazywamy wyrażenie (1), gdzi $a_0 \neq 0$.

Ogólnie więc wyrażenie (1) jest wielomianem stopnia co naj wyżej m.

Dla krótkości będziemy oznaczali wielomian $W(x)$ poprost przez W. Każdy wielomian ma w zupełności oznaczony stopień który jest liczbą całkowitą nieujemną.

Stopień wielomianu W będziemy oznaczali przez st W. Nie równość st $W>0$ oznacza więc, że wielomian W nie jest stał

Dwa wielomiany uważamy za *równe* wtedy i tylko wtedy jeżeli są tym samym wielomianem, t.j. jeżeli są tego samego stopni i ich współczynniki przy kolejnych potęgach zmiennej są odpo wiednio równe.

Pojęcie to należy odróżniać od *tożsamościowej równości* dwóch wielomianów, która oznacza, że wielomiany te jako funkcje zmiennej x przyjmują te same wartości dla każdej wartości (rzeczywistej lub zespolonej) tej zmiennej.

Dwa wielomiany równe są tożsamościowo równe; słuszność twierdzenia odwrotnego wynika z twierdzenia 19, które udowodnimy w § 11 tego Rozdziału (ob. str. 124) [1]).

[1]) Rozróżnianie pojęć równości i tożsamościowej równości wielomianów jest ważne w dalszych działach Algebry przy rozpatrywaniu wielomianów zmiennej x, przebiegającej ciało o charakterystyce różnej od 0. Por. Rozdział XX, § 2.

Stopień sumy dwóch wielomianów nie przenosi większego z ich stopni, może jednak być od nich mniejszy, jeżeli współczynniki przy najwyższych potęgach zmiennej w tych wielomianach znoszą się wzajemnie. Mamy więc dla wszelkich wielomianów W_1 i W_2:

$$\text{st}\,(W_1+W_2) \leqslant \max\,(\text{st}\,W_1, \text{st}\,W_2).$$

Natomiast, jak łatwo wykazać, słuszna jest zawsze równość:

$$\text{st}\,W_1W_2 = \text{st}\,W_1 + \text{st}\,W_2.$$

Dla praktycznego obliczania wartości wielomianu (1) dla danej wartości x_0 zmiennej x stosuje się następujący sposób, zalecany przez Runge'go [1]). Obliczamy kolejno:

$$y_1 = a_0x_0 + a_1, \quad y_2 = y_1x_0 + a_2, \quad y_3 = y_2x_0 + a_3, \quad \ldots, \quad y_m = y_{m-1}x_0 + a_m.$$

Jak to czytelnik z łatwością udowodni, będzie $y_m = W(x_0)$.

Sposób ten jest wygodny zwłaszcza przy przybliżonych obliczeniach za pomocą suwaka, o ile dokładność suwaka wystarcza do danego celu.

Twierdzenie 1. *Jeżeli W_1 i W_2 oznaczają dwa wielomiany i st $W_2>0$, to istnieją wielomiany Q i R takie, że:*

$$(2)\quad W_1 = QW_2 + R \quad \text{i} \quad (3)\quad \text{st}\,R < \text{st}\,W_2.$$

Dowód. Jeżeli st $W_1<$ st W_2, to możemy oczywiście przyjąć $Q=0$ oraz $R=W_1$. Przypuśćmy więc, że st $W_1 \geqslant$ st W_2, i niechaj

$$W_1(x) = a_0x^m + a_1x^{m-1} + \ldots + a_m, \qquad W_2(x) = b_0x^n + b_1x^{n-1} + \ldots + b_n,$$

gdzie $a_0 \neq 0$ i $b_0 \neq 0$. Jest tu więc st $W_1 = m$ i st $W_2 = n$, przy czym $m \geqslant n$. Przyjmijmy:

$$Q_1 = \frac{a_0}{b_0}x^{m-n}, \qquad R_1 = W_1 - Q_1W_2 = a_1x^{m-1} + a_2x^{m-2} + \ldots + a_m -$$
$$- \left(\frac{a_0b_1}{b_0}x^{m-1} + \frac{a_0b_2}{b_0}x^{m-2} + \ldots + \frac{a_0b_n}{b_0}x^{m-n}\right).$$

Będzie więc:

$$W_1 = Q_1W_2 + R_1 \quad \text{i} \quad \text{st}\,R_1 \leqslant m-1 < \text{st}\,W_1.$$

Jeżeli st $R_1 \geqslant$ st W_2, to znajdziemy w podobny sposób jednomian Q_2 i wielomian R_2, takie iż

$$R_1 = Q_2W_2 + R_2 \quad \text{i} \quad \text{st}\,R_2 < \text{st}\,R_1.$$

[1]) C. Runge, *Praxis der Gleichungen*, Sammlung Schubert XIV, Lipsk 1900, str. 94.

Jeżeli $\operatorname{st} R_2 \geqslant \operatorname{st} W_2$, to możemy postąpić tak samo z wielomianem R_2 i t.d. Rozumowanie to nie może powtarzać się w nieskończoność, gdyż mamy tu stale

$$\operatorname{st} R_1 > \operatorname{st} R_2 > \operatorname{st} R_3 > \dots$$

Dojdziemy więc do ostatniego wzoru tego rodzaju

$$R_{k-1} = Q_k W_2 + R_k,$$

gdzie już nie będzie $\operatorname{st} R_k \geqslant \operatorname{st} W_2$, a więc będzie $\operatorname{st} R_k < \operatorname{st} W_2$. Kolejne te wzory dadzą $W_1 = (Q_1 + Q_2 + \dots + Q_k) W_2 + R_k$.

Przyjmując $Q = Q_1 + Q_2 + \dots + Q_k$ i $R = R_k$, otrzymujemy stąd od razu wzory (2) i (3), c. b. d. d.

Udowodniliśmy więc twierdzenie 1, przy czym dowód pozwala wyznaczyć wielomiany Q i R, jeśli wielomiany W_1 i W_2 są dane. Co więcej, wielomiany Q i R, spełniające warunki (2) i (3), są przez wielomiany W_1 i W_2 wyznaczone jednoznacznie. Wykażemy mianowicie, że jeśli wielomiany Q' i R' spełniają wzory:

$$(2') \quad W_1 = Q'W_2 + R' \qquad \text{i} \qquad (3') \quad \operatorname{st} R' < \operatorname{st} W_2,$$

to wielomiany Q i Q' są równe, a wielomiany R i R' są tożsamościowo równe.

Istotnie, z (2) otrzymujemy $QW_2 + R = Q'W_2 + R'$, skąd

$$(4) \qquad (Q - Q')W_2 = R' - R.$$

Otóż gdyby Q' nie było tym samym wielomianem co Q, lew strona wzoru (4) byłaby wielomianem stopnia nie mniejszego ni $\operatorname{st} W_2$, gdy tymczasem prawa strona jest wielomianem stopni mniejszego niż $\operatorname{st} W_2$ na mocy (3) i (3'). Mamy więc $Q = Q'$ i wzór (4 dowodzi, że różnica $R - R'$ jest tożsamościowo równa 0, t.j. że wielc mian R jest tożsamościowo równy R'.

Z dowodu twierdzenia 1 widzimy, że współczynniki wielomia nów Q i R, spełniających warunki (2) i (3), otrzymuje się ze współ czynników wielomianów W_1 i W_2 za pomocą czterech *działań wymiernych* $(+, -, \cdot$ i $:)$. Mamy więc

Twierdzenie 2. *Wielomiany Q i R, spełniające warunki* (2) *i* (3), *są wyznaczone jednoznacznie przez wielomiany W_1 i W_2, a ich współczynniki otrzymują się za pomocą działań wymiernych ze współczynników wielomianów W_1 i W_2. W szczególności, jeżeli współczynniki wielomianów W_1 i W_2 są liczbami wymiernymi, to i współczynniki wielomianów Q i R są liczbami wymiernymi.*

Wielomian R, wyznaczony przez wielomiany W_1 i W_2, nazywamy *resztą z dzielenia* wielomianu W_1 przez wielomian W_2.

Każdy wielomian daje więc przy dzieleniu przez każdy wielomian dodatniego stopnia w zupełności oznaczoną resztę, która jest wielomianem stopnia niższego niż stopień dzielnika.

§ 2. Dzielenie wielomianu przez dwumian $x - \alpha$. Pochodna wielomianu. Wyznaczymy w szczególności iloraz i resztę z dzielenia dowolnego wielomianu (1) przez dwumian $W_2(x) = x - \alpha$ (gdzie α jest liczbą niezależną od x).

Mamy oczywiście:

$$W_1(x) - W(\alpha) = a_0(x^m - \alpha^m) + a_1(x^{m-1} - \alpha^{m-1}) + \dots + a_{m-1}(x - \alpha).$$

Lecz dla $k = 1, 2, \dots, m$ mamy tożsamość:

$$x^k - \alpha^k = (x - \alpha)(x^{k-1} + \alpha x^{k-2} + \alpha^2 x^{k-3} + \dots + \alpha^{k-2}x + \alpha^{k-1}).$$

Zatem:

$$(5) \qquad W_1(x) - W_1(\alpha) = (x - \alpha) Q(x),$$

gdzie

$$\begin{aligned} Q(x) = {} & a_0(x^{m-1} + \alpha x^{m-2} + \alpha^2 x^{m-3} + \dots + \alpha^{m-2}x + \alpha^{m-1}) + \\ & + a_1(x^{m-2} + \alpha x^{m-1} + \dots + \alpha^{m-3}x + \alpha^{m-2}) + \\ & + a_2(x^{m-3} + \alpha x^{m-4} + \dots + \alpha^{m-3}) + \\ & \dots\dots\dots\dots \\ & + a_{m-2}(x + \alpha) + \\ & + a_{m-1} = \\ = {} & a_0 x^{m-1} + (a_0\alpha + a_1)x^{m-2} + (a_0\alpha^2 + a_1\alpha + a_2)x^{m-3} + \dots \\ & \dots + (a_0\alpha^{m-2} + a_1\alpha^{m-3} + \dots + a_{m-2})x + \\ & + (a_0\alpha^{m-1} + a_1\alpha^{m-2} + \dots + a_{m-2}\alpha + a_{m-1}). \end{aligned}$$

Zatem:

Resztą z dzielenia wielomianu $W_1(x)$ przez $x - \alpha$ jest $W_1(\alpha)$.

Co się tyczy ilorazu $Q(x) = Q(x, \alpha)$, to jest to oczywiście wielomian stopnia $m - 1$ zarówno zmiennej x jak i zmiennej α, *symetryczny* ze względu na x i α, t.j. taki, że przy wszelkich x i α jest $Q(x, \alpha) = Q(\alpha, x)$.

W szczególności, jak łatwo obliczyć:

$$Q(x, x) = m a_0 x^{m-1} + (m-1) a_1 x^{m-2} + (m-2) a_2 x^{m-3} + \dots + 2 a_{m-2} x + a_{m-1}.$$

Wielomian $Q(x, x)$ nazywamy *pochodną wielomianu* $f(x) = W_1(x)$ i oznaczamy przez $f'(x)$.

To określenie pochodnej wielomianu $a_0x^m+a_1x^{m-1}+\ldots+a_{m-1}x+a_m$ jako $ma_0x^{m-1}+(m-1)a_1x^{m-2}+\ldots+a_{m-1}$ jest czysto formalne. Wychodząc jednak z tej formalnej definicji pochodnej wielomianu, można wyprowadzić elementarnie (bez wprowadzenia pojęcia granicy) różne jej własności, jak np.: pochodna sumy (różnicy) dwóch wielomianów jest sumą (różnicą) pochodnych tych wielomianów; pochodna iloczynu wyraża się wzorem $(W_1W_2)'=W_1'W_2+W_2'W_1$, i niektóre inne.

Dla $x\neq a$ wzór (5) daje

$$Q(x,a)=\frac{W_1(x)-W_1(a)}{x-a}, \tag{6}$$

skąd wobec ciągłości wielomianu wnosimy, że $f'(x)=Q(x,x)$ jest granicą wyrażenia (6), gdy a zmierza do x. Dowodzi to, że podana tu definicja pochodnej jest równoważna przyjmowanej w Rachunku różniczkowym.

Dla $x=a$ będzie więc $f'(a)=Q(a,a)=Q(a)$, zatem wobec (5):

Jeżeli $f(a)=0$, czyli gdy a jest pierwiastkiem wielomianu $f(x)$, to $f'(a)$ jest wartością dla $x=a$ ilorazu z dzielenia wielomianu $f(x)$ przez $x-a$.

ĆWICZENIA. 1. Podzielić wielomian

$$x^{10}-36x^8+528x^6-3897x^4+14354x^2-21025$$

przez wielomian

$$x^5-8x^4+14x^3+41x^2-162x+145.$$

Odp.: Iloraz wynosi $x^5+8x^4+14x^3-41x^2-162x-145$.

2. Dla dowolnie danego wielomianu W_n stopnia n oraz danych n liczb $\alpha_1,\alpha_2,\ldots,\alpha_n$ (różnych lub nie) wyznaczyć liczby $A_0,A_1,\ldots,A_n$, tak, aby było tożsamościowo

$$W_n=A_0+A_1(x-\alpha_1)+A_2(x-\alpha_1)(x-\alpha_2)+A_3(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)+\ldots$$
$$\ldots+A_n(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n). \tag{*}$$

Odp.: Dzieląc W_n przez $x-\alpha_1$ otrzymujemy iloraz W_{n-1}, będący wielomianem stopnia $n-1$, oraz resztę A_0, będącą stałą. Podobnie, dzieląc W_{n-1} przez $x-\alpha_2$, otrzymujemy iloraz W_{n-2}, będący wielomianem stopnia $n-2$, oraz resztę A_1, będącą stałą, i t.d., wreszcie $W_1=A_n(x-\alpha_n)+A_{n-1}$. Stąd z łatwością otrzymujemy wzór (*).

3. Dowieść, że *każdy wielomian $W(x)$ stopnia n daje się przedstawić tożsamościowo w postaci*

$$W(x)=b_0\binom{x}{n}+b_1\binom{x}{n-1}+\ldots+b_{n-1}\binom{x}{1}+b_n, \tag{⁑}$$

przy czym wtedy i tylko wtedy wszystkie wartości jego dla x całkowitych są całkowite, gdy wszystkie współczynniki $b_0,b_1,\ldots,b_n$ są całkowite.

Odp.: Dowód, iż wielomian $W(x)$ daje się przedstawić w postaci (⁑), otrzymuje się natychmiast z ćwiczenia 2 przez podstawienie $\alpha_1=0$, $\alpha_2=1,\ldots,\alpha_n=n-1$. Że w razie całkowitych b wartości $W(x)$ dla całkowitych x są całkowite, wynika to z całkowitości współczynników newtonowskich $\binom{k}{n}$ dla całkowitych k i naturalnych n. Wreszcie dowód, że i na odwrót, t.j. że w razie całkowitości liczb

$W(0),W(1),W(2),\ldots,W(n)$ współczynniki $b_0,b_1,\ldots,b_n$ są całkowite, wynika natychmiast ze wzorów na $W(k)$ dla $k=n,n-1,\ldots,2,1,0$, z których kolejno obliczamy $b_0,b_1,\ldots,b_n$.

4. Dowieść, że *wielomian stopnia n przybiera dla x wymiernych wtedy i tylko wtedy same wartości wymierne, gdy wszystkie jego współczynniki są wymierne.*

§ 3. Podzielność wielomianów. Ich dzielniki wspólne. Największy wspólny dzielnik. Z twierdzeń 1 i 2 wynika natychmiast, że $R=0$ wtedy i tylko wtedy, gdy istnieje wielomian Q taki, że

$$W_1=QW_2. \tag{7}$$

Mówimy wówczas, że wielomian W_1 jest *podzielny* przez wielomian W_2 lub że wielomian W_2 jest *dzielnikiem* wielomianu W_1 lub wreszcie, że wielomian W_1 jest *wielokrotną* wielomianu W_2, co wyrażamy, pisząc

$$W_2\,|\,W_1.$$

Ze wzoru (5) wynika od razu

Twierdzenie 3. *Wielomian $W_1(x)$ jest wtedy i tylko wtedy podzielny przez $x-a$, gdy $W_1(a)=0$, t.j. gdy liczba a jest pierwiastkiem wielomianu W_1.*

Jeżeli wielomian W_2 jest stałą różną od 0, to przyjmując $Q=W_1/W_2$, będziemy mieli wzór (7), przy czym Q będzie wielomianem tegoż stopnia co W_1. Będziemy więc uważali każdy wielomian za podzielny przez każdą stałą różną od zera.

Jeżeli wielomian W_1 nie jest podzielny przez wielomian W_2 (nie będący stale zerem), to reszta z dzielenia wielomianu W_1 przez W_2 jest wielomianem (stopnia nie ujemnego), nie będącym stale zerem.

Z określenia podzielności wielomianów wynika natychmiast, że:

1° *jeżeli* $W_2|W_1$, *to* $\mathrm{st}\,W_2\leqslant\mathrm{st}\,W_1$;

2° *jeżeli* $W_2|W_1$ *i* $W_3|W_2$, *to* $W_3|W_1$, *czyli dzielnik dzielnika danego wielomianu jest znowu dzielnikiem tego wielomianu*;

3° *jeżeli* $W|W_1$ *i* $W|W_2$, *to* $W|MW_1+NW_2$ *dla wszelkich wielomianów* M *i* N.

Z twierdzeń 1 i 2 wynika zaś

Wniosek. *Jeżeli* $\mathrm{st}\,W>0$ *i* $QW=Q_1W$, *to* $Q=Q_1$.

Wniosek ten jest oczywiście prawdziwy również w przypadku, gdy W jest stałą różną od zera.

Twierdzenie 4. *Dla każdych dwóch wielomianów W_1 i W_2, z których co najmniej jeden nie jest tożsamościowo równy 0, istnieje wielomian H taki, iż*

$$H \mid W_1 \quad i \quad H \mid W_2, \tag{8}$$

przy czym wielomian H daje się przedstawić w postaci

$$H = W_1 X + W_2 Y, \tag{9}$$

gdzie X i Y oznaczają wielomiany.

Dowód. Ponieważ $W_1 = W_1 \cdot 1 + W_2 \cdot 0$ i $W_2 = W_1 \cdot 0 + W_2 \cdot 1$, więc istnieją wielomiany H postaci (9), nie będące stale zerem. Spośród nich weźmy którykolwiek, możliwie najniższego stopnia (ewentualnie redukujący się do stałej). Wystarczy dowieść, że taki wielomian H spełnia warunki (8).

Istotnie, przypuśćmy, że wielomian W_1 nie jest podzielny przez H. W myśl twierdzenia 1 możemy więc przyjąć

$$W_1 = QH + R, \tag{10}$$

przy czym $\mathrm{st}\, R < \mathrm{st}\, H$ oraz wielomian R nie jest stałą równą zeru, gdyż wówczas byłoby $H|W_1$, wbrew założeniu. Wzory (10) i (9) dają $R = W_1 - QH = W_1(1-QX) - W_2QY$, skąd dla $X_1 = 1-QX$ i $Y_1 = -QY$ dostajemy $R = W_1X_1 + W_2Y_1$, wbrew założeniu, że H jest wielomianem postaci (9) możliwie najniższego stopnia i nie będącym stale zerem. Musi więc być $H|W_1$ i podobnie uzasadnia się podzielność $H|W_2$, c. b. d. o.

Zajmiemy się teraz wspólnymi dzielnikami wielomianów W myśl wzorów (9) wielomian H jest *wspólnym dzielnikiem* wielomianów W_1 i W_2.

Niech teraz wielomian D będzie jakimkolwiek wspólnym dzielnikiem wielomianów W_1 i W_2, t.j. załóżmy, że $D|W_1$ i $D|W_2$, czyli że istnieją wielomiany Q_1 i Q_2 takie, iż $W_1 = Q_1D$ i $W_2 = Q_2D$. Otóż wzór (9) daje $H = (Q_1X + Q_2Y)D$, skąd $D|H$.

Wielomian H, spełniający twierdzenie 4, jest więc takim dzielnikiem wspólnym wielomianów W_1 i W_2, który jest podzielny przez każdy inny dzielnik wspólny tych wielomianów.

Jeżeli H_1 i H_2 oznaczają dwa wielomiany o tej własności, to mamy $H_1|H_2$ i $H_2|H_1$, skąd $\mathrm{st}\, H_1 \leqslant \mathrm{st}\, H_2$ i $\mathrm{st}\, H_2 \leqslant \mathrm{st}\, H_1$, co daje $\mathrm{st}\, H_1 = \mathrm{st}\, H_2$. Wielomiany H_1 i H_2, jako wielomiany tego samego stopnia, podzielne jeden przez drugi, są więc równe jeden drugiemu, pomnożonemu przez jakiś czynnik stały.

Otóż wśród wielomianów H, spełniających twierdzenie 4, istnieje jeden i tylko jeden, którego współczynnik przy najwyższej potędze zmiennej jest równy 1.

Wielomian ten nazywamy *największym wspólnym dzielnikiem wielomianów* W_1 i W_2.

Z twierdzenia 4 wynika zatem

Twierdzenie 5. *Każde dwa wielomiany W_1 i W_2, z których co najmniej jeden nie redukuje się do stałej 0, posiadają jednoznacznie oznaczony największy wspólny dzielnik, który jest podzielny przez każdy inny wspólny dzielnik tych wielomianów.*

Powyższe dowody twierdzeń 4 i 5 są t.zw. *czystymi dowodami istnienia*, ponieważ nie podaliśmy w nich żadnego sposobu wyznaczenia zarówno wielomianu H, jak i największego wspólnego dzielnika dwóch danych wielomianów. Podamy obecnie taki sposób; jest nim t.zw. *algorytm kolejnych dzieleń* (Euklidesa).

§ 4. Algorytm kolejnych dzieleń.

Niech W_1 i W_2 oznaczają dwa wielomiany, z których co najmniej jeden, np. W_2, nie jest stałą równą 0.

Jeżeli $W_2|W_1$, to wielomiany $H = W_2$, $X = 0$ i $Y = 1$ spełniają warunki (8) i (9) twierdzenia 4 i największym wspólnym dzielnikiem wielomianów W_1 i W_2 będzie wielomian, otrzymany przez podzielenie wielomianu W_2 przez współczynnik przy jego najwyższej potędze.

Załóżmy więc, że nie jest $W_2|W_1$. Wówczas reszta z dzielenia wielomianu W_1 przez wielomian W_2 jest wielomianem, nie będącym stałą równą 0. Oznaczmy go przez W_3. Na mocy twierdzenia 1 istnieje więc wielomian Q_1 taki, iż $W_1 = Q_1W_2 + W_3$, skąd wynika na mocy 3⁰ (str. 107), że każdy wspólny dzielnik wielomianów W_2 i W_3 jest dzielnikiem wielomianu W_1, a więc też wspólnym dzielnikiem wielomianów W_1 i W_2; oraz (wobec $W_3 = W_1 - Q_1W_2$), że każdy wspólny dzielnik wielomianów W_1 i W_2 jest dzielnikiem wielomianu W_3, a więc też wspólnym dzielnikiem wielomianów W_2 i W_3.

Widzimy więc, że wspólne dzielniki wielomianów W_1 i W_2 są te same, co wspólne dzielniki wielomianów W_2 i W_3. W ten sposób wyznaczanie wspólnych dzielników wielomianów W_1 i W_2 sprowadziliśmy do wyznaczania wspólnych dzielników wielomianów W_2 i W_3, przy czym $\mathrm{st}\, W_3 < \mathrm{st}\, W_2$.

Jeżeli $W_3|W_2$, to jedynymi wspólnymi dzielnikami wielomianów W_2 i W_3 są dzielniki wielomianu W_3, a największy wspólny dzielnik wielomianów W_2 i W_3 otrzymamy, dzieląc wielomian W_3 przez współczynnik przy najwyższej jego potędze.

Jeżeli zaś nie jest $W_3|W_2$, to niech W_4 oznacza resztę z dzielenia W_2 przez W_3; wielomian W_4 nie będzie więc stałą równą 0, a na mocy twierdzenia 1 będzie istniał wielomian Q_2 taki, iż $W_2=Q_2W_3+W_4$. Podobnie jak wyżej, dowodzimy, że wielomiany W_2 i W_3 mają te same wspólne dzielniki co i wielomiany W_3 i W_4, przy czym st $W_4<$ st W_3.

Rozumowanie to możemy powtórzyć, otrzymując nowy wielomian W_5 i t.d. Powtarzanie to musi się jednak urwać, ponieważ st $W_2>$st $W_3>$st $W_4>\ldots$ Dojdziemy więc wreszcie do wielomianu W_k takiego, iż $W_k|W_{k-1}$. Wielomiany W_1 i W_2 posiadają więc te same wspólne dzielniki, co wielomiany W_{k-1} i W_k, a więc w myśl twierdzenia 5 oraz określenia największego wspólnego dzielnika dwóch wielomianów, mają one też jeden i ten sam największy wspólny dzielnik. Jest nim mianowicie wielomian W_k podzielony przez współczynnik przy jego najwyższej potędze.

Mamy w ten sposób ***regułę*** wyznaczania największego wspólnego dzielnika dwóch wielomianów, z których żaden nie jest stałą równą 0, za pomocą kolejnych dzieleń.

Z algorytmu tego oraz z twierdzenia 2 wynika natychmiast

Twierdzenie 6. *Współczynniki największego wspólnego dzielnika dwóch wielomianów otrzymuje się za pomocą działań wymiernych ze współczynników tych wielomianów. W szczególności, największy wspólny dzielnik dwóch wielomianów o współczynnikach wymiernych jest wielomianem o współczynnikach wymiernych.*

Podany algorytm pozwala również wyznaczyć efektywnie wielomiany H, X i Y, spełniające warunki (8) i (9) twierdzenia 4. Mianowicie, otrzymaliśmy wyżej ciąg równości:

$$
\begin{aligned}
W_1 &= Q_1W_2+W_3,\\
W_2 &= Q_2W_3+W_4,\\
&\cdots\cdots\\
W_{k-2} &= Q_{k-2}W_{k-1}+W_k,\\
W_{k-1} &= Q_{k-1}W_k.
\end{aligned}
\tag{11}
$$

Przyjmijmy $X_1=0$, $Y_1=1$, $X_2=1$, $Y_2=-Q_1$ i wyznaczmy dla $i=3,4,\ldots,k-1$ wielomiany X_i i Y_i przez wzory zwrotne:

$$X_i=X_{i-2}-Q_{i-1}X_{i-1},\qquad Y_i=Y_{i-2}-Q_{i-1}Y_{i-1}. \tag{12}$$

Mamy oczywiście $W_2=X_1W_1+Y_1W_2$ i wobec (11) dowodzimy z łatwością przez indukcję, że

$$W_i=X_{i-1}W_1+Y_{i-1}W_2 \quad \text{dla} \quad i=2,3,\ldots,k.$$

Jest więc w szczególności

$$W_k=X_{k-1}W_1+Y_{k-1}W_2. \tag{13}$$

Lecz, jak wiemy, W_k jest wspólnym dzielnikiem wielomianów W_1 i W_2. Zatem wielomiany $H=W_k$, $X=X_{k-1}$ i $Y=Y_{k-1}$ istotnie spełniają warunki (8) i (9) twierdzenia 4.

Podane wzory zwrotne (12) nie tylko dają sposób efektywnego wyznaczania wielomianów H, X i Y, ale ponadto dowodzą, że współczynniki tych wielomianów otrzymują się za pomocą działań wymiernych ze współczynników wielomianów W_1 i W_2. Wreszcie, dzieląc obie strony wzoru (13) przez współczynnik przy najwyższej potędze wielomianu W_k, otrzymamy wyrażenie dla największego wspólnego dzielnika D wielomianów W_1 i W_2:

$$D=MW_1+NW_2. \tag{14}$$

Dla każdych dwóch danych wielomianów W_1 i W_2, z których żaden nie jest stałą równą 0, potrafimy więc wyznaczyć wielomiany M i N, spełniające wzór (14), gdzie D oznacza największy wspólny dzielnik tych wielomianów.

Uwaga. Metoda kolejnych dzieleń, jakkolwiek teoretycznie niezmiernie prosta, może doprowadzić w praktyce, nawet dla stosunkowo prostych wielomianów, do rachunków żmudnych i uciążliwych. Tak np. kolejne dzielenia dla znalezienia największego wspólnego dzielnika wielomianów:

$$W_1=x^6+x^5-x^4-x^3+x^2-x+1 \quad \text{i} \quad W_2=6x^5+5x^4-4x^3-3x^2+2x-1$$

doprowadzają do ułamków, których liczniki i mianowniki mają po kilkadziesiąt cyfr[1]).

ĆWICZENIE. Znaleźć największy wspólny dzielnik wielomianów

$$x^5-2x^4-2x^3+8x^2-7x+2 \quad \text{i} \quad x^4-4x+3.$$

Odp.: x^2-2x+1.

[1]) Por. J. A. Serret, *Cours d'Algèbre Supérieure*, Tom I, Wyd. 5, Paryż 1885, str. 304 i 305.

§ 5. Wielomiany względnie pierwsze. Wielomiany W_1 i W_2, których największym wspólnym dzielnikiem jest stała 1, nazywamy *względnie pierwszymi.*

Jeżeli dwa wielomiany nie są względnie pierwsze, to ich największy wspólny dzielnik jest różny od 1, a więc jest wielomianem stopnia dodatniego, gdyż (w myśl definicji, podanej na str. 109) jest on wielomianem, którego współczynnik przy najwyższej potędze jest równy 1. Jeżeli zaś wielomiany W_1 i W_2 są względnie pierwsze, to na mocy twierdzeń 4 i 5 istnieją wielomiany M i N takie, iż

$$MW_1 + NW_2 = 1. \tag{15}$$

Na odwrót, jeżeli istnieją wielomiany M i N, spełniające wzór (15), to wielomiany W_1 i W_2 są względnie pierwsze. Istotnie, niech D oznacza największy wspólny dzielnik wielomianów W_1 i W_2. Mamy więc $D|W_1$ oraz $D|W_2$, skąd, wobec (15), $D|1$. Dowodzi to, w myśl definicji podzielności wielomianów, że D jest stałą, a że w myśl definicji największego wspólnego dzielnika dwóch wielomianów, jest to wielomian o współczynniku 1 przy najwyższej potędze, więc $D=1$. Mamy zatem

Twierdzenie 7. *Na to, żeby wielomiany W_1 i W_2 były względnie pierwsze, potrzeba i wystarcza, aby istniały wielomiany M i N takie, iż $MW_1+NW_2=1$.*

Największy wspólny dzielnik dwóch wielomianów W_1 i W_2 będziemy oznaczali przez (W_1,W_2). Wzór

$$(W_1,W_2) = 1$$

wyraża więc, że wielomiany W_1 i W_2 są względnie pierwsze.

Warunek konieczny i dostateczny na to, aby dwa wielomiany były względnie pierwsze, daje się też wyrazić przez przyrównanie do zera pewnego wyznacznika, utworzonego z ich współczynników. Udowodnimy w tym celu następujący

Lemat. *Na to, żeby wielomiany W_1 stopnia $m>0$ oraz W_2 stopnia $n>0$ nie były względnie pierwsze, potrzeba i wystarcza, iżby istniały wielomiany V_1 stopnia mniejszego od m oraz V_2 stopnia mniejszego od n, z których jeden przynajmniej nie jest stałą równą 0, przy czym*

$$W_1V_2 = W_2V_1. \tag{16}$$

D o w ó d. Jeżeli wielomiany W_1 i W_2 nie są względnie pierwsze, to ich największy wspólny dzielnik D jest, jak widzieliśmy (str. 112), wielomianem stopnia dodatniego i możemy napisać

$$W_1 = DV_1, \qquad W_2 = DV_2, \tag{17}$$

gdzie V_1 jest wielomianem stopnia mniejszego od m, zaś V_2 stopnia mniejszego od n, przy czym żaden z tych wielomianów nie jest stałą równą 0, gdyż nie są stałymi ani W_1, ani W_2, jako wielomiany stopni dodatnich. Wobec (17) znajdujemy natychmiast wzór (16), podany w lemacie. Warunek jest więc k o n i e c z n y.

Na odwrót, jeżeli wielomiany W_1 i W_2 są względnie pierwsze, to w myśl twierdzenia 7 istnieją wielomiany M i N, takie iż

$$MW_1 + NW_2 = 1. \tag{18}$$

Gdyby istniały wielomiany V_1 stopnia mniejszego od m oraz V_2 stopnia mniejszego od n, dla których zachodzi równość (16), i gdyby co najmniej jeden z nich, np. V_1, nie był stałą równą 0, to wobec (18) i (16) znaleźlibyśmy:

$$V_1 = (MW_1 + NW_2)V_1 = (MV_1 + NV_2)W_1,$$

co nie jest możliwe, gdyż $\operatorname{st} V_1 < m = \operatorname{st} W_1$. Warunek jest więc zarazem d o s t a t e c z n y, c. b. d. o.

Załóżmy teraz, że $m \geqslant n$ i niech:

$$W_1 = W_1(x) = a_0x^m + a_1x^{m-1} + \ldots + a_m,$$
$$W_2 = W_2(x) = b_0x^n + b_1x^{n-1} + \ldots + b_n.$$

Na to, żeby istniały wielomiany V_1 stopnia mniejszego od m oraz V_2 stopnia mniejszego od n, z których co najmniej jeden nie jest stałą równą 0, spełniające równość (16), potrzeba więc i wystarcza, żeby istniało $m+n$ liczb $p_0, p_1, \ldots, p_{m-1}$ i $q_0, q_1, \ldots, q_{n-1}$, z których jedna co najmniej nie jest zerem, a przy tym takich, iżby zachodziła równość wielomianów:

$$(a_0x^m + a_1x^{m-1} + \ldots + a_m)(q_0x^{n-1} + q_1x^{n-2} + \ldots + q_{n-1}) =$$
$$= (b_0x^n + b_1x^{n-1} + \ldots + b_n)(p_0x^{m-1} + p_1x^{m-2} + \ldots + p_{m-1}),$$

czyli — innymi słowy — liczb spełniających układ $m+n$ równań liniowych jednorodnych:

$$a_0 q_0 - b_0 p_0 = 0,$$
$$a_1 q_0 + a_0 q_1 - b_1 p_0 - b_0 p_1 = 0,$$
$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$
$$a_m q_0 + a_{m-1} q_1 + \ldots + a_{m-n+1} q_{n-1} - b_n p_{m-n} - b_{n-1} p_{m-n+1} - \ldots - b_1 p_{m-1} = 0,$$
$$a_m q_1 + a_{m-1} q_2 + \ldots + a_{m-n+2} q_{n-1} - b_n p_{m-n+1} - b_{n-1} p_{m-n+2} - \ldots - b_2 p_{m-1} = 0,$$
$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$
$$a_m q_{n-1} - b_n p_{m-1} = 0.$$

Lecz, jak wiemy (ob. Rozdział III, § 6, tw. 6, str. 50), na to, żeby ten układ równań (o niewiadomych $-p_0, -p_1, \ldots, -p_{m-1}, q_0, q_1, \ldots, q_{n-1}$) posiadał rozwiazanie niezerowe, potrzeba i wystarcza, iżby jego wyznacznik

$$\Delta = \left| \begin{array}{ccccccc|ccccccccccc}
a_0 & 0 & \cdot & \cdot & \cdot & \cdot & 0 & b_0 & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\
a_1 & a_0 & 0 & \cdot & \cdot & \cdot & 0 & b_1 & b_0 & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\
a_2 & \cdot & a_0 & 0 & \cdot & \cdot & 0 & b_2 & \cdot & b_0 & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\
\cdot & \cdot & \cdot & a_0 & 0 & \cdot & 0 & \cdot & \cdot & \cdot & b_0 & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \\
\cdot & \cdot & \cdot & \cdot & a_0 & 0 & 0 & \cdot & \cdot & \cdot & \cdot & b_0 & 0 & \cdot & \cdot & \cdot & \cdot & 0 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & a_0 & b_{n-1} & \cdot & \cdot & \cdot & \cdot & \cdot & b_0 & 0 & \cdot & \cdot & 0 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & a_1 & b_n & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & b_0 & 0 & \cdot & 0 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 & b_n & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & b_0 & 0 & 0 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
a_{m-1} & \cdot & \cdot & \cdot & \cdot & \cdot & a_{m-n} & 0 & \cdot & 0 & b_n & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & b_0 \\
\hline
a_m & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 & \cdot & \cdot & 0 & b_n & \cdot & \cdot & \cdot & \cdot & \cdot & b_1 \\
0 & a_m & \cdot & \cdot & \cdot & \cdot & \cdot & 0 & \cdot & \cdot & \cdot & 0 & b_n & \cdot & \cdot & \cdot & \cdot & b_2 \\
0 & 0 & a_m & \cdot & \cdot & \cdot & \cdot & 0 & \cdot & \cdot & \cdot & \cdot & 0 & b_n & \cdot & \cdot & \cdot & \cdot \\
0 & \cdot & 0 & a_m & \cdot & \cdot & \cdot & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & 0 & b_n & \cdot & \cdot & \cdot \\
0 & \cdot & \cdot & 0 & a_m & \cdot & \cdot & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 & b_n & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
0 & \cdot & \cdot & \cdot & \cdot & 0 & a_m & 0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 & b_n
\end{array} \right| \begin{array}{l} \left.\vphantom{\begin{array}{c}1\\1\\1\\1\\1\\1\\1\\1\\1\\1\\1\end{array}}\right\} m \text{ wierszy} \\ \left.\vphantom{\begin{array}{c}1\\1\\1\\1\\1\\1\\1\end{array}}\right\} n \text{ wierszy} \end{array}$$

n kolumn $\qquad$ m kolumn

był równy zeru. Mamy zatem

Twierdzenie 8. *Na to żeby wielomiany $a_0x^m + a_1x^{m-1} + \ldots + a_m$ oraz $b_0x^n + b_1x^{n-1} + \ldots + b_n$ były względnie pierwsze, potrzeba i wystarcza, iżby wyznacznik Δ (stopnia $m+n$) był różny od zera.*

Jako przykład, weźmy dwa wielomiany stopnia drugiego:

$$a_0x^2 + a_1x + a_2 \qquad \text{i} \qquad b_0x^2 + b_1x + b_2.$$

Na to, żeby te wielomiany były względnie pierwsze, potrzeba i wystarcza, iżby było

$$\Delta = \begin{vmatrix} a_0 & 0 & b_0 & 0 \\ a_1 & a_0 & b_1 & b_0 \\ a_2 & a_1 & b_2 & b_1 \\ 0 & a_2 & 0 & b_2 \end{vmatrix} \neq 0,$$

czyli, aby było

$$(a_0b_2 - a_2b_0)^2 + (a_1b_0 - a_0b_1)(a_1b_2 - a_2b_1) \neq 0.$$

Inny przykład: warunkiem, aby wielomiany

$$a_0x^3 + a_1x^2 + a_2x + a_3 \qquad \text{i} \qquad b_0x^2 + b_1x + b_2$$

były względnie pierwsze, jest

$$\Delta = \begin{vmatrix} a_0 & 0 & b_0 & 0 & 0 \\ a_1 & a_0 & b_1 & b_0 & 0 \\ a_2 & a_1 & b_2 & b_1 & b_0 \\ a_3 & a_2 & 0 & b_2 & b_1 \\ 0 & a_3 & 0 & 0 & b_2 \end{vmatrix} \neq 0.$$

Uwaga. Jeżeli wielomiany $f(x)$ i $g(x)$ o współczynnikach całkowitych są względnie pierwsze, to niekoniecznie przy całkowitym a liczby $f(a)$ i $g(a)$ są względnie pierwsze; np. wielomiany $f(x) = x+6$ oraz $g(x) = x$ są względnie pierwsze, ale $f(3) = 9$ oraz $g(3) = 3$ nie są względnie pierwsze.

§ 6. Największy wspólny dzielnik wielu wielomianów.

Twierdzenie 9. *Jeżeli W_1, W_2 i W_3 są wielomianami takimi, że $(W_1, W_2) = 1$ i $W_1 | W_2W_3$, to $W_1 | W_3$.*

Dowód. Jeżeli $(W_1, W_2) = 1$, to w myśl twierdzenia 7 istnieją wielomiany M i N, dla których zachodzi wzór (15), skąd, mnożąc przez W_3, otrzymujemy:

$$W_3 = MW_1W_3 + NW_2W_3. \tag{19}$$

Jeżeli nadto $W_1 | W_2W_3$, to W_1 jest oczywiście dzielnikiem każdego ze składników prawej strony wzoru (19), skąd $W_1 | W_3$, c. b. d. o.

Twierdzenie 10. *Jeżeli W_1, W_2 i W_3 są wielomianami takimi, że $(W_1, W_2) = 1$ i $(W_1, W_3) = 1$, to $(W_1, W_2W_3) = 1$.*

Dowód. Skoro $(W_1,W_2)=1$ oraz $(W_1,W_3)=1$, to w myśl twierdzenia 7 istnieją wielomiany M, N, P i Q takie, iż $MW_1+NW_2=1$ i $PW_1+QW_3=1$, skąd, mnożąc stronami:

$$(MPW_1+MQW_3+NPW_2)W_1+NQW_2W_3=1,$$

co dowodzi w myśl twierdzenia 7, że $(W_1,W_2W_3)=1$, c. b. d. o.

Powróćmy jeszcze do twierdzenia 4. Daje się ono z łatwością uogólnić, jak następuje:

Twierdzenie 4^{bis}. *Jeżeli jeden co najmniej z wielomianów $W_1,W_2,\dots,W_m$ (gdzie m jest daną liczbą naturalną) nie jest stałą równą zeru, to istnieje wielomian H taki, iż*

(20) $$H|W_i \quad dla \quad i=1,2,\dots,m,$$

przy czym dla odpowiednio dobranych wielomianów $X_1,X_2,\dots,X_m$ zachodzi równość

(21) $$H=W_1X_1+W_2X_2+\dots+W_mX_m.$$

Dowód tego twierdzenia jest taki sam, jak twierdzenia 4: bierzemy spośród wielomianów postaci (21), nierównych stałej 0, którykolwiek możliwie najniższego stopnia i tak samo, jak w twierdzeniu 4, dowodzimy, że spełnia on oba żądane warunki.

Dla efektywnego wyznaczenia wielomianów $X_1,X_2,\dots,X_n$ należałoby zastosować indukcję. Mianowicie, potrafimy wyznaczyć te wielomiany dla $m=2$. Załóżmy, że potrafimy to zrobić dla danego naturalnego m i niech $W_1,W_2,\dots,W_m,W_{m+1}$ oznaczają $m+1$ danych wielomianów, z których co najmniej jeden, np. W_1, nie jest stałą 0. W myśl założenia, potrafimy wyznaczyć wielomiany $X_1,X_2,\dots,X_m$ spełniające wzory (20) i (21), przy czym wielomian H, jak wiemy nie jest stałą 0. Potrafimy też wyznaczyć wielomiany K, Y_1 i Y takie, iż

(22) $$K|H, \qquad K|W_{m+1},$$

(23) $$K=HY_1+W_{m+1}Y_2.$$

Wzory (22) i (20) dają natychmiast $K|W_i$ dla $i=1,2,\dots,m,m+1$, zaś wzory (23) i (21) dają:

$$K=W_1X_1Y_1+W_2X_2Y_1+\dots+W_mX_mY_1+W_{m+1}Y_2.$$

Zatem wielomiany $X_1Y_1,X_2Y_1,\dots,X_mY_1$ i Y_2 spełniają żądane warunki dla wielomianów $X_1,X_2,\dots,X_{m+1}$.

Wreszcie wielomian H, spełniający twierdzenie 4^{bis}, jest, jak łatwo wykazać, takim wspólnym dzielnikiem wielomianów $W_1,W_2,\dots,W_m$, który jest podzielny przez każdy inny wspólny dzielnik tych wielomianów.

Podzielony przez współczynnik przy najwyższej potędze zmiennej x, nosi on nazwę *największego wspólnego dzielnika wielomianów* $W_1,W_2,\dots,W_m$.

§ 7. Najmniejsza wspólna wielokrotność wielomianów. Jeżeli wielomian W jest podzielny przez każdy z wielomianów $W_1,W_2,\dots,W_m$, to nazywamy go *wspólną wielokrotnością wielomianów* $W_1,W_2,\dots,W_m$.

Jeżeli żaden z wielomianów $W_1,W_2,\dots,W_m$ nie jest stałą 0, to istnieją wspólne wielokrotności tych wielomianów, również nie będące stałą 0 (np. ich iloczyn).

Spośród wszystkich wielomianów, które nie są stałą 0 i są wspólnymi wielokrotnościami wielomianów $W_1,W_2,\dots,W_m$, weźmy którykolwiek, możliwie najniższego stopnia; niech to będzie wielomian N. Wykażemy, że N jest dzielnikiem każdej wspólnej wielokrotności wielomianów $W_1,W_2,\dots,W_m$.

Istotnie, przypuśćmy, że wspólna wielokrotność W wielomianów $W_1,W_2,\dots,W_m$ nie jest podzielna przez N. Niech Q oznacza iloraz, zaś R resztę z dzielenia W przez N. Byłoby więc

(24) $$W=QN+R,$$

przy czym st $R<$ st N, oraz R nie byłoby stałą 0. Wzór (24) daje $R=W-QN$, co wobec $W_i|N$ oraz $W_i|W$ dla $i=1,2,\dots,m$ (gdyż N i W są wspólnymi wielokrotnościami wielomianów $W_1,W_2,\dots,W_m$) dowodzi, że $W_i|R$ dla $i=1,2,\dots,m$. Wielomian R byłby więc wspólną wielokrotnością wielomianów $W_1,W_2,\dots,W_m$ stopnia niższego od st N, o którym założyliśmy, że jest z możliwych najniższy.

Udowodniliśmy więc

Twierdzenie 11. *Dla każdej skończonej liczby wielomianów, z których żaden nie jest stałą 0, istnieje taka ich wspólna wielokrotność, która jest dzielnikiem każdej innej wspólnej wielokrotności tych wielomianów.*

Nazywamy ją *najmniejszą wspólną wielokrotnością* tych wielomianów.

ĆWICZENIA. 1. Dowieść, że przy naturalnym n wielomian

$$nx^{n+1}-(n+1)x^n+1$$

jest podzielny przez $(x-1)^2$. Wyznaczyć iloraz.

Odp.: $nx^{n-1}+(n-1)x^{n-2}+\ldots+3x^2+2x+1$.

2. Dowieść, że przy naturalnym n wielomian $(x^n-1)(x^{n+1}-1)(x^{n+2}-1)$ jest podzielny przez wielomian $(x-1)(x^2-1)(x^3-1)$ [1].

§ 8. Wzór Taylora dla wielomianów jednej zmiennej.

Pochodną wielomianu $f(x)=W(x)$, gdzie $W(x)$ oznacza wielomian (1), określiliśmy na str. 105 czysto formalnie, bez pojęcia granicy, jako wielomian

$$f'(x)=ma_0x^{m-1}+(m-1)a_1x^{m-2}+\ldots+a_{m-1}. \tag{25}$$

Pochodne wyższych rzędów określamy przez indukcję za pomocą wzoru zwrotnego:

$$f^{(k+1)}(x)=\left(f^{(k)}(x)\right)',$$

t.j. $(k+1)$-*sza pochodna wielomianu* $f(x)$ *jest pierwszą pochodną jego* k-*tej pochodnej*.

Będzie więc:

$$f''(x)=m(m-1)a_0x^{m-2}+(m-1)(m-2)a_1x^{m-3}+\ldots+2\cdot 1a_{m-2}$$

i ogólnie:

$$f^{(k)}(x)=k!\left[\binom{m}{k}a_0x^{m-k}+\binom{m-1}{k}a_1x^{m-k-1}+\ldots+\binom{k}{k}a_{m-k}\right], \tag{26}$$

gdzie $\binom{m}{j}$ oznacza współczynnik newtonowski

$$\binom{m}{j}=\frac{m(m-1)\ldots(m-j+1)}{1\cdot 2\ldots j}=\frac{m!}{j!(m-j)!}.$$

W szczególności, *pochodna wielomianu, będącego stałą, jest zerem*. Ponieważ zaś, w myśl wzoru (26), mamy dla wielomianu (1)

$$f^{(m)}(x)=m!\,a_0,$$

więc:

Wszystkie pochodne wielomianu $f(x)$, *których rząd jest wyższy od stopnia wielomianu, są równe zeru.*

[1] Gauss dowiódł, że przy wszelkich naturalnych n i k wielomian $(x^n-1)(x^{n+1}-1)\ldots(x^{n+k-1}-1)$ jest podzielny przez wielomian $(x-1)(x^2-1)\ldots(x^k-1)$.

Wobec wzoru (25) mamy:

$$\begin{aligned}
f(x+h)&=a_0(x+h)^m+a_1(x+h)^{m-1}+\ldots+a_{m-1}(x+h)+a_m=\\
&=a_0\left[x^m+\binom{m}{1}x^{m-1}h+\binom{m}{2}x^{m-2}h^2+\ldots+\binom{m}{m}h^m\right]+\\
&+a_1\left[x^{m-1}+\binom{m-1}{1}x^{m-2}h+\binom{m-1}{2}x^{m-3}h^2+\ldots+\binom{m-1}{m-1}h^{m-1}\right]+\ldots\\
&\ldots+a_{m-1}[x+h]+a_m=\\
&=(a_0x^m+a_1x^{m-1}+\ldots+a_m)+\\
&+h\left[\binom{m}{1}a_0x^{m-1}+\binom{m-1}{1}a_1x^{m-2}+\ldots+\binom{1}{1}a_{m-1}\right]+\\
&+h^2\left[\binom{m}{2}a_0x^{m-2}+\binom{m-1}{2}a_1x^{m-3}+\ldots+\binom{2}{2}a_{m-2}\right]+\ldots+h^m\binom{m}{m}a_0,
\end{aligned}$$

zatem w myśl wzorów (25) i (26):

$$f(x+h)=f(x)+\frac{h}{1!}f'(x)+\frac{h^2}{2!}f''(x)+\ldots+\frac{h^m}{m!}f^{(m)}(x). \tag{27}$$

Zastępując w tej tożsamości x przez a, zaś h przez $x-a$, otrzymamy nową tożsamość:

$$f(x)=f(a)+\frac{x-a}{1!}f'(a)+\frac{(x-a)^2}{2!}f''(a)+\ldots+\frac{(x-a)^m}{m!}f^{(m)}(a). \tag{28}$$

Jest to *wzór Taylora*.

Zastępując we wzorze (27) x przez h i na odwrót, otrzymujemy wzór:

$$f(x+h)=f(h)+\frac{x}{1!}f'(h)+\frac{x^2}{2!}f''(h)+\ldots+\frac{x^m}{m!}f^{(m)}(h).$$

Niech $f(x)$ będzie wielomianem o współczynnikach rzeczywistych. Dla dostatecznie wielkich h liczby $f(h), f'(h),\ldots, f^{(m)}(h)$ mają ten sam znak co a_0. Wynika stąd, że liczbę h można tak dobrać, aby $f(x+h)$ było wielomianem względem x o współczynnikach, które wszystkie mają ten sam znak (taki jak a_0). Stąd wniosek, że znajdywanie pierwiastków wielomianu o współczynnikach rzeczywistych daje się zawsze sprowadzić do znajdywania pierwiastków wielomianu (tego samego stopnia) o współczynnikach dodatnich.

ĆWICZENIA. 1. Dowieść, że dla naturalnych m, n i k:

$$\binom{m}{0}\binom{n}{k}+\binom{m}{1}\binom{n}{k-1}+\binom{m}{2}\binom{n}{k-2}+\ldots+\binom{m}{k}\binom{n}{0}=\binom{m+n}{k}.$$

2. Dowieść, że dla naturalnych m i k:

$$\binom{k}{k}+\binom{k+1}{k}+\binom{k+2}{k}+\ldots+\binom{k+m}{k}=\binom{k+m+1}{k+1}.$$

3. Dowieść, że dla naturalnych m:

$$\binom{m}{0}^2+\binom{m}{1}^2+\ldots+\binom{m}{m}^2=\binom{2m}{m}.$$

Wskazówka: Porównać współczynniki przy x^m w rozwinięciach $(1+x)^m\cdot(1+x)^m$ oraz $(1+x)^{2m}$, korzystając ze wzoru $\binom{m}{k}=\binom{m}{m-k}$.

4.[1]) Dowieść (przez indukcję), że dla naturalnych m:

$$(a^2+ab+b^2)^m=a_m^2+a_mb_m+b_m^2,$$

gdzie:

$$a_m=a^m-\binom{m}{2}a^{m-2}b^2-\binom{m}{3}a^{m-3}b^3+\binom{m}{5}a^{m-5}b^5+\binom{m}{6}a^{m-6}b^6-\ldots,$$

$$b_m=\binom{m}{1}a^{m-1}b+\binom{m}{2}a^{m-2}b^2-\binom{m}{4}a^{m-4}b^4-\binom{m}{5}a^{m-5}b^5+\ldots$$

Przy pomocy tożsamości A. Gérardin'a:

$$2(a^2+ab+b^2)^4=(a^2-b^2)^4+(a^2+2ab)^4+(2ab+b^2)^4,$$

wyprowadzić stąd, że:

$$2(a^2+ab+b^2)^{4m}=(a_m^2-b_m^2)^4+(a_m^2+2a_mb_m)^4+(2a_mb_m+b_m^2)^4.$$

5. Udowodnić tożsamość:

$$[2^9 5^2(2^{10}-1)^2z^5-1]^5+[-2^9 5^2(2^{10}-1)^2z^5-1]^5+[2^8 5^2(2^{10}-1)^2z^4+2^4]^5+$$
$$+[2^4-2^8 5^2(2^{10}-1)^2z^5]^5+[2^4 5(1-2^{10})z^2]^5=2(2^{20}-1). \qquad \text{(Chowla).}$$

§ 9. Pierwiastki wielokrotne wielomianu.

Twierdzenie 12. *Wielomian $f(x)$ jest wtedy i tylko wtedy podzielny przez $(x-a)^k$, jeżeli*

$$(29) \qquad f(a)=0,\quad f'(a)=0,\quad \ldots,\quad f^{(k-1)}(a)=0,$$

t.j. jeżeli a jest wspólnym pierwiastkiem wielomianu $f(x)$ oraz $k-1$ kolejnych jego pochodnych.

Dowód. Dostateczność tego warunku wynika natychmiast ze wzoru (28), konieczność zaś udowodnić można, jak następuje. Jeżeli $f^{(p)}(a)$ jest pierwszą z liczb ciągu $f(a), f'(a), f''(a), \ldots$, która nie jest zerem, to wobec (28):

$$f(x)=\frac{(x-a)^p}{p!}f^{(p)}(a)+(x-a)^{p+1}Q(x),$$

[1]) A. S. Bang, Mathematisk Tiddskrift, Tom 13 (1940) str. 62-65.

gdzie $Q(x)$ jest wielomianem; dowodzi to, że $\frac{(x-a)^p}{p!}f^{(p)}(a)$ jest resztą z dzielenia $f(x)$ przez $(x-a)^{p+1}$ i to resztą różną od zera, skoro $f^{(p)}(a)\neq 0$. Wielomian $f(x)$ nie jest więc podzielny przez $(x-a)^{p+1}$. Jest on jednak podzielny przez $(x-a)^k$, zatem $p+1>k$, skąd $k\leqslant p$, czyli (wobec definicji liczby p) $f(a)=f'(a)=\ldots=f^{(k-1)}(a)=0$.

Z twierdzenia 11 wynikają następujące wnioski:

Wniosek 1. *Jeżeli wielomian $f(x)$ jest podzielny przez $(x-a)^k$, to jego pochodna $f'(x)$ jest podzielna przez $(x-a)^{k-1}$.*

Bowiem przyjmując $\varphi(x)=f'(x)$, otrzymamy:

$$(30) \qquad \varphi'(x)=f''(x),\quad \varphi''(x)=f^{(3)}(x),\quad \ldots,\quad \varphi^{(k-2)}(x)=f^{(k-1)}(x).$$

Jeżeli $f(x)$ jest podzielne przez $(x-a)^k$ to, w myśl twierdzenia 11 i (30) będzie

$$(31) \qquad \varphi(a)=\varphi'(a)=\varphi''(a)=\ldots=\varphi^{(k-2)}(a)=0,$$

co, w myśl twierdzenia 11, dowodzi, że $\varphi(x)$ jest podzielne przez $(x-a)^{k-1}$.

Odwrócenie tego wniosku nie jest prawdziwe. Np. wielomian $f(x)=1+x^3$ nie jest podzielny przez x^2, ani nawet przez x, mimo że jego pochodna $f'(x)=3x^2$ jest podzielna przez x^2. Natomiast mamy

Wniosek 2. *Jeżeli a jest pierwiastkiem wielomianu $f(x)$, t.zn. jeżeli $f(a)=0$, i jeżeli jego pochodna $f'(x)$ jest podzielna przez $(x-a)^{k-1}$, gdzie k jest liczbą naturalną, to $f(x)$ jest podzielne przez $(x-a)^k$.*

Dla $k=1$ wniosek ten jest oczywisty, gdyż wobec $f(a)=0$ $f(x)$ musi być podzielne przez $x-a$ na mocy twierdzenia 3, § 2, str. 107. Jeżeli zaś $k>1$ i $\varphi(x)$ jest podzielne przez $(x-a)^{k-1}$, to w myśl twierdzenia 12 mamy równości (31), zatem wobec (30) i wobec $f(a)=0$, zachodzą równości (29), a przeto, w myśl twierdzenia 12, $f(x)$ jest podzielne przez $(x-a)^k$.

Liczbę a nazywamy *k-krotnym pierwiastkiem* $f(x)$, jeżeli $f(x)$ jest podzielne przez $(x-a)^k$, lecz nie jest już podzielne przez $(x-a)^{k+1}$.

Pierwiastki co najmniej jednokrotne nazywamy po prostu *pierwiastkami* $f(x)$.

Jeżeli a nie jest pierwiastkiem wielomianu $f(x)$, to możemy powiedzieć, że a jest *0-krotnym* pierwiastkiem wielomianu $f(x)$.

Udowodnione dwa wnioski z twierdzenia 12 dają następujące

Twierdzenie 13. Na to, żeby pierwiastek a wielomianu $f(x)$ był k-krotny, gdzie k jest liczbą naturalną, potrzeba i wystarcza, iżby a było $(k-1)$-krotnym pierwiastkiem pochodnej $f'(x)$.

§ 10. Pozbywanie się pierwiastków wielokrotnych wielomianu. Udowodnimy teraz

Twierdzenie 14. Jeżeli $d(x)$ oznacza największy wspólny dzielnik wielomianów $f(x)$ i $f'(x)$, to wielomian $\varphi(x)=\dfrac{f(x)}{d(x)}$ posiada wszystkie te i tylko te pierwiastki, które są pierwiastkami wielomianu $f(x)$, przy czym każdy jest pierwiastkiem jednokrotnym wielomianu $\varphi(x)$.

Dowód. Z tego, że $\varphi(x)|f(x)$, wynika, że każdy pierwiastek wielomianu $\varphi(x)$ jest pierwiastkiem wielomianu $f(x)$; wystarczy więc dowieść, że każdy pierwiastek wielomianu $f(x)$ jest jednokrotnym pierwiastkiem wielomianu $\varphi(x)$.

Niech a oznacza pierwiastek wielomianu $f(x)$, a k jego krotność. W myśl twierdzenia 13, a jest więc $(k-1)$-krotnym pierwiastkiem wielomianu $f'(x)$. Wielomian $f'(x)$ jest zatem podzielny przez $(x-a)^{k-1}$, ale nie jest podzielny przez $(x-a)^k$. Wynika stąd że największy wspólny dzielnik $d(x)$ wielomianów $f(x)$ i $f'(x)$ jest podzielny przez $(x-a)^{k-1}$, lecz nie jest podzielny przez $(x-a)^k$. Zachodzi więc równość $d(x)=(x-a)^{k-1}g(x)$, gdzie $g(x)$ jest wielomianem niepodzielnym przez $x-a$, dla którego zatem $g(a)\neq 0$. Wobec $\varphi(x)=f(x)/d(x)$ mamy więc $f(x)=d(x)\varphi(x)=(x-a)^{k-1}g(x)\varphi(x)$.

Gdyby było $\varphi(a)\neq 0$, mielibyśmy $g(a)\varphi(a)\neq 0$ i wielomian $g(x)\varphi(x)$ nie byłby podzielny przez $x-a$. Przeto wielomian $f(x)$ nie byłby podzielny przez $(x-a)^k$, wbrew założeniu, że a jest k-krotnym pierwiastkiem wielomianu $f(x)$. Musi więc być $\varphi(a)=0$. Liczba a jest zatem pierwiastkiem wielomianu $\varphi(x)$.

Gdyby a nie było jednokrotnym pierwiastkiem wielomianu $\varphi(x)$, to $\varphi(x)$ byłoby podzielne przez $(x-a)^2$ i, z uwagi na to, że $d(x)$ jest podzielne przez $(x-a)^{k-1}$, wynikałoby, że $f(x)=d(x)\varphi(x)$ jest podzielne przez $(x-a)^{k+1}$, wbrew założeniu, że a jest k-krotnym pierwiastkiem wielomianu $f(x)$. Liczba a jest więc jednokrotnym pierwiastkiem wielomianu $\varphi(x)$.

Udowodniliśmy zatem twierdzenie 14.

Jak wiemy z tw. 2, współczynniki wielomianu $d(x)$ potrafimy obliczyć za pomocą działań wymiernych, jeżeli dane są współczyn-

niki wielomianu $f(x)$. Zatem dla każdego danego wielomianu $f(x)$ potrafimy za pomocą działań wymiernych na jego współczynnikach obliczyć współczynniki wielomianu $\varphi(x)$. Twierdzenie 14 pozwala więc sprowadzić badanie pierwiastków każdego wielomianu do badania pierwiastków wielomianu, nie wyższego od niego stopnia, ale mającego same tylko pierwiastki jednokrotne.

§ 11. Rozkład wielomianu na czynniki liniowe. Wnioski.

Twierdzenie 15. Jeżeli $\alpha_1,\alpha_2,\ldots,\alpha_k$ są różnymi pierwiastkami wielomianu $f(x)$, to wielomian ten jest podzielny przez

$$(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_k).$$

Dowód. Niech $\alpha_1,\alpha_2,\ldots,\alpha_k$ będą różnymi pierwiastkami wielomianu $f(x)$. W myśl twierdzenia 3 wielomian $f(x)$ jest podzielny przez $x-\alpha_1$, czyli zachodzi równość:

$$f(x)=(x-\alpha_1)f_1(x), \tag{32}$$

gdzie $f_1(x)$ jest wielomianem.

Skoro α_2 jest pierwiastkiem wielomianu $f(x)$, więc $f(\alpha_2)=0$ i wzór (32) daje $(\alpha_2-\alpha_1)f_1(\alpha_2)=0$, co wobec założenia, że $\alpha_2\neq\alpha_1$, daje $f_1(\alpha_2)=0$. Liczba α_2 jest więc pierwiastkiem wielomianu $f_1(x)$ i, w myśl twierdzenia 3, wielomian $f_1(x)$ jest podzielny przez $x-\alpha_2$; wynika stąd, że

$$f_1(x)=(x-\alpha_2)f_2(x), \tag{33}$$

gdzie $f_2(x)$ jest wielomianem. Wobec (32) i (33) jest więc

$$f(x)=(x-\alpha_1)(x-\alpha_2)f_2(x). \tag{34}$$

Ponieważ α_3 jest pierwiastkiem wielomianu $f(x)$, różnym od α_1 i α_2, więc mamy $f(\alpha_3)=0$, zatem na mocy (34) $(\alpha_3-\alpha_1)(\alpha_3-\alpha_2)f_2(\alpha_3)=0$, co, wobec $\alpha_3\neq\alpha_1$ i $\alpha_3\neq\alpha_2$, daje $f_2(\alpha_3)=0$ i dowodzi, w myśl twierdzenia 3, że wielomian $f_3(x)$ jest podzielny przez $x-\alpha_3$, czyli że

$$f_3(x)=(x-\alpha_3)f(x), \tag{35}$$

gdzie $f_3(x)$ jest wielomianem. Wzory (34) i (35) dają

$$f(x)=(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)f_3(x).$$

Rozumując w ten sposób dalej, dojdziemy do wzoru

$$f(x)=(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_k)f_k(x), \tag{36}$$

gdzie $f_k(x)$ jest wielomianem (oczywiście stopnia $m-k$). Twierdzenie 15 wynika bezpośrednio ze wzoru (36).

W szczególności, jeżeli $k=m$, t.j. k jest równe stopniowi wielomianu $f(x)$, to $f_k(x)$ jest stałą; przez porównanie po obu stronach wzoru (36) współczynników przy najwyższych potęgach x wnosimy, że stała ta równa jest a_0. Mamy więc:

Twierdzenie 16. *Jeżeli liczby $a_1, a_2, \ldots, a_m$ są różnymi pierwiastkami wielomianu $f(x)=a_0x^m+a_1x^{m-1}+\ldots+a_m$, to*

$$f(x)=a_0(x-a_1)(x-a_2)\ldots(x-a_m). \tag{37}$$

Liczby $a_1, a_2, \ldots, a_m$ są wówczas wszystkimi pierwiastkami wielomianu $f(x)$. Jeżeli bowiem $f(a)=0$, to, w myśl wzoru (37), mamy $a_0(a-a_1)(a-a_2)\ldots(a-a_m)=0$, co wobec $a_0 \neq 0$ może zachodzić tylko wówczas, gdy a jest jedną z liczb $a_1, a_2, \ldots, a_m$.

Wynika stąd

Twierdzenie 17. *Wielomian m-go stopnia (gdzie $m \geqslant 1$) nie może posiadać więcej niż m różnych pierwiastków.*

Jako wniosek stąd otrzymujemy

Twierdzenie 18. *Jeżeli wielomian $a_0x^m+a_1x^{m-1}+\ldots+a_m$ ma więcej niż m różnych pierwiastków, to $a_0=a_1=\ldots=a_m=0$.*

Dowód. Gdyby było $a_k \neq 0$, gdzie k jest jedną z liczb $0, 1, 2, \ldots, m$, to wielomian $a_0x^m+a_1x^{m-1}+\ldots+a_m$ albo byłby stałą różną od 0 albo też wielomianem stopnia niewiększego od m, mającym więcej niż m pierwiastków, wbrew twierdzeniu 17.

Z twierdzenia 18 wynika następujący

Wniosek. *Każdy wielomian jednej zmiennej stopnia dodatniego może być tylko w jeden sposób przedstawiony w postaci*

$$a_0x^m+a_1x^{m-1}+\ldots+a_{m-1}x+a_m,$$

gdzie m jest liczbą naturalną, zaś $a_0, a_1, \ldots, a_m$ są liczbami niezależnymi od x, przy czym $a_0 \neq 0$.

Innym wnioskiem z twierdzenia 18 jest

Twierdzenie 19. *Jeżeli dwa wielomiany stopni m i n, gdzie $m \geqslant n$, przyjmują równe wartości dla więcej niż m różnych wartości x, to odpowiednie współczynniki tych wielomianów są sobie równe, t.zn. wielomiany te są identyczne.*

Dowód. Załóżmy, że wielomiany $f(x)$ i $g(x)$ są oba stopnia niewiększego niż m i że $f(x)=g(x)$ dla więcej niż m różnych wartości zmiennej x. Wartości te są pierwiastkami wielomianu $f(x)-g(x)$ stopnia niewiększego od m. Stosując do tego wielomianu twierdzenie 18, otrzymujemy żądany wynik.

Twierdzenia 15-19 wyprowadziliśmy elementarnie, nie korzystając z zasadniczego twierdzenia Algebry (Rozdział VII, § 2, str. 100). W myśl tego twierdzenia każdy wielomian zmiennej zespolonej z

$$f(z)=a_0z^m+a_1z^{m-1}+\ldots+a_{m-1}z+a_m \tag{38}$$

stopnia $m \geqslant 1$ o współczynnikach zespolonych posiada co najmniej jeden (zespolony) pierwiastek. Istnieje zatem liczba zespolona z_1, taka iż $f(z_1)=0$. Wielomian $f(z)$ jest więc podzielny przez $z-z_1$ i zachodzi wzór

$$f(z)=(z-z_1)f_1(z),$$

gdzie $f_1(z)$ jest wielomianem stopnia $m-1$, mającym przy z^{m-1} współczynnik a_0.

Jeżeli $m \geqslant 2$, to $f_1(z)$ jest wielomianem stopnia co najmniej 1, a więc, znowu w myśl zasadniczego twierdzenia Algebry, posiada co najmniej jeden pierwiastek (zespolony) z_2. Mamy więc $f_1(z_2)=0$ i możemy przyjąć

$$f_1(z)=(z-z_2)f_2(z),$$

gdzie $f_2(z)$ jest wielomianem stopnia $m-2$. Rozumując tak dalej, dojdziemy wreszcie do wzoru

$$f_{m-2}(z)=(z-z_{m-1})f_{m-1}(z),$$

gdzie $f_{m-1}(z)$ jest wielomianem stopnia 1, mającym przy z współczynnik a_0, czyli $f_{m-1}(z)=a_0z+b$ lub, przyjmując $z_m=-b/a_0$,

$$f(z)=(z-z_m)a_0.$$

Uwzględniając kolejne wzory na $f(z), f_1(z), \ldots, f_m(z)$, otrzymamy

$$f(z)=a_0(z-z_1)(z-z_2)\ldots(z-z_m). \tag{39}$$

Mamy zatem

Twierdzenie 20. *Każdy wielomian stopnia m-go jest iloczynem m czynników liniowych (zespolonych) i stałej, różnej od 0.*

Ze wzoru (39) wynika natychmiast, że liczby $z_1, z_2, \ldots, z_m$ są pierwiastkami wielomianu $f(z)$; wielomian ten nie posiada przy tym innych pierwiastków, gdyż jeżeli $f(z)=0$, to jeden co najmniej z czynników prawej strony wzoru (39) musi być równy 0, a że $a_0 \neq 0$, więc przy pewnym k z ciągu liczb $1, 2, \ldots, m$ musi być $z-z_k=0$ czyli $z=z_k$. Pierwiastki $z_1, z_2, \ldots, z_m$ niekoniecznie jednak są różne.

W § 9 (zob. str. 121) wprowadziliśmy pojęcie *krotności* pierwiastków wielomianu $f(z)$. Jeżeli różnymi pierwiastkami wielomianu $f(z)$ są tylko pierwiastki $z_1, z_2, \dots, z_p$, przy czym z_1 jest k_1-krotnym pierwiastkiem tego wielomianu, z_2 k_2-krotnym,..., wreszcie z_p k_p-krotnym pierwiastkiem, to w rozwinięciu (39) będzie k_1 czynników równych $(z-z_1)$, k_2 czynników równych $(z-z_2), \dots$, wreszcie k_p czynników równych $(z-z_p)$, zatem będzie

$$f(z) = a_0(z-z_1)^{k_1}(z-z_2)^{k_2} \dots (z-z_p)^{k_p} \tag{40}$$

przy czym

$$k_1 + k_2 + \dots + k_p = m.$$

Uwzględniając krotność pierwiastków możemy więc wypowiedzieć

Twierdzenie 21. *Każdy wielomian ma tyle pierwiastków, ile wynosi jego stopień, przy czym każdy pierwiastek liczony jest tyle razy, ile wynosi jego krotność.*

Ze wzoru (39), po rozwinięciu jego prawej strony według potęg z, otrzymujemy:

$$f(z) = a_0z^m - a_0(z_1+z_2+\dots+z_m)z^{m-1} + \\ + a_0(z_1z_2+z_1z_3+\dots+z_{m-1}z_m)z^{m-2} - \;.\;.\;.\; + (-1)^m a_0 z_1 z_2 \dots z_m$$

skąd, wobec (38) otrzymujemy tożsamość, która, przez przyrównanie współczynników przy różnych potęgach z po obu stronach daje:

$$\begin{aligned} z_1+z_2+\dots+z_m &= -\frac{a_1}{a_0}, \\ z_1z_2+z_1z_3+\dots+z_{m-1}z_m &= \frac{a_2}{a_0}, \\ \dots\dots\dots&\dots\dots \\ z_1z_2\dots z_m &= (-1)^m\frac{a_m}{a_0}. \end{aligned} \tag{41}$$

Są to z w i ą z k i m i ę d z y p i e r w i a s t k a m i w i e l o m i a n u a j e g o w s p ó ł c z y n n i k a m i.

Pozwalają one zbudować wielomian o dowolnie danym układzie pierwiastków, mających dowolnie dane krotności. Dowodzą one też, że współczynniki wielomianu, w którym współczynnik przy najwyższej potędze jest równy jedności, są wielomianami, a więc funkcjami ciągłymi pierwiastków. Można dowieść, że i na odwrót, pierwiastki wielomianu są funkcjami ciągłymi jego współczynników.

Zachodzi mianowicie

Twierdzenie [1]. *Jeśli wielomian stopnia $m \geqslant 1$ o współczynnikach zespolonych*

$$W(z) = a_0z^m + a_1z^{m-1} + \dots + a_{m-1}z + a_m,$$

gdzie $a_0 \neq 0$, rozwija się na czynniki liniowe (wśród których mogą być i równe)

$$f(z) = a_0(z-z_1)(z-z_2)\dots(z-z_m),$$

to dla każdej liczby rzeczywistej $\varepsilon > 0$ istnieje liczba rzeczywista $\delta > 0$, taka że każdy wielomian

$$V(z) = b_0z^m + b_1z^{m-1} + \dots + b_{m-1}z + b_m,$$

którego współczynniki są liczbami zespolonymi, spełniającymi nierówności

$$|b_k - a_k| < \delta \qquad dla \quad k = 0, 1, 2, \dots, m,$$

daje rozwinięcie na czynniki liniowe

$$V(z) = b_0(z-t_1)(z-t_2)\dots(z-t_m),$$

gdzie t_k są liczbami zespolonymi, spełniającymi nierówności

$$|t_k - z_k| < \varepsilon \qquad dla \quad k = 1, 2, \dots, m.$$

Jeżeli, w szczególności, $f(z)$ jest wielomianem o współczynnikach r z e c z y w i s t y c h, to oznaczając przez z' liczbę zespoloną, sprzężoną z liczbą z, mamy, jak wiadomo (Rozdział VI, § 4) $[f(z)]' = f(z')$ i wzór (40) daje wobec własności działań na liczbach sprzężonych oraz wzoru $a_0' = a_0$:

$$f(z') = a_0(z'-z_1')^{k_1}(z'-z_2')^{k_2} \;.\;.\;.\; (z'-z_p')^{k_p}$$

przy wszelkim zespolonym z. Zastępując z przez z', będziemy więc też mieli przy wszelkim zespolonym z:

$$f(z) = a_0(z-z_1')^{k_1}(z-z_2')^{k_2} \;.\;.\;.\; (z-z_p')^{k_p}.$$

Mamy zatem

Twierdzenie 21. *Jeżeli liczba zespolona u jest k-krotnym pierwiastkiem wielomianu o współczynnikach rzeczywistych, to sprzężona z nią liczba u' również jest k-krotnym pierwiastkiem tego wielomianu.*

Pierwiastki z e s p o l o n e (nierzeczywiste) wielomianu o współczynnikach rzeczywistych są więc parami sprzężone, skąd wynika, że liczba ich jest zawsze p a r z y s t a i to niezależnie od tego, czy przy liczeniu pierwiastków będziemy uwzględniali ich krotności, czy nie.

[1]) Dowód tego twierdzenia, jakkolwiek elementarny, jest dość długi. Znajdzie go czytelnik w mojej *Analizie*, Tom I, Część 1-sza, Wyd. 2-e, Warszawa 1923, § 67, tw. 76, str. 211-218.

Ponieważ przy uwzględnieniu krotności pierwiastków wielomian o współczynnikach rzeczywistych stopnia nieparzystego posiada nieparzystą liczbę pierwiastków a — jak widzieliśmy przed chwilą — liczba jego pierwiastków zespolonych jest parzysta, więc otrzymujemy

Wniosek 1. *Każdy wielomian stopnia nieparzystego o współczynnikach rzeczywistych posiada co najmniej jeden pierwiastek rzeczywisty.*

Niech teraz $f(z)$ oznacza jakikolwiek wielomian o współczynnikach rzeczywistych i niech z_j będzie jego pierwiastkiem nierzeczywistym. Liczba z'_j będzie więc również pierwiastkiem wielomianu $f(z)$, przy czym różnym od z_j, gdyż z równości $z'_j=z_j$ wynikałoby, że z_j jest liczbą rzeczywistą, wbrew założeniu. Rozwinięcie (39) będzie więc zawierało dwa różne czynniki $(z-z_j)$ i $(z-z'_j)$, których iloczyn

$$(z-z_j)(z-z'_j)=z^2-(z_j+z'_j)z+z_jz'_j$$

jest trójmianem 2-go stopnia względem z o współczynnikach rzeczywistych; istotnie, jeżeli $z_j=a+bi$, to $z'_j=a-bi$ oraz $z_j+z'_j=2a$ i $z_jz'_j=a^2+b^2$.

Każda para pierwiastków nierzeczywistych sprzężonych wielomianu $f(z)$ daje więc w jego rozwinięciu (39) dwa różne czynniki, których iloczyn jest trójmianem 2-go stopnia względem z o współczynnikach rzeczywistych. Z uwagi na to, że w myśl twierdzenia 21 wszystkie pierwiastki nierzeczywiste wielomianu $f(z)$ są parami sprzężone, otrzymujemy

Wniosek 2. *Każdy wielomian o współczynnikach rzeczywistych jest iloczynem skończonej liczby czynników, będących wielomianami co najwyżej 2-go stopnia o współczynnikach rzeczywistych.*

ĆWICZENIA. 1. Dowieść, że trójmian

$$5x^2-19x+18$$

można przedstawić tożsamościowo w postaci

$$a(x-2)(x-3)+b(x-3)(x-1)+c(x-1)(x-2)$$

i znaleźć liczby a, b i c. (G. Chrystal).

Dowód. Jeżeli przy danych a, b i c zachodzi podana tożsamość, to z tw. 19 wynikają dla liczb a, b i c trzy równania liniowe:

$$a+b+c=5,\quad 5a+4b+3c=19,\quad 6a+3b+2c=18.$$

Rozwiązując je, otrzymujemy $a=2$, $b=0$ i $c=3$.

2. W ćwiczeniu 1 zastąpić trójmian $5x^2-19x+18$ przez px^2+qx+r.
Odp.: $a=\frac{1}{2}(p+q+r)$, $b=-(4p+2q+r)$, $c=\frac{1}{2}(9p+3q+r)$.

3. Dowieść, że jeżeli α, β i γ są trzema dowolnie danymi, różnymi liczbami zespolonymi, to każdy trójmian

$$f(x)=px^2+qx+r$$

można tożsamościowo przedstawić w postaci

$$a(x-\alpha)(x-\beta)+b(x-\beta)(x-\gamma)+c(x-\gamma)(x-\alpha).$$

Dowód sprowadza się do okazania, że wyznacznik

$$\begin{vmatrix} 1 & 1 & 1 \\ \alpha+\beta & \beta+\gamma & \gamma+\alpha \\ \alpha\beta & \beta\gamma & \gamma\alpha \end{vmatrix}=(\alpha-\beta)(\alpha-\gamma)(\beta-\gamma)$$

jest w danym razie różny od 0. Jak łatwo sprawdzić, będzie tu tożsamościowo

$$f(x)=\frac{(x-\alpha)(x-\beta)}{(\gamma-\alpha)(\gamma-\beta)}f(\gamma)+\frac{(x-\beta)(x-\gamma)}{(\alpha-\beta)(\alpha-\gamma)}f(\alpha)+\frac{(x-\gamma)(x-\alpha)}{(\beta-\gamma)(\beta-\alpha)}f(\beta).$$

Por. § 12, wzór (42), str. 130.

4. Dowieść, że dla każdej liczby naturalnej s istnieje jeden i tylko jeden wielomian stopnia $s+1$

$$W_s(x)=a_0^{(s)}x^{s+1}+a_1^{(s)}x^s+\ldots+a_s^{(s)}x$$

taki, iż dla wszelkich całkowitych $n\geqslant 0$ mamy

$$0^s+1^s+2^s+\ldots+n^s=W_s(n).$$

Wsk.: Na to, żeby wielomian $W_s(x)$ miał podaną własność, potrzeba wystarcza, żeby dla całkowitych $x\geqslant 0$ było

$$W_s(x+1)-W_s(x)=(x+1)^s.$$

Równość ta ma więc zachodzić dla nieskończenie wielu całkowitych x, a zatem tożsamościowo (dla wszelkich x). Porównywując po obu stronach współczynniki przy x^k (dla $k=0,1,2,\ldots,s$), otrzymujemy wzory

$$\binom{s+1}{k}a_0^{(s)}+\binom{s}{k}a_1^{(s)}+\ldots+\binom{k+1}{k}a_{s-k}^{(s)}-\binom{s}{k}=0 \qquad \text{dla } k=s,s-1,\ldots,0.$$

Wzory te pozwalają obliczać kolejno $a_0^{(s)},a_1^{(s)},\ldots,a_s^{(s)}$. Znajdujemy w ten sposób np. $a_0^{(s)}=\frac{1}{s+1}$, $a_1^{(s)}=\frac{1}{2}$, $a_2^{(s)}=\frac{s}{12}$ i t.d. Wszystkie współczynniki wielomianu $W_s(x)$ są, oczywiście, wymierne.

5. Opierając się na ćwiczeniu 4, wyprowadzić wzory na sumy

$$0^s+1^s+\ldots+n^s=W_s(n) \qquad \text{dla } s=1,2,3$$

oraz sprawdzić, że będzie

$$W_3(n)=[W_1(n)]^2 \qquad \text{dla } n=0,1,2,\ldots$$

§ 12. Wzory interpolacyjne Lagrange'a i Newtona.

Z twierdzenia 19 wynika, że istnieje co najwyżej jeden wielomian stopnia niższego niż m, który dla danych m różnych wartości zmiennej przyjmuje dane wartości. Okażemy teraz, że wielomian taki zawsze istnieje.

Niech $a_1, a_2, \ldots, a_m$ oraz $A_1, A_2, \ldots, A_m$ będą dwoma danymi ciągami po m liczb. Mamy znaleźć wielomian $f(x)$ stopnia niższego niż m i taki, żeby było:

$$f(a_1) = A_1, \quad f(a_2) = A_2, \quad \ldots, \quad f(a_m) = A_m.$$

Jak łatwo sprawdzić przez podstawienie, szukanym wielomianem będzie wielomian:

$$(42)\qquad \begin{aligned} P(x) = {} & \frac{(x-a_2)(x-a_3)\ldots(x-a_m)}{(a_1-a_2)(a_1-a_3)\ldots(a_1-a_m)} A_1 + \\ & + \frac{(x-a_1)(x-a_3)\ldots(x-a_m)}{(a_2-a_1)(a_2-a_3)\ldots(a_2-a_m)} A_2 + \\ & \ldots\ldots\ldots\ldots\ldots \\ & + \frac{(x-a_1)(x-a_2)\ldots(x-a_{m-1})}{(a_m-a_1)(a_m-a_2)\ldots(a_m-a_{m-1})} A_m. \end{aligned}$$

Jest to tzw. *wzór interpolacyjny Lagrange'a*[1]).

Udowodniliśmy w ten sposób

Twierdzenie 22. *Istnieje jeden i tylko jeden wielomian stopnia niższego niż m (gdzie m jest daną liczbą naturalną), który dla danych m różnych wartości zmiennej przyjmuje dane wartości.*

Zauważmy, że wielomian $P(x)$, dany wzorem (42), jest zawsze stopnia nie wyższego niż $m-1$, może jednak być niekiedy stopnia niższego niż $m-1$. Np. dla $m=3$, $a_1=-1$, $a_2=0$, $a_3=1$, $A_1=0$, $A_2=1$ i $A_3=2$, znajdujemy

$$P(x) = \frac{(x+1)(x-1)}{1\cdot(-1)} + \frac{(x+1)x}{2\cdot 1}\cdot 2 = x+1,$$

a więc $P(x)$ jest stopnia 1.

Wielomian (42) możemy przedstawić w postaci:

$$(43)\qquad \begin{aligned} P(x) = c_0 + c_1(x-a_1) + c_2(x-a_1)(x-a_2) + \ldots \\ \ldots + c_{m-1}(x-a_1)\ldots(x-a_{m-1}), \end{aligned}$$

gdzie $c_0, c_1, \ldots, c_{m-1}$ są współczynnikami niezależnymi od x.

[1]) Uogólnienie wzoru interpolacyjnego Lagrange'a podał A. Łomnicki w Biuletynie Polskiej Akademii Umiejętności z r. 1920, str. 109.

Przypuśćmy istotnie, że zachodzi tożsamość (43). Znajdujemy stąd kolejno dla $x = a_1, a_2, \ldots, a_n$:

$$(44)\qquad \begin{aligned} c_0 = A_1, \quad c_0 + c_1(a_2-a_1) = A_2, \\ c_0 + c_1(a_3-a_1) + c_2(a_3-a_1)(a_3-a_2) = A_3, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ c_0 + c_1(a_m-a_1) + \ldots + c_{m-1}(a_m-a_1)\ldots(a_m-a_{m-1}) = A_m, \end{aligned}$$

co pozwala kolejno wyznaczyć $c_0, c_1, c_2, \ldots, c_{m-1}$.

Z drugiej strony, jeżeli liczby $c_0, c_1, c_2, \ldots, c_{m-1}$ wyznaczymy z równań (44) i przyjmiemy

$$\varphi(x) = c_0 + c_1(x-a_1) + c_2(x-a_1)(x-a_2) + \ldots + c_{m-1}(x-a_1)\ldots(x-a_{m-1}),$$

to będzie $\varphi(a_i) = A_i$ dla $i = 1, 2, \ldots, m$, zatem wobec twierdzenia 22 $\varphi(x) = P(x)$.

Wzór (43) nazywa się *wzorem interpolacyjnym Newtona*.

Można dowieść, że dla każdej funkcji ciągłej $f(x)$, określonej w przedziale zamkniętym $0 \leqslant x \leqslant 1$, oraz dla każdej liczby rzeczywistej $\varepsilon > 0$ istnieje liczba naturalna μ taka, iż

$$|f(x) - P_m(x)| < \varepsilon \qquad \text{dla } m > \mu \text{ i } 0 \leqslant x \leqslant 1,$$

gdzie

$$P_m(x) = \sum_{k=0}^{m} \binom{m}{k} f\left(\frac{k}{m}\right) x^k (1-x)^{m-k} \qquad \text{dla } m = 1, 2, \ldots$$

Wynika stąd, że

$$f(x) = \lim_{m=\infty} \sum_{k=0}^{m} \binom{m}{k} f\left(\frac{k}{m}\right) x^k (1-x)^{m-k}.$$

Wzór ten nosi nazwę *ogólnego wzoru interpolacyjnego S. Bernsteina*[1]).

J. Chłodowski dowiódł[2]), że *każda funkcja ciągła w przedziale otwartym* $0 < x < 1$ *jest w tym przedziale granicą ciągu wielomianów o współczynnikach całkowitych*. Przedział $0 < x < 1$ można w tym twierdzeniu zastąpić dowolnym przedziałem, nie zawierającym żadnej liczby całkowitej. Warunek ten jest zresztą konieczny, gdyż granica ciągu wielomianów o współczynnikach całkowitych jest dla całkowitej wartości zmiennej, liczbą całkowitą; granica taka nie może więc np. dawać wartości funkcji ciągłej, stale równej liczbie $\sqrt{2}$.

[1]) Dowód tego wzoru podałem w Wiadomościach Matematycznych, Tom 22 (1918), str. 177; por. też podany przeze mnie dowód elementarny t.zw. *ogólnego wzoru interpolacyjnego Borela*, Prace Matematyczno-Fizyczne, Tom 22 (1911), str. 67. Ob. także moją *Analizę*, Część II, Wyd. 2-e, Warszawa 1925, str. 221.

[2]) J. Chłodowski, Matematiczeskij Sbornik, Tom 32 (Moskwa 1925), str. 472-474.

§ 13. Własności wielomianów o współczynnikach całkowitych. Wielomian $f(x)$ o współczynnikach (rzeczywistych) całkowitych nazywamy *pierwotnym*, jeżeli współczynniki jego nie mają wspólnego dzielnika większego od 1.

Twierdzenie 23. *Iloczyn dwóch wielomianów pierwotnych jest wielomianem pierwotnym.*

Dowód. Niech $f=gh$ będzie iloczynem dwóch wielomianów pierwotnych:

$$g=g(x)=b_0x^k+b_1x^{k-1}+\ldots+b_k,\qquad h=h(x)=c_0x^l+c_1x^{l-1}+\ldots+c_l.$$

Gdyby wielomian f nie był pierwotny, istniałaby liczba pierwsza p, będąca dzielnikiem każdego z jego współczynników. Ponieważ wielomian g jest pierwotny, więc p nie może być dzielnikiem każdej z liczb $b_0, b_1, \ldots, b_k$. Niech b_i oznacza najwcześniejszą z liczb tego ciągu, niepodzielną przez p. Podobnie istnieje najwcześniejsza liczba ciągu $c_0, c_1, \ldots, c_l$ — niech to będzie liczba c_j — niepodzielna przez p.

Obliczmy teraz współczynnik przy $x^{k+l-(i+j)}$ w wielomianie f. Będzie to oczywiście suma

$$b_ic_j+b_{i-1}c_{j+1}+b_ic_{j+2}+\ldots+b_{i+1}c_{j-1}+b_{i+2}c_{j-2}+\ldots \tag{45}$$

Z definicji liczb b_i oraz c_j wynika, że liczby $b_{i-1}, b_{i-2}, \ldots$ i liczby $c_{j-1}, c_{j-2}, \ldots$ są wszystkie podzielne przez p; zaś liczby b_i i c_j, a więc i liczba b_ic_j, nie są podzielne przez p. Ponieważ wszystkie składniki sumy (45), prócz pierwszego, są podzielne przez liczbę pierwszą p, więc suma ta nie jest podzielna przez p, wbrew założeniu, że p jest dzielnikiem każdego ze współczynników wielomianu f. Wielomian f musi więc być pierwotny, c. b. d. o.

Twierdzenie 24. *Wielomian o współczynnikach całkowitych, będący iloczynem dwóch wielomianów o współczynnikach wymiernych, jest zarazem iloczynem dwóch wielomianów o współczynnikach całkowitych odpowiednio tych samych stopni.*

Dowód. Niech $f=gh$ będzie wielomianem o współczynnikach całkowitych, zaś g i h wielomianami o współczynnikach wymiernych. Wielomian g możemy, po sprowadzeniu jego współczynników do wspólnego mianownika i po podzieleniu liczników przez ich największy wspólny dzielnik, przedstawić w postaci $g=\frac{m_1g_1}{n_1}$, gdzie m_1 i n_1 są liczbami naturalnymi, a g_1 jest wielomianem pierwotnym. Podobnie przedstawimy wielomian h w postaci $h=\frac{m_2h_1}{n_2}$.

Będzie więc $f=\frac{m_1m_2}{n_1n_2}g_1h_1$.

Pozostaje do dowiedzenia, że liczba $\frac{m_1m_2}{n_2n_1}$ jest całkowita.

Przypuśćmy, że tak nie jest. Zachodziłaby więc równość $\frac{m_1m_2}{n_1n_2}=\frac{m}{n}$, gdzie m i n są liczbami względnie pierwszymi, przy czym $n>1$. Stąd $nf=mg_1h_1$, co dowodzi, że współczynniki wielomianu nf są wszystkie podzielne przez m. Ponieważ liczby m i n są względnie pierwsze, więc wnosimy stąd, że współczynniki wielomianu f są wszystkie podzielne przez m, t. j. $f=mf_1$, gdzie f_1 jest wielomianem o współczynnikach całkowitych. Mamy więc $nf_1=g_1h_1$, wbrew twierdzeniu 23, że iloczyn dwóch wielomianów pierwotnych jest wielomianem pierwotnym. Zatem $\frac{m_1m_2}{n_1n_2}$ jest liczbą całkowitą, c. b. d. o.

§ 14. Wielomiany nieprzywiedlne. Wielomian o współczynnikach wymiernych, który nie jest iloczynem dwóch wielomianów stopnia dodatniego o współczynnikach wymiernych, nazywamy *nieprzywiedlnym*.

Twierdzenie 25. *Na to, żeby wielomian stopnia nie wyższego niż 3 o współczynnikach wymiernych był nieprzywiedlny, potrzeba i wystarcza, żeby nie posiadał pierwiastków wymiernych.*

Dowód. Każdy wielomian o współczynnikach wymiernych, posiadający pierwiastek wymierny a, jest, jak wiemy z twierdzenia 3, str. 107, podzielny przez $x-a$, zatem przywiedlny, gdyż iloraz z tego dzielenia jest, jak wiemy z twierdzenia 2, str. 104, wielomianem o współczynnikach wymiernych. Z drugiej strony, jeżeli wielomian stopnia nie wyższego niż 3 jest iloczynem dwóch wielomianów stopnia dodatniego, to jeden co najmniej z nich musi być stopnia pierwszego, skąd wnosimy, że wtedy wielomian nasz posiada pierwiastek wymierny, c. b. d. o.

Udowodnione twierdzenie nie jest prawdziwe dla wielomianów stopnia większego niż 3; np. wielomian $x^4-4=(x^2-2)(x^2+2)$ jest przywiedlny, a nie posiada pierwiastków wymiernych.

Twierdzenie 26. *Wielomian $x^n+a_1x^{n-1}+\ldots+a_n$ o współczynnikach całkowitych jest nieprzywiedlny, jeśli współczynniki $a_1, a_2, \ldots, a_n$ są podzielne przez liczbę pierwszą p, zaś a_n jest niepodzielne przez p^2.*

Dowód. Wobec twierdzenia 24 wystarczy dowieść, że dany wielomian nie jest iloczynem dwóch wielomianów (stopnia dodatniego) o współczynnikach całkowitych.

Przypuśćmy, że wielomian ten jest takim iloczynem, t. j. że

$$x^n + a_1x^{n-1} + \ldots + a_n = (x^k + b_1x^{k-1} + \ldots + b_k)(x^l + c_1x^{l-1} + \ldots + c_l).$$

Mielibyśmy stąd $a_n = b_kc_l$. Skoro a_n jest podzielne przez p, lecz niepodzielne przez p^2, więc jedna z liczb b_k i c_l jest podzielna przez p, a druga nie, np. $p|b_k$.

Wykażemy przede wszystkim, że wszystkie liczby $b_1, b_2, \ldots, b_k$ są podzielne przez p. Przypuśćmy bowiem, że jest przeciwnie, i niech i oznacza największy wskaźnik taki, że b_i nie jest podzielne przez p. Jest więc $i<k$ (gdyż $p|b_k$), zatem $i+l<k+l=n$. Mamy oczywiście

$$a_{i+l} = b_ic_l + b_{i+1}c_{l-1} + b_{i+2}c_{l-2} + \ldots$$

Lewa strona jest podzielna przez p, zaś po prawej stronie pierwszy składnik nie jest podzielny przez p, gdyż ani b_i ani c_l nie są podzielne przez p, zaś pozostałe składniki są podzielne przez p, ponieważ na mocy określenia liczby b_i, liczby $b_{i+1}, b_{i+2}, \ldots$ są podzielne przez p. Wynik ten jest niemożliwy, co dowodzi, że każda z liczb $b_1, b_2, \ldots, b_k$ jest podzielna przez p.

Lecz

$$a_{n-k} = c_l + b_1c_{l-1} + b_2c_{l-2} + \ldots,$$

przy czym a_{n-k} jest podzielne przez p, a także, jak udowodniliśmy, każda z liczb $b_1, b_2, \ldots$ jest podzielna przez p. Liczba c_l byłaby więc podzielna przez p, wbrew założeniu. Przypuszczenie, że wielomian $x^n + a_1x^{n-1} + \ldots + a_n$ jest przywiedlny, doprowadza więc do sprzeczności.

Wyprowadzony w tym twierdzeniu *sprawdzian nieprzywiedlności wielomianów* nosi w literaturze nazwę *kryterium Eisensteina*.

Bezpośrednio z twierdzenia 26 wynika

Wniosek 1. *Wielomian $x^n - p$, gdzie p jest liczbą pierwszą, jest nieprzywiedlny (dla $n = 2, 3, \ldots$).*

Wniosek 2. *Wielomian $x^{p-1} + x^{p-2} + \ldots + x + 1$, gdzie p jest liczbą pierwszą, jest nieprzywiedlny.*

Gdyby bowiem wielomian ten — oznaczmy go przez $f(x)$ — był przywiedlny, to byłby też przywiedlny wielomian $\varphi(x) = f(x+1)$. Lecz $f(x) = \dfrac{x^p - 1}{x-1}$, skąd:

$$\varphi(x) = f(x+1) = \frac{(x+1)^p - 1}{x} =$$
$$= x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \ldots + \binom{p}{p-1}.$$

Współczynniki $\binom{p}{1}, \binom{p}{2}, \ldots, \binom{p}{p-1}$ są wszystkie podzielne przez liczbę pierwszą p, zaś $\binom{p}{p-1} = p$ jest niepodzielne przez p^2. W myśl twierdzenia 26 wielomian $\varphi(x)$ jest więc nieprzywiedlny, c. b. d. o.

Wniosek 3. *Wielomian x^4+1 jest nieprzywiedlny.*

W przeciwnym bowiem razie byłby też przywiedlny wielomian $(x+1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2$, wbrew twierdzeniu 26.

Twierdzenie 27. *Jeżeli wielomian $f(x)$ jest nieprzywiedlny i ma pierwiastek wspólny z wielomianem $g(x)$ o współczynnikach wymiernych, to $g(x)$ jest podzielne przez $f(x)$.*

Dowód. Jeżeli wielomiany f i g mają wspólny pierwiastek a, to są oba podzielne przez $x-a$, a więc największy wspólny ich dzielnik $d(x)$ jest wielomianem stopnia dodatniego. Lecz z twierdzenia 6 wynika, że $d(x)$ jest wielomianem o współczynnikach wymiernych, zaś z twierdzenia 2 wynika, że iloraz $h = f/d$ też jest wielomianem o współczynnikach wymiernych. Mamy więc rozkład $f = dh$, a że wielomian f jest nieprzywiedlny, więc h musi być wielomianem stopnia 0 czyli stałą. Wobec $d|g$ mamy więc $\frac{f}{h}|g$, a zatem również (skoro h jest stałą) $f|g$, c. b. d. o.

Z twierdzenia 27 wynika natychmiast następujący

Wniosek. *Wszystkie pierwiastki wielomianu nieprzywiedlnego są różne.*

Istotnie, gdyby wielomian nieprzywiedlny $f(x)$ posiadał pierwiastek wielokrotny a, to w myśl twierdzenia 12 byłoby $f'(a) = 0$, a więc wielomiany $f(x)$ i $f'(x)$ miałyby wspólny pierwiastek; zatem, w myśl twierdzenia 27, $f'(x)$ byłoby podzielne przez $f(x)$, co nie jest możliwe, gdyż $f'(x)$ jest wielomianem stopnia dodatniego, lecz mniejszego od stopnia wielomianu $f(x)$.

Przytoczymy wreszcie następujące twierdzenie, którego łatwy dowód pozostawiamy czytelnikowi:

Twierdzenie 28. *Każdy wielomian rozkłada się na iloczyn skończonej liczby wielomianów nieprzywiedlnych.*

ĆWICZENIE. 1. Zbadać, czy dwumian x^4+4 jest nieprzywiedlny.

Rozwiązanie. Dwumian ten nie posiada pierwiastków wymiernych (porównaj § 15, ćwiczenie 1), a zatem nie może posiadać dzielnika pierwszego stopnia. Jeżeli więc jest on przywiedlny, to w myśl twierdzenia 24 musi on być iloczynem dwóch wielomianów 2-go stopnia o współczynnikach całkowitych; zatem:

$$x^4+4=(x^2+px+q)\,(x^2+rx+s).$$

Przez przyrównanie współczynników otrzymujemy:

$$p+r=0,\quad q+s+pr=0,\quad ps+qr=0,\quad qs=4.$$

Z pierwszego z tych równań otrzymujemy $r=-p$, wobec czego trzecie daje $p(s-q)=0$. Gdyby było $p=0$, to drugie równanie dałoby $s=-q$ i z czwartego wynikłoby $s^2=-4$, wbrew założeniu, że s jest liczbą całkowitą. Jest więc $p\neq 0$, zatem $s-q=0$ i czwarte równanie daje $q^2=4$, skąd $q=\pm 2$. Lecz drugie równanie (wobec $r=-p$ i $s=q$) daje $2q=p^2$, skąd $q>0$; zatem $q=2$, $p=\pm 2$, $s=2$ i $r=\mp 2$. Wartości te spełniają wszystkie cztery równania. Stąd rozkład:

$$x^4+4=(x^2+2x+2)\,(x^2-2x+2).$$

§ 15. Wyznaczanie dzielników wielomianów o współczynnikach całkowitych. Niech $f(x)=a_0x^m+a_1x^{m-1}+\ldots+a_m$ oznacza, jak poprzednio, wielomian o współczynnikach całkowitych. Istnieje metoda, pochodząca od Kroneckera, pozwalająca wyznaczyć za pomocą skończonej liczby działań elementarnych wszystkie wielomiany o współczynnikach całkowitych, które są dzielnikami wielomianu $f(x)$. Metodą tą można więc rozstrzygnąć, czy wielomian $f(x)$ jest nieprzywiedlny, oraz znaleźć rozkład wielomianu $f(x)$ na czynniki nieprzywiedlne.

Niech n oznacza daną liczbę naturalną, mniejszą od m. Wyznaczymy wszystkie dzielniki stopnia n wielomianu $f(x)$. Niech $a_1,a_2,\ldots,a_n,a_{n+1}$ będą $n+1$ różnymi liczbami całkowitymi. Jeżeli $\varphi(x)$ jest wielomianem o współczynnikach całkowitych, a przy tym dzielnikiem wielomianu $f(x)$, to $\varphi(a_i)\,|\,f(a_i)$ dla $i=1,2,\ldots,n+1$. Wszystkich ciągów

$$d_1,\ d_2,\ \ldots,\ d_{n+1},$$

gdzie d_i jest dzielnikiem liczby $f(a_i)$ dla $i=1,2,\ldots,n+1$, jest oczywiście liczba skończona. Dla każdego takiego ciągu wyznaczmy, np. za pomocą wzoru interpolacyjnego Lagrange'a, wielomian $W(x)$

stopnia nie większego od n, taki iż $W(a_i)=d_i$ dla $i=1,2,\ldots,n+1$. Jasnym jest, że $\varphi(x)$ musi być jednym z tych wielomianów. Aby więc znaleźć wszystkie wielomiany stopnia n o współczynnikach całkowitych, będące dzielnikami wielomianu $f(x)$, należy wziąć te spośród wyznaczonych wyżej wielomianów $W(x)$, które są stopnia n (a nie niższego), mają wszystkie współczynniki całkowite i dla których iloraz $f(x)/W(x)$ jest wielomianem o współczynnikach całkowitych.

Załóżmy teraz, że idzie w szczególności o wielomiany stopnia 1-go o współczynnikach całkowitych, będące dzielnikami danego wielomianu $f(x)$ o współczynnikach całkowitych. Jeżeli $\varphi(x)=qx-p$ jest takim dzielnikiem (gdzie $q\neq 0$), to $x=p/q$ jest pierwiastkiem wielomianu $f(x)$, zatem $a_0p^m+a_1p^{m-1}q+\ldots+a_mq^m=0$. Jeżeli liczby p i q są względnie pierwsze (a to musi zachodzić, o ile współczynniki wielomianu $f(x)$ nie mają wspólnego dzielnika większego od 1, co możemy zawsze założyć), to wnosimy, że $p\,|\,a_m$ i $q\,|\,a_0$. Szukane dzielniki wyznaczymy więc za pomocą skończonej liczby prób.

Wynika stąd metoda wyznaczania za pomocą skończonej liczby prób wszystkich pierwiastków wymiernych wielomianu o współczynnikach całkowitych.

ĆWICZENIA. 1. Dowieść, że każdy pierwiastek wymierny wielomianu $x^m+a_1x^{m-1}+\ldots+a_m$, gdzie liczby $a_1,a_2,\ldots,a_m$ są całkowite, musi być całkowity.

Dowód wynika z uwagi, że jeśli liczba p/q, gdzie p i q są względnie pierwsze, jest pierwiastkiem danego wielomianu, to musi być $q\,|\,1$.

2. Dowieść, że liczba całkowita a, która nie jest m-tą potęgą (m naturalne) liczby całkowitej, nie jest też m-tą potęgą żadnej liczby wymiernej.

Wskazówka: Zastosować ćw. 1 do wielomianu x^m-a.

§ 16. Wielomiany n zmiennych. *Wielomianem n zmiennych* $x_1,x_2,\ldots,x_n$ nazywamy sumą skończonej liczby jednomianów postaci

$$ax_1^{\alpha_1}x_2^{\alpha_2}\ldots x_n^{\alpha_n},$$

gdzie a jest liczbą rzeczywistą lub zespoloną, niezależną od $x_1,x_2,\ldots,x_n$, zaś $\alpha_1,\alpha_2,\ldots,\alpha_n$ są liczbami całkowitymi nieujemnymi.

Po ewentualnej redukcji wyrazów podobnych, układy wykładników $\alpha_1,\alpha_2,\ldots,\alpha_n$, odpowiadające różnym składnikom wielomianu, są różne.

Wielomian n zmiennych $x_1,x_2,\ldots,x_n$ możemy uporządkować według potęg jednej ze zmiennych, np. x_1; wówczas współczynniki będą wielomianami pozostałych $n-1$ zmiennych $x_2,x_3,\ldots,x_n$.

W teorii ułamków łańcuchowych grają ważną rolę wielomiany n zmiennych $f_n(x_1,x_2,\ldots,x_n)$, określone przez indukcję w sposób następujący:

$$f_1(x_1)=x_1,\qquad f_2(x_1,x_2)=x_1x_2+1,$$
$$f_n(x_1,x_2,\ldots,x_n)=x_nf_{n-1}(x_1,x_2,\ldots,x_{n-1})+f_{n-2}(x_1,x_2,\ldots,x_{n-2})\qquad \text{dla}\quad n=3,4,\ldots$$

Wielomiany te są liniowe ze względu na każdą ze zmiennych. Można udowodnić (co czytelnik zechce sprawdzić dla $n=4$), że zawsze:

$$f_n(x_1,x_2,\ldots,x_n)=f_n(x_n,x_{n-1},\ldots,x_1),$$
$$f_n(x_1,x_2,\ldots,x_n)=x_1f_{n-1}(x_2,x_3,\ldots,x_n)+f_{n-2}(x_3,x_4,\ldots,x_n)\qquad \text{dla}\quad n=3,4,\ldots$$

Wartością ułamka łańcuchowego $a_0+\frac{1|}{|a_1}+\frac{1|}{|a_2}+\ldots+\frac{1|}{|a_n}$ jest iloraz $f_{n+1}(a_0,a_1,\ldots,a_n)/f_n(a_1,a_2,\ldots,a_n)$.

Mamy też dla $n=1,2,\ldots$:

$$f_n(x_1,x_2,\ldots,x_n)=\begin{vmatrix} x_1 & -1 & 0 & 0 & . & 0\\ 1 & x_2 & -1 & 0 & . & 0\\ 0 & 1 & x_3 & -1 & . & 0\\ . & . & . & . & . & .\\ 0 & 0 & . & . & x_{n-1} & -1\\ 0 & 0 & . & . & 1 & x_n \end{vmatrix}.$$

Mówimy, że wielomian n zmiennych $f(x_1,x_2,\ldots,x_n)$ jest *podzielny* przez wielomian n zmiennych $g(x_1,x_2,\ldots,x_n)$, jeżeli istnieje wielomian n zmiennych $h(x_1,x_2,\ldots,x_n)$, taki iż dla wszystkich wartości $x_1,x_2,\ldots,x_n$ zachodzi równość

$$f(x_1,x_2,\ldots,x_n)=g(x_1,x_2,\ldots,x_n)\,h(x_1,x_2,\ldots,x_n).$$

Mówimy wówczas, że równość ta *zachodzi tożsamościowo ze względu na zmienne* $x_1,x_2,\ldots,x_n$.

Zajmiemy się zagadnieniem, w jaki sposób można poznać, czy dany wielomian $f(x_1,x_2,\ldots,x_n)$ jest podzielny przez wielomian $g(x_1,x_2,\ldots,x_n)$ i, ewentualnie, jak można znaleźć iloraz $h(x_1,x_2,\ldots,x_n)$ z tego dzielenia.

Gdybyśmy uporządkowali wielomian $f(x_1,x_2,\ldots,x_n)$ według potęg zmiennej x_1 i chcieli stosować postępowanie takie, jak przy wielomianach jednej zmiennej (ob. dowód twierdzenia 1 z § 1), doprowadziłoby to nas na ogół do wyrażeń ułamkowych, w których w mianownikach byłyby wielomiany zmiennych $x_2,x_3,\ldots,x_n$. Następujące twierdzenie umożliwia nam uniknięcie tej niedogodności:

Twierdzenie 29. *Jeżeli $f(x_1,x_2,\ldots,x_n)$ i $g(x_1,x_2,\ldots,x_n)$ są wielomianami n zmiennych $x_1,x_2,\ldots,x_n$, z których drugi jest względem x_1 stopnia dodatniego, to istnieją wielomiany n zmiennych $h(x_1,x_2,\ldots,x_n)$ i $r(x_1,x_2,\ldots,x_n)$ oraz wielomian $b(x_2,x_3,\ldots,x_n)$ $n-1$ zmiennych $x_2,x_3,\ldots,x_n$, nie będący tożsamościowo zerem, takie iż:*

$$b(x_2,x_3,\ldots,x_n)f(x_1,x_2,\ldots,x_n)=g(x_1,x_2,\ldots,x_n)\,h(x_1,x_2,\ldots,x_n)+r(x_1,x_2,\ldots,x_n),$$

przy czym stopień wielomianu $r(x_1,x_2,\ldots,x_n)$ względem zmiennej x_1 jest niższy niż stopień wielomianu $g(x_1,x_2,\ldots,x_n)$ względem tej zmiennej.

Wielomiany $h(x_1,x_2,\ldots,x_n)$, $r(x_1,x_2,\ldots,x_n)$ i $b(x_2,\ldots,x_n)$ dają się obliczyć przy pomocy skończonej liczby działań algebraicznych, jeśli współczynniki wielomianów $f(x_1,x_2,\ldots,x_n)$ i $g(x_1,x_2,\ldots,x_n)$ są znane.

Dowód. Jeżeli stopień wielomianu $g(x_1,x_2,\ldots,x_n)$ względem x_1 jest wyższy niż stopień wielomianu $f(x_1,x_2,\ldots,x_n)$ względem tej zmiennej, to wystarczy oczywiście przyjąć $h=0$ i $r=f$. Załóżmy więc, że stopień q wielomianu g względem x_1 nie jest wyższy niż stopień p wielomianu f względem x_1. Porządkując te wielomiany według potęg zmiennej x_1, otrzymamy:

$$f(x_1,x_2,\ldots,x_n)=a_0(x_2,x_3,\ldots,x_n)x_1^p+a_1(x_2,x_3,\ldots,x_n)x_1^{p-1}+\ldots$$
$$\ldots+a_p(x_2,x_3,\ldots,x_n),$$
$$g(x_1,x_2,\ldots,x_n)=b_0(x_2,x_3,\ldots,x_n)x_1^q+b_1(x_2,x_3,\ldots,x_n)x_1^{q-1}+\ldots$$
$$\ldots+b_q(x_2,x_3,\ldots,x_n),$$

przy czym wielomiany a_0 oraz b_0 nie są tożsamościowo równe 0.

Przyjmiemy:

$$h_1(x_1,x_2,\ldots,x_n)=a_0(x_2,x_3,\ldots,x_n)x_1^{p-q},$$
$$r_1(x_1,x_2,\ldots,x_n)=b_0(x_2,x_3,\ldots,x_n)f(x_1,x_2,\ldots,x_n)-g(x_1,x_2,\ldots,x_n)h_1(x_1,x_2,\ldots,x_n).$$

Będziemy mieli:

$$b_0(x_2,x_3,\ldots,x_n)f(x_1,x_2,\ldots,x_n)=g(x_1,x_2,\ldots,x_n)h_1(x_1,x_2,\ldots,x_n)+r_1(x_1,x_2,\ldots,x_n),$$

przy czym wielomian

$$r_1(x_1,x_2,\ldots,x_n)=$$
$$=b_0a_1x_1^{p-1}+b_0a_2x_1^{p-2}+\ldots+b_0a_p-(a_0b_1x_1^{p-1}+a_0b_2x_1^{p-2}+\ldots+a_0b_qx_1^{p-p})$$

jest względem x_1 stopnia nie większego niż $p-1$, a więc stopnia mniejszego niż stopień wielomianu f względem tej zmiennej. Jeżeli stopień wielomianu g względem x_1 nie jest wyższy niż stopień wielomianu r_1 względem tej zmiennej, to w podobny sposób znajdziemy wielomiany $h_2(x_1,x_2,\ldots,x_n)$ i $r_2(x_1,x_2,\ldots,x_n)$ takie, że

$$b_0(x_2,x_3,\ldots,x_n)r_1(x_1,x_2,\ldots,x_n)=g(x_1,x_2,\ldots,x_n)h_2(x_1,x_2,\ldots,x_n)+r_2(x_1,x_2,\ldots,x_n),$$

przy czym $r_2(x_1,x_2,\ldots,x_n)$ będzie wielomianem, którego stopień względem x_1 jest niższy niż stopień wielomianu r_1 względem x_1.

Rozumowanie to możemy powtórzyć tylko skończoną liczbę razy, gdyż stopnie wielomianów $r_1,r_2,\ldots$ względem x_1 maleją. Dojdziemy więc do ostatniego tego rodzaju wzoru:

$$b_0(x_2,x_3,\ldots,x_n)r_{k-1}(x_1,x_2,\ldots,x_n) = \\ = g(x_1,x_2,\ldots,x_n)h_k(x_1,x_2,\ldots,x_n)+r(x_1,x_2,\ldots,x_n),$$

gdzie już stopień wielomianu r_k względem x_1 będzie niższy, niż stopień wielomianu g względem x_1. Przyjmując

$$h(x_1,x_1,\ldots,x_n)=b_0^{k-1}h_1+b_0^{k-2}h_2+\ldots+b_0h_{k-1}+h_k \quad \text{i} \quad r=r_k,$$

będziemy mieli

$$b_0^k(x_2,x_3,\ldots,x_n)f(x_1,x_2,\ldots,x_n)=g(x_1,x_2,\ldots,x_n)h(x_1,x_2,\ldots,x_n)+r(x_1,x_2,\ldots,x_n),$$

gdzie $r(x_1,x_2,\ldots,x_n)$ jest wielomianem, którego stopień względem x_1 jest niższy niż stopień wielomianu g względem x_1, c. b. d. o.

Twierdzenie 29 przedstawia pewną analogię z twierdzeniem 1 z § 1; różni się ono jednak od niego tym, że wielomiany $b(x_2,x_3,\ldots,x_n)$, $h(x_1,x_2,\ldots,x_n)$ oraz $r(x_1,x_2,\ldots,x_n)$ nie są jednoznacznie wyznaczone przez wielomiany $f(x_1,x_2,\ldots,x_n)$ i $g(x_1,x_2,\ldots,x_n)$, moglibyśmy bowiem np. pomnożyć wszystkie trzy przez dowolny wielomian zmiennych $x_2,x_3,\ldots,x_n$.

Twierdzenie 29 pozwala stosować algorytm kolejnych dzieleń (por. § 4, str. 109) do dowolnych wielomianów n zmiennych $f_1(x_1,x_2,\ldots,x_n)$ i $f_2(x_1,x_2,\ldots,x_n)$, z których drugi jest względem x_1 stopnia dodatniego. Algorytm ten prowadzi do ciągu równości

(46) $$b_1f_1=f_2h_1+f_3,\quad b_2f_2=f_3h_2+f_4,\quad \ldots,$$

gdzie $f_1,f_2,\ldots$ i $h_1,h_2,\ldots$ są wielomianami n zmiennych $x_1,x_2,\ldots,x_n$, a $b_1,b_2,\ldots$ wielomianami $n-1$ zmiennych $x_2,x_3,\ldots,x_n$, nie równymi tożsamościowo zeru, przy czym stopnie wielomianów $f_1,f_2,\ldots$ względem x_1 stale maleją. Wynika stąd, że dojdziemy po skończonej liczbie kroków do równości

(47) $$b_{k-2}f_{k-2}=f_{k-1}h_{k-2}+f_k,$$

gdzie f_k będzie wielomianem stopnia 0 względem x_1, a więc wielomianem tylko $n-1$ zmiennych $x_2,x_3,\ldots,x_n$.

W następnych §§ pokażemy, w jaki sposób algorytm ten daje się zastosować przy znajdywaniu największego wspólnego dzielnika dwóch wielomianów wielu zmiennych. Przy tym zajmiemy się tylko wielomianami dwóch zmiennych, ponieważ dla większej liczby zmiennych sposób postępowania jest analogiczny[1]).

§ 17. Badanie podzielności wielomianów dwóch zmiennych. Uporządkujmy wielomian $f(x,y)$ dwóch zmiennych x i y według potęg zmiennej x:

$$f(x,y)=a_0(y)x^p+a_1(y)x^{p-1}+\ldots+a_p(y),$$

przy czym $a_0(y),a_1(y),\ldots,a_p(y)$ są wielomianami zmiennej y, które mogą się redukować do stałych. Udowodnimy najpierw

Twierdzenie 30. *Wielomian $f(x,y)$ jest wtedy i tylko wtedy podzielny przez wielomian $h(y)$ jednej zmiennej y, gdy każdy ze współczynników $a_i(y)$ dla $i=0,1,\ldots,p$ wielomianu $f(x,y)$ jest podzielny przez wielomian $h(y)$.*

Dowód. Dostateczność tego warunku jest oczywista; pozostaje do okazania jego konieczność.

Przypuśćmy, że $h(y)|f(x,y)$. Mamy więc $f(x,y)=h(y)g(x,y)$, gdzie $g(x,y)$ jest wielomianem dwóch zmiennych x i y; stopień wielomianu $g(x,y)$ względem x jest równy p:

$$g(x,y)=b_0(y)x^p+b_1(y)x^{p-1}+\ldots+b_p(y).$$

Mamy zatem tożsamościowo względem x i y:

(48) $$a_0(y)x^p+a_1(y)x^{p-1}+\ldots+a_p(y)= \\ =h(y)b_0(y)x^p+h(y)b_1(y)x^{p-1}+\ldots+h(y)b_p(y).$$

Ponieważ dla każdego y równość (48) jest tożsamością ze względu na x, co — jak wiemy (ob. twierdzenie 19) — pociąga za sobą równość współczynników po obu stronach, więc mamy

(49) $$a_0(y)=h(y)b_0(y),\quad a_1(y)=h(y)b_1(y),\quad \ldots,\quad a_p(y)=h(y)b_p(y).$$

Równości (49) zostały wyprowadzone dla każdego y, są więc one tożsamościami ze względu na y. Z (49) wynika, że każdy ze współczynników wielomianu $f(x,y)$ jest podzielny przez $h(y)$, c. b. d. o.

[1]) Ob. M. Bôcher, *Einführung in die höhere Algebra*, Wyd. 2-e (Tłum. na niemiecki), Lipsk-Berlin 1925, str. 230 (§ 76).

Dzięki twierdzeniu 30 badanie, czy wielomian $f(x,y)$ posiada dzielniki zależne jedynie od y, sprowadza się do wyznaczania wspólnych dzielników wielomianów jednej zmiennej. Mamy mianowicie

Twierdzenie 31. *Dzielnik wielomianu $f(x,y)$, zależny tylko od y i możliwie najwyższego stopnia względem y, jest największym wspólnym dzielnikiem współczynników wielomianu $f(x,y)$ w jego rozwinięciu według potęg x i na odwrót.*

Potrzebne nam będzie jeszcze następujące

Twierdzenie 32. *Jeżeli iloczyn dwóch wielomianów $g(x,y)$ i $h(x,y)$ jest podzielny przez wielomian $\varphi(y)$ jednej zmiennej y i jeżeli wielomian $g(x,y)$ nie posiada dzielnika stopnia dodatniego, zależnego jedynie od y, to wielomian $h(x,y)$ jest podzielny przez $\varphi(y)$.*

Dowód. Załóżmy, że

$$g(x,y)\,h(x,y)=\varphi(y)\psi(x,y), \tag{50}$$

i niech $\varphi_1(y)$ oznacza jeden z czynników liniowych wielomianu $\varphi(y)$. Iloczyn $g(x,y)\,h(x,y)$ jest więc podzielny przez $\varphi_1(y)$. Niech:

$$g(x,y)=b_0(y)x^q+b_1(y)x^{q-1}+\ldots+b_q(y),$$
$$h(x,y)=c_0(y)x^r+c_1(y)x^{r-1}+\ldots+c_r(y).$$

Wykażemy, że $\varphi_1(y)|h(x,y)$. Istotnie, gdyby tak nie było, to, jak wiemy z twierdzenia 30, nie wszystkie współczynniki wielomianu $h(x,y)$ byłyby podzielne przez $\varphi_1(y)$; niech $c_n(y)$ oznacza pierwszy z nich. Ponieważ wielomian $g(x,y)$ nie posiada dzielnika zależnego jedynie od y, więc istnieje pierwszy jego współczynnik $b_m(y)$ niepodzielny przez $\varphi_1(y)$. Wielomian $g(x,y)\cdot h(x,y)$ jest na mocy założenia podzielny przez $\varphi_1(y)$. Na mocy twierdzenia 31 wynika stąd, że każdy współczynnik jego rozwinięcia według potęg x musi być podzielny przez $\varphi_1(y)$. W szczególności słuszne to jest dla współczynnika przy $x^{(q-m)+(r-n)}$ czyli dla wielomianu

$$b_m(y)c_n(y)+b_{m-1}(y)c_{n+1}(y)+b_{m-2}(y)c_{n+2}(y)+\ldots$$
$$\ldots+b_{m+1}(y)c_{n-1}(y)+b_{m+2}(y)c_{n-2}(y)+\ldots$$

Z określenia liczb m i n wynika, że wielomiany $b_{m-1}(y), b_{m-2}(y),\ldots$ jako też $c_{n-1}(y), c_{n-2}(y),\ldots$ są podzielne przez $\varphi_1(y)$; iloczyn $b_m(y)c_n(y)$ musi więc też być podzielny przez $\varphi_1(y)$.

Zauważmy teraz, że wielomiany $b_m(y)$ i $\varphi_1(y)$ nie mają żadnego wspólnego czynnika, różnego od stałej. Istnieją więc wielomiany $P(y)$ i $Q(y)$ takie, że

$$P(y)b_m(y)+Q(y)\varphi_1(y)=1,$$

skąd, przez pomnożenie przez $c_n(y)$, otrzymamy:

$$P(y)b_m(y)c_n(y)+Q(y)c_n(y)\varphi_1(y)=c_n(y).$$

Wielomian, występujący po lewej stronie tego wzoru, jest podzielny przez $\varphi_1(y)$, wbrew określeniu wielomianu $c_n(y)$. Zatem $\varphi_1(y)|h(x,y)$.

Dowiedliśmy w ten sposób, że istnieje wielomian $h_1(x,y)$ taki, iż $h(x,y)=\varphi_1(y)\,h_1(x,y)$. Przyjmując $\varphi(y)=\varphi_1(y)\vartheta(y)$, otrzymamy z (50):

$$g(x,y)h_1(x,y)=\vartheta(y)\psi(x,y). \tag{51}$$

Jeżeli $\vartheta(y)$ posiada czynnik liniowy $\varphi_2(y)$, to powtarzając dla równości (51) rozumowanie, przeprowadzone wyżej dla równości (50), dojdziemy do wzoru $h_1(x,y)=\varphi_2(y)\,h_2(x,y)$.

W ten sposób otrzymamy ciąg równości:

$$h(x,y)=\varphi_1(y)\,h_1(x,y),\qquad h_1(x,y)=\varphi_2(y)\,h_2(x,y),\quad \ldots,$$

w których $\varphi_1(y), \varphi_2(y),\ldots$ oznaczają czynniki liniowe wielomianu $\varphi(y)$. Ponieważ $\varphi(y)$ daje się na mocy twierdzenia 20 przedstawić jako iloczyn czynników liniowych

$$\varphi(y)=\varphi_1(y)\varphi_2(y)\ldots,$$

więc wnosimy stąd, że $\varphi(y)|h(x,y)$, c. b. d. o.

Przypuśćmy teraz, że chcemy zbadać, czy wielomian $f(x,y)$ jest podzielny przez wielomian $g(x,y)$, który jest stopnia dodatniego względem x.

Niech $\varphi(y)$ oznacza wielomian zmiennej y, możliwie najwyższego stopnia, będący dzielnikiem wielomianu $g(x,y)$. Widzieliśmy, że wielomian taki potrafimy znaleźć. Jeżeli wielomian $f(x,y)$ jest podzielny przez $g(x,y)$, to musi być $\varphi(y)|f(x,y)$, zatem $\varphi(y)$ musi być, jak dowiedliśmy w twierdzeniu 31, dzielnikiem każdego ze współczynników rozwinięcia wielomianu $f(x,y)$ według potęg x. Jeśli warunek ten jest spełniony, to możemy przyjąć $f(x,y)=\varphi(y)f_1(x,y)$ oraz $g(x,y)=\varphi(y)g_1(x,y)$, gdzie wielomian g_1 nie ma dzielnika, będącego wielomianem stopnia dodatniego, zależnym tylko od y.

Na to, żeby było $g(x,y)|f(x,y)$, potrzeba więc i wystarcza, żeby było $g_1(x,y)|f_1(x,y)$. W myśl twierdzenia 29 znajdziemy dalej wielomiany $h(x,y)$, $r(x,y)$ oraz wielomian $b(y)$, nie będący tożsamościowo zerem, takie iż

(52) $$b(y)f_1(x,y) = g_1(x,y)h(x,y) + r(x,y),$$

przy czym wielomian $r(x,y)$ jest względem x stopnia niższego niż wielomian $g_1(x,y)$.

Jeżeli $g_1(x,y)|f_1(x,y)$, to z równości (52) wynika natychmiast, że $g_1(x,y)|r(x,y)$, zatem że $r(x,y)=0$, gdyż $r(x,y)$ jest względem x wielomianem stopnia niższego niż $g_1(x,y)$.

Okażemy teraz, że i na odwrót: jeżeli tożsamościowo $r(x,y)=0$, to $g_1(x,y)|f_1(x,y)$. Istotnie, jeżeli $r(x,y)=0$, to wzór (51) daje

(53) $$b(y)f_1(x,y) = g_1(x,y)h(x,y),$$

skąd $b(y)|g_1(x,y)h(x,y)$, a że $g_1(x,y)$ nie posiada dzielnika zależnego jedynie od y, więc w myśl twierdzenia 32 mamy $b(y)|h(x,y)$, zatem $h(x,y)=b(y)h_1(x,y)$ i wzór (53) daje $f_1(x,y)=g_1(x,y)h_1(x,y)$, skąd $g_1(x,y)|f_1(x,y)$.

Mamy więc zawsze możność przekonania się, czy wielomian $f(x,y)$ jest podzielny przez wielomian $g(x,y)$ i ewentualnego znalezienia ilorazu.

§ 18. Wyznaczanie największego wspólnego dzielnika wielomianów dwóch zmiennych. Zajmiemy się teraz wyznaczaniem wspólnych dzielników dwóch danych wielomianów $f(x,y)$ i $g(x,y)$. Znajdziemy najpierw wspólne dzielniki tych wielomianów, zależne jedynie od y. W tym celu przedstawimy te wielomiany w postaci

$$f(x,y) = \varphi(y)f_1(x,y), \qquad g(x,y) = \psi(y)g_1(x,y),$$

gdzie wielomiany f_1 i g_1 nie mają już dzielników, będących wielomianami stopni dodatnich i zależnymi tylko od zmiennej y. Z twierdzenia 32 wynika, że każdy zależny jedynie od y wspólny dzielnik wielomianów $f(x,y)$ i $g(x,y)$ musi być wspólnym dzielnikiem wielomianów $\varphi(y)$ i $\psi(y)$ i, oczywiście, na odwrót.

Zajmiemy się więc dalej wspólnymi dzielnikami $d(x,y)$ dwóch wielomianów $f(x,y)$ i $g(x,y)$, będącymi względem x stopnia dodatniego i nie mającymi dzielników stopnia dodatniego zależnych jedynie od y. Oznaczając te wielomiany przez $f_1(x,y)$ i $f_2(x,y)$, zastosujemy do nich algorytm kolejnych dzieleń z § 16, dochodząc do wzorów (46) i (47), str. 140.

Z pierwszej z równości (46) wynika, że każdy wspólny dzielnik $d(x,y)$ wielomianów f_1 i f_2 jest dzielnikiem wielomianu f_3. Z drugiej z równości (46) wnosimy podobnie, że $d|f_4$ i t.d., wreszcie z równości (47), że $d|f_k$. Ponieważ jednak f_k jest stopnia 0 względem x, zaś d jest stopnia dodatniego względem x, więc musi być tożsamościowo $f_k=0$.

Wzór (47) daje zatem

(54) $$b_{k-2}f_{k-2} = f_{k-1}h_{k-2};$$

jeśli przy tym założymy, że k jest najmniejszą liczbą naturalną, dla której wielomian f_k jest niezależny od x, to f_{k-1} będzie stopnia dodatniego względem x.

Wielomian d, jako dzielnik wielomianów $f_1, f_2, f_3, \ldots$, jest w szczególności dzielnikiem wielomianu f_{k-1}. Każdy dzielnik wspólny wielomianów f_1 i f_2 stopnia dodatniego względem x jest więc dzielnikiem wielomianu f_{k-1}.

Na odwrót, niech teraz $d(x,y)$ oznacza wielomian stopnia dodatniego względem x i załóżmy, że $d(x,y)$ nie posiada dzielnika, zależnego jedynie od y i nie redukującego się do stałej. Pokażemy, że jeśli $d(x,y)$ jest dzielnikiem wielomianu f_{k-1}, to $d(x,y)$ jest wspólnym dzielnikiem wielomianów f_1 i f_2.

Istotnie, jeśli $f_{k-1}=d\varphi$, to wzór (54) daje

(55) $$b_{k-2}f_{k-2} = d\varphi h_{k-2}.$$

Ponieważ b_{k-2} zależy jedynie od y, zaś d nie posiada dzielnika zależnego jedynie od y i różnego od stałej, więc w myśl twierdzenia 32 $b_{k-2}|\varphi h_{k-2}$, zatem $\varphi h_{k-2}=b_{k-2}\psi$, gdzie ψ jest wielomianem zmiennych x i y. Wnosząc to do (55) i dzieląc obie strony przez wielomian b_{k-2}, który — jak wiemy z twierdzenia 29 — nie jest tożsamościowo równy 0, otrzymamy $f_{k-2}=d\psi$. Z równości $b_{k-3}f_{k-3}=f_{k-2}b_{k-3}+f_{k-1}$ wnosimy dalej, iż $d|b_{k-3}f_{k-3}$, skąd wnosimy jak wyżej, że $d|f_{k-3}$. Powtarzając to rozumowanie, otrzymamy wreszcie $d|f_2$ i $d|f_1$. Dowiedliśmy zatem, że każdy dzielnik wspólny wielomianów f_1 i f_2, będący stopnia dodatniego względem x i nie posiadający dzielnika zależnego jedynie od y i różnego od stałej, jest dzielnikiem wielomianu f_{k-1} i na odwrót.

Jeżeli teraz wielomian f_{k-1} przedstawimy w postaci $f_{k-1}=bh$, gdzie b jest wielomianem zależnym jedynie od y, redukującym się ewentualnie do stałej, zaś h jest wielomianem zmiennych x i y, nie mającym żadnego dzielnika różnego od stałej i zależnego jedynie od y, to h będzie największym ze wspólnych dzielników wielomianów f_1 i f_2, które są stopnia dodatniego względem x i nie posiadają różnych od stałej dzielników, zależnych jedynie od y. Mnożąc h przez największy wspólny dzielnik współczynników w rozwinięciach obu wielomianów f_1 i f_2 według potęg x, otrzymamy największy wspólny dzielnik wielomianów f_1 i f_2. Możemy więc wypowiedzieć

Twierdzenie 33. *Na to, żeby wielomiany f_1 i f_2 miały wspólny dzielnik, będący wielomianem stopnia dodatniego względem x, potrzeba i wystarcza, żeby było $f_h=0$.*

ĆWICZENIA. 1. Dowieść, że przy każdym naturalnym n wielomian

$$(y-z)^{2n+1}+(z-x)^{2n+1}+(x-y)^{2n+1}$$

jest podzielny przez wielomian

$$(y-z)\,(z-x)\,(x-y).$$

2. Dowieść, że przy każdym naturalnym n wielomian

$$(x+y+z)^{2n+1}-x^{2n+1}-y^{2n+1}-z^{2n+1}$$

jest podzielny przez wielomian

$$(y+z)\,(z+x)\,(x+y).$$

§ 19. Wyznaczanie dzielników wielomianów wielu zmiennych. Załóżmy, że $f(x_1,x_2,\dots,x_n)$ jest wielomianem n zmiennych o współczynnikach dowolnych (wzgl. o współczynnikach całkowitych). Niech g oznacza liczbę naturalną, większą od największego wykładnika każdej ze zmiennych $x_1,x_2,\dots,x_n$ w rozwinięciu wielomianu f. Jeżeli wielomian f rozkłada się na czynniki, to liczba g jest oczywiście większa od wykładnika każdej ze zmiennych $x_1,x_2,\dots,x_n$ w każdym z tych czynników. Podstawmy

$$x_1=x,\qquad x_2=x^g,\qquad x_3=x^{g^2},\qquad \dots,\qquad x_n=x^{g^{n-1}}$$

i przyjmijmy

$$F(x)=f(x,x^g,x^{g^2},\dots,x^{g^{n-1}}).$$

Jeżeli wielomian f (n zmiennych) rozkłada się na czynniki, będące wielomianami n zmiennych o współczynnikach dowolnych (wzgl. całkowitych), to i wielomian $F(x)$ (jednej zmiennej) rozkłada się na czynniki, będące wielomianami jednej zmiennej o współczynnikach dowolnych (wzgl. całkowitych). Każdemu rozkładowi wielomianu f odpowiada więc pewien rozkład wielomianu F, lecz niekoniecznie na odwrót.

Mając jednak dany rozkład wielomianu F, np. $F(x)=F_1(x)F_2(x)$, łatwo sprawdzić, czy odpowiada on jakiemuś rozkładowi wielomianu f i ewentualnie wyznaczyć wszystkie takie rozkłady. Jeżeli bowiem rozkład $F(x)=F_1(x)F_2(x)$ odpowiada rozkładowi $f=f_1f_2$, to f_1 jest sumą składników postaci $Ax_1^{\alpha_1}x_2^{\alpha_2}\dots x_n^{\alpha_n}$. Składnikowi takiemu odpowiada w wielomianie $F_1(x)$ składnik Ax^k, gdzie $k=\alpha_1+\alpha_2g+\dots+\alpha_ng^{n-1}$. Lecz wobec $g>\alpha_i$ dla $i=1,2,\dots,n$ liczby $\alpha_1,\alpha_2,\dots,\alpha_n$ są jednoznacznie wyznaczone przez liczbę k, gdyż każda liczba całkowita ma jedno tylko rozwinięcie przy zasadzie g. Wynika stąd, że dany rozkład $F(x)=F_1(x)F_2(x)$ odpowiada co najwyżej jednemu tylko rozkładowi $f=f_1f_2$. Czy istotnie takiemu rozkładowi odpowiada, przekonywujemy się, sprawdzając po wyznaczeniu w powyższy sposób wielomianów f_1 i f_2, odpowiadających wielomianom $F_1(x)$ i $F_2(x)$, czy zachodzi tożsamość $f=f_1f_2$.

W ten sposób wyznaczanie dzielników wielomianu wielu zmiennych sprowadza się do wyznaczania dzielników wielomianu jednej zmiennej.

§ 20. Przykłady. Metoda, wyłożona w § 19, pozwala rozstrzygnąć, czy dany wielomian n zmiennych $f(x_1,x_2,\dots,x_n)$ o współczynnikach całkowitych jest rozkładalny na iloczyn dwóch innych wielomianów, nie redukujących się do stałej.

W poszczególnych jednak przypadkach zagadnienie to może być rozstrzygnięte w krótszy sposób.

Udowodnimy np., że *wielomian*

$$f(x,y)=W(x)+y,$$

gdzie $W(x)$ jest dowolnym wielomianem jednej zmiennej x, nie jest rozkładalny.

Przypuśćmy w tym celu, że istnieje rozkład $f=f_1f_2$. Ponieważ wielomian $f(x,y)$ jest 1-go stopnia względem zmiennej y, więc jeden tylko z wielomianów f_1 i f_2 jest zależny od y. Przypuśćmy np., że f_2 nie zależy od y i niech $f_2=f_2(x)$. Wielomian f_1 ma wtedy postać $f_1=f_1(x,y)=P(x)+Q(x)y$, skąd wynika, że tożsamościowo spełniona jest równość:

$$W(x)+y=f(x,y)=[P(x)+Q(x)y]f_2(x)=P(x)f_2(x)+Q(x)f_2(x)y.$$

Wnosimy stąd, że $Q(x)f_2(x)=1$, co dowodzi, że $f_2(x)$ musi być stałą. Wielomian $f(x,y)$ nie może więc być iloczynem dwóch wielomianów, z których żaden nie jest stałą, c.b.d.o.

W szczególności np. *wielomian x^2+y jest nierozkładalny.*

Jako inny przykład, udowodnimy, że *wyznacznik*

$$f = \begin{vmatrix} x_{1,1} & \cdot & \cdot & \cdot & x_{1,n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ x_{n,1} & \cdot & \cdot & \cdot & x_{n,n} \end{vmatrix},$$

uważany za wielomian n^2 zmiennych $x_{1,1}, x_{1,2}, \dots, x_{n,n}$, jest nierozkładalny [1]).

Przypuśćmy w tym celu, że istnieje rozkład $f=f_1f_2$ wielomianu f na iloczyn dwóch wielomianów f_1 i f_2, nie redukujących się do stałej; f_1 musi więc być wielomianem co najmniej jednej z wymienionych n^2 zmiennych, np. zmiennej $x_{k,l}$. Podobnie f_2 jest wielomianem co najmniej jednej z tych n^2 zmiennych, np. zmiennej $x_{p,q}$. Nie może tu być jednocześnie $k=p$ oraz $l=q$, gdyż wtedy wyznacznik $f=f_1f_2$ zawierałby składnik, mający czynnik $x_{k,l}x_{p,q}=x_{k,l}^2$, co — jak wynika z definicji wyznacznika — jest niemożliwe. Przypuśćmy więc np., że $k\neq p$. Gdyby było $l=q$, to wyznacznik $f=f_1f_2$ zawierałby czynnik $x_{k,l}x_{p,q}=x_{k,l}x_{p,l}$, co też jest dla $k\neq p$ niemożliwe, gdyż każdy składnik rozwinięcia wyznacznika zawiera po jednym tylko czynniku z każdej (a więc i l-tej) kolumny. Mamy więc zarazem $l\neq q$. Z drugiej strony, wyznacznik f zawiera w swoim rozwinięciu składnik, którego jednym z czynników jest $x_{p,l}$, skąd wynika, że co najmniej jeden z wielomianów f_1 i f_2 jest wielomianem zmiennej $x_{p,l}$. Gdyby był nim wielomian f_1, to wyznacznik $f=f_1f_2$ zawierałby składnik o czynniku $x_{p,l}x_{p,q}$, co wobec $l\neq q$ jest niemożliwe, gdyż każdy składnik rozwinięcia wyznacznika zawiera po jednym tylko czynniku z każdego (a więc i p-go) wiersza; gdyby zaś był nim wielomian f_2, to wyznacznik f zawierałby składnik o czynniku $x_{k,l}x_{p,l}$, co wobec $k\neq p$ też jest niemożliwe.

Założenie, że wielomian f jest rozkładalny, doprowadza więc do sprzeczności.

ĆWICZENIE. Udowodnić, że dwumian x^2-y^3 jest nierozkładalny.

---

[1]) Ob. M. Bôcher, *Einführung in die höhere Algebra*, Wyd. 2-e (Tłum. na niemiecki), Lipsk-Berlin 1925, str. 192.

§ 21. Rozkład wielomianów jednorodnych 2-go stopnia na sumy kwadratów wielomianów liniowych. Jak łatwo sprawdzić, zachodzi tożsamość:

$$xy = \left(\frac{x+y}{2}\right)^2 + \left(\frac{ix-iy}{2}\right)^2. \tag{56}$$

Oznaczając przez $\sqrt{a}, \sqrt{b}, \sqrt{c}$ którekolwiek z drugich pierwiastków liczb (zespolonych) a, b, c, mamy więc:

$$ax^2+bxy+cy^2 = (\sqrt{a}\,x)^2 + \left(\frac{\sqrt{b}}{2}x+\frac{\sqrt{b}}{2}y\right)^2 + \left(\frac{i\sqrt{b}}{2}x-\frac{i\sqrt{b}}{2}y\right)^2 + (\sqrt{c}\,y)^2,$$

co daje rozkład wielomianu jednorodnego 2-go stopnia dwóch zmiennych na sumę czterech kwadratów wielomianów jednorodnych liniowych tych zmiennych (z których dwa są jednomianami).

Ogólniej można na tej drodze z łatwością wywnioskować, że każdy wielomian jednorodny 2-go stopnia n zmiennych jest sumą skończonej liczby kwadratów wielomianów (jednomianów) jednorodnych liniowych tych zmiennych.

Można jednak dowieść nieco więcej, mianowicie

Twierdzenie 34. *Wielomian jednorodny 2-go stopnia n zmiennych jest sumą n lub mniej kwadratów wielomianów (lub jednomianów) jednorodnych liniowych tych zmiennych.*

Udowodnimy to naprzód dla $n=2$, a dalej przez indukcję. Jeżeli $a\neq 0$, to — jak łatwo sprawdzić — mamy:

$$ax^2+bxy+cy^2 = \left(\sqrt{a}\,x+\frac{b}{2\sqrt{a}}y\right)^2 + \left(\sqrt{c-\frac{b^2}{4a}}\,y\right)^2;$$

podobnie traktujemy przypadek $c\neq 0$; wreszcie, jeżeli $a=c=0$, to:

$$ax^2+bxy+cy^2 = bxy = \left(\frac{\sqrt{b}}{2}x+\frac{\sqrt{b}}{2}y\right)^2 + \left(\frac{i\sqrt{b}}{2}x-\frac{i\sqrt{b}}{2}y\right)^2.$$

Łatwo stąd dalej wywnioskować, że jeżeli współczynniki a, b i c są rzeczywiste, to wielomian $ax^2+bxy+cy^2$ daje się przedstawić jako suma dwóch (lub mniej), poprzedzonych znakiem $+$ lub $-$, kwadratów wielomianów (lub jednomianów) jednorodnych liniowych zmiennych x, y o współczynnikach rzeczywistych.

Załóżmy teraz, że twierdzenie jest prawdziwe dla $n-1$ zmiennych, i niech W oznacza wielomian jednorodny 2-go stopnia n zmiennych $x_1, x_2, \dots, x_n$. Rozróżnimy dwa przypadki:

1^0 Kwadrat jednej co najmniej ze zmiennych ma współczynnik różny od 0, np. $W=ax_1^2+\ldots$, gdzie $a\neq 0$. Z uwagi na to, że W jest wielomianem jednorodnym 2-go stopnia zmiennych $x_1, x_2, \ldots, x_n$, mamy:

$$W=ax_1^2+Px_1+Q,$$

gdzie P i Q są wielomianami jednorodnymi $n-1$ zmiennych $x_2, x_3, \ldots, x_n$, pierwszy stopnia pierwszego, a drugi drugiego. Wobec $a\neq 0$ możemy więc napisać:

$$W=\left(\sqrt{a}\,x_1+\frac{P}{2\sqrt{a}}\right)^2+\left(Q-\frac{P^2}{4a}\right). \tag{57}$$

Pierwszy składnik po prawej stronie jest oczywiście kwadratem wielomianu jednorodnego liniowego n zmiennych $x_1, x_2, \ldots, x_n$, zaś drugi jest wielomianem jednorodnym 2-go stopnia $n-1$ zmiennych $x_2, x_3, \ldots, x_n$, zatem, w myśl założenia, sumą co najwyżej $n-1$ kwadratów wielomianów jednorodnych liniowych tych zmiennych. Ostatecznie więc prawa strona wzoru (57) jest w rozpatrywanym przypadku sumą co najwyżej n kwadratów wielomianów jednorodnych liniowych zmiennych $x_1, x_2, \ldots, x_n$.

2^0 Kwadrat każdej ze zmiennych $x_1, x_2, \ldots, x_n$ w rozwinięciu wielomianu W ma współczynnik 0. Jeżeli wielomian W nie jest tożsamościowo równy 0, to jeden co najmniej z iloczynów dwóch różnych zmiennych ma w rozwinięciu W współczynnik różny od 0, np. $W=ax_1x_2+\ldots$, gdzie $a\neq 0$. Możemy oczywiście napisać:

$$W=ax_1x_2+Px_1+Qx_2+R,$$

gdzie P i Q są to wielomiany jednorodne pierwszego stopnia $n-2$ zmiennych $x_3, x_4, \ldots, x_n$, zaś R jest wielomianem jednorodnym 2-go stopnia $n-2$ zmiennych $x_3, x_4, \ldots, x_n$. Wobec $a\neq 0$ możemy więc napisać:

$$W=a\left(x_1+\frac{Q}{a}\right)\left(x_2+\frac{P}{a}\right)+\left(R-\frac{PQ}{a}\right),$$

skąd wobec (56) $\left(\text{dla } x=x_1+\dfrac{Q}{a} \quad \text{i} \quad y=x_2+\dfrac{P}{a}\right)$:

$$W=\left(\frac{\sqrt{a}}{2}x_1+\frac{\sqrt{a}}{2}x_2+\frac{P}{2\sqrt{a}}+\frac{Q}{2\sqrt{a}}\right)^2+\left(\frac{i\sqrt{a}}{2}x_1-\frac{i\sqrt{a}}{2}x_2-\frac{iP}{2\sqrt{a}}+\frac{iQ}{2\sqrt{a}}\right)^2+$$
$$+R-\frac{PQ}{a}.$$

Pierwsze dwa składniki prawej strony są oczywiście kwadratami wielomianów jednorodnych liniowych n zmiennych $x_1, x_2, \ldots, x_n$, zaś trzeci jest wielomianem jednorodnym 2-go stopnia $n-2$ zmiennych $x_3, x_4, \ldots, x_n$, a zatem, w myśl założenia, sumą co najwyżej $n-2$ kwadratów wielomianów jednorodnych liniowych tych zmiennych. Ostatecznie więc W jest sumą co najwyżej $2+(n-2)=n$ kwadratów wielomianów jednorodnych liniowych zmiennych $x_1, x_2, \ldots, x_n$, c. b. d. o.

§ 22. Funkcje wymierne i niewymierne. *Funkcją wymierną* nazywamy iloraz dwóch wielomianów.

Funkcja wymierna jednej zmiennej jest zatem postaci:

$$\varphi(x)=f(x)/g(x),$$

gdzie $f(x)$ i $g(x)$ są wielomianami. Ma więc ona oznaczoną (skończoną) wartość dla każdej liczby x, która nie jest pierwiastkiem wielomianu $g(x)$, a zatem dla wszystkich wartości zespolonych z wyjątkiem co najwyżej skończonej ich liczby.

Przykładem funkcji wymiernej jest funkcja $f(x)=1/x$, mająca oznaczoną wartość dla każdej liczby zespolonej $x\neq 0$.

Istnieją proste funkcje $\varphi(x)$, które nie dają się przedstawić jako iloraz dwóch wielomianów dla wszystkich takich wartości zmiennej, które nie są pierwiastkami wielomianu, będącego dzielnikiem.

Okażemy, że własność taką ma funkcja $\varphi(x)=|x|$.

Przypuśćmy w tym celu, że istnieją wielomiany $f(x)$ i $g(x)$ takie, że dla wszystkich rzeczywistych x, dla których $g(x)\neq 0$, mamy:

$$|x|=\frac{f(x)}{g(x)}; \tag{58}$$

zatem $|x|g(x)=f(x)$, skąd $f(x)-xg(x)=(|x|-x)g(x)$. Z uwagi na to, że $|x|-x=0$ dla $x\geqslant 0$, mielibyśmy więc równość $f(x)-xg(x)=0$ dla wszystkich $x\geqslant 0$, które nie są pierwiastkami wielomianu $g(x)$, a więc w każdym razie dla nieskończenie wielu różnych x, skąd wnosimy w myśl twierdzenia 18, str. 124, że wielomian $f(x)-xg(x)$ musi być tożsamościowo równy 0, czyli że $f(x)/g(x)=x$ dla wszystkich x nie będących pierwiastkami wielomianu $g(x)$, w szczególności więc dla (nieskończenie wielu) liczb ujemnych nie będących pierwiastkami wielomianu $g(x)$. Lecz dla takich ujemnych x mamy równość (58); byłoby więc dla nich $|x|=x$, co jest niemożliwe. A więc:

Funkcja $\varphi(x)=|x|$ nie jest wymierna.

Okażemy jeszcze, że funkcja $\varphi(x)=\sqrt{x}$ dla $x>0$, gdzie przez $\sqrt{}$ rozumiemy pierwiastek arytmetyczny, nie daje się przedstawić jako iloraz dwóch wielomianów dla wartości x, nie będących pierwiastkami dzielnika.

Przypuśćmy w tym celu, że istnieją wielomiany $f(x)$ i $g(x)$ takie, że dla wszystkich $x>0$, dla których $g(x)\neq 0$, mamy $\varphi(x)=f(x)/g(x)$. Byłoby więc $x=f(x^2)/g(x^2)$ dla wszystkich $x>0$, dla których $g(x^2)\neq 0$; dla takich x, a więc dla nieskończenie wielu różnych x, byłoby zatem $f(x^2)-xg(x^2)=0$, czyli wielomian $f(x^2)-xg(x^2)$ musiałby być tożsamościowo zerem. Mielibyśmy zatem tożsamościowo $f(x^2)=xg(x^2)$, co nie jest możliwe, gdyż lewa strona jest wielomianem stopnia parzystego, zaś $xg(x^2)$ — stopnia nieparzystego. A więc:

Funkcja $\varphi(x)=\sqrt{x}$ dla $x>0$ nie jest wymierna.

Nie wynika to jeszcze z niewymierności liczby $\sqrt{2}$, gdyż w definicji funkcji wymiernej nie robiliśmy założenia, że współczynniki wielomianów, których ta funkcja ma być ilorazem, muszą być wymierne.

ĆWICZENIE. Dowieść, że funkcja $\sin x$ nie jest wymierna.

Dowód. Gdyby istniały takie wielomiany $f(x)$ i $g(x)$, iż $\sin x=f(x)/g(x)$ dla wszystkich x, nie będących pierwiastkami wielomianu $g(x)$, to wobec $\sin(2k+\frac{1}{2})\pi=1$ dla całkowitych k równość $g(x)=f(x)$ zachodziłaby dla nieskończenie wielu różnych x, a więc wielomiany $f(x)$ i $g(x)$ byłyby tożsamościowo równe, co nie jest możliwe, gdyż $\sin x\neq 1$ dla nieskończenie wielu różnych x (np. dla $x=k\pi$, gdzie k całkowite).

§ 23. Rozkład funkcji wymiernej na ułamki proste.

Ułamkiem prostym nazywamy wyrażenie:

$$\frac{A}{(z-a)^m}, \tag{59}$$

gdzie A i a są liczbami zespolonymi stałymi, m liczbą naturalną, a z zmienną zespoloną.

Oczywiście, wyrażenie (59) ma określoną wartość zespoloną tylko dla $z\neq a$.

Wyrażenie:

$$f(z)=\frac{\varphi(z)}{\psi(z)}, \tag{60}$$

gdzie $\varphi(z)$ i $\psi(z)$ są wielomianami zmiennej zespolonej z, przy czym $\varphi(z)$ jest stopnia niższego niż $\psi(z)$, nazywamy *ułamkiem właściwym*.

Oczywiście, wyrażenie (60) ma określoną wartość zespoloną tylko dla liczb zespolonych z, nie będących pierwiastkami wielomianu $\psi(z)$.

Twierdzenie 35. *Każdy ułamek właściwy daje się przedstawić w jeden i tylko jeden sposób jako suma skończonej liczby ułamków prostych* (naturalnie dla takich wartości zmiennej, które nie są pierwiastkami jego mianownika).

Dowód. Niech $\varphi(z)$ i $\psi(z)$ będą danymi wielomianami, odpowiednio stopni $m\geqslant 0$ i $n>m$. Niech dalej a_1 oznacza jeden z pierwiastków wielomianu $\psi(z)$, zaś n_1 jego krotność. Przyjmijmy:

$$\psi(z)=(z-a_1)^{n_1}\psi_1(z); \tag{61}$$

$\psi_1(z)$ będzie więc wielomianem stopnia $n-n_1\geqslant 0$, przy czym

$$\psi_1(a_1)\neq 0. \tag{62}$$

Liczba:

$$A=\frac{\varphi(a_1)}{\psi_1(a_1)} \tag{63}$$

jest wobec (62) pewną liczbą zespoloną. Wobec (63) będzie więc $\varphi(a_1)-A\psi_1(a_1)=0$, co dowodzi, że a_1 jest pierwiastkiem wielomianu $\varphi(z)-A\psi_1(z)$. Wynika stąd w myśl twierdzenia 3, str. 107, tożsamość:

$$\varphi(z)-A\psi_1(z)=(z-a_1)\varphi_1(z), \tag{64}$$

gdzie $\varphi_1(z)$ jest wielomianem stopnia co najwyżej $n-2$, gdyż inaczej prawa strona wzoru (64) byłaby wielomianem stopnia co najmniej n, gdy tymczasem $\varphi(z)$ jest stopnia $m<n$, zaś $\psi_1(z)$ jest stopnia $n-n_1<n$.

Wobec (61) i (64) zachodzi przy wszelkim zespolonym z, nie będącym pierwiastkiem wielomianu $\psi(z)$, tożsamość:

$$\frac{\varphi(z)}{\psi(z)}=\frac{\varphi(z)}{(z-a_1)^{n_1}\psi_1(z)}=\frac{A}{(z-a_1)^{n_1}}+\frac{\varphi_1(z)}{(z-a_1)^{n_1-1}\psi_1(z)}, \tag{65}$$

przy czym wielomian $\varphi_1(z)$ stopnia co najwyżej $n-2$ jest stopnia niższego od wielomianu $(z-a_1)^{n_1-1}\psi_1(z)$, który jest stopnia $n-1$. Drugi składnik prawej strony wzoru (65) jest więc ułamkiem właściwym, którego mianownik jest wielomianem stopnia o jedność niższego niż mianownik ułamka $\varphi(z)/\psi(z)$.

Dowiedliśmy zatem, że każdy ułamek właściwy możemy przedstawić jako sumę: 1^0 ułamka prostego, którego mianownik jest potęgą jednego z czynników pierwszych mianownika danego ułamka i 2^0 ułamka właściwego, którego mianownik jest stopnia o jedność niższego niż mianownik danego ułamka i który jest przy tym jego dzielnikiem.

Stosując dowiedzioną własność $n-1$ razy, dojdziemy do ułamka właściwego, którego mianownik będzie 1-go stopnia, zaś licznik liczbą stałą, a więc do ułamka prostego.

Każdy zatem ułamek właściwy $\varphi(z)/\psi(z)$, gdzie $\psi(z)$ jest wielomianem n-go stopnia, rozwijającym się na czynniki pierwsze:

$$\psi(z)=(z-a_1)^{n_1}(z-a_2)^{n_2}\dots(z-a_k)^{n_k},$$

daje się przedstawić jako suma n ułamków prostych; otrzymamy wtedy dla zespolonych z, nie będących pierwiastkami mianownika $\psi(z)$, tożsamość:

$$
\begin{aligned}
\frac{\varphi(z)}{\psi(z)} = & \frac{A_1'}{(z-a_1)^{n_1}}+\frac{A_2'}{(z-a_1)^{n_1-1}}+\dots+\frac{A_{n_1}'}{z-a_1}+\\
(66)\qquad & +\frac{A_1''}{(z-a_2)^{n_2}}+\frac{A_2''}{(z-a_2)^{n_2-1}}+\dots+\frac{A_{n_2}''}{z-a_2}+\\
& \dots\dots\dots\dots\dots\dots\dots\\
& +\frac{A_1^{(k)}}{(z-a_k)^{n_k}}+\frac{A_2^{(k)}}{(z-a_k)^{n_k-1}}+\dots+\frac{A_{n_k}^{(k)}}{z-a_k},
\end{aligned}
$$

gdzie $A_1',\dots,A_{n_k}^{(k)}$ są liczbami stałymi, wśród których mogą być też równe 0.

Pozostaje do dowiedzenia, że każdy ułamek właściwy ma tylko jedno rozwinięcie na ułamki proste. Przypuśćmy w tym celu, że dla danego ułamka właściwego $\varphi(z)/\psi(z)$ mamy prócz rozwinięcia (66) jeszcze inne rozwinięcie na ułamki proste, zachodzące dla każdego zespolonego z, nie będącego pierwiastkiem wielomianu $\psi(z)$. Mianownik każdego z tych ułamków musi być postaci $(z-a)^l$, gdzie przy pewnym naturalnym $j\leqslant k$ mamy $a=a_j$ i $l\leqslant n_j$. Gdyby bowiem było $a\neq a_j$ dla wszystkich $j=1,2,\dots,k$, to rozwinięcie nie mogłoby zachodzić dla $z=a$; gdyby zaś przy pewnym naturalnym $j\leqslant k$ było $a=a_j$, lecz $l>n_j$, to zakładając, że rozpatrywany ułamek prosty zawiera wyższą niż inne potęgę różnicy $z-a$, otrzymalibyśmy po sprowadzeniu prawej strony do wspólnego mianownika iloraz dwóch wielomianów względnie pierwszych, gdzie mianownik jest

podzielny przez $(z-a)^l$, a więc tym bardziej przez $(z-a)^{n_j+1}$; otóż taki iloraz nie mógłby być równy $\varphi(z)/\psi(z)$, gdyż $\psi(z)$ nie jest podzielne przez $(z-a_j)^{n_j+1}$.

Jeżeli więc ułamek $\varphi(z)/\psi(z)$ daje prócz rozwinięcia (66) inne jeszcze rozwinięcie na ułamki proste, to musi ono być postaci:

$$(67)\qquad \frac{\varphi(z)}{\psi(z)}=\frac{B_1'}{(z-a_1)^{n_1}}+\frac{B_2'}{(z-a_1)^{n_1-1}}+\dots+\frac{B_{n_k}^{(k)}}{z-a_k}.$$

Wobec (66) i (67) otrzymujemy przy wszelkim zespolonym z, dla którego $\psi(z)\neq 0$:

$$(68)\qquad \frac{A_1'-B_1'}{(z-a_1)^{n_1}}+\frac{A_2'-B_2'}{(z-a_1)^{n_1-1}}+\dots+\frac{A_{n_k}^{(k)}-B_{n_k}^{(k)}}{z-a_k}=0,$$

skąd, mnożąc przez $\psi(z)=(z-a_1)^{n_1}\dots(z-a_k)^{n_k}$:

$$(69)\qquad (A_1'-B_1')(z-a_2)^{n_2}\dots(z-a_k)^{n_k}+(z-a_1)P(z)=0,$$

gdzie $P(z)$ jest wielomianem. Równość (69) zachodzi więc dla nieskończenie wielu różnych z, skąd w myśl twierdzenia 18, str. 124, wnosimy, że zachodzi ona tożsamościowo. Dla $z=a_1$ otrzymamy stąd z uwagi na to, że $a_1\neq a_j$ dla $j=2,3,\dots,k$, równość $A_1'-B_1'=0$ czyli $A_1'=B_1'$. Podobnie udowodnilibyśmy dalej, ze wzoru (68), że $A_2'=B_2'$ i t. d., wreszcie, że $A_{n_k}^{(k)}=B_{n_k}^{(k)}$, c. b. d. o.

Dla praktycznego wyznaczania współczynników $A_1',A_2',\dots,A_{n_k}^{(k)}$ rozwinięcia (66) można użyć metody współczynników nieoznaczonych. Mianowicie, po pomnożeniu obu stron wzoru (66) przez $\psi(z)$ i porównaniu po obu stronach współczynników przy jednakowych potęgach z otrzymujemy dla n współczynników $A_1',A_2',\dots,A_n^{(k)}$ układ n równań liniowych.

Można dowieść, że gdy φ i ψ są wielomianami zmiennej rzeczywistej o współczynnikach rzeczywistych, to ułamek właściwy $\varphi(x)/\psi(x)$ jest sumą skończonej liczby wyrażeń postaci $\dfrac{A}{(x-a)^p}$ lub $\dfrac{Bx+C}{[(x-a)^2+b^2]^q}$, gdzie liczby p i q są naturalne, zaś liczby A, B, C, a i $b>0$ — rzeczywiste.

PRZYKŁADY I ĆWICZENIA. Mamy rozwinięcia:

1. $\dfrac{2}{z^3-z}=-\dfrac{2}{z}+\dfrac{1}{z+1}+\dfrac{1}{z-1}$;

2. $\dfrac{z+2}{z^4+z^3}=\dfrac{2}{z^3}-\dfrac{1}{z^2}+\dfrac{1}{z}-\dfrac{1}{z+1}$;

3. $\dfrac{1+z+3z^2}{z(1-z)(1-3z)(1-5z)}=\dfrac{1}{z}+\dfrac{5}{8(1-z)}-\dfrac{90}{8(1-3z)}+\dfrac{165}{8(1-5z)}$;

4. $\dfrac{1+z^2}{(1-2z)^3(1+z)}=\dfrac{5}{6(1-2z)^3}-\dfrac{1}{18(1-2z)^2}+\dfrac{4}{27(1-2z)}+\dfrac{2}{27(1+z)}$ [1].

5. Rozwinąć na ułamki proste następujące funkcje wymierne [2]:

$$u_1=\frac{9z^2-3z+8}{z^3-z^2-z+1}; \qquad u_2=\frac{z^2-7}{z^3+2z^2-5z-6};$$

$$u_3=\frac{7z-3}{z^3-3z^2+z+5}; \qquad u_4=\frac{1}{z^3(z-1)^2(z+1)}; \qquad u_5=\frac{z+1}{(z^2+1)^2(z-1)}.$$

Odp.: $u_1=\dfrac{7}{(z-1)^2}+\dfrac{4}{z-1}+\dfrac{5}{z+1}$;

$$u_2=\frac{1}{z+1}-\frac{1}{5}\,\frac{1}{z-2}+\frac{1}{5}\,\frac{1}{z+3};$$

$$u_3=\frac{\frac{1}{2}-2i}{z-2-i}+\frac{\frac{1}{2}+2i}{z-2+i}-\frac{1}{z+1};$$

$$u_4=\frac{1}{z^3}+\frac{1}{z^2}+\frac{2}{z}+\frac{1}{2(z-1)^2}-\frac{7}{4(z-1)}-\frac{1}{4(z+1)};$$

$$u_5=\frac{i}{4}\left[\frac{1}{(z-i)^2}-\frac{1}{(z+i)^2}\right]-\frac{1}{4}\left[\frac{1-i}{z-i}+\frac{1+i}{z+i}\right]+\frac{1}{2}\,\frac{1}{z-1}.$$

---

[1] Ostatnie dwa rozwinięcia podaje Jan Śniadecki na str. 183 i 186 swej *Rachunku algebraicznego teoryi* (cytowanej tu w Rozdziale X, § 8, str. 195, odnośnik).

[2] Szczegółowo wyprowadza te rozwinięcia O. Schlömilch w *Compendium der höheren Analysis*, Brunświk 1881, str. 291-300.