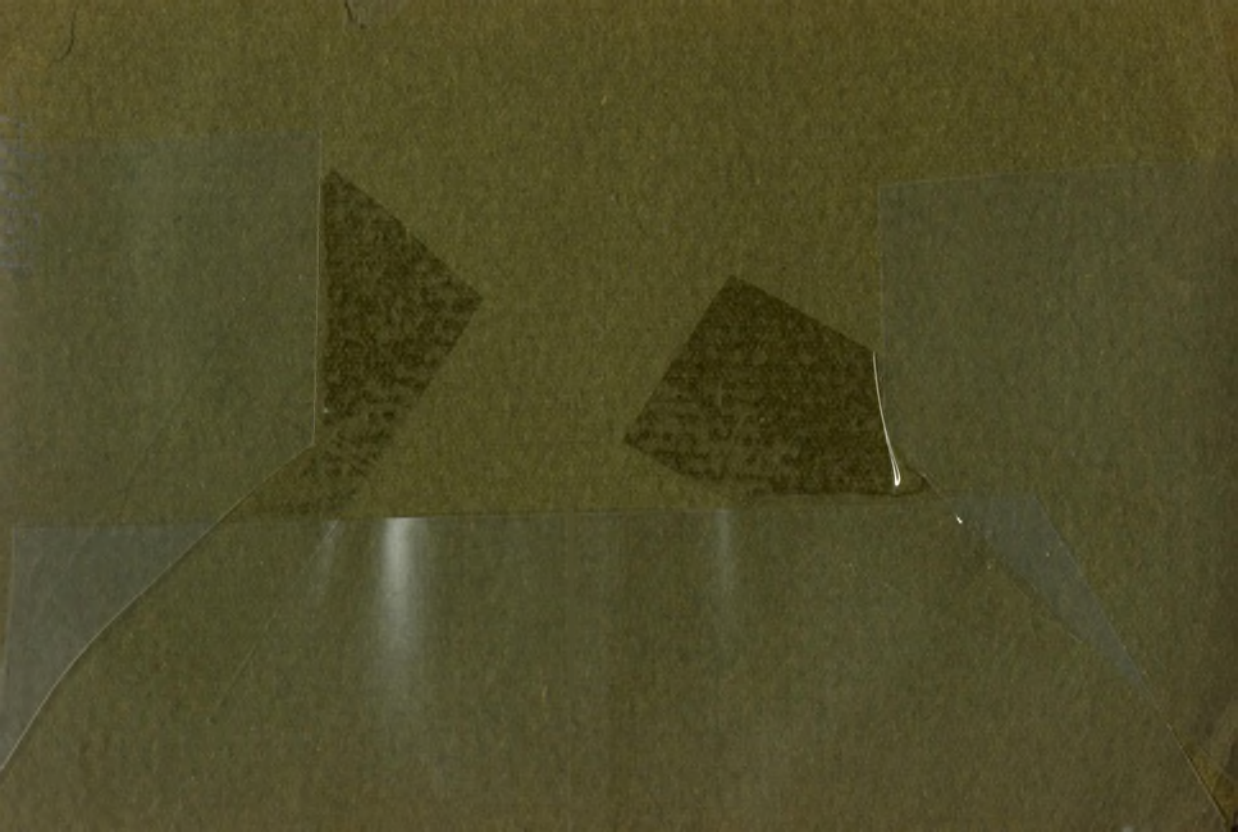
-FIZ. U. U. J. Nr. 5
A
WILKOSZA

DR WITOLD WILKOSZ
PROFESOR UNIWERSYTETU JAGIELLOŃSKIEGO

ZARYS ALGEBRY
W UJĘCIU KLASYCZNEM

CZĘŚĆ I.

KRAKÓW 1934



BIBLJOTECZKA KÓŁKA MAT.-FIZ. U. U. J. Nr. 5
POD REDAKCJĄ
PROF. DRA WITOLDA WILKOSZA

DR WITOLD WILKOSZ
PROFESOR UNIWERSYTETU JAGIELLOŃSKIEGO

ZARYS ALGEBRY
W UJĘCIU KLASYCZNEM

CZĘŚĆ I.

KRAKÓW 1934
NAKŁADEM KÓŁKA MATEMATYCZNO-FIZYCZNEGO U.U.J.
SKŁAD GŁÓWNY W KSIĘGARNIACH GEBETHNERA i WOLFFA
Warszawa — Kraków — Lublin — Łódź — Poznań — Wilno — Zakopane

DRUKARNIA NARODOWA W KRAKOWIE

Ukończona obecnie I cz. Zarysu Algebry zawiera nieomal tylko najniezbędniejsze wiadomości z zakresu Algebry Klasycznej, bezustannie przydatne w Analizie i Geometrji.

Druga część, której druk jest w toku, zajmie się wykładem nieco mniej elementarnych rozdziałów tej gałęzi matematyki.

Na tem miejscu chciałbym złożyć podziękowanie P. Lidji Stankiewiczównie, asyst. U. J. za dzielną pomoc przy kontroli tekstu, jakoteż Kółku Mat. Fiz. U. U. J. za nieszczędzenie trudów i kosztów, związanych z wydaniem niniejszej książki.

Wstęp.

Algebra w ujęciu *klasycznem* jest właściwie rozdziałem ogólnej teorji *funkcyj analitycznych* o jednej lub więcej zmiennych *zespolonych* (w sensie klasycznym). Zajmuje się ona własnościami szczególnej klasy tych funkcyj, a mianowicie *wielomianami*. W drugiej połowie XIX wieku rozwija się, zapoczątkowana już w pierwszej połowie i kontynuowana gorliwie w XX w., algebra w ujęciu odrębnem. Tworzy ją (w szerokiem tego słowa znaczeniu) teorja grup, pierścieni, ciał oraz liczb algebraicznych. Algebra ta (a raczej algebry), rozwija się jako doktryna autonomiczna, niezależna od teorji funkcyj analitycznych, której twierdzenia w zastosowaniu nawet do wielomianów klasycznych uchodzą w oczach rygorystycznego algebraika za coś obcego algebrze właściwej. Algebrą w takiem ujęciu nie będziemy się zasadniczo zajmowali w dziełku obecnem. Jednakże algebra w sensie klasycznym stanowi tak ważny środek pomocniczy wielu rozdziałów analizy, jak i geometrji, że znajomość jej musi uchodzić za nieodzowną potrzebę dla każdego matematyka. Poświęcamy jej zarysowi obecny tomik, przyczem nie zamierzamy zrywać związku z teorją funkcyj analitycznych, lecz przeciwnie wskazywać będziemy na istotne źródło pewnych twierdzeń algebry, które znajduje się niejednokrotnie właśnie w obrębie tej teorji.

Zakładamy u czytelnika znajomość początków teorji funkcyj *rzeczywistych zmiennych*, znajomość teorji *liczb rzeczywistych* oraz elementów nauki o *wyznacznikach*.

Rozdział I.

Teorja Liczb Zespolonych.

§ 1. Konstrukcja Hamiltona.

Znakomity angielski matematyk Sir William Rowan Hamilton [1805—1865] profesor astronomji na uniwersytecie w Dublinie i „Royal Astronomer of Ireland" stworzył nam w pracy pod tytułem: *Theory of conjugates functions or algebraic couples,* drukowanej w Transactions of the Royal Irish Academy (t. 17, r. 1835) teorję konstruktywną liczb zespolonych; liczb, którym już pełne prawo obywatelstwa w matematyce nadali K. F. Gauss, J. L. Lagrange i A. Cauchy. Teorję Hamiltona, zwaną często teorją „par Hamiltońa", wyłożymy obecnie z nieistotnemi zmianami natury terminologicznej.

1. **Pary elementów.** Z wielu względów uważamy za konieczne podanie precyzyjnej definicji *pary elementów,* jakkolwiek z pojęciem tem spotkał się zapewne już nawet początkujący matematyk.

Df. Przez parę elementów a i b (dowolnych), oznaczaną jako (a, b), rozumieć będziemy *ciąg skończony* o dwóch członach, którego *początkowym* członem jest a, *końcowym* zaś b.

Zgodnie z definicją ciągu skończonego omó-

wioną przezemnie gdzieindziej [1], parą (a, b) będzie zatem *przepis* (funkcja, operator, relacja jednoznaczna), który liczbie 1 przypisuje element a oraz liczbie 2 przypisuje element b.

Tw. Używając tak tu, jak i nadal znaku „=“ **jedynie** dla zaznaczenia identyczności, uzyskamy z definicji klasyczne własności par, a mianowicie:

(α) $(a, b) = (a, b)$

(β) $(a, b) = (c, d) . \supset . a = c \text{ i } b = d$

(γ) $a = c \text{ i } b = d . \supset . (a, b) = (c, d)$

(δ) $a \neq b . \supset . (a, b) \neq (b, a)$

(ε) $(a, b) = (b, a) . \supset . a = b.$

(ζ) Każda para posiada jednoznacznie określony element początkowy i jednoznacznie określony element końcowy.

Oznaczmy początkowy element pary (a, b) przez $p'(a, b)$, końcowy przez $k'(a, b)$

$$p'(a, b) = a, \quad k'(a, b) = b.$$

Uw. 1. Znak „$\supset$“ czytać należy „*pociąga*“.

Uw. 2. Definicja pary oraz własności (δ) i (ε) wskazują dosadnie, że **para** elementów (a, b) jest pojęciem **różnem** od **klasy** złożonej z elementów a i b, klasy którą wedle znakowań mej Teorji Mnogości Punktowych [Nr. 2 obecnej bibljoteczki] oznaczylibyśmy przez $\{a, b\}$ lub $\{a\} +_m \{b\}$.

2. **Wielkości zespolone** (Hamiltona).

Ogół par (a, b), gdzie tak a, jak i b są *liczbami rzeczywistemi* oznaczymy przez q_2. Ogół liczb rze-

[1] p. moja Arytmetyka Liczb Całkowitych Nr. 1 obecnej bibljoteczki, str. 98.

czywistych oznaczymy wraz z Peaną [Formulario] przez q.

Df. *Wielkością zespoloną* (Hamiltonowską) nazwiemy każdą parę należącą do q_2, a więc każdą parę (a, b), gdzie a i b należą do q.

Uw. 1. Określamy tu pewne szczególne wielkości zespolone, co zaznacza dopisek „Hamiltona". Termin „wielkość zespolona" lub, jak będziemy mówili później, „liczba zespolona", posiada w algebrze dzisiejszej rozległe znaczenie Tutaj oznacza on pewne klasyczne wielkości zespolone. Sam termin pochodzi od Gaussa.

Oznaczać będziemy w obecnym rozdziale liczby rzeczywiste przeważnie małemi łacińskiemi literami, względnie ich zespołami takiemi, jak $a+b$, $a.b$ i t. p., wielkości zaś zespolone przeważnie małemi greckiemi, względnie ich kombinacjami.

Tw. Jeżeli α jest wielkością zespoloną (należy do q_2), to istnieją jednoznacznie określone liczby rzeczywiste a i b takie, że

$$\alpha = (a, b),$$

przyczem:

$$a = p'\alpha$$
$$b = k'\alpha.$$

Uw. 2. Możnaby odrazu napisać, że:

jeżeli $\alpha \varepsilon q_2$,

to $\alpha = (p'\alpha, k'\alpha)$,

przyczem $p'\alpha \varepsilon q, k'\alpha \varepsilon q$.

[Znak „ε" czytamy: „należy do"].

Z uwagi tej skorzystamy niejednokrotnie.

3. **Równość.** Oznacza u nas, jak zawsze, *identyczność,* dlatego twierdzenia odnośne są zna-

nemi twierdzeniami o identyczności, których niema potrzeby osobno wysławiać. Conajwyżej zaznaczymy:

Tw.

(1) $\alpha, \beta \varepsilon q_2 . \alpha = \beta : \supset : p'\alpha = p'\beta . k'\alpha = k'\beta,$

(2) $\alpha, \beta \varepsilon q_2 . p'\alpha = p'\beta . k'\alpha = k'\beta : \supset : \alpha = \beta.$

Uw. Znak „." między zdaniami należy czytać „i"; zwrot taki, jak

$\alpha, \beta \varepsilon q_2$ jest skrótem dla: $\alpha \varepsilon q_2 . \beta \varepsilon q_2.$

4. Uwagi o pojęciu działania.

Jeżeli mamy daną jakąś klasę $(\mathfrak{A})$ dowolnych elementów $A, B, \ldots$, to wprowadzenie pewnego *działania* w obrębie klasy $\mathfrak{A}$ polega na ustaleniu drogą umów pewnego *przepisu* (funkcji, operatora), któryby pewnym lub nawet wszystkim *parom* elementów należących do klasy $(\mathfrak{A})$ przypisywał jakieś określone elementy w sposób jednoznaczny. Będzie to zatem pewna funkcja f, która przypisuje pewnym parom (A, B), gdzie $A, B \varepsilon (\mathfrak{A})$, elementy oznaczone każdorazowo przez $f(A, B)$, przyczem elementy $f(A, B)$ mogą, lecz nie muszą, należeć do klasy $(\mathfrak{A})$.

Z treści umów co do znaczenia przepisu f wyniknie dla jakich par (A, B) elementów należących do $(\mathfrak{A})$ symbol $f(A, B)$ *ma sens*, to znaczy umowy te zadecydują jakie jest *pole działania* (funkcji) f. Jeżeli dla *każdej* pary (A, B) elementów z klasy $(\mathfrak{A})$ $f(A, B)$ oznacza określony element, to mówimy, że działanie f jest *nieograniczenie wykonalne* w klasie $(\mathfrak{A})$. Wartość funkcji (wogóle) jest określona przy pomocy *opisu jednostkowego*, jako „jedyne coś spełniające pewne warunki" czyli przy

pomocy *definicji jednostkowej* [1] lub *deskryptu* (Russella). Aby symbolem typu $f(A, B)$ można się było posługiwać, musimy więc stwierdzić czy ma on *sens*, to znaczy czy żądany przedmiot określany jako $f(A, B)$ *istnieje* i czy jest *jedynym* żądanego rodzaju.

Opisaliśmy powyżej właściwie tylko typ działania na *parach* elementów czyli działania *dwójkowego*, spotykanego najczęściej w praktyce; możnaby z łatwością rozszerzyć to pojęcie na działanie *trójkowe, czwórkowe* i t. d.

Metoda zapisywania wyniku działania f na parze (A, B) w postaci *funkcyjnej* $f(A, B)$ nie zawsze jest wygodna. Praktyka pokazuje, że lepiej jest stworzyć sobie jakiś znak działania, dajmy na to „$\circ$“ dla działania f, by zapisywać

$$f(A, B) = A \circ B.$$

Korzystność tego znakowania staje się widoczną, gdy naprz. działanie f posiada t. zw. własność „łączności“ to znaczy, gdy zachodzi (pod pewnemi warunkami) związek:

$$f(f(A, B), C) = f(A, f(B, C)),$$

co zanotowalibyśmy w nowym systemie znakowania jako:

$$(A \circ B) \circ C = A \circ (B \circ C).$$

Również niekorzystnym wielokrotnie jest t. zw. system „komórkowy“ znakowań, polegający na tem, że zapisujemy wynik działania na parze (A, B)

---

[1] w przeciwieństwie do *klasowej*. Bliższe szczegóły o pojęciu deskryptu znajdzie czytelnik w mej Arytm. L. C. str. 43 nast. oraz 93 nast.

przez ujęcie A i B w nawias szczególnego kształtu, dajmy na to:

$$[A, B] \text{ czy } \{A, B\}\ldots,$$

gdzie kształt nawiasu oznacza dane działanie.

Jeżeli działanie wykonywane wśród par elementów klasy $(\mathfrak{A})$ posiada tę własność, że wynikiem jego (o ile tylko ma sens) jest zawsze jakiś element klasy $(\mathfrak{A})$, powiemy, że jest ono *działaniem wewnętrznem* w tej klasie.

5. **Dodawanie** wielkości zespolonych.

Df. Jeżeli (a, b) i (c, d) są wielkościami zespolonemi, to przez ich *sumę* rozumiemy parę

$$(a + c, b + d).$$

Formalnie:

$$(a, b), (c, d) \varepsilon q_2 : \supset : (a, b) +_z (c, d) \overset{\text{df}}{=} (a + c, b + d).$$

O ile piszemy wielkości zespolone przy pomocy jednej litery, to definicja będzie miała postać:

$$\alpha, \beta \varepsilon q_2 . \supset . \alpha +_z \beta \overset{\text{df}}{=} (p'\alpha + p'\beta, k'\alpha + k'\beta).$$

Znak $\overset{\text{df}}{=}$ czytamy: „oznacza (lub równa się) z definicji".

Uw. Znak $+_z$ przypomina, że mamy tu do czynienia z nowem pojęciem w zakresie wielkości zespolonych w przeciwieństwie do $+$ w zakresie liczb rzeczywistych.

Przechodzimy do własności sumy.

Tw. 1. Jeżeli α i β są zespolone, to $\alpha +_z \beta$ ma sens i jest wielkością zespoloną, jednoznacznie określoną; krótko:

$$\alpha, \beta \varepsilon q_2 . \supset . \alpha +_z \beta \varepsilon q_2$$

[wykonalność $+_z$ nieograniczona i to *wewnątrz* q_2].

2. $\alpha, \beta \varepsilon q_2 . \supset . \alpha +_z \beta = \beta +_z \alpha$
[przemienność sumy].

3. $\alpha, \beta, \gamma \varepsilon q_2 . \supset . (\alpha +_z \beta) +_z \gamma = \alpha +_z (\beta +_z \gamma)$
[łączność sumy].

4. $\alpha, \beta, \gamma \varepsilon q_2 . \alpha +_z \beta = \alpha +_z \gamma : \supset : \beta = \gamma$
[monotonja sumy].

Dem. (1) Skoro $\alpha, \beta \varepsilon q_2$, to $p'\alpha$, $p'\beta$, $k'\alpha$, $k'\beta$ mają sens i są liczbami rzeczywistemi. Mają sens zatem: $p'\alpha + p'\beta$ oraz $k'\alpha + k'\beta$ i są znów liczbami rzeczywistemi dzięki odnośnym własnościom „+". Zatem $(p'\alpha + p'\beta, k'\alpha + k'\beta)$ jest oznaczoną parą liczb rzeczywistych, a więc wielkością zespoloną.

(2) Wtedy: $\alpha +_z \beta = (p'\alpha + p'\beta, k'\alpha + k'\beta) =$
$= (p'\beta + p'\alpha, k'\beta + k'\alpha) = \beta +_z \alpha,$

gdyż $p'\alpha, p'\beta, k'\alpha, k'\beta \varepsilon q,$

więc $p'\alpha + p'\beta = p'\beta + p'\alpha,$
$k'\alpha + k'\beta = k'\beta + k'\alpha,$

dzięki przemienności „+".

Dowody (3) i (4) zupełnie analogiczne i elementarne, zostawiamy czytelnikowi.

Dzięki prawu łączności dla $+_z$ opłaca się, tak jak dla $+$, postawienie definicji:

$$\alpha +_z \beta +_z \gamma \overset{df}{=} (\alpha +_z \beta) +_z \gamma$$

i analogicznych.

6. **Zero** zespolone.

Df. Nazwiemy *zerem zespolonem* parę $(0, 0)$,

$$0_z \overset{df}{=} (0, 0).$$

Tw. (1) $0_z \varepsilon q_2$,

(2) $\alpha \varepsilon q_2 . \supset . \alpha +_z 0_z = 0_z +_z \alpha = \alpha_z$ [zerowe dodawanie],

(3) $\alpha, \beta \varepsilon q_2 . \alpha +_z \beta = \alpha : \supset : \beta = 0_z$.

Dem. Dowody elementarne.

7. Pojęcie działania odwrotnego.

Rozważmy klasę $\mathfrak{A}$ dowolnych elementów oraz pewne działanie „$\circ$“ *wewnętrzne* w klasie $\mathfrak{A}$. Mając dane elementy A i B klasy $\mathfrak{A}$, postawmy problem:

(1) Czy istnieje choć jeden element X klasy $\mathfrak{A}$ taki, by zachodził związek:

$$B \circ X = A.$$

(2) Czy mogą istnieć *różne* między sobą elementy wymaganego rodzaju?

Df. Otóż: *jedyny* element X klasy $\mathfrak{A}$ taki, że

$$B \circ X = A$$

nazwiemy *wynikiem prawostronnego działania odwrotnego do działania* „$\circ$“, zastosowanego do pary (A, B).

Gdybyśmy analogiczne pytania postawili co do elementu X spełniającego związek

$$X \circ B = A,$$

mielibyśmy do czynienia z *wynikiem lewostronnego działania odwrotnego do* „$\circ$“, zastosowanego do pary (A, B).

Wprowadzając naprzykład znaki $\cup'$ i $\cup''$ dla działania odwrotnego prawostronnego, względnie lewostronnego, zapisalibyśmy:

$$A \cup' B \overset{\text{df}}{=} \text{jedyne takie } X, \text{ że } X \varepsilon \mathfrak{A} \text{ i że } B \circ X = A,$$

$A \cup'' B \overset{df}{=}$ jedyne takie X, że $X \varepsilon \mathfrak{A}$ i że
$$X \circ B = A.$$

Umowy dotyczące działania „$\circ$" pozwoliłyby rozstrzygnąć, w których wypadkach symbole
$$A \cup' B \text{ i } A \cup'' B$$
miałyby sens, to znaczy pozwalałyby ustalić przy jakich wartościach A i B żądany element *istnieje* i *jest jedyny.* Gdyby się okazało, że dla pewnych A i B z klasy $\mathfrak{A}$ symbole $A \cup' B$, względnie $A \cup'' B$, *mają sens,* to wtedy mielibyśmy fakty następujące:

(1) $A \cup' B \varepsilon \mathfrak{A}$,
(2) $B \circ (A \cup' B) = A$,
(3) $C \varepsilon \mathfrak{A} . B \circ C = A : \supset : C = A \cup' B$,

względnie analogiczne związki dla $A \cup'' B$.

Jeżeli działanie „$\circ$" jest *przemiennem,* co znaczy, że o ile $A \circ B$ ma sens, to $B \circ A$ ma go również i
$$A \circ B = B \circ A,$$
wtedy jasnem jest, że działanie prawostronne odwrotne i lewostronne są jednem i tem samem, krótko mówiąc, *odwrotnem* do działania „$\circ$".

8. **Odejmowanie** zespolone.

Df. Określimy działanie odejmowania jako odwrotne do działania $+_z$. Położymy więc:
$$\alpha -_z \beta \overset{df}{=} \text{jedyne } \xi \text{ takie, że } \xi \varepsilon q_2$$
i że
$$\beta +_z \xi = \alpha.$$

Uw. Działanie $+_z$ jest *przemienne!!*

Mamy tu podstawowe twierdzenie:

Tw. Działanie $-_z$ jest nieograniczenie wykonalne i wewnętrzne w klasie q_2.

Inaczej:

$$\alpha, \beta \varepsilon q_2 . \supset . \alpha -_z \beta \varepsilon q_2.$$

Uw. Stwierdzenie, że $\alpha -_z \beta \varepsilon q_2$ powiada już tem samem, że $\alpha -_z \beta$ jest określonym elementem, że więc symbol $\alpha -_z \beta$ *ma sens*, jak to wynika z ogólnych umów co do opisu jednostkowego.[1]

Dem. (1) W założeniu, że $\alpha, \beta \varepsilon q_2$ mamy:

$$\beta +_z (p'\alpha - p'\beta, k'\alpha - k'\beta) = (p'\beta, k'\beta) +_z$$
$$+_z (p'\alpha - p'\beta, k'\alpha - k'\beta) = (p'\alpha, k'\alpha) = \alpha,$$

gdyż $p'\alpha - p'\beta, k'\alpha - k'\beta$ mają sens, dzięki nieograniczonej wykonalności działania „$-$“ w q oraz

$$p'\alpha - p'\beta, k'\alpha - k'\beta \varepsilon q,$$

elementem szukanym jest zatem choćby

$$(p'\alpha - p'\beta, k'\alpha - k'\beta).$$

Jeżeli jednak: $\alpha, \beta, \xi, \eta \varepsilon q_2$ i zachodzi

równość $\beta +_z \xi = \alpha, \beta +_z \eta = \alpha,$

to $\beta +_z \xi = \beta +_z \eta$

a więc $\xi = \eta$

dzięki monotonji sumy. Zatem *różnych* elementów żądanych niema. Z uwag o działaniu odwrotnem wynika już, że wtedy

$$\alpha -_z \beta \varepsilon q_2,$$

a prócz tego, że

$$\beta +_z (\alpha -_z \beta) = (\alpha -_z \beta) +_z \beta = \alpha$$

i jeszcze:

$$\alpha, \beta, \gamma \varepsilon q_2 . \beta +_z \gamma = \alpha : \supset : \gamma = \alpha -_z \beta.$$

Opuszczamy inne łatwe do przewidzenia i udowodnienia twierdzenia o odejmowaniu.

---

[1] p. Arytm. L. C., str. 43 nast.

9. **Mnożenie** zespolone.

Df. Iloczyn wielkości zespolonych α i β określamy formułą:

$$\alpha \times_z \beta \overset{df}{=} (p'\alpha . p'\beta - k'\alpha . k'\beta , p'\alpha . k'\beta + k'\alpha . p'\beta).$$

Pisząc: $\alpha = (a, b)$ i $\beta = (c, d)$, mielibyśmy:

$$(a, b) \times_z (c, d) = (ac - bd , ad + bc).$$

Uw. Wyjaśnimy później, skąd zrodziła się powyższa, dość sztucznie wyglądająca definicja.

Tw.

(1) $$\alpha , \beta \varepsilon q_2 . \supset . \alpha \times_z \beta \varepsilon q_2$$
[nieograniczona wykonalność mnożenia wewnątrz q_2],

(2) $$\alpha , \beta \varepsilon q_2 . \supset . \alpha \times_z \beta = \beta \times_z \alpha$$
[przemienność mnożenia],

(3) $$\alpha , \beta , \gamma \varepsilon q_2 . \supset . (\alpha \times_z \beta) \times_z \gamma = \alpha \times_z (\beta \times_z \gamma),$$
[łączność mnożenia].

(4) $$\left.\begin{array}{l} \alpha , \beta , \gamma \varepsilon q_2 . \supset . \alpha \times_z (\beta +_z \gamma) = \\ (\alpha \times_z \beta) +_z (\alpha \times_z \gamma) \overset{df}{=} , \\ \alpha \times_z \beta +_z \alpha \times_z \gamma \end{array}\right.$$
[rozdzielność mnożenia wobec dodawania].

(5) $$\alpha \varepsilon q_2 . \supset . \alpha \times_z 0_z = 0_z \times_z \alpha = 0_z$$
[prawo zerowego mnożenia].

(6) $$\alpha , \beta \varepsilon q_2 . \alpha \times_z \beta = 0_z : \supset : \alpha = 0_z \text{ lub } \beta = 0_z$$
[prawo zerowego iloczynu].

Dem. Dowody twierdzeń (1)—(5) są najzupełniej elementarne i otrzymujemy je, bądź dla tw. (1) przez analogję do dowodu o sensie dla $+_z$, względnie przez proste przerachowanie.

Zatrzymamy się jedynie nad dowodem tw. (6),

będącego jednem z *najważniejszych praw teorji wielkości zespolonych*. Oto dowód:

Połóżmy: $\alpha = (a, b), \beta = (c, d)$, więc

$$a, b, c, d \varepsilon q.$$

Związek: $\alpha \times_z \beta = 0_z$ da nam

$$\left.\begin{aligned} ac - bd &= 0 \\ ad + bc &= 0 \end{aligned}\right\} (*).$$

O ile $\beta = 0_z$, to twierdzenie słuszne. Jeżeli założymy $\beta \neq 0_z$, to $c \neq 0$ lub $d \neq 0$, więc wyznacznik

$$\begin{vmatrix} c, & -d \\ d, & c \end{vmatrix} = c^2 + d^2 \neq 0,$$

a związki $(*)$ dadzą nam:

$$a = 0, b = 0,$$

czyli $\alpha = (a, b) = (0, 0) = 0_z$.

10. **Jedynka** zespolona.

Df. Oznaczymy przez 1_z parę $(1, 0)$,

$$1_z \overset{df}{=} (1, 0).$$

Tw. (1) $1_z \varepsilon q_2$,

(2) $\alpha \varepsilon q_2 . \supset . \alpha \times_z 1_z = 1_z \times_z \alpha = \alpha$

[prawo jednostkowego mnożenia].

Dem. Dowody elementarne.

11. **Odwrotność** wielkości zespolonej.

Df. Przez odwrotność α^{-1} wielkości zespolonej α rozumiemy jedyne takie ξ zespolone, że

$$\alpha \times_z \xi = 1_z.$$

Połóżmy $\alpha = (a, b), a, b \varepsilon q.$

Szukajmy x i y rzeczywistych tak, by

$$\alpha \times_z (x, y) = 1_z,$$

a więc tak, by

$$\left.\begin{aligned} a\,x - b\,y &= 1 \\ b\,x + a\,y &= 0 \end{aligned}\right\} (*).$$

Pierwszy wypadek: $\alpha \neq 0_z$, więc $a \neq 0$ lub $b \neq 0$.

Wtedy: $\begin{vmatrix} a, & -b \\ b, & a \end{vmatrix} = a^2 + b^2 \neq 0$

i układowi (*) uczyni zadość w jedyny sposób para:

$$\left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2}\right).$$

Drugi wypadek: $\alpha = 0_z$, $a = b = 0$.

Układ (*) nie może być spełniony przez żadne x i y rzeczywiste. Otrzymamy łącznie:

Tw.

(1) $$\alpha \varepsilon q_2 . \alpha \neq 0_z . \supset . \alpha^{-1} \varepsilon q_2.$$

(2) $$\left.\begin{aligned} &\alpha \varepsilon q_2 . \alpha \neq 0_z . \supset . \alpha^{-1} = \\ &= \left(\frac{p'\alpha}{(p'\alpha)^2 + (k'\alpha)^2}, -\frac{k'\alpha}{(p'\alpha)^2 + (k'\alpha)^2}\right). \end{aligned}\right\}$$

(3) Symbol 0_z^{-1} niema sensu.

(4) $$\alpha \varepsilon q_2 . \alpha \neq 0_z . \supset . \alpha \times_z \alpha^{-1} = 1_z.$$

(5) $$\left.\begin{aligned} &\alpha, \beta \varepsilon q_2 . \alpha \times_z \beta = 1_z : \supset : \alpha \neq 0_z . \\ &. \beta \neq 0_z . \alpha = \beta^{-1} . \beta = \alpha^{-1}. \end{aligned}\right\}$$

Dem. Dowody (1)—(4) wynikają wprost z badania przeprowadzonego powyżej. Dowód (5) wynika również z tego badania łącznie z uwagą, że gdyby $\alpha = 0_z$ lub $\beta = 0_z$, to $\alpha \times_z \beta = 0_z \neq 1_z$.

12. **Dzielenie** zespolone.

Df. Określamy iloraz $\alpha /_z \beta$ jako wynik działania odwrotnego do $\times_z$.

Kładziemy więc:

$\alpha /_z \beta \overset{df}{=}$ jedyne ξ takie, że $\xi \varepsilon q_2$ i że $\beta \times_z \xi = \alpha$.

Jeżeli $\beta \neq 0_z$ i $\beta \varepsilon q_2$, to ma sens β^{-1} i należy do q_2.

Wtedy dla $\alpha \varepsilon q_2$ mamy jeszcze:

$$\beta \times_z (\alpha \times_z \beta^{-1}) = (\beta \times_z \alpha) \times_z \beta^{-1} =$$
$$= (\alpha \times_z \beta) \times_z \beta^{-1} = \alpha \times_z (\beta \times_z \beta^{-1}) =$$
$$= \alpha \times_z 1_z = \alpha.$$

A więc $\alpha \times_z \beta^{-1}$ czyni zadość wymaganiu, by było

$$\beta \times_z \xi = \alpha.$$

Jeżeli jednak:

$$\beta \times_z \xi = \alpha \text{ i } \beta \neq 0_z,$$

to:

$$\beta^{-1} \times_z (\beta \times_z \xi) = \beta^{-1} \times_z \alpha,$$
$$(\beta^{-1} \times_z \beta) \times_z \xi = \alpha \times_z \beta^{-1},$$
$$1_z \times_z \xi = \alpha \times_z \beta^{-1},$$
$$\xi = \alpha \times_z \beta^{-1},$$

więc *jedynie* $\alpha \times_z \beta^{-1}$ czyni zadość wymaganiom co do ilorazu.

Jeżeli $\beta = 0_z$, lecz $\alpha \neq 0_z$, to związki

$$\beta \times_z \xi = \alpha, \xi \varepsilon q_2$$

zachodzić nie mogą, gdyż pociągałoby to, że

$$0_z = \beta \times_z \xi = \alpha \neq 0_z.$$

Jeżeli $\alpha = 0_z$ i $\beta = 0_z$, to związki:

$$\beta \times_z 1_z = \beta = 0_z = \alpha,$$
$$\beta \times_z 0_z = 0_z = \alpha,$$
$$1_z \neq 0_z$$

stwierdzają, że wymaganiom:

$$\beta \times_z \xi = \alpha \quad \text{i} \quad \xi \varepsilon q_2$$

uczynić możemy zadość przynajmniej na *dwa różne* sposoby. Otrzymamy łącznie:

Tw.

$$(1)\quad \begin{cases} \alpha, \beta \varepsilon q_2 . \beta \neq 0_z . \supset . \alpha \diagup_z \beta \varepsilon q_2 . \\ . \alpha \diagup_z \beta = \alpha \times_z \beta^{-1}, \end{cases}$$

(2) symbol $\alpha \diagup_z 0_z$ nie posiada nigdy sensu.

Uw. ad 2. Dla $\alpha \varepsilon q_2 . \alpha \neq 0_z$ brak sensu pochodzi z *nieistnienia,* dla $\alpha = \beta = 0_z$ z *niejednotliwości.*

$$(3)\quad \alpha, \beta \varepsilon q_2 . \beta \neq 0_z : \supset : \beta \times_z (\alpha \diagup_z \beta) = \alpha.$$

$$(4)\quad \alpha, \beta, \gamma \varepsilon q_2 . \beta \neq 0_z . \beta \times_z \gamma = \alpha : \supset : \gamma = \alpha \diagup_z \beta.$$

Dem. Dowody wynikają z przeprowadzonego badania.

Uw. Nie piszemy wyraźnie formuły dla ilorazu w postaci pary liczb rzeczywistych, gdyż poznamy wkrótce wygodne sposoby mnożenia i dzielenia zespolonego.

§ 2. Wielkości rzeczywiste. Izomorfja.

1. Wielkości rzeczywisto-zespolone.

Df. Wielkością rzeczywisto-zespoloną nazwiemy każdą wielkość zespoloną α, dla której mamy $k'\alpha = 0$. Są to zatem pary:

$$(a, 0),$$

gdzie $a \varepsilon q$.

Oznaczymy parę $(a, 0)$ w tym wypadku przez: a_z czytając: *a zespolone.*

Uw. Dwie z tych wielkości poznaliśmy poprzednio. Były to 0_z i 1_z.

Df. Ogół wielkości rzeczywisto-zespolonych oznaczymy przez q_z. Jest to klasa będąca *częścią* klasy q_2.

Df. Dla wielkości klasy q_z wprowadzimy pojęcie *mniejszości zespolonej* $<_z$, kładąc:

$$a_z <_z b_z \overset{\text{df}}{=} a < b \quad (a, b \varepsilon q).$$

A więc naprz.: $1_z < 2_z$, $0_z < 1_z$ i t. d.

2. **Izomorfja** rzeczywisto-zespolonych i liczb rzeczywistych.

Zauważmy następujące fakty:

Tw. Jeżeli $a, b, c, \ldots \varepsilon q$, więc $a_z, b_z, c_z, \ldots \varepsilon q_z$, to:

(1) $a < b \,.\equiv.\, a_z < b_z$,
(2) $(a + b)_z = a_z +_z b_z$,
(3) $(a - b)_z = a_z -_z b_z$,
(4) $(a \times b)_z = a_z \times_z b_z$,
(5) $a = 0 \,.\equiv.\, a_z = 0_z$,
(6) $b \neq 0 \,.\supset.\, (a : b)_z = a_z :_z b_z$,
(7) $a = b \,.\equiv.\, a_z = b_z$.

Uw. Znak $\equiv$ między zdaniami oznacza: „jest równoważne“, a więc: „pociąga i odwrotnie“ lub „jest warunkiem koniecznym i dostatecznym, by“.

Rozważmy operację φ, która zamienia każdą liczbę rzeczywistą x w odpowiednią rzeczywisto-zespoloną x_z;

$$\varphi(x) = x_z.$$

Operacja ta, której polem jest q, stanowi przyporządkowanie czy odpowiedniość *doskonałą* (jednojednoznaczną) między elementami klasy q a klasy q_z. Oznacza to, że:

(1) Każda liczba x z klasy q ma określony odpowiednik $\varphi(x) = x_z$ w klasie q_z.

(2) Każda wielkość ξ z klasy q_z jest wynikiem

działania φ na pewnej liczbie z klasy q, a mianowicie: $\varphi(p'\xi) = \xi$.

(3) *Różne* elementy x i y z klasy q otrzymują *różne* odpowiedniki x_z, y_z.

(4) *Różne* elementy ξ, η z klasy q_z powstały z *różnych* elementów $p'\xi, p'\eta$ klasy q.

Odpowiedniość φ ma atoli kapitalną jeszcze własność: „*zachowuje*“ ona $<, +, -, \times, /, =$, to znaczy, że zachodzą fakty wyrażone powyżej jako Tw. (1—7).

Rozważmy jakieś twierdzenie mówiące o liczbach rzeczywistych, naprz.:

(α) $a, b, c \varepsilon q \,.\, a < b \,.\, b < c : \supset : a < c.$

Załóżmy teraz, że:

(β) $a_z, b_z, c_z \varepsilon q_z, a_z <_z b_z \,.\, b_z <_z c_z$

stąd wyniknie zaraz, że:

(γ) $a, b, c \varepsilon q \,.\, a < b \,.\, b < c,$

a więc dzięki tw. (α) zawnioskujemy:

(δ) $a < c$, co pozwoli na stwierdzenie, że:

(ε) $a_z <_z c_z$.

Otrzymamy zatem twierdzenie:

(ζ) $a_z, b_z, c_z \varepsilon q_z \,.\, a_z <_z b_z \,.\, b_z <_z c_z : \supset : a_z <_z c_z$

lub znakując ogólniej:

(η) $\alpha, \beta, \gamma \varepsilon q_z \,.\, \alpha <_z \beta \,.\, \beta <_z \gamma : \supset : \alpha <_z \gamma,$

a zatem twierdzenie ściśle analogiczne do twierdzenia (α).

Nasuwa się przypuszczenie, że *każde twierdzenie z teorji liczb rzeczywistych* da się w powyższy sposób, dzięki operacji φ i własnościom wielkości zespolonych, przekształcić na analogiczne twierdzenie teorji wielkości rzeczywisto-zespolonych, jeżeli tylko w zrozumiały przez się sposób uzupełnimy tę

ostatnią potrzebnemi definicjami, jak naprz.:

$$\alpha >_z \beta \overset{df}{=} \beta <_z \alpha \text{ i t. p....}$$

Musimy się zastanowić nad treścią tego przypuszczenia. Aby zrozumieć i uzasadnić nasze twierdzenie, posiadamy w obecnym stanie wiedzy jedną zdaje się tylko drogę. Cofnijmy się do uświadomienia sobie odpowiedzi na pytanie: co to jest teorja liczb rzeczywistych? Otóż najpierw określimy pojęcie *abstrakcyjnej teorji wielkości rzeczywistych.* Wedle E. v. Huntingtona teorja ta powstaje w następujący sposób (aksjomatyczny):

(I) Obieramy: pewną *klasę* C, *dwa działania* „$\bigcirc$“ i „$\square$“ (powiedzmy) i pewną *relację* R.

(II) Zakładamy, że dane te spełniają układ następujących związków:

II_1: $a, b \varepsilon C . \supset . a \bigcirc b \varepsilon C.$

II_2: $a, b \varepsilon C . \supset . a \bigcirc b = b \bigcirc a.$

II_3: $a, b, c \varepsilon C . \supset . (a \bigcirc b) \bigcirc c = a \bigcirc (b \bigcirc c).$

II_4: $a, b, b' \varepsilon C . a \bigcirc b = a \bigcirc b' : \supset : b = b'.$

II_5: Istnieje takie k, że $k \varepsilon C . k \bigcirc k = k.$

Df. Jeżeli istnieje *jedyny* taki element jak w II_5, to nazywamy go *zerem* systemu: $\widetilde{0}$.

II_6 : $a \varepsilon C : \supset :$ istnieje x, że $x \varepsilon C . a \bigcirc x = \widetilde{0}.$

II_7 : $a, b \varepsilon C . \supset . a \square b \varepsilon C.$

II_8 : $a, b \varepsilon C . \supset . a \square b = b \square a.$

II_9 : $a, b, c \varepsilon C . \supset . (a \square b) \square c = a \square (b \square c).$

II_{10}: $a, b, b' \varepsilon C . a \neq \widetilde{0} . a \square b = a \square b' : \supset : b = b'.$

II_{11}: $a, b, c \varepsilon C . \supset . a \square (b \bigcirc c) = (a \square b) \bigcirc (a \square c).$

II_{12}: Istnieje takie x, że $x \varepsilon C . x \neq \widetilde{0} . x \square x = x.$

Df. Jeżeli taki element jak w II_{12} istnieje *jedyny*, to nazywamy go *jedynką systemu:* $\widetilde{1}$.

II_{13}: $a \varepsilon C . a \neq \widetilde{0} : \supset :$ istnieje z takie, że $z \varepsilon C .$ $. a \square z = \widetilde{1}.$

II_{14}: $a, b \varepsilon C . a \neq b . \supset . a R b$ lub $b R a.$

II_{15}: $a, b \varepsilon C . a R b . \supset . a \neq b.$

II_{16}: $a, b, c \varepsilon C . a R b . b R c : \supset : a R c.$

II_{17}: Jeżeli M jest dowolną, niepustą podklasą klasy C i jeżeli w klasie C istnieje taki element c, że dla każdego elementu a podklasy M zachodzi związek $a R c$, w takim razie istnieje w klasie C element x taki, że:

(1) $a \varepsilon M . \supset . a R x$ lub $a = x$,

(2) $y \varepsilon C . y R x . \supset .$ istnieje takie z, że $z \varepsilon M .$ $. y R z.$

II_{18}: $a, x, y \varepsilon C . x R y . a \circ x \neq a \circ y : \supset :$ $: (a \circ x) R (a \circ y).$

II_{19}: $a, b \varepsilon C . \widetilde{0} R a . \widetilde{0} R b : \supset : \widetilde{0} R (a \square b).$

(III) Uważamy za *jedyne* i *wszystkie pojęcia* teorji te, które z pojęć $C, \circ, \square, R$ („pierwotnych" teorji) zdołamy skonstruować drogą *definicji logicznej*.

Uważamy za *jedyne* i *wszystkie* twierdzenia teorji te, które ze związków (postulatów teorji) II_1—II_{19} można uzasadnić drogą *dowodu logicznego*. [Obejmuje to również II_1—II_{19} jako twierdzenia teorji].

W teorji konstrukcyjnej liczb rzeczywistych *określamy* przy pomocy liczb wymiernych (naprz. metodą przekrojów Dedekinda) klasę q oraz pojęcia $+, \times, <$. Zadajmy sobie trud sprawdzenia, czy kładąc w miejsce $C, \circ, \square, R$ odpowiednio $q, +, \times, <$ uczynimy związkom II_1—II_{19} zadość? Tak, i w ten sposób uzyskujemy pewien *szczególny*

egzemplarz teorji abstrakcyjnej, który jest *naszą zwykłą teorją liczb rzeczywistych.*

A teraz przyjmijmy za C, $\bigcirc$, $\square$, R elementy: q_z, $+_z$, $\times_z$, $<_z$. Z łatwością sprawdzimy znowu postulaty II_1—II_{19} i otrzymamy znów *egzemplarz teorji;* tym razem *teorję wielkości rzeczywisto-zespolonych.*

Ustalmy teraz następującą odpowiedniość T między elementami klasy q a elementami zbioru q_z:

Jeżeli $a \varepsilon q$, niechaj odpowiednikiem elementu a w relacji T będzie:

$$T(a) = a_z = (a, 0).$$

Z łatwością spostrzeżemy, że odpowiedniość T jest *doskonała* (jedno-jednoznaczna) i że wyczerpuje z jednej strony wszystkie elementy klasy q, a z drugiej wszystkie elementy klasy q_z. Dzięki własnościom powyżej uzasadnionym mieć będziemy:

jeżeli $a, b \varepsilon q$, to:

(1) $T(a+b) = T(a) +_z T(b)$,

(2) $T(a \times b) = T(a) \times_z T(b)$,

(3) $a < b$ wtedy i tylko, gdy $T(a) <_z T(b)$.

Odpowiedniość T „zachowuje" zatem oba działania i relację „porządkującą".

Fakt ten wypowiemy w postaci następującej:

$$(q, +, \times, <) \text{ i } (q_z, +_z, \times_z, <_z)$$

są dwoma egzemplarzami abstrakcyjnej teorji *wielkości rzeczywistych,* **izomorfijnemi.** *Każde* twierdzenie teorji **abstrakcyjnej** da nam dwa odpowiednie twierdzenia — po jednym w każdym egzemplarzu — przyczem, aby przejść od jednego do drugiego wystarczyłoby usunąć znaczki odróżniające (z) lub przeciwnie, dołączyć je w odpowiednich miejscach.

W obrębie twierdzeń teorji abstrakcyjnej egzemplarze są *formalnie* nieodróżnialne. **Nie jest** atoli prawdą, że **każde** twierdzenie teorji $(q, +, \times, <)$ jest odpowiednikiem twierdzenia teorji $(q_z, +_z, \times_z, <_z)$: naprz. twierdzenie:

$$x \varepsilon q \,.\supset.\, (x, 0) \varepsilon q_z$$

takiem nie jest. Podobieństwo formalne odnosi się tylko do twierdzeń wypływających z założeń abstrakcyjnej teorji. O tem się często zapomina!

Zauważmy z **naciskiem,** że **żadna** wielkość r z e c z y w i s t o-z e s p o l o n a **nie** jest nigdy identyczna z żadną l i c z b ą rzeczywistą. Wracając do precyzyjnego określenia p a r y, widzimy przecież, że *para* liczb rzeczywistych nie może być *identyczna* z *liczbą* rzeczywistą.

Dzięki formalnemu podobieństwu stworzonemu przez *izomorfję* możemy jednak wprowadzić następującą *konwencję:*

Zarzucimy całkowicie dawny egzemplarz $(q, +, \times, <)$ i zastąpimy go *wszędzie* przez $(q_z, +_z, \times_z, <_z)$. W praktyce jednak nie będziemy pisali znaczka $(_z)$. Jest to tak zwana *symboliczna identyfikacja* wielkości rzeczywisto-zespolonych z rzeczywistemi (Hamilton).

O żadnej identyczności typu:

$$a = (a, 0)$$

niema tu oczywiście mowy. Byłby to absurd świadczący o niedostatecznej znajomości zawiłego dosyć pojęcia izomorfji i symbolicznej identyfikacji.

Ponieważ klasa q_z jest częścią klasy q_2, *nieidentyczną z całością*, możemy powiedzieć, że *wielkości zespolone* stanowią rozszerzenie zakresu wielkości

rzeczywisto-zespolonych. W myśl konwencji możemy to wypowiedzieć w postaci:

Liczby *zespolone* stanowią *rozszerzenie* zakresu **liczb** *rzeczywistych*.[1]

3. Dalsza rozbudowa teorji.

Niech będzie:

$$z \varepsilon q_2,\ p'z = a,\ k'z = b,\ (a, b \varepsilon q).$$

Zauważmy, że:

$$z = (a, b) = (a, 0) + (0, b) = (a, 0) \times (1, 0) + (b, 0) \times (0, 1).$$

Df. Nazwijmy dla z zespolonego:

(1) $(p'z, 0) \overset{\text{df}}{=}$ część rzeczywista liczby $z =$ pars realis $z = R'z$,

(2) $(k'z, 0) \overset{\text{df}}{=}$ część urojona liczby $z =$ pars imaginaria $z = I'z$.

(3) $(0, 1) \overset{\text{df}}{=} i$ („jednostka urojona“).

Otrzymamy twierdzenia:

Tw. Każda liczba zespolona z da się przedstawić w postaci:

$$z = a + bi, \text{ gdzie } a, b \varepsilon q.^2$$

Dem. Kładziemy:

$$z = R'z + I'z \,.\, i \text{ [piszemy „.“ zamiast „}\times\text{“]}$$
$$R'z,\ I'z \varepsilon q.$$

Tw. Jeżeli $z \varepsilon q_2$;

$$z = a + bi, \text{ gdzie } a, b \varepsilon q,$$

to:

$$a = R'z,\ b = I'z.$$

Dem. Pamiętając o konwencji wiemy, że: $z = a + bi, a, b \varepsilon q$ mówi właściwie, iż:

---

[1] i tylko w tym sensie!!

[2] a więc właściwie do q_z!!

$$z = a_z +_z b_z \times_z i = (a, 0) +_z (b, 0) \times (0, 1) =$$
$$= (a, b),\ a, b \varepsilon q.$$
$$z = R'z + I'z.i = (p'z, 0) +_z (k'z, 0) \times_z (0, 1)$$
$$= (p'z, k'z);$$

skąd: $p'z = a,\ k'z = b,\ R'z = (a, 0) = a_z,$
$I'z = (b, 0) = b_z,$

a więc symbolicznie:

$$R'z = a,\ I'z = b.$$

Df. Rozkład $z = a + bi$, gdzie $a, b \varepsilon q$, jedyny tego rodzaju, zwiemy rozkładem *kanonicznym liczby zespolonej* na część rzeczywistą a i „czysto urojoną“ bi.

Liczba z jest *rzeczywistą* wtedy i tylko, gdy $I'z = 0$; *czysto urojoną* wtedy i tylko, gdy $R'z = 0$.

D z i a ł a n i a: Sprawdzimy wedle reguł poprzednich: jeżeli $a, b, c, d \varepsilon q$, to:

(1) $(a + bi) + (c + di) = (a + c) + (b + d)i,$
(2) $(a + bi) - (c + di) = (a - c) + (b - d)i,$
(3) $(a + bi).(c + di) = (ac - bd) + (ad + bc)i.$

Ostatni związek otrzymamy łatwo, operując, tak jak w teorji liczb rzeczywistych, prawami mnożenia i dodawania, jeśli tylko zauważymy kapitalny związek: $i.i = -1.$

(4) Aby wykonać dzielenie:

$$\frac{a + bi}{c + di}$$ (przy założeniu, że $c \neq 0$ lub $d \neq 0$)

pomnożymy licznik i mianownik ilorazu przez $(c - di)$ $(\neq 0)$

$$\frac{a+bi}{c+di}=\frac{(a+bi)(c-di)}{(c+di)(c-di)}=\frac{(ac+bd)+(bc-ad)i}{c^2+d^2}$$

$$=\frac{ac+bd}{c^2+d^2}+\frac{bc-ad}{c^2+d^2}\,i.$$

Potęgi jednostki urojonej:

Sprawdźmy, że:

$$i^0=1,\ i^2=-1,\ i^3=-i,\ i^4=1.$$

Ogólniej:

$$i^{4n}=1,\ i^{4n+1}=i,\ i^{4n+2}=-1,\ i^{4n+3}=-i,$$
$$n=0,\pm 1,\pm 2,\ldots$$

Uw. Widzimy, że równanie:

$$x^2\stackrel{?}{=}-1 \qquad (\alpha)$$

posiada przynajmniej dwa rozwiązania w zakresie liczb zespolonych, a mianowicie:

$$i,\ -i.$$

Są to *jedyne* rozwiązania równania (α), gdyż (α) jest równoważne równaniu:

$$x^2+1\stackrel{?}{=}0$$

lub:

$$(x+i)(x-i)\stackrel{?}{=}0,$$

co da nam układ alternatyw:

$$x+i\stackrel{?}{=}0 \quad \textbf{lub} \quad x-i\stackrel{?}{=}0;$$

a więc odpowiedzi:

$$i,\ -i.$$

Uw. Fizycy i elektrotechnicy piszą często, dla uniknięcia nieporozumień, jednostkę zespoloną przy pomocy litery j.[1]

---

[1] u elektrotechników „i" oznacza zwyczajowo *natężenie prądu*.

4. **Reprezentacja geometryczna.**

I. Metoda Gaussa: Obierzmy w płaszczyźnie układ prostokątny osi $\overrightarrow{0x}$ i $\overrightarrow{0y}$. Nazwiemy oś $\overrightarrow{0x}$ *osią rzeczywistą*, $\overrightarrow{0y}$ *osią urojoną*. Reprezentantem liczby zespolonej z będzie *ten punkt* M płaszczyzny (xy), którego *odciętą* w układzie $(x0y)$ jest $R'z$, *rzędną* zaś $I'z$.

Punkt M o spółrzędnych (x, y) reprezentuje zatem naodwrót liczbę zespoloną:

$$z = x + yi.$$

Tak ustalona odpowiedniość między *punktami płaszczyzny*, a *liczbami zespolonemi* jest *doskonała*.

Powiadamy zwykle, że rozważamy liczby zespolone na „płaszczyźnie Gaussa".

Odmiankę powyższej reprezentacji stanowi:

II. Reprezentacja wektorjalna: Reprezentantem liczby zespolonej z będzie tu *wektor* $\overrightarrow{AB}$ o dowolnym początku A na płaszczyźnie $(x\,0\,y)$ i o *składowych*

$$R'z \text{ i } I'z.$$

Zazwyczaj za początek wektora obieramy początek układu. Zatem wektor $\overrightarrow{OM}$ jest reprezentantem liczby $z = x + yi$, gdy spółrzędnemi punktu M są x i y.

Konstrukcja sumy i różnicy liczb zespolonych.

Zważywszy, że:

$$\left.\begin{aligned}(a+bi)+(c+di) &= (a+c)+(b+d)i\\ (a+bi)-(c+di) &= (a-c)+(b-d)i\end{aligned}\right\} a, b, c, d \varepsilon q.$$

i biorąc pod uwagę elementarne wiadomości z geometrji analitycznej, otrzymamy konstrukcje.

Suma: W układzie $(x0y)$ obieramy wektor: $\overrightarrow{OM}$ o składowych a i b, następnie obieramy wektor $\overrightarrow{MP}$ o składowych c i d. Wtedy wektor *wypadkowy* $\overrightarrow{OP}$ reprezentuje *sumę:* $(a+bi)+(c+di)$.

Różnica: Obieramy $\overrightarrow{OM}$ o składowych a i b, następnie $\overrightarrow{ON}$ o składowych c i d. Wektor $\overrightarrow{NP}$ (który możemy przenieść później do początku O) reprezentuje różnicę $(a+bi)-(c+di)$.

III. Reprezentacja biegunowa.

Df. Nazwiemy *bezwzględną wartością* liczby zespolonej α *liczbę nieujemną,* daną przez wzór:

$$|\alpha| \overset{\text{df}}{=} \sqrt{(R'\alpha)^2+(I'\alpha)^2}.$$

Df. Nazwiemy *amplitudą* liczby zespolonej α *różnej od zera* $(\alpha \neq 0)$, **każdą** *liczbę* φ *rzeczywistą,* spełniającą związki:

$$\cos\varphi = \frac{R'\alpha}{|\alpha|}, \quad \sin\varphi = \frac{I'\alpha}{|\alpha|}.$$

Df. Nazwiemy *amplitudą* liczby zespolonej 0 *każdą liczbę rzeczywistą.*

Tw. (1) Każda liczba zespolona posiada określoną wartość bezwzględną. Wartość ta jest liczbą rzeczywistą, nieujemną.

(2) $|0|=0$ i odwrotnie.

(3) $|\alpha+\beta| \leqq |\alpha|+|\beta|$, $(\alpha, \beta$ zespolone).

(4) $|\alpha-\beta| \geqq |\alpha|-|\beta|$ „ „

(5) $|\alpha.\beta|=|\alpha|.|\beta|$ (α,β zespolone),

(6) $\left|\frac{\alpha}{\beta}\right|=\frac{|\alpha|}{|\beta|}\cdot(\beta\neq 0$ α,β zespolone).

Dem. Kładziemy: $\alpha=a+bi$, $\beta=c+di$, $a,b,c,d\,\varepsilon\,q$.

(1) $|\alpha|=\sqrt{a^2+b^2}$, co posiada sens i jest $\geqq 0$.

(2) wtedy $a=0$, $b=0$ $|\alpha|=\sqrt{0^2+0^2}=0$
i odwrotnie: $\sqrt{a^2+b^2}=0$ pociąga $a=b=0$, $\alpha=0$.

(3) $|\alpha+\beta|=\sqrt{(a+c)^2+(b+d)^2}\leqq$
$\leqq\sqrt{a^2+b^2}+\sqrt{c^2+d^2}=|\alpha|+|\beta|$,

co wynika z nierówności:

$$(ac+bd)^2\leqq(a^2+b^2)(c^2+d^2),$$

będącej następstwem *identyczności Lagrange'a:*
$(ac+bd)^2+(ad-bc)^2=(a^2+b^2)(c^2+d^2)$.

(4) Dzięki (3):

$$|\alpha-\beta|+|\beta|\geqq|\alpha-\beta+\beta|=|\alpha|,$$

skąd: $$|\alpha-\beta|\geqq|\alpha|-|\beta|.$$

(5) $|\alpha.\beta|=\sqrt{(ac-bd)^2+(ad+bc)^2}=$
$=\sqrt{(a^2+b^2)(c^2+d^2)}=|\alpha|.|\beta|$

dzięki *identyczności Lagrange'a.*

(6) Gdy $\beta\neq 0$, to $\frac{\alpha}{\beta}\cdot\beta=\alpha$ i $|\beta|\neq 0$, więc:
$\left|\frac{\alpha}{\beta}\right|\cdot|\beta|=|\alpha|$, skąd $\left|\frac{\alpha}{\beta}\right|=\frac{|\alpha|}{|\beta|}$.

Tw. (1) Każda liczba zespolona posiada nieskończenie wiele amplitud.

(2) Jeżeli φ_o jest amplitudą liczby α, różnej *od zera,* to *wszystkie* amplitudy liczby α są dane przez wzór: $\varphi = \varphi_0 + 2k\pi \quad k = 0, \pm 1, \pm 2, \ldots$

Dem. (1) Wystarczy okazać dla $\alpha \neq 0$, wtedy:

$$\left|\frac{a}{\sqrt{a^2+b^2}}\right| \leqq 1, \quad \left|\frac{b}{\sqrt{a^2+b^2}}\right| \leqq 1, \ (\alpha = a+bi, a, b \in q),$$

więc równania:

$$\cos\varphi \overset{?}{=} \frac{a}{\sqrt{a^2+b^2}}, \quad \sin\varphi \overset{?}{=} \frac{b}{\sqrt{a^2+b^2}}$$

posiadają nieskończenie wiele rozwiązań w liczbach rzeczywistych.

(2) z elementarnej trygonometrji.

Tw. (1) Jeżeli φ jest amplitudą α, ψ amplitudą β, to $\varphi + \psi$ jest amplitudą $\alpha.\beta$.

(2) Jeżeli φ i ψ są odpowiednio amplitudami dla α i β, przyczem $\beta \neq 0$, to $\varphi - \psi$ jest jedną z amplitud ilorazu $\frac{\alpha}{\beta}$.

Dem. (1) Załóżmy $\alpha \neq 0$ i $\beta \neq 0$, $\alpha = a+bi$, $\beta = c+di$, $a, b, c, d \in q$.

$$\cos\varphi = \frac{a}{\sqrt{a^2+b^2}}, \quad \sin\varphi = \frac{b}{\sqrt{a^2+b^2}},$$

$$\cos\psi = \frac{c}{\sqrt{c^2+d^2}}, \quad \sin\psi = \frac{d}{\sqrt{c^2+d^2}}.$$

Stąd:

$$\cos(\varphi+\psi) = \frac{ac-bd}{|\alpha\beta|}, \quad \sin(\varphi+\psi) = \frac{ad+bc}{|\alpha\beta|},$$

co dowodzi twierdzenia.

Uzupełnimy z łatwością dowód w wypadkach, gdy $\alpha = 0$ lub $\beta = 0$.

(2) Dowód analogiczny.

Uw. W przypadku liczby zespolonej różnej od zera, amplitudy są miarami kąta, jaki tworzy kierunek dodatni osi rzeczywistej z kierunkiem wektora $\overrightarrow{OM}$, reprezentującego naszą liczbę. Sprawa mierzenia kątów w sensie uogólnionym jest omówiona szczegółowo w t. I. znakomitego *Zarysu Mechaniki Teoretycznej,* prof. St. Zaremby (Kraków 1933).

Konstrukcja iloczynu i ilorazu.

Iloczyn. Twierdzenia poprzednie dowodzą, że jeżeli φ i ψ są odpowiednio amplitudami dla α i β, to obracając w kierunku dodatnim wektor o początku w O, reprezentujący liczbę 1, o kąt $\varphi + \psi$ i odcinając na jego nowym kierunku wielkość $|\alpha| . |\beta|$, otrzymamy punkt M taki, że $\overrightarrow{OM}$ reprezentuje iloczyn $\alpha . \beta$.

Iloraz ($\beta \neq 0$). Obracamy wektor jednostkowy osi rzeczywistej o kąt $\varphi - \psi$ i odcinamy na nim wielkość $|\alpha| : |\beta|$.

Nowa postać kanoniczna liczby zespolonej.

Niechaj α będzie liczbą zespoloną. Oznaczmy:

$$r = |\alpha|, \quad \varphi = \text{jedna z amplitud } \alpha.$$

Wtedy: $$\alpha = r(\cos\varphi + i \sin\varphi).$$

Jeżeli $|\alpha| = 1$, to:

$$\alpha = \cos\varphi + i \sin\varphi.$$

Geometrja analityczna. Biorąc pod uwagę wszystkie trzy reprezentacje geometryczne, możemy całą geometrję analityczną na płaszczyźnie wysłowić

w języku liczb zespolonych. Jest to niekiedy bardzo wygodne. Zauważmy jedynie kilka możliwości:

1. Wielkość $|\alpha - \beta|$ reprezentuje *odległość* punktów M i N przedstawiających α i β.

2. Równanie *koła* o środku (a, b) i promieniu r ma postać:

$$|z - \alpha| \overset{?}{=} r, \text{ gdzie } \alpha = a + bi.$$

3. $|z - \alpha| < r$ względnie $|z - \alpha| > r$

reprezentują *wnętrze* względnie *zewnętrze* naszego koła.

4. Równanie *parametryczne prostej* ma postać:

$$\left.\begin{matrix} z \overset{?}{=} \alpha + \beta t \\ t \varepsilon q \end{matrix}\right\} [\alpha, \beta \text{ zespolone}. \beta \neq 0].$$

Uw.! *Żmurko* [Wykłady Matematyki, Lwów] i *Puzyna* [Teorja Funkcyj Analitycznych, Lwów 1900] wprowadzają oznaczenie:
$\alpha = r_\varphi$, gdzie $r = |\alpha|$, φ jest amplitudą liczby α, co czytają „*r z obrotem* φ“.

5. Liczby sprzężone.

Df. Liczbą sprzężoną do zespolonej α jest z definicji:

$$\bar{\alpha} \overset{df}{=} R'\alpha - I'\alpha . i.$$

Reprezentacja geometryczna. Jeżeli $\overrightarrow{OM}$ reprezentuje liczbę α, to $\overrightarrow{OM'}$, gdzie M' jest punktem symetrycznym do M wobec osi rzeczywistej, reprezentuje sprzężoną $\bar{\alpha}$.

Czytelnik udowodni z łatwością następujące elementarne twierdzenia, gdzie α i β oznaczają liczby zespolone:

Tw. 1. $\alpha \varepsilon q_2 . \supset . \bar{\alpha} \varepsilon q_2$.

2. $\bar{\bar{\alpha}} = \alpha$.

3. $\alpha = \bar{\alpha} . \supset . \alpha \varepsilon q$ i odwrotnie.

4. $\overline{\alpha + \beta} = \bar{\alpha} + \bar{\beta}$.

5. $\overline{\alpha - \beta} = \bar{\alpha} - \bar{\beta}$.

6. $\overline{\alpha . \beta} = \bar{\alpha} . \bar{\beta}$.

7. $\overline{\left(\frac{\alpha}{\beta}\right)} = \frac{\bar{\alpha}}{\bar{\beta}}$ $\quad (\beta \neq 0!)$.

8. $\overline{\alpha^n} = (\bar{\alpha})^n$ $\quad (n$ całkowite, a gdy $n < 0$, to $\alpha \neq 0)$.

9. $|\bar{\alpha}| = |\alpha|$.

10. $\alpha . \bar{\alpha} = (R'\alpha)^2 + (I'\alpha)^2 \overset{\text{df}}{=}$ *„norma“* α.

§ 3. Funkcje zespolonej zmiennej.

1. **Zbiory liczb zespolonych.** Mając na oku geometryczną reprezentację Gaussa liczb zespolonych, w której *liczbom* odpowiadają *punkty* na płaszczyźnie, mówimy o *zbiorach* liczb zespolonych, a więc o zbiorach A takich, że:

$$A \subset q_2, \quad [„\subset“ = \text{zawiera się}]$$

jako o zbiorach *„punktów“* na płaszczyźnie.

Df. *Otoczeniem* „punktu“ (l. zesp.) α nazwiemy *wnętrze* każdego koła o środku w α i promieniu dodatnim, a więc każdy zbiór określony przez nierówność:

$$|z - \alpha| < r \qquad (r > 0).$$

Sąsiedztwem punktu α nazwiemy każdy zbiór,

który powstał z *otoczenia* punktu α przez wyjęcie zeń samego punktu α, dany zatem przez:

$$0 < |z - \alpha| < r \qquad (r > 0).$$

Df. Jeżeli A jest zbiorem liczb zespolonych, to punkt z nazwiemy jego *punktem skupienia*, gdy w *każdem otoczeniu* punktu z znajduje się *nieskończenie* wiele punktów *należących* do zbioru A.

Df. Jeżeli A jest zbiorem liczb zespolonych, to z nazwiemy jego *punktem wewnętrznym*, gdy istnieje takie *otoczenie* punktu z, które *całkowicie zawiera się* w zbiorze A.

Czytelnik znający moją Teorję Mnogości Punktowych [Nr. 2 bibljoteczki niniejszej] zauważy, że definicje powyższe są, po ustaleniu pojęcia otoczenia, przeniesione dosłownie z wypadku linjowych zbiorów na zbiory płaszczyźniane liczb zespolonych. Czytelnik zechce na podstawie tej książeczki przenieść i odpowiednio zainterpretować wszystkie umowy i twierdzenia tej książeczki w sposób zupełnie analogiczny, o ile są one tam zaznaczone gwiazdką (*).

2. Funkcje.

Df. Pojęcie *funkcji* jest tu zupełnie analogiczne do tego, które czytelnik zna z teorji rzeczywistej zmiennej. Przez funkcję f zmiennej z rozumiemy *przepis* (operator), który każdej liczbie określonego zbioru liczb zespolonych, zwanego *polem* funkcji, przypisuje odpowiednio określoną liczbę zespoloną $f(z)$. Liczby $w = f(z)$ otrzymane w ten sposób tworzą, gdy z przebiega *pole* funkcji, zbiór zwany *zapasem* (wartości) funkcji f.

Ponieważ liczby tworzące pole jak i tworzące zapas funkcji są tu rozłożone na płaszczyźnie Gaussa, więc wygodne pojęcie wykresu na płaszczyźnie, tak pożyteczne w teorji rzeczywistej zmiennej, zawodzi tu całkowicie. Posługujemy się, od biedy, *dwiema* płaszczyznami: płaszczyzną, powiedzmy, „z — *tów*“ i płaszczyzną „w“, przyczem na pierwszej wynotujemy wszystkie punkty z *pola* funkcji, a na drugiej odnośne wartości $w = f(z)$ *zapasu*. Funkcję *dwu* lub *więcej* zmiennych zespolonych określamy w sposób analogiczny.

W dalszym ciągu ustalimy kilka pojęć z dziedziny funkcyj zespolonych jednej zmiennej; czytelnik przeniesie je sam z łatwością na wypadek kilku zmiennych.

Df. Powiadamy, że funkcja f, przy z dążącem do z_0, zdąża do wartości A, gdy:

(1) z_0 należy do punktów skupienia pola $P(f)$ funkcji,

(2) do każdego $\varepsilon > 0$ można dobrać $\delta > 0$ tak, że skoro:

z należy do pola $P(f)$

$$\text{i} \quad 0 < |z - z_0| < \delta,$$

to już: $$|f(z) - A| < \varepsilon.$$

Uw. Jest to, podobnie jak i inne, definicja wzorowana całkowicie na analogicznej dla funkcyj rzeczywistej zmiennej.

Df. Powiadamy, że $f(z)$ zdąża do ∞, gdy z zdąża do z_0, o ile:

(1) z_0 należy do punktów skupienia pola funkcji,

(2) do każdego $R > 0$ dobrać można $\varepsilon > 0$, tak iż, skoro:

$$z \varepsilon P(f) \text{ i } 0 < |z - z_0| < \varepsilon,$$

to już: $$|f(z)| > R.$$

Uw. Definicja *ta nie jest analogiczną* do definicji w wypadku rzeczywistej zmiennej, odpowiada ona raczej wypadkowi:

$$\lim_{x|x_0} |f(x)| = +\infty$$

gdyby $f(x)$, jak i x były stale rzeczywiste.

Df. Funkcja f jest *ciągła* w punkcie z_0, gdy: $$\lim_{z|z_0} f(z) = f(z_0).$$

Df. O ile założymy jeszcze w wypadku granicy, że funkcja f jest określona w *sąsiedztwie* punktu z_0, a w wypadku *ciągłości* w *otoczeniu* tegoż punktu, to mamy do czynienia z granicą czy ciągłością w sensie *„zwyczajnym"*.

Czytelnik przełoży teraz znane mu z Analizy rzeczywistych zmiennych twierdzenia o granicy i ciągłości na język Analizy zespolonej.

3. Ciągi. Szeregi.

Df. Prostym wypadkiem funkcji jest t. zw. *ciąg*, to znaczy funkcja, której polem jest zbiór liczb całkowitych:

$$0, 1, 2, \ldots$$

[ew. zbiór całkowitych od pewnej dopiero począwszy], a wartościami liczby zespolone, powiedzmy:

$$u_0, u_1, u_2, \ldots$$

Df. Orzeczenie, że:

$$\lim_{k|\infty} u_k = A$$

oznacza, że do każdej liczby $\varepsilon > 0$ można dobrać

całkowite n_0 tak, by związki:

$$k \geqq n_0 \text{ i } k \text{ jest całkowite}$$

pociągały stale:

$$|u_k - A| < \varepsilon.$$

Df. Orzeczenie:

$$\lim_{k|\infty} u_k = \infty$$

oznacza:

do każdej liczby $R > 0$ można dobrać całkowite n_0 tak, że związki:

$$k \text{ jest całkowite i } k \geqq n_0$$

pociągają stale:

$$|u_k| > R.$$

Uw. Odpowiadałoby to znowu w rzeczywistych zmiennych wypadkowi:

$$\lim_{k|+\infty} |u_k| = +\infty.$$

Tw. Warunkiem koniecznym i dostatecznym, by:

$$\lim_{k|\infty} u_k = A$$

jest:

$$\lim_{k|\infty} R' u_k = R'A \text{ i } \lim_{k|\infty} I' u_k = I'A.$$

Dem. (1) *Konieczność.* Nb. $\varepsilon > 0$, obieramy n_0 całkowite tak, że związki:

$$k \geqq n_0, \ k \text{ całkowite}$$

pociągają: $|u_k - A| < \varepsilon$

stąd: $\sqrt{(R'u_k - R'A)^2 + (I'u_k - I'A)^2} < \varepsilon,$

co pociąga, że:

$$|R'u_k - R'A| < \varepsilon \text{ i } |I'u_k - I'A| < \varepsilon.$$

Stąd już:

$$\lim_{k|\infty} R'u_k = R'A \text{ i } \lim_{k|\infty} I'u_k = I'A.$$

(2) *Dostateczność.* Założywszy, że:

$$\lim_{k|\infty} R'u_k = R'A; \lim_{k|\infty} I'u_k = I'A \text{ i } \varepsilon > 0,$$

obierzmy n_0 całkowite tak, by związki:

$$k \geqslant n_0, \ k \text{ całkowite}$$

pociągały:

$$|R'u_k - R'A| < \frac{\varepsilon}{\sqrt{2}} \text{ i } |I'u_k - I'A| < \frac{\varepsilon}{\sqrt{2}},$$

Da nam to:

$$|u_k - A| < \varepsilon.$$

Stąd: $\lim_{k|\infty} u_k = A.$

Df. Szereg zespolony:

Symbol: $u_0 + u_1 + u_2 + \ldots$

oznacza:

(1) albo *ciąg:* $u_0, u_0 + u_1, u_0 + u_1 + u_2, \ldots$

(2) lub *granicę* ciągu:

$$u_0, u_0 + u_1, u_0 + u_1 + u_2 \ldots$$

w wypadku, gdy granica ta ma sens.

Uw. Pojmowanie *podwójne* sensu symbolu szeregu jest uświęcone przez tradycję; nie odpowiada ono w zupełności nowoczesnym tendencjom, aby każdy symbol oznaczał *tylko jedno* pojęcie.

Df. Szereg: $u_0 + u_1 + \ldots$

jest *bezwzględnie zbieżny*, gdy *zbieżnym* jest szereg (rzeczywisty):

$$|u_0| + |u_1| + |u_2| + \ldots$$

A teraz czytelnik przeniesie znowu z łatwością

główne twierdzenia z teorji szeregów rzeczywistej zmiennej na wypadek zespolony.

4. **Funkcje:** e^z, $\cos z$, $\sin z$.

Df. Szeregi:

$$1+\frac{z}{1!}+\frac{z^2}{2!}+\frac{z^3}{3!}+\dots$$

$$1-\frac{z^2}{2!}+\frac{z^4}{4!}-+\dots$$

$$z-\frac{z^3}{3!}+\frac{z^5}{5!}-+\dots$$

są *bezwzględnie zbieżne dla każdej wartości* zespolonej z. Określają one trzy funkcje o polu $=q_2$, które przez analogję oznaczymy symbolami:

$$e^z, \cos z, \sin z.$$

Przez klasyczne mnożenie szeregów (ważne w stosunku do naszych szeregów) otrzymamy dla tych funkcyj trzy fundamentalne związki:

(1) $e^z \cdot e^{z'} = e^{z+z'}$,

(2) $\cos(z+z') = \cos z \cos z' - \sin z \cdot \sin z'$,

(3) $\sin(z+z') = \sin z \cos z' + \cos z \cdot \sin z'$

ważne dla wszelkich z i z' zespolonych. Są one, jak wiadomo z teorji funkcyj rzeczywistych zmiennych, podstawą do uzyskania rozlicznych innych identyczności.

5. **Formuły:** *De Moivre'a* i *Eulera.*

Niechaj będzie φ *rzeczywiste,*

$$e^{\varphi i} = 1+\frac{\varphi i}{1!}-\frac{\varphi^2}{2!}-\frac{\varphi^3 i}{3!}+\frac{\varphi^4}{4!}+\frac{\varphi^5 i}{5!}+\dots$$

$$\cos\varphi = 1 - \frac{\varphi^2}{2!} + \frac{\varphi^4}{4!} - + \dots$$

$$\sin\varphi = \varphi - \frac{\varphi^3}{3!} + \frac{\varphi^5}{5!} - + \dots,$$

więc:

$$\cos\varphi + i\sin\varphi = \left(1 + \frac{\varphi i}{1!}\right) + \left(-\frac{\varphi^2}{2!} - \frac{\varphi^3 i}{3!}\right) +$$

$$+ \left(\frac{\varphi^4}{4!} + \frac{\varphi^5 i}{5!}\right) + - \dots$$

Zważywszy, że szeregi są (bezwzględnie) zbieżne, możemy rozwiązać nawiasy:

$$\cos\varphi + i\ \sin\varphi = 1 + \frac{\varphi i}{1!} - \frac{\varphi^2}{2!} - \frac{\varphi^3 i}{3!} +$$

$$+ \frac{\varphi^4}{4!} + \frac{\varphi^5 i}{5!} + - \dots = e^{\varphi i}.$$

Zatem:

Tw. Dla każdego φ rzeczywistego mamy:

$$e^{\varphi i} = \cos\varphi + i\sin\varphi.$$

[Euler].

Uw. Stąd: $|e^{\varphi i}| = 1 \qquad (\varphi \in q).$

Dzięki związkowi fundamentalnemu dla e^z otrzymamy:

$$(e^z)^m = e^{mz} \quad (m \textit{ całkowite}).$$

Stąd: $(e^{\varphi i})^m = e^{m\varphi i} \qquad (\varphi \in q).$

Ostatecznie:

Tw. Dla każdego φ rzeczywistego i m całkowitego mamy:

$$(\cos\varphi + i\sin\varphi)^m = \cos m\varphi + i\sin m\varphi.$$

[De Moivre].

Uw. Związek de Moivre'a zachodzi dla wszelkich m rzeczywistych, lecz to nam jest niepotrzebne.

Uw. Jeżeli $|\alpha| = r$ i φ jest amplitudą liczby α, to

$$\alpha = re^{\varphi i} \qquad \text{[p. § 2, ust. 4]}.$$

Zauważmy związki:

$$e^0 = 1,\ e^{\frac{1}{2}\pi i} = +i,\ e^{\pi i} = -1,\ e^{\frac{3}{2}\pi i} = -i,\ e^{2\pi i} = 1.$$

6. **Pochodne.** Określamy pochodną funkcji zespolonej zmiennej zupełnie tak, jak w analizie rzeczywistych zmiennych.

Df. Pochodną funkcji f w punkcie z_0 jest granica:

$$\lim_{h|0} \frac{f(z_0+h) - (z_0)}{h},$$

gdzie oczywiście h przebiega wartości zespolone. Analogicznie określamy wyższe pochodne względnie cząstkowe pochodne czy różniczki zupełne funkcyj wielu zmiennych.

Dzięki zachowaniu się klasycznych własności granicy, czytelnik przeniesie z łatwością znane mu elementarne twierdzenia o pochodnej sumy, różnicy, iloczynu, ilorazu, funkcji złożonej i odwrotnej na wypadek zespolonej zmiennej czy zmiennych.

Zachodzi jednak kapitalna różnica między funkcjami rzeczywistej a zespolonej zmiennej: Jeżeli założymy mianowicie, że funkcja *zespolona* $f(z)$ posiada pochodną w otoczeniu pewnego punktu z_0, to fundamentalnego znaczenia twierdzenie, pochodzące od Cauchy'ego powiada, że w tem otoczeniu *będzie ona posiadała wszystkie pochodne*

wszystkich rzędów!! Nie dość na tem! Będzie ona *w otoczeniu punktu* z_0 rozwijalna *na szereg Taylora* o środku w z_0, to znaczy szereg:

$$f(z) = \alpha_0 + \alpha_1 (z - z_0) + \alpha_2 (z - z_0)^2 + \dots$$

Szereg ten będzie zbieżny bezwzględnie wewnątrz pewnego koła $|z - z_0| < r$ $(r > 0)$ o promieniu *przynajmniej tak wielkim,* by koło to *zmieściło się* jeszcze w danem *nam otoczeniu punktu* z_0.

Dowód tego fundamentalnego twierdzenia odszukać trzeba w traktatach *funkcyj analitycznych* (tak się bowiem nazywają funkcje rozwijalne w szereg Taylora). Z pośród niezliczonej ilości książek zajmujących się tym tematem cytuję małą, lecz bardzo piękną książeczkę K. Knoppa: Funktionentheorie (2 tomiki Sammlung Göschen).

Szereg:

$$f(z) = \alpha_0 + \alpha_1 (z - z_0) + \alpha_2 (z - z_0)^2 + \dots$$

ważny, powiedzmy, dla $|z - z_0| < r$, można różniczkować dowolnie wiele razy wyraz po wyrazie tak, że:

$$f'(z) = \alpha_1 + 2\alpha_2 (z - z_0) + 3\alpha_3 (z - z_0)^2 + \dots$$
$$f''(z) = 2\alpha_2 + 2 \cdot 3\, \alpha_3 (z - z_0) + \dots$$
$$\dots\dots\dots\dots\dots\dots\dots\dots$$

i wszystkie te związki ważne będą dla $|z - z_0| < r$. Stąd też, kładąc $z = 0$ otrzymamy:

$$f(z_0) = \alpha_0 \dots, f^{(n)}(z_0) = n!\, \alpha_n \qquad n = 1, 2, 3, \dots$$

Uw. Zwykle mówimy, że sama funkcja f jest swą pochodną *rzędu zero* $f^{(0)}(z) = f(z)$, wtedy związki powyższe zapiszemy krótko:

$$f^{(n)}(z_0) = n!\, \alpha_n \qquad n = 0, 1, 2, \dots$$

Uw. Kładąc $z - z_0 = h$ dostaniemy szereg:

$$f(z_0 + h) = f(z_0) + \frac{f'(z_0)}{1!} h + \frac{f''(z_0)}{2!} h^2 + \ldots,$$

ważny dla $|h| < r$.

Rozdział II.

Wielomiany.

§ 1. Jednomiany i Wielomiany.

1. Jednomiany jednej zmiennej.

Df. Jednomianem zmiennej zespolonej z nazywamy każdą funkcję f zmiennej z, dla której znajdzie się liczba zespolona a i całkowita nieujemna n, taka, że:

$$f(z) \equiv a z^n.$$

Uw. Równoważność ($\equiv$) funkcyj f i g oznacza, że (1) f i g mają to samo *pole określenia* (sensu) i (2) w obrębie (wspólnego) pola stale $f(z) = g(z)$.

Uw. $f(z)$ oznacza *wartość* funkcji f dla *wartości argumentu* z. Znakiem *funkcji* (przepisu) jest f lub, jeżeli, jak to się zdarza w wyrażeniach złożonych, trudno nam odrzucić zmienną z, znakiem funkcji będzie u nas $f(\hat{z})$ {„gaszenie zmiennej"}. *Nie jest to* znakowanie *powszechnie* przyjęte, aczkolwiek z wielką niejednokrotnie szkodą dla jasności i poprawności logicznej. Będziemy z niego korzystali w wypadkach budzących obawę nieporozumienia.

Uw. Postać $a\hat{z}^n$ nie jest *jedyną* postacią jednomianu danego, mamy przecież równie dobrze naprz.:

$$a z^n \equiv a z^n + e^z - e^z.$$

Uw. Począwszy od obecnego rozdziału oznaczać będziemy liczby zespolone najczęściej małemi literami łacińskiego alfabetu.

Tw. Jeżeli $az^n \equiv bz^m$

(a, b zespolone, n, m całk. $\geqq 0$),

to albo: $a = b = 0$

lub: $a \neq 0, b \neq 0, a = b$ i $n = m$.

Dem. 1. Jeżeli $a = b = 0$, to twierdzenie słuszne. Załóżmy $a \neq 0$, to dla $z = 1$ otrzymamy: $a = b$, więc $b \neq 0$ i $z^n \equiv z^m$.

Kładziemy naprz. $z = 2$, skąd:

$$2^n = 2^m,$$

więc: $2^{n-m} = 1, n - m = 0, n = m$.

Tw. Jeżeli $az^n \equiv 0$, to $a = 0$.

Tw. Jednomian zmiennej z albo jest *identycznie zerem* lub ma postać $a\hat{z}^n$, gdzie $a \neq 0$, $n \geqq 0$ całkowite, przyczem a i n są jedynemi tego rodzaju.

Df. Jeżeli jednomian nie jest *zerowym* (identycznie zerem), to wykładnik n (całkowity, $\geqq 0$) nazywa się jego *stopniem*. Jednomian *zerowy nie posiada* stopnia.

Df. W jednomianie niezerowym:

$$a\hat{z}^n$$

nazywamy a *spółczynnikiem*, $\hat{z}^n$ *zasadą* jednomianu.

Df. Jednomiany az^n i bz^m są *podobne*, gdy mają identyczne *zasady*, a więc gdy $n = m$.

Tw. Suma, różnica jednomianów *podobnych* jest jednomianem podobnym do swych składników lub zerowym.

Dem. $az^n \pm bz^n \equiv (a \pm b)z^n$ (redukcja).

Tw. Iloczyn jednomianu przez stałą jest jednomianem podobnym do danego lub zerowym.

Dem. $k \,.\, az^n = (ka)z^n$.

Tw. Iloczyn jednomianów jest jednomianem, który jest zerowym wtedy i tylko, gdy choć jeden z czynników był identycznie zerem.

Dem. $az^n \,.\, bz^m \equiv (ab)z^{n+m}$.

Gdyby $(ab)z^{n+m} \equiv 0$, to $ab = 0$, skąd $a = 0$ lub $b = 0$, więc $az^n \equiv 0$ lub $bz^m \equiv 0$.

Odwrotnie: $az^n \equiv 0$ lub $bz^m \equiv 0$ pociągają odpowiednio: $a = 0$ lub $b = 0$, skąd $(ab)z^{n+m} \equiv 0$.

Uw. Wkracza tu zasadnicze prawo arytmetyki liczb zespolonych:

$$ab = 0 \,.\equiv.\, a = 0 \text{ lub } b = 0!!$$

2. Wielomiany jednej zmiennej.

Df. Wielomianem zmiennej z zwiemy każdą funkcję równoważną *jednomianowi* lub sumie *skończonej* ilości *jednomianów* zmiennej z.

Jeżeli $f(z)$ jest wielomianem, wtedy istnieją liczby:

$$k_1, k_2, \ldots k_s \text{ zespolone}$$
$$\text{i } n_1, n_2, \ldots n_s \text{ całk.} \geqq 0$$

takie, że:

$$f(z) \equiv k_1 z^{n_1} + k_2 z^{n_2} + \ldots + k_s z^{n_s}.$$

Redukując jednomiany *podobne* (o ile takie istnieją) otrzymamy nakoniec:

(1) albo $f(z) \equiv 0$,

(2) albo $f(z) \equiv a_0 z^n + a_1 z^{n-1} + \ldots + a_n$,

gdzie: $a_0 \neq 0$, $a_0, a_1 \ldots a_n$ zespolone

n całkowite, $\geqq 0$.

[$a_1, a_2 \ldots a_n$ mogą być także zerami].

Stąd:

Tw. Każdy wielomian zmiennej z jest albo zerowym lub może być przedstawiony w postaci:

$$f(z) \equiv a_0 z^n + a_1 z^{n-1} + \ldots + a_n, \quad (*)$$

gdzie $a_0 \neq 0$, $a_0, a_1, \ldots a_n$ zespolone

n całk., $\geqq 0$.

Df. Postać (*) nazywamy *zredukowaną* postacią wielomianu *niezerowego*.

Tw. Każdy wielomian jest funkcją określoną dla całego q_2, ciągłą i dowolnie wiele razy różniczkowalną w całem q_2.

Dem. Z elementarnych własności funkcyj ciągłych i pochodnych.

Tw. Postać *zredukowana* wielomianu jest *jedyną*.

Dem. Zauważmy, że gdy:

$$f(z) \equiv a_0 z^n + a_1 z^{n-1} + \ldots + a_n,$$

$a_0, a_1 \ldots a_n$ zespolone, n całk. $\geqq 0$,

to:

$$f(0) = a_n, \frac{f'(0)}{1!} = a_{n-1}, \ldots \frac{f^{(n)}(0)}{n!} = a_0, f^{(n+k)}(0) = 0.$$

$$(k = 1, 2 \ldots)$$

Stąd: Jeżeli $f(z) \equiv 0$ musi być:

$$a_n = a_{n-1} = \ldots = a_0 = 0.$$

Jeżeli: $f(z) \equiv a_0 z^n + a_1 z^{n-1} + \ldots + a_n$, $a_0 \neq 0$

i $f(z) \equiv b_0 z^m + b_1 z^{m-1} + \ldots + b_m$

i gdyby: $m > n$, to:

$$a_n = b_m = f(0), \; a_{n-1} = b_{m-1} = \frac{f'(0)}{1!} \ldots$$

$$a_0 = b_{m-n} = \frac{f^{(n)}(0)}{n!}, \; b_{m-n+k} = f^{(n+k)}(0) = 0,$$

stąd: $f(z) \equiv b_{m-n} z^n + b_{n-m+1} z^{n-1} + \ldots + b_m$
przyczem: $b_{m-n} = a_0$, $b_{m-n+1} = a_1 \ldots$ $b_m = a_n$,
$b_{m-n} \neq 0$.

Uw. Jeżeli wielomian $f(z) \equiv \text{const} \neq 0$, to
$f(z) \equiv az^0 \equiv a$ $(a = \text{const} \neq 0)$,
zatem stopień f jest *zerem* (i odwrotnie).

Df. Stopniem wielomianu niezerowego nazywamy wykładnik n przy najwyższej potędze jego postaci *zredukowanej*. Wielomian identycznie zerowy *nie posiada stopnia.*

Umowa: Powiemy, że wielomian $f(z)$ jest *niższego* stopnia niż wielomian $g(z)$, gdy $g(z) \neq 0$ i $f(z) \neq 0$ i f ma stopień *niższy* niż g **lub** gdy $f(z) \equiv 0$ i $g(z) \neq 0$.[1]

Tw. Suma i różnica wielomianów $f(z)$ i $g(z)$, stopni n i m odpowiednio, jest wielomianem
(1) stopnia $p_1 = \max(n, m)$, gdy $n \neq m$,
(2) stopnia niższego lub równego $p = \max(n, m)$, gdy $n = m$.

Suma wielomianu stopnia n i wielomianu zerowego jest wielomianem stopnia n. Suma wielomianów zerowych jest wielomianem zerowym.

Dem. Przedstawimy f i g w postaci zredukowanej:

$$f(z) \equiv a_0 z^n + a_1 z^{n-1} + \ldots + a_n \,,\ a_0 \neq 0,$$
$$g(z) \equiv b_0 z^m + b_1 z^{m-1} + \ldots + b_m \,,\ b_0 \neq 0$$

i położmy naprz. $n > m$. Wtedy:

$$f(z) \pm g(z) \equiv a_0 z^n + \ldots + (a_{n-m} \pm b_0) z^m + \ldots$$
$$\ldots + (a_n \pm b_m)$$
$$a_0 \neq 0,$$

[1] Wygodną tę umowę przejąłem z *Perrona*, *Algebra*. Tom. I.

gdyby $n = m$, to

$f(z) \pm g(z) \equiv (a_0 \pm b_0) z^n + (a_1 \pm b_1) z^{n-1} \ldots (a_n \pm b_n)$,

przyczem $a_0 \pm b_0 \neq 0$ lub $a_0 \pm b_0 = 0$.

Reszta widoczna.

Tw. Iloczyn wielomianów stopni n i m odpowiednio, jest wielomianem stopnia $n + m$.

Dem. Nb. $f(z) \equiv a_0 z^n + \ldots + a_n$, $a_0 \neq 0$,

$g(z) \equiv b_0 z^m + \ldots + b_m$, $b_0 \neq 0$,

to $f(z)\, g(z) = a_0 b_0 z^{n+m} + (a_0 b_1 + a_1 b_0) z^{n+m-1} + \ldots$,

gdzie widocznie wyraz $a_0 b_0 z^{n+m}$ nie podlega redukcji i $a_0 b_0 \neq 0$.

Tw. Iloczyn wielomianu stopnia n przez liczbę stałą, różną od zera jest wielomianem stopnia n.

Dem. Liczba stała a $(\neq 0)$ jest identycznie równa wartościom wielomianu $a\hat{z}^0$ stopnia 0, stąd iloczyn jest stopnia $n + 0 = n$.

Uw. Mówi się wprawdzie dość często, że *liczba stała* a jest *identyczna* wielomianowi az^0 lecz *niesłusznie*. Wielomian az^0 — poprawniej $a\hat{z}^0$ — jest *funkcją* (przepisem, operatorem) i nie jest *liczbą!*

Tw. Wielomian $f(z)$ nie zerowy można zawsze „uporządkować wedle potęg $(z - a)$“, gdzie a jest dowolną zespoloną, w następujący sposób:

$$f(z) \equiv a_0 z^n + \ldots + a_n = a_0 [(z - a) + a]^n + \\ + a_1 [(z - a) + a]^{n-1} + \ldots + a_n \\ \equiv A_0 (z - a)^n + A_1 (z - a)^{n-1} + \ldots + A_n.$$

Wystarczy tylko rozwinąć potęgi:

$$[(z - a) + a]^k, \qquad k = 0, 1, 2 \ldots n$$

wedle dwumianu *Newtona*.

Z łatwością zauważymy, że:

$$A_n = f(a),\ A_{n-1} = \frac{f'(a)}{1!} \cdots \quad A_0 = \frac{f^{(n)}(a)}{n!}.$$

Tw. Jeżeli $f(z)$ jest wielomianem, to:

$$\lim_{z|\infty} f(z) = 0, \text{ gdy } f(z) \equiv 0.$$

$$\lim_{z|\infty} f(z) = a \neq 0, \text{ gdy } st'f = 0.$$

$$\lim_{z|\infty} f(z) = \infty, \text{ gdy } st'f > 0.$$

$[st'f = stopień\ f]$.

Dem. (1) widoczne, (2) również, gdyż wtedy:

$$f(z) \equiv \text{const} \neq 0,$$

(3): $f(z) \equiv a_0 z^n + a_1 z^{n-1} + \ldots + a_n,\ a_0 \neq 0,\ n > 0.$

Dla $z \neq 0$ mamy:

$$f(z) = a_0 z^n \left\{ 1 + \frac{a_1}{a_0 z} + \frac{a_2}{a_0 z^2} + \ldots + \frac{a_n}{a_0 z_n} \right\};$$

otóż:

$$\lim_{z|\infty} \frac{1}{z} = \lim_{z|\infty} \frac{1}{z^2} = \ldots = \lim_{z|\infty} \frac{1}{z^n} = 0,$$

a więc:

$$\lim_{z|\infty} f(z) = \lim_{z|\infty} a_0 z^n = \infty.$$

Uw. Definicja $\lim_{z|\infty} f(z)$ analogiczna do def. na str. 34—35.

3. *Wielomiany jednej zmiennej z punktu widzenia teorji funkcyj analitycznych.*

Rozważmy funkcję $f(z)$ *określoną w całej* płaszczyźnie q_2 i *posiadającą pochodną w każdym* punkcie tej płaszczyzny. Dzięki twierdzeniu cytowanemu wyżej będziemy tę funkcję mogli rozwinąć na szereg Taylora około punktu $z = 0$, a więc przedstawić ją jako:

$$f(z) = A_0 + A_1 z + A_2 z^2 + \ldots \qquad (1)$$

Szereg ten będzie bezwzględnie zbieżny w *każdem* kole zatoczonem z początku układu, gdyż funkcja $f(z)$ posiada

wszędzie pochodną. Zatem będzie on bezwzględnie zbieżny w całem q_2 i wszędzie wartością jego będzie $f(z)$. Funkcja analityczna powyższego rodzaju zwie się funkcją *całkowitą (entière)*. Spotkaliśmy już takie funkcje, a mianowicie: e^z, $\cos z$, $\sin z$ są właśnie tego rodzaju.

Lecz również i wielomian:

$$f(z) \equiv A_0 + A_1 z + \ldots + A_n z^n,$$

napisany w postaci:

$$f(z) \equiv A_0 + A_1 z + \ldots + A_n z^n + A_{n+1} z^{n+1} + \ldots,$$

gdzie: $A_{n+1} = A_{n+2} = \ldots = 0$

jest widocznie funkcją *całkowitą*.

Zauważmy, mimochodem, że rozwinięcie funkcji na szereg (1) jest *jedynem*, gdyż spółczynniki $A_0, A_1, A_2 \ldots$ są określone jednoznacznie przez to, iż:

$$A_n = \frac{f^{(n)}(0)}{n!} \qquad n = 0, 1, 2, \ldots$$

Otóż teorja funkcyj analitycznych klasyfikuje funkcje całkowite w następujący sposób.

I *wyp.* nie istnieje $\lim_{z|\infty} f(z)$.

Funkcja zwie się wtedy *przestępną*.

II *wyp.* $\lim_{z|\infty} f(z) = \infty$.

Teorja funkcyj udawadnia, że istnieje wtedy (jedyna) liczba naturalna n taka, że:

$$\lim_{z|\infty} \frac{f(z)}{z^n} \text{ jest liczbą } \neq 0.$$

III *wyp.* $\lim_{z|\infty} f(z) = a$, gdzie a jest liczbą zespoloną.

W tym wypadku t. zw. twierdzenie Liouville'a głosi, że: $f(z) \equiv \text{const.}$ Zatem:

$$f(z) \equiv f(0) = A_0.$$

Otóż, albo: $A_0 = 0$, wtedy $f(z) \equiv 0$,

lub: $A_0 \neq 0$, wtedy $f(z) \equiv A_0 \neq 0$ i $f(z)$ jest wielomianem stopnia zerowego.

W wypadku *drugim* analitycy mówią krótko, że $f(z)$ *„posiada biegun rzędu n w nieskończoności“*.

Zauważmy, że dla $z \neq 0$ mieć będziemy:

$$\frac{f(z)}{z^n} = \frac{A_0}{z^n} + \frac{A_1}{z^{n-1}} + \cdots + \frac{A_{n-1}}{z} + A_n + \\ + A_{n+1} z + A_{n+2} z^2 + \ldots$$

Nazwijmy:

$$g(z) \equiv A_{n+1} z + A_{n+2} z^2 + \ldots \qquad (2)$$

Będzie to znów funkcja całkowita, gdyż dla $z = 0$ szereg (2) jest oczywiście bezwzględnie zbieżny, a dla każdego $z \neq 0$ szereg $A_{n+1} z^{n+1} + A_{n+2} z^{n+2} + \ldots$ był bezwzględnie zbieżny, więc również:

$$A_{n+1} z + A_{n+2} z^2 + \ldots \qquad (3)$$

który powstał zeń drogą podzielenia przez z^n ($\neq 0$), będzie bezwzględnie zbieżny i wedle znanych własności szeregu potęgowego funkcja $g(z)$ będzie posiadała wszędzie pochodną.

Atoli, oznaczywszy przez a granicę:

$$\lim_{z|\infty} \frac{f(z)}{z^n} = a$$

otrzymamy:

$$\lim_{z|\infty} g(z) = \lim \left\{ \frac{f(z)}{z^n} - \frac{A_0}{z^n} - \frac{A_1}{z^{n-1}} - \cdots - A_n \right\} \\ = a - A_n .$$

Zatem, wedle twierdzenia Liouville'a:

$$g(z) \equiv \text{const} \equiv g(0) = 0.$$

Stąd: $A_{n+1} = A_{n+2} = \ldots = 0$ i:

$$\frac{f(z)}{z^n} = \frac{A_0}{z^n} + \frac{A_1}{z^{n-1}} + \cdots + A_n , \qquad (4)$$

dla każdego $z \neq 0$. Wtedy też:

$$f(z) \equiv A_0 + A_1 z + \ldots + A_n z^n ,$$

gdyż dla $z \neq 0$ słuszne wedle (4), a dla $z = 0$ jest $f(0) = A_0$.

Widzimy więc, że w wypadku drugim funkcja nasza jest *wielomianem stopnia n*. Z twierdzenia w poprzednim ustępie wynika, że *wielomian* posiada zawsze granicę dla $z \to \infty$, skończoną lub nie. Wobec tego możemy scharakteryzować wielomiany mówiąc:

Wielomian jest to funkcja analityczna całkowita, która posiada w nieskończoności *biegun* lub *granicę skończoną* („biegun rzędu zero“ moglibyśmy powiedzieć). Rząd bieguna daje nam *stopień* wielomianu za wyjątkiem, gdy wielomian jest identycznie zerem.

Z badania poprzedniego wynikają następujące konsekwencje:

(1) Funkcje: e^z, $\cos z$, $\sin z$ *nie są* wielomianami, ponieważ nieprawdą jest, by spółczynniki ich rozwinięcia na szereg Taylora około $z = 0$ (szereg Mac-Laurina) były od pewnego miejsca zerem.

(2) Nie istnieją granice (skończone ani nieskończone):

$$\lim_{z|\infty} e^z, \quad \lim_{z|\infty} \cos z, \quad \lim_{z|\infty} \sin z.$$

Uw. Dla rzeczywistych zmiennych:

$$\lim_{x|+\infty} e^x = +\infty, \quad \lim_{x|-\infty} e^x = 0,$$

ale w zespolonych niema granicy w nieskończoności.

4. Jednomiany wielu zmiennych.

Df. Jednomianem zmiennych $z_1, z_2, \ldots z_k$ nazywamy funkcję równoważną następującej:

$$a\hat{z}_1^{\alpha_1} \ldots \hat{z}_k^{\alpha_k},$$

gdzie: $a \varepsilon q_2$ i $\alpha_1, \ldots \alpha_k$ całkowite, $\geqq 0$.

Tw. Jeżeli:

$$a z_1^{\alpha_1} \ldots z_k^{\alpha_k} \equiv b z_1^{\beta_1} \ldots z_k^{\beta_k}$$

$$a, b \varepsilon q_2, \ \alpha_1 \ldots \alpha_k, \beta_1 \ldots \beta_k \text{ całk.} \geqq 0,$$

to (1) albo: $a = b = 0$,

(2) albo: $a \neq 0, b \neq 0, a = b$

i $\alpha_1 = \beta_1, \ldots \alpha_k = \beta_k$.

Dem. (1) Gdy $a = b = 0$ to, twierdzenie słuszne, załóżmy (2), że $a \neq 0$, wtedy dla $z_1 = z_2 = \ldots = z_k = 1$ otrzymamy: $a = b \neq 0$.

Kładąc: $z_1 = 1, \ldots z_{s-1} = 1, z_s = 2, z_{s+1} = 1, \ldots z_k = 1,$

dostaniemy: $2^{\alpha_s} = 2^{\beta_s}$, więc $\alpha_s = \beta_s$
dla: $s = 1, \ldots k.$

Tw. Jeżeli $a z_1^{\alpha_1} \ldots z_k^{\alpha_k} \equiv 0$, to $a = 0$ i odwrotnie.

Tw. Jednomian zmiennych $z_1, z_2, \ldots z_k$ jest albo *zerowym* (identycznie zerem) lub ma postać:

$$a z_1^{\alpha_1} \ldots z_k^{\alpha_k},$$

gdzie $a \neq 0$, $\alpha_1 \ldots \alpha_k$ całk. ≥ 0, wyznaczone jednoznacznie.

Df. *Stopniem* jednomianu *niezerowego* zmiennych $z_1, \ldots z_k$ *względem* zmiennej z_s $(s = 1, 2, \ldots k)$ nazywamy wykładnik α_s jego postaci (jedynej) typu:

$$a z_1^{\alpha_1} \ldots z_k^{\alpha_k}.$$

Rzędem lub *stopniem ogólnym* (względem wszystkich zmiennych) nazwiemy wtedy *sumę:*

$$m = \alpha_1 + \alpha_2 + \ldots + \alpha_k.$$

Jednomian *zerowy nie posiada* stopnia ani względem z_s ani ogólnego.

Df. W postaci $a\hat{z}_1^{\alpha_1} \ldots \hat{z}_k^{\alpha_k}$ $(a \neq 0)$ zwiemy a *spółczynnikiem*, $\hat{z}_1^{\alpha_1} \ldots \hat{z}_k^{\alpha_k}$ *zasadą* jednomianu. Jednomiany podobne mają identyczne zasady.

Tw. Suma, różnica, iloczyn jednomianów zmiennych $z_1 \ldots z_k$ są dalej jednomianami tych zmiennych.

Tw. *Stopień iloczynu* jednomianów niezerowych zmiennych $z_1, z_2, \ldots z_k$ jest równy *sumie* stopni czynników. [Stopień względem którejkolwiek z_s lub *ogólny*].

Dem. Elementarne, analogiczne jak w wypadku jednej zmiennej.

5. Uporządkowanie jednomianów.

Wprowadzimy za przykładem Gaussa pewien sposób uporządkowania jednomianów *niezerowych*.

Df. Jednomian: $f \equiv a z_1^{\alpha_1} \dots z_k^{\alpha_k} \quad (a \neq 0)$ będzie *niższego typu* niż:

$$g \equiv b z_1^{\beta_1} \dots z_k^{\beta_k} \quad (b \neq 0),$$

gdy w ciągu różnic:

$$(\beta_1 + \dots + \beta_k) - (\alpha_1 + \dots + \alpha_k),\ \beta_1 - \alpha_1, \dots \beta_k - \alpha_k$$

pierwsza, która *nie jest zerem ma wartość dodatnią*. Zapiszemy to: $f \prec g$.

Czytelnik uzasadni z łatwością następujące własności, odnoszące się *jedynie* do jednomianów *niezerowych*, zmiennych $z_1 \dots z_k$.

1. gdy rząd $f <$ rząd g, to $f \prec g$,
2. gdy rząd $f =$ rząd g i f nie jest *podobne* do g, to $f \prec g$ lub $g \prec f$,
3. $f \prec g$ wyklucza $g \prec f$,
4. $f \prec g$ i $g \prec h$ pociąga, że $f \prec h$,
5. $f \prec g$ pociąga, że $f . h \prec g . h$.

Przykład: (dla trzech zmiennych):

$$3 z_1^2 z_2 z_3 \prec z_1^5 z_2^2 z_3, \qquad 2 z_1^3 z_2 z_3 \prec z_1^3 z_2^2 z_3^0.$$

Uw. 1. Związki 1, 2 i 3 powodują, że relacja $\prec$ *porządkuje* w sensie *Cantora* każdą klasę złożoną z jednomianów tych samych zmiennych, *niepodobnych* między sobą.

2. Porządek ustalony przez relację $\prec$ zwie się też *leksykograficznym*, w podobny sposób porządkuje autor słownika wyrazy wedle następstwa alfabetycznego, nie zwraca jedynie uwagi na ilość

liter w słowie (co odpowiadałoby pominięciu rozważania różnicy $(\beta_1 + \ldots + \beta_k) - (\alpha_1 + \ldots \alpha_k)$.

6. **Wielomiany wielu zmiennych.**

Df. *Wielomianem* zmiennych $z_1 \ldots z_k$ zwiemy każdą funkcję równoważną jednomianowi lub sumie skończonej ilości jednomianów zmiennych $z_1 \ldots z_k$.

Jeżeli $f(z_1 \ldots z_k)$ jest wielomianem, to istnieje

(1) ciąg liczb zespolonych:

$$a_1, \ldots a_p, \qquad (p \text{ całkowite}, > 0),$$

(2) ciąg układów liczb całkowitych nieujemnych:

$$(\alpha_{11} \ldots \alpha_{1k}), \ldots \quad (\alpha_{p1} \ldots \alpha_{pk})$$
$$(k \text{ całkowite}, > 0)$$

takich, że:

$$f(z_1 \ldots z_k) \equiv \sum_{s|1}^{p} a_s z_1^{\alpha_{s1}} \ldots z_k^{\alpha_{sk}}.$$

Redukując jednomiany podobne dostaniemy nakoniec:

(1) albo: $f(z_1 \ldots z_k) \equiv 0$.

(2) albo:

$$f(z_1 \ldots z_k) \equiv A z_1^{\alpha_1} \ldots z_k^{\alpha_k} + B z_1^{\beta_1} \ldots z_k^{\beta_k} + \\ + \ldots + L z_1^{\lambda_1} \ldots z_k^{\lambda_k} \qquad (*)$$

$A, B, \ldots L \neq 0$, $\alpha_1 \ldots \alpha_k$, $\beta_1 \ldots \beta_k$, $\ldots \lambda_1 \ldots \lambda_k$ całkowite, $\geqslant 0$, przyczem jednomiany po stronie prawej *nie są* między sobą *podobne.*

Df. Postać $(*)$ poprzedniego twierdzenia nazywamy *zredukowaną* wielomianu *niezerowego.*

Tw. Każdy wielomian wielu zmiennych jest funkcją ciągłą i dowolnie wiele razy różniczkowalną dla wszelkich układów wartości zmiennych zespolonych występujących w wielomianie.

Tw. Postać *zredukowana* wielomianu jest *jedyną*.

Dem. Zauważmy, że gdy:

$$f(z_1 \dots z_k) = \sum_{s|1}^{p} A_s z_1^{\alpha_{s1}} \dots z_k^{\alpha_{sk}},$$

przyczem jednomiany $A_s z_1^{\alpha_{s1}} \dots z_k^{\alpha_{sk}}$ *nie są podobne* między sobą, to:

$$\alpha_{s1}! \dots \alpha_{sk}! \; A_s = \frac{\partial^{\alpha_{s1}+\dots+\alpha_{sk}} f(0, \dots 0)}{\partial z_1^{\alpha_{s1}} \dots \partial z_k^{\alpha_{sk}}}$$

$$(s = 1, 2 \dots p),$$

i widocznie A_s jak i układy $(\alpha_{s1} \dots \alpha_{sk})$ są wyznaczone jednoznacznie jako wartości pochodnych cząstkowych typu:

$$\frac{\partial^{\beta_1+\dots+\beta_k} f(0, \dots 0)}{\partial z_1^{\beta_1} \dots \partial z_k^{\beta_k}}$$

pod warunkiem, o ile wartości te są różne od zera.

Df. *Rzędem* lub *stopniem ogólnym* wielomianu $f(z_1 \dots z_k)$ jest najwyższy ze stopni jednomianów figurujących w postaci zredukowanej, o ile wielomian nie jest zerowy. Wielomian zerowy nie posiada rzędu. Stopniem $f(z_1 \dots z_k)$ względem z_s nazywa się analogicznie najwyższy ze stopni *względem* z_s jednomianów figurujących w postaci zredukowanej, o ile taka istnieje. Wielomian zerowy stopnia względem z_s nie posiada.

Tw. Wielomian $f(z_1 \dots z_k)$ posiadający postać zredukowaną *nie jest identycznie zerem.*

Dem. Wtedy bowiem choć jedna pochodna cząstkowa któregoś rzędu obliczona dla $z_1 = z_2 = \dots = z_k = 0$ nie jest zerem, co byłoby niemożliwem dla $f \equiv 0$.

Umowa. $f(z_1 \dots z_k)$ jest rzędu niższego od $g(z_1 \dots z_k)$, gdy (1) $f \not\equiv 0$ i rząd $f <$ rząd g lub (2) $f \equiv 0$, lecz $g \not\equiv 0$.

Tw. Gdy wielomian $f(z_1 \dots z_k) = \text{const} \neq 0$, to f posiada postać zredukowaną:

$$\text{const.}\, z_1^{0} \dots z_k^{0} \qquad (\text{const.} \neq 0)$$

i jest *rzędu zero.*

Df. *Wyrazem głównym* wielomianu *niezerowego* $f(z_1 \dots z_k)$ nazywa się ten jednomian jego postaci *zredukowanej*, który jest *najwyższego typu.*

Tw. Każdy wielomian niezerowy $f(z_1 \dots z_k)$ posiada określony główny człon.

Dem. W postaci zredukowanej mamy jedynie wielomiany *niepodobne* w skończonej ilości. Wśród nich istnieje określony najwyższego typu.

Tw. *Wielomian* niezerowy i jego *wyraz główny* mają ten sam *rząd.*

Tw. Suma, różnica i iloczyn wielomianów zmiennych $z_1 \dots z_k$ są dalej wielomianami tych zmiennych.

Dem. Z definicji wielomianu.

Tw. Rząd sumy (różnicy) wielomianów $f(z_1 \dots z_k)$ i $g(z_1 \dots z_k)$, gdzie $m =$ rząd f, $n =$ rząd g.

(1) równa się $\max(m, n)$, gdy $m \neq n$,

(2) równa się $\max(m, n)$ lub suma (różnica) jest rzędu niższego niż $\max(m, n)$, gdy $n = m$.

Dem. (1) Nb. naprz. $m > n$ oraz niechaj:

$$A z_1^{\alpha_1} \dots z_k^{\alpha_k}, \quad B z_1^{\beta_1} \dots z_k^{\beta_k}$$

oznaczają główne wyrazy dla f i g odpowiednio. Musi być $\alpha_1 + \dots + \alpha_k > \beta_1 + \dots + \beta_k$, więc wyraz $A z_1^{\alpha_1} \dots z_k^{\alpha_k}$ nie ulegnie w sumie (różnicy) redukcji.

Tw. Rząd iloczynu wielomianów $f(z_1 \dots z_k)$ i $g(z_1 \dots z_k)$, gdzie $m =$ rząd f, $n =$ rząd g, jest równy $m + n$.

Dem. Uzyskajmy iloczyn mnożąc wielomiany f i g w ich postaci zredukowanej. Niechaj $f_1 = A z_1^{\alpha_1} \dots z_k^{\alpha_k}$ i $g_1 = B z_1^{\beta_1} \dots z_k^{\beta_k}$ będą głównemi wyrazami wielomianów f czy g.

Dadzą one w iloczynie wyraz:

$$h_1 = A B z_1^{\alpha_1 + \beta_1} \dots z_k^{\alpha_k + \beta_k}.$$

Dla jakichkolwiek wyrazów f' i g' wziętych z postaci zredukowanych wielomianów f i g mamy:

$$f' \preceq f_1, \; g' \preceq g_1,$$

więc:

$$f' g' \preceq f_1 g' \preceq f_1 g_1 = h_1.$$

Jeżeli obierzemy $f' \prec f_1$, lub $g' \prec g_1$, to już $f' g' \prec h_1$, zatem wyraz h_1 nie posiada w iloczynie podobnego sobie i nie ulegnie redukcji. Będzie to przytem *wyraz główny* iloczynu.

Stąd: rząd $f.g =$ rząd $h_1 = (\alpha_1 + \dots + \alpha_k) + (\beta_1 + \dots + \beta_k) = m + n$.

7. **Różne sposoby przedstawiania** wielomianów wielu zmiennych.

Jeżeli napiszemy wielomian niezerowy w postaci *zredukowanej:*

$$f(z_1 \dots z_k) = A z_1^{\alpha_1} \dots z_k^{\alpha_k} + \dots + L z_1^{\lambda_1} \dots z_k^{\lambda_k},$$

to możemy zawsze dołączyć po prawej stronie dowolną ilość składników postaci:

$$O . z_1^{\sigma_1} \dots z_k^{\sigma_k}.$$

Jest to niekiedy przydatne ze względów na symetrję.

Jeżeli *typem* jednomianu $A z_1^{\alpha_1} \dots z_k^{\alpha_k}$ nazwiemy układ liczb $(\alpha_1 \dots \alpha_k)$, to wielomian $f(z_1 \dots z_k)$ na-

zwiemy *zupełnym* rzędu n, o ile w jego postaci zredukowanej figurują jednomiany *wszystkich możliwych typów rzędu* $\leqslant n$, to znaczy takich, że:

$$0 \leqq \alpha_1 + \ldots + \alpha_k \leqq n.$$

Rozważmy wielomian *niezerowy* $f(z_1 \ldots z_k)$, gdzie $k > 1$. Napiszmy go w postaci zredukowanej i zwróćmy uwagę na jedną z jego zmiennych, naprz. z_s. Łącząc ze sobą te wyrazy postaci zredukowanej, gdzie z_s figuruje w tej samej potędze (przez wyłączenie tej potęgi z_s za nawias) otrzymamy:

$$f(z_1 \ldots z_k) = f_1 . z_s^{\sigma_1} + \ldots + f_p . z_s^{\sigma_p},$$

gdzie: (1) $f_1, \ldots f_p$ są wielomianami zmiennych: $z_1, \ldots z_{s-1}, z_{s+1}, \ldots z_k$, *niezerowemi*,

(2) $\sigma_1 > \sigma_2 > \ldots > \sigma_p$,

(3) σ_1 jest stopniem f względem z_s.

Zauważmy, że każdy wielomian niezerowy *posiada stopień* względem *każdej* ze swych zmiennych. Dodając ewentualnie wielomiany zerowe, możemy przedstawić f w postaci:

$$g_0 z_s^{\sigma} + g_1 z_s^{\sigma-1} + \ldots + g_\sigma,$$

gdzie znów: (1) $g_0 \ldots g_\sigma$ są wielomianami (ew. zerowemi) zmiennych: $z_1, \ldots z_{s-1}, z_{s+1}, \ldots z_k$,

(2) $g_0(z_1 \ldots z_{s-1} z_{s+1} \ldots z_k)$ *nie* jest *wielomianem zerowym*,

(3) $\sigma =$ stopień f względem z_s.

Niechaj $f(\hat{z}_1 \ldots \hat{z}_k)$ będzie wielomianem zmiennych $z_1 \ldots z_k$ i niechaj $w_1 \ldots w_p$ będą zmiennemi zespolonemi, *różnemi* od $z_1 \ldots z_k$. Utwórzmy wyrażenie:

$$F(\hat{z}_1 \ldots \hat{z}_k, \hat{w}_1 \ldots \hat{w}_p) = f(\hat{z}_1, \ldots \hat{z}_k) . \hat{w}_1^{0} \ldots \hat{w}_p^{0}.$$

Jest to oczywiście *wielomian* zmiennych:

$$z_1 \ldots z_k, w_1 \ldots w_p$$

o tej własności, że *jakikolwiek* obierzemy system wartości:

$$a_1 \ldots a_k, b_1 \ldots b_p$$

dla zmiennych: $z_1 \ldots z_k, w_1 \ldots w_p$, to:

$$F(a_1 \ldots a_k, b_1 \ldots b_p) = f(a_1 \ldots a_k).$$

Niezbyt precyzyjnie możnaby to zapisać jako:

$$f(z_1 \ldots z_k) \equiv F(z_1 \ldots z_k, w_1 \ldots w_p).$$

Wielomian F nazwiemy *rozszerzeniem* wielomianu f, *zmiennych* $z_1 \ldots z_k$ do *zmiennych:*

$$z_1 \ldots z_k, w_1 \ldots w_p.$$

Możemy teraz objaśnić tworzenie sum, różnic, iloczynów i t. d. wielomianów o *różnych* zmiennych w obu wielomianach.

Naprz. rozważmy *sumę* wielomianów:

$$f(\hat{x}, \hat{y}) + g(\hat{x}, \hat{z}),$$

gdzie x, y, z są zmiennemi zespolonemi. Rozumiemy przez to, że:

(1) rozszerzyliśmy $f(\hat{x}, \hat{y})$ i $g(x, \hat{z})$, do wielomianów zmiennych x, y, z,

(2) rozszerzone wielomiany dodaliśmy do siebie.

A więc:

$$f(\hat{x}, \hat{y}) + g(\hat{x}, \hat{z}) \overset{\text{df}}{=} f(\hat{x}, \hat{y}) \cdot \hat{z}^0 + g(\hat{x}, \hat{z}) \cdot \hat{y}^0.$$

Analogicznie w innych, podobnych wypadkach.

8. **Wielomiany jednorodne.**

Df. Wielomian $f(z_1 \ldots z_k)$ jest *jednorodny*, gdy (1) albo jest identycznie zerem (2) albo wszystkie *jednomiany* jego postaci *zredukowanej* mają

ten sam rząd:

$$f(z_1 \dots z_k) = Az^{\alpha_1} \dots z_k^{\alpha_k} + Bz_1^{\beta_1} \dots z_k^{\beta_k} + \dots + Lz_1^{\lambda_1} \dots z_k^{\lambda_k},$$

gdzie:

$$\alpha_1 + \dots + \alpha_k = \beta_1 + \dots + \beta_k = \dots = \lambda_1 + \dots + \lambda_k.$$

Df. Wielomian *jednorodny* rzędu m jest *zupełnym*, gdy w jego postaci *zredukowanej* figurują jednomiany *wszystkich typów* rzędu m.

Rozważmy dowolny wielomian: $f(z_1 \dots z_k)$ rzędu m. Pisząc go w postaci zredukowanej i zbierając razem jednomiany tego samego *rzędu*, możemy f przedstawić w postaci:

$$f(z_1 \dots z_k) \equiv \varphi_m(z_1 \dots z_k) + \varphi_n(z_1 \dots z_k) + \dots + \varphi_w(z_1 \dots z_k),$$

gdzie: $\varphi_m, \varphi_n, \dots \varphi_w$ są wielomianami *jednorodnemi* rzędów $m, n, \dots w$, powstałemi przez zebranie jednomianów tego samego rzędu w postaci zredukowanej wielomianu f i gdzie $m > n > \dots > w$. Dołączając ewentualnie, dla symetrji, jednomiany zerowe, moglibyśmy napisać:

$$(*) \quad f(z_1 \dots z_k) \equiv \varphi_m(z_1 \dots z_k) + \varphi_{m-1}(z_1 \dots z_k) + \dots + \varphi_0(z_1 \dots z_k).$$

gdzie pewnym $\varphi_s(z_1 \dots z_k)$ nadano postać jednorodnych wielomianów rzędu s, przez wpisanie jednomianów, których zasady mają typy rzędu s, gdzie jednak spółczynniki są zerem. Jednakże $\varphi_m(z_1 \dots z_k) \not\equiv 0$.

Formuła $(*)$ przedstawia: *rozkład* $f(z_1 \dots z_k)$ na *części jednorodne*.

Mając dany wielomian $f(z_1 \dots z_k)$ rzędu m, napiszemy go w postaci poprzedniej:

$$f(z_1 \dots z_k) \equiv \varphi_m(z_1 \dots z_k) + \varphi_{m-1}(z_1 \dots z_k) + \dots + \varphi_0(z_1 \dots z_k).$$

Df. Rozważmy teraz wielomian: $F(z_1 \ldots z_k, t)$ zmiennych $z_1 \ldots z_k, t$ określony w następujący sposób:

$$F(z_1 \ldots z_k, t) \equiv \varphi_m(z_1 \ldots z_k) + \varphi_{m-1}(z_1 \ldots z_k) \cdot t + \ldots + \varphi_s(z_1 \ldots z_k) \cdot t^{m-s} + \ldots + \varphi_0(z_1 \ldots z_k)\, t^m.$$

Widać odrazu, że F jest wielomianem *jednorodnym rzędu* m zmiennych: $z_1 \ldots z_k, t$. Nazywamy go *wielomianem* powstałym z $f(z_1 \ldots z_k)$ *przez ujednorodnienie* lub krótko: *„ujednorodnionem f“*.

Oczywistem jest też następujące twierdzenie:

Tw. Jeżeli $f(z_1 \ldots z_k)$ jest wielomianem **zupełnym** *rzędu* m, to *ujednorodnione* $f(z_1 \ldots z_k)$ do $F(z_1 \ldots z_k, t)$ jest *wielomianem jednorodnym* **zupełnym** zmiennych: $z_1 \ldots z_k, t$.

Df. Ujednorodnieniem wielomianu *zerowego* zmiennych $z_1 \ldots z_k$ nazwiemy wielomian zerowy zmiennych $z_1 \ldots z_k, t$.

Tw. *Ilość wyrazów* (jednomianów) w postaci zredukowanej wielomianu *zupełnego* $f(z_1 \ldots z_k)$ rzędu m wynosi: $\binom{m+k}{k}$

[z definicji $\binom{m+k}{k} = \frac{(m+k)!}{m!\,k!}$ dla m i k całkowitych nieujemnych].

Dem. Ilość wyrazów jest oczywiście równa ilości możliwych rozwiązań w *liczbach całkowitych, nieujemnych* nierówności:

$$\alpha_1 + \ldots + \alpha_k \overset{?}{\leqq} m.$$

Jest ona zależną jedynie od k i m. Oznaczmy ją przez P_k^m.

Każdemu takiemu rozwiązaniu:

$$\alpha_1, \alpha_2, \ldots \alpha_k \qquad (1)$$

przypiszmy jednoznacznie system:

$$\alpha_1 + 1,\ \alpha_1 + \alpha_2 + 2, \ldots, \alpha_1 + \cdots + \alpha_k + k. \quad (2)$$

Ponieważ: $0 < \alpha_1 + 1 < \alpha_1 + \alpha_2 + 2 <$

$$< \alpha_1 + \alpha_2 + \cdots + \alpha_k + k \leqq m + k,$$

więc (2) przedstawi określoną kombinację bez powtórzeń z liczb: $1, 2, \ldots, m + k.$ (3)

Niech będzie naodwrót:

$$\beta_1, \beta_2, \ldots \beta_k \quad (4)$$

taką kombinacją bez powtórzeń z liczb (3)

Możemy zawsze założyć, że:

$$0 < \beta_1 < \beta_2 < \cdots < \beta_k,$$

gdyż w kombinacjach bez powtórzeń elementy systemu są różne a porządek ich nie wchodzi w rachubę. Kładąc: $\alpha_1 = \beta_1 - 1,\ \alpha_2 = \beta_2 - \beta_1 - 1, \ldots$

$$\alpha_k = \beta_k - \beta_{k-1},$$

widzimy, że: $0 \leqq \alpha_1,\ 0 \leqq \alpha_2 \ldots 0 \leqq \alpha_k,$

$0 \leqq \alpha_1 + \alpha_2 + \cdots + \alpha_k \leqq \beta_k - k \leqq m + k - k = m,$

zatem: $\alpha_1, \alpha_2, \ldots \alpha_k$ jest rozwiązaniem nierówności:

$$0 \overset{?}{\leqq} \alpha_1 + \cdots + \alpha_k \leqq m \quad (5)$$

w liczbach całkowitych nieujemnych.

Odpowiedniość między systemami (1) i (2) jest więc jedno-jednoznaczna, co pociąga, że ilość żądanych rozwiązań nierówności (5) jest równa ilości kombinacyj bez powtórzeń z liczb systemu (3). Ta ostatnia wynosi jak wiadomo:

$$\binom{m+k}{k},$$

co ostatecznie kończy nasz dowód.

Uw. Powyższy piękny dowód podał O. Perron w swej Algebrze. Inne znajdziemy w dziełach E. Netto i H. Webera, poświęconych wykładom algebry.

Tw. Ilość wyrazów wielomianu *zupełnego jednorodnego* $f(z_1 \dots z_k)$ rzędu m wynosi:

$$\binom{m+k-1}{k-1}.$$

Dem. Ilość ta równa się oczywiście:

$$s = P_k^m - P_k^{m-1}, \text{ gdy } m > 0,$$

a więc:

$$s = \binom{m+k}{k} - \binom{m+k-1}{k} = \binom{m+k-1}{k-1}.$$

Dla $m = 0$ mamy jednak:

$$s = 1 = \binom{0+k-1}{k-1} = \binom{m+k-1}{k-1},$$

co dowodzi ważności formuły i dla $m = 0$.

Niechaj $f(z_1 \dots z_k)$ będzie wielomianem *jednorodnym rzędu* m. Położmy za: $z_1 \dots z_k$ odpowiednio: $\lambda z_1 \dots \lambda z_k$, gdzie λ jest dowolną zespoloną. Będziemy mieć oczywiście:

$$f(\lambda z_1 \dots \lambda z_k) \equiv \lambda^m f(z_1 \dots z_k). \qquad (*)$$

Załóżmy odwrotnie, że identyczność $(*)$ ma miejsce dla danego wielomianu *niezerowego* $f(z_1 \dots z_k)$ i że m jest całkowitą nieujemną. Oznaczmy rząd wielomianu f przez p i rozłóżmy $f(z_1 \dots z_k)$ na części jednorodne:

$$f(z_1 \dots z_k) \equiv \varphi_p(z_1 \dots z_k) + \dots + \varphi_0(z_1 \dots z_k).$$

Po podstawieniu:

$$\lambda^m f(z_1 \dots z_k) \equiv \lambda^p \varphi_p(z_1 \dots z_k) + \dots + \lambda_0 \varphi_0(z_1 \dots z_k).$$

Różniczkując obie strony aż do rzędu m względem λ i kładąc $\lambda = 0$, otrzymamy dla $p \geqq m$:

$$f(z_1 \dots z_k) \equiv \varphi_m(z_1 \dots z_k),$$

zatem f jest wielomianem jednorodnym rzędu m

Hipoteza: $p < m$ jest niemożliwa, gdyż wtedy przy m-krotnem różniczkowaniu otrzymalibyśmy, że $f(z_1 \ldots z_k) \equiv 0$.

Mamy zatem *kryterjum:*

Tw. Warunkiem koniecznym i dostatecznym, by wielomian *niezerowy* $f(z_1 \ldots z_k)$ był *jednorodnym* rzędu m jest *identyczność:*

$$f(\lambda z_1, \ldots \lambda z_k) \equiv \lambda^m f(z_1 \ldots z_k)$$

dla wszelkich wartości $\lambda, z_1 \ldots z_k$.

Rozdział III.

Podzielność Wielomianów.

§ 1. Ogólne określenia i twierdzenia.

1. Podzielność.

Df. Wielomian $f(z_1 \ldots z_k)$ jest *podzielny* przez wielomian $g(z_1 \ldots z_k)$, jeżeli *istnieje wielomian* $h(z_1 \ldots z_k)$ taki, że:

$$f(z_1 \ldots z_k) \equiv g(z_1 \ldots z_k) \cdot h(z_1 \ldots z_k)$$

i gdy *jeszcze* $g(z_1 \ldots z_k) \not\equiv 0$.

Piszemy to krótko:

$$g \mid f \quad \text{(czytaj „}g \textit{ dzieli } f\text{“)}.$$

Wielomian g jest *podzielnikiem* f, przeciwnie: wielomian f jest *wielokrotnością* g.

Df. Wielomian $g(z_1 \ldots z_k)$ jest *wspólnym podzielnikiem* wielomianów $f_1(z_1 \ldots z_k) \ldots f_p(z_1 \ldots z_k)$, gdy:

$$g \mid f_1, \ldots g \mid f_p.$$

Jest on natomiast *wspólną wielokrotną dla* $f_1 \ldots f_p$, gdy:

$$f_1 \mid g, \ldots f_p \mid g.$$

Df. Wielomian g jest *największym wspólnym podzielnikiem* dla $f_1, \ldots f_p$, gdy:

(1) g *jest wspólnym podzielnikiem* dla $f_1, \ldots f_p$,

(2) *każdy wspólny podzielnik* h *wielomianów* $f_1, \ldots f_p$ *dzieli* g:

$$h \mid g.$$

Uw. Termin „*największy wspólny podzielnik*" jest terminem *ogólnym*, nie *jednostkowym*, gdyż, jak to zobaczymy, istnieje nieskończenie wiele największych wspólnych podzielników danych wielomianów.

Df. Wielomian g jest *najmniejszą wspólną wielokrotną* wielomianów $f_1, \ldots f_p$, gdy:

(1) g *jest wspólną wielokrotną* $f_1, \ldots f_p$

i (2) g *dzieli każdą wspólną wielokrotną tych wielomianów.*

Tw. 1. Gdy f jest dowolnym wielomianem, a g wielomianem rzędu *zero*, to $g \mid f$,

2. gdy f jest wielomianem *niezerowym*, to $f \mid f$,

3. $h \mid g \,.\, g \mid f : \supset : h \mid f$,

4. $h \mid g \,.\, h \mid f : \supset : h \mid (f \pm g)$,

5. $h \mid g$ i f jest dowolnym wielomianem, to $h \mid g \,.\, f$.

Uw. Mamy tu na myśli wielomiany *tych samych zmiennych*, ewentualnie rozumielibyśmy nasze twierdzenia w ten sposób, że wielomiany zastąpiono przez odpowiednie *rozszerzenie* [p. str. 58] do potrzebnej ilości zmiennych.

Dem. 1. Gdy $f \equiv 0$, to widocznie: $f \equiv g \,.\, f$, $g \not\equiv 0$; gdy $f \not\equiv 0$, to:

$$f(z_1 \ldots z_k) \equiv A z_1^{\alpha_1} \ldots z_k^{\alpha_k} + \ldots + L z_1^{\lambda_1} \ldots z_k^{\lambda_k},$$

stąd: $f \equiv g \,.\, h$, gdzie:

$$h \equiv \frac{A}{s} z_1^{\alpha_1} \dots z_k^{\alpha_k} + \dots + \frac{L}{s} z_1^{\lambda_1} \dots z_k^{\lambda_k},$$

$$0 \neq s \equiv g(z_1 \dots z_k).$$

2. Wtedy: $f \equiv f \,.\, g$, gdzie $g \equiv 1 \,.\, z_1^0 \dots z_k^0, f \not\equiv 0$.
3. Wtedy: $g \equiv h \,.\, g_1, f \equiv g \,.\, f_1$, gdzie g_1 i f_1 są wielomianami, więc:
$$f \equiv h \,.\, (f_1 \,.\, g_1),$$
gdzie $f_1 \,.\, g_1$ jest wielomianem.
4. Nb.: $g \equiv h \,.\, g_1, f \equiv h \,.\, f_1$, ($f_1$ i g_1 wielomiany), to:
$$f \pm g \equiv h \,.\, (f_1 \pm g_1),$$
gdzie $f_1 \pm g_1$ jest wielomianem.
5. Nb. $g \equiv h \,.\, g_1$ (g_1 wielomian), to:
$f \,.\, g \equiv h \,.\, (f g_1)$ ($f g_1$ jest wielomianem).

Df. Wielomiany $f_1, \dots f_p$ są *pierwsze względem siebie,* gdy *jedynemi ich wspólnemi podzielnikami są wielomiany rzędu zero.*

Df. Wielomian $f(z_1 \dots z_k)$ jest *rozkładalny,* jeżeli *istnieją* wielomiany g i h, oba *rzędów większych niż zero* i *takie,* że:

$$f \equiv g \,.\, h$$

w przeciwnym wypadku f jest wielomianem *nierozkładalnym.*

Z łatwością możemy podać przykłady wielomianów nierozkładalnych rzędu większego niż jeden w wypadku wielomianów *więcej* niż *jednej* zmiennych. Takim jest naprz. wielomian: $x^2 + y$, co łatwo udowodnić.

W następnym rozdziale przekonamy się, że jedy-

nemi wielomianami nierozkładalnemi *jednej* zmiennej są wielomiany *zerowe* oraz rzędów: *zerowego* i *pierwszego*.

§ 2. Algorytm Euklidesa.

1. **Rozkład Euklidesowski** dla jednej zmiennej.

Tw. Jeżeli $f(z)$ i $g(z)$ są wielomianami, przyczem $g(z) \not\equiv 0$, to istnieją wielomiany $Q(z)$ i $R(z)$ takie, że:

(1) $f(z) \equiv Q(z) \,.\, g(z) + R(z)$,

(2) $R(z)$ jest niższego stopnia niż $g(z)$

[p. **Umowa** na str. 46].

Dem. 1. *wypadek:* $f(z) \equiv 0$; wtedy:

$$f(z) \equiv f(z) \,.\, g(z) + f(z)$$

i $f(z) \equiv 0$, więc stopnia niższego niż $g(z)$ $(\not\equiv 0)$ wedle brzmienia umowy na str. 46.

2. *wypadek:* $st'f < st'g$; wtedy:

$$f(z) \equiv (0 \,.\, z^0) g(z) + f(z),$$

przyczem: $st'f < st'g$.

3. *wypadek:* $st'f \geqq st'g$.

Zapiszmy f i g w postaci:

$$f(z) \equiv a_0 z^m + \ldots + a_m, \; g(z) \equiv b_0 z^n + \ldots + b_n,$$

$a_0 \neq 0$, $b_0 \neq 0$, zatem $st'f = m$, $st'g = n$, $m \geqq n$,

$$f(z) \equiv Q_1(z) g(z) + R_1(z), \text{ gdzie:}$$

$$Q_1(z) \equiv \frac{a_0}{b_0} \cdot z^{m-n}, \; R_1(z) = \left(a_1 - \frac{a_0}{b_0} b_1 \right) z^{m-1} + \ldots,$$

więc: $st'R_1 < st'f$ lub $R_1 \equiv 0$.

Jeżeli jeszcze: $st'R_1 \geqq st'g$, to przedstawmy dalej:

$$R_1(z) \equiv Q_2(z) \,.\, g(z) + R_2(z),$$

gdzie: $Q_2(z)$ obliczono znów „dzieląc najwyższy wyraz w $R_1(z)$ przez $b_0 z^n$ "...

Będziemy mieli:

$$f(z) \equiv \{Q_1(z) + Q_2(z)\} \cdot g(z) + R_2(z),$$
$$st' R_2 < st' R_1 < st' f \text{ lub } R_2(z) \equiv 0.$$

Posuwając ten proces dalej, o ile tego zachodzi potrzeba, dojdziemy po skończonej ilości kroków do wyniku:

$$f(z) \equiv Q(z) g(z) + R(z), \quad \text{gdzie:}$$
$$st' R < st' g \quad \text{lub} \quad R(z) \equiv 0.$$

Uw. Rozkład: $f(z) \equiv Q(z) g(z) + R(z)$, gdzie Q i R są wielomianami i gdzie $R(z)$ jest niższego stopnia niż $g(z)$, nazwiemy *rozkładem Euklidesowskim.*

Tw. Rozkład Euklidesowski jest możliwy tylko w jeden sposób:

Dem. Załóżmy, że:

$$\left.\begin{array}{l} f(z) \equiv Q(z) g(z) + R(z) \\ f(z) \equiv Q'(z) g(z) + R'(z) \end{array}\right\} \quad \left\{\begin{array}{l} Q, Q', R, R' \\ \text{wielomiany} \end{array}\right\}$$

R i R' niższego stopnia niż g.

Wtedy: $\{Q(z) - Q'(z)\} g(z) \equiv R'(z) - R(z)$.

Jeżeli: $Q(z) - Q'(z) \not\equiv 0$, to:

$st' \{(Q(z) - Q'(z)) g(z)\} \geq st' g$, lecz:

$R'(z) - R(z)$ stopnia niższego niż $g(z)$.

Jest to niemożliwe, więc $Q(z) \equiv Q'(z)$ i co zatem idzie: $R(z) \equiv R'(z)$.

Df. Wielomiany $Q(z)$ i $R(z)$, wyznaczone przez rozkład Euklidesowski:

$$f(z) \equiv Q(z) g(z) + R(z),$$

zwiemy odpowiednio: *całkowitą częścią ilorazu* i *resztą ilorazu* wielomianów f i g.

Tw. Całkowita część ilorazu i reszta mają określony sens zawsze, gdy dzielna i dzielnik są wielomianami i dzielnik nie jest wielomianem zerowym.

2. **Największy wspólny podzielnik** dla jednej zmiennej.

Rozważmy najpierw wypadek dwu wielomianów $f(z)$ i $g(z)$.

1. *wypadek:* $f \equiv 0$, $g \equiv 0$. W tym wypadku *każdy* wielomian $h(z)$ niezerowy jest wspólnym podzielnikiem dla f i g, zatem *największego wspólnego* **niema.**

2. *wypadek:* $f \not\equiv 0$, $g \equiv 0$. Jednym z największych wspólnych podzielników jest widocznie wielomian $f(z)$.

3. *wypadek:* $g \not\equiv 0$, $f \equiv 0$ analogiczny.

4. *wypadek:* $f \not\equiv 0$, $g \not\equiv 0$. Niechaj będzie:

$$st' f \geqq st' g \qquad \text{(wyp. } st' f \leqq st' g \text{ zupełnie analogiczny).}$$

Utwórzmy szereg rozkładów Euklidesa:

$$f(z) \equiv Q_1(z)\, g(z) + R_1(z) \qquad (1)$$
$$g(z) \equiv Q_2(z)\, .\, R_1(z) + R_2(z) \qquad (2)$$
$$\vdots$$
$$R_{\rho-1}(z) \equiv Q_{\rho+1}(z)\, .\, R_\rho(z) + R_{\rho+1}(z) \qquad (\rho+1)$$
$$R_\rho(z) \equiv Q_{\rho+2}(z)\, .\, R_{\rho+1}(z), \qquad (\rho+2)$$

[„*łańcuchowe dzielenie*“ lub „*algorytm Euklidesa*“]

przyczem prowadzimy rozkłady tak długo, aż w łańcuchu stopni:

$$st' g > st' R_1 > st' R_2 > \ldots > st' R_{\rho+1}$$

zejdziemy do tego miejsca, że $R_{\rho+2} \equiv 0$. Zatrzymujemy się jednak na ostatnim kroku tak, że $R_{\rho+1} \not\equiv 0$.

Twierdzimy, że $R_{\rho+1}(z)$ jest jednym z największych wspólnych podzielników dla f i g.

Rzeczywiście:

(1) $R_{\rho+1} \mid R_\rho$ ze związku $(\rho+2)$, stąd $R_{\rho+1} \mid R_{\rho-1}$ ze związku $(\rho+1) \ldots R_{\rho+1} \mid g$ [z (2)] i $R_{\rho+1} \mid f$ [z (1)], zatem $R_{\rho+1}$ jest wspólnym podzielnikiem dla f i g.

(2) Niechaj $h \mid f$ i $h \mid g$. Wtedy $h \mid R_1$ [z (1)], stąd: $h \mid R_2$ [z (2)] $\ldots h \mid R_{\rho+1}$ [z $(\rho+1)$].

Zatem każdy wspólny podzielnik $h(z)$ dzieli $R_{\rho+1}(z)$.

Tw. Jeżeli $h(z)$ i $k(z)$ są *największemi wspólnemi podzielnikami* dla $f(z)$ i $g(z)$, to:

$$h(z) = Ak(z), \text{ gdzie } A \varepsilon q_2 . A \not\equiv 0.$$

Dem. Wedle definicji [str. 65]

$$h \mid k \text{ i } k \mid h,$$

zatem istnieją takie wielomiany $\varphi(z)$ i $\psi(z)$, że:

$$h(z) \equiv \varphi(z) k(z),\ k(z) \equiv \psi(z) . h(z),$$

stąd: $h(z) \equiv \varphi(z)\psi(z)h(z)$, $[h(z) \not\equiv 0$. z def.],

więc: $st' h = st'(\varphi\psi) + st' h,\ st'(\varphi\psi) = 0,$

$$st'\varphi = 0 \quad \varphi \equiv \text{const} = A \not\equiv 0,$$

$$h(z) \equiv A\,k(z),\ A \varepsilon q_2,\ A \not\equiv 0.$$

Tw. Jeżeli $h(z)$ jest największym wspólnym podzielnikiem dla $f(z)$ i $g(z)$ i $A \varepsilon q_2 . A \not\equiv 0$, to $Ah(z)$ jest również największym wspólnym podzielnikiem dla f i g.

Dem. Widoczne.

Tw. Wszystkie największe wspólne podzielniki dla $f(z)$ i $g(z)$ są tego *samego stopnia* i każdy

z nich powstaje z innego przez mnożenie przez stałą, $\neq 0$.

Tw. Wśród największych wspólnych podzielników dla $f(z)$ i $g(z)$, taki, dla którego przy najwyższej potędze z spółczynnikiem jest *jedność* istnieje tylko *jeden*.

Dem. Gdy takiemi są $h(z)$ i $k(z)$, to:

$$h(z) \equiv z^p + \ldots + a_p,\ k(z) \equiv z^p + \ldots + b_p,$$
$$h(z) \equiv A\,k(z),\ A \varepsilon q_2,\ A \neq 0,$$
$$z^p + \ldots + a_p \equiv A\,z^p + \ldots + A\,b_p.$$

Biorąc n-tą pochodną obu stron, otrzymamy:

$$A = 1,$$
$$h(z) \equiv k(z).$$

Df. Największy wspólny podzielnik dla $f(z)$ i $g(z)$, w którym *spółczynnik najwyższego wyrazu* formy zredukowanej jest *jednością*, nazywamy *głównym* i będziemy oznaczali przez:

$$[f, g].$$

Tw. Gdy $h(z)$ jest największym wspólnym podzielnikiem dla $f(z)$ i $g(z)$, to istnieją wielomiany $P(z)$ i $Q(z)$ takie, że:

$$P(z) \cdot f(z) + Q(z) \cdot g(z) \equiv h(z).$$

Dem. Przypomnijmy sobie łańcuchowe dzielenie [str. 69] i największy wspólny podzielnik $R_{\rho+1}(z)$. Otrzymamy kolejno:

$$f - Q_1 g \equiv R_1,$$
$$g - Q_2(f - Q_1 g) \equiv -Q_2 f + (1 + Q_1 Q_2) g \equiv R_2,$$
$$f - Q_1 g - Q_3[-Q_2 f + (1 + Q_1 Q_2) g] \equiv R_3, \text{ więc:}$$
$$(1 + Q_2 Q_3) f + (-Q_1 - Q_3 - Q_1 Q_2 Q_3) g \equiv R_3 \text{ i t. d.}$$

Ostatecznie, wprowadzając odpowiednie oznaczenia:

$$\overline{P}(z)f(z)+\overline{Q}(z)g(z)\equiv R_{\rho+1}(z).$$

Jeżeli teraz $h(z)$ jest dowolnym największym wspólnym podzielnikiem, to:

$$h(z)\equiv AR_{\rho+1}(z),\ A\varepsilon q_2,\ A\neq 0.$$

Wtedy zastępując $A\overline{P}$ i $A\overline{Q}$ przez P i Q, mamy:

$$Pf+Qg\equiv h.$$

Cor. Wielomiany $P(z)$ i $Q(z)$ poprzedniego tw. są *pierwsze* względem siebie.

Dem. Zapiszmy:

$$f(z)\equiv M(z)h(z),\ g(z)\equiv N(z)h(z),$$

[$M(z)$ i $N(z)$ wielomiany]. Stąd:

$$h(z)[PM+QN]\equiv h(z),$$

zatem:

$$st'(PM+QN)=0,$$

$$PM+QN\equiv \text{const}=1.$$

Gdy: $s(z)\,|\,P(z)$ i $s(z)\,|\,Q(z)$, to $s(z)$ musi dzielić $1(\equiv 1\,.\,z^0)$, więc $st's=0$, co dowodzi twierdzenia.

Tw. Gdy $h\,|\,f$ i $h\,|\,g$ i $Pf+Qg\equiv h$, to h jest największym wspólnym podzielnikiem dla f i g.

Dem. Gdy bowiem $s\,|\,f$ i $s\,|\,g$, to $s\,|\,Pf+Qg$, więc $s\,|\,h$.

Tw. Warunek konieczny i dostateczny, by f i g były *pierwsze względem siebie,* brzmi:

$$[f,g]\equiv 1.$$

Dem. Widoczne z definicji i poprzednich twierdzeń.

Tw. Inny warunek konieczny i dostateczny, by wielomiany f i g były *pierwsze względem siebie,* brzmi: Istnieją wielomiany $P(z)$ i $Q(z)$ takie, że:

$$P\,.\,f+Q\,.\,g\equiv 1.$$

Dem. Konieczność z tw. poprzedniego, dostateczność stąd, że gdy $s \mid f$ i $s \mid g$, to $s \mid Pf + Qg$, więc $s \mid 1$ i $st's = 0$.

Mamy teraz *trzy ważne twierdzenia o podzielności.*

Tw. Gdy $h \mid f.g$ i $[h, g] \equiv 1$, to $h \mid f$.

[h, f, g wielomiany jednej zmiennej].

Dem. Istnieją P i Q takie, że $Ph + Qg \equiv 1$, stąd: $Phf + Qgf \equiv f$,

$h \mid hf$ i $h \mid gf$, więc $h \mid Phf + Qgf$,

skąd: $h \mid f$.

Tw. Gdy $h \mid f.g$ i h jest *nierozkładalne*, to: $h \mid f$ lub $h \mid g$.

Dem. Jeżeli $h \mid f$, to twierdzenie słuszne.

Załóżmy, że nie zachodzi: $h \mid f$;

wtedy $f \not\equiv 0$ i $[h, f] \equiv 1$,

gdyż, skoro: $s \mid h$ i $s \mid f$, to $st's = 0$ lub $st's = st'h$.

Gdyby $st's = st'h$, byłoby:

$$s = Ah,\ A \varepsilon q_2,\ A \neq 0 \text{ i } h \mid f.$$

Zatem istnieją P i Q takie, że:

$$Ph + Qf \equiv 1.$$

Stąd: $Phg + Qgf \equiv g$, $h \mid hg$, $h \mid gf$,

$h \mid Phg + Qgf$, więc ostatecznie: $h \mid g$.

Tw. Gdy h jest największym wspólnym podzielnikiem dla f i g i zaznaczymy:

$$f \equiv Mh,\ g \equiv Nh, \text{ to: } [M, N] \equiv 1.$$

Dem. Gdyby $s \mid M$ i $s \mid N$ i $st's > 0$, to:

$M \equiv s.M'$, $N = s.N'$, $f \equiv M'.hs$, $g \equiv N'.hs$,

więc: $hs \mid f$, $hs \mid g$ i $st'hs > st'h$, co niemożliwe.

Największy wspólny podzielnik funkcyj $f_1, \ldots f_p$, gdzie $p > 2$, otrzymamy z uwagi, że skoro:

h jest najw. wsp. podz. dla $f_1, \ldots f_{p-1}$,
k jest najw. wsp. podz. dla f_p i h, to:
k jest najw. wsp. podz. dla $f_1, \ldots f_p$.

Uwaga ta wynika wprost stąd, że:

(1) $k \mid h$, $k \mid f_p$, więc $k \mid f_1, \ldots k \mid f_{p-1}$ i $k \mid f_p$.

(2) gdy $s \mid f_1, \ldots s \mid f_p$, to $s \mid f_1, \ldots s \mid f_{p-1}$, więc $s \mid h$ i $s \mid f_p$, więc $s \mid k$.

Czytelnik przeniesie sam z łatwością potrzebne twierdzenia z wypadku dwu funkcyj na dowolną, skończoną ich ilość.

3. **Rozkład Euklidesa** dla wielomianów dwóch zmiennych.

Nieco odmiennie przedstawia się sprawa rozkładu Euklidesa, jako też największego wspólnego podzielnika, dla wielomianów *dwu* lub *więcej* zmiennych. Przeprowadzimy badanie dla **dwu** zmiennych, gdyż dalej już przedstawia się ono analogicznie.

Dla wielomianów dwóch zmiennych mamy *dwa rozkłady* Euklidesa: *względem pierwszej* i *względem drugiej zmiennej*. Analogicznie dla k zmiennych mamy k *rozkładów* względem każdej ze zmiennych.

W wypadku dwu zmiennych oznaczymy zmienne przez x i y. Rozważymy naprzykład:

Rozkład względem y.

Tw. Niechaj $f(xy)$ i $g(xy)$ będą wielomianami i niechaj $g(xy) \not\equiv 0$. Wtedy istnieją **trzy** wielomiany: $P(x)$, $Q(xy)$, $R(xy)$, takie, że:

(1) $P(x) \cdot f(xy) \equiv Q(xy) \cdot g(xy) + R(xy)$,

(2) $R(xy)$ jest *niższego* stopnia *względem* y niż $g(xy)$.

Dem.

1. *wypadek:* $f \equiv 0$, $g \not\equiv 0$. Połóżmy wtedy:
$P(x) \equiv 1$, $Q(xy) \equiv 0$, $R(xy) \equiv 0$, stąd:
$P(x)f(xy) \equiv Q(xy)\,g(xy) + R(xy)$,
przyczem $R(xy)$ $\{\equiv 0\}$ jest niższego stopnia niż $g(xy)$ względem y [1]

2. *wypadek:* $st'_y f < st'_y g$ [st'_y = stopień względem y].
Kładziemy: $P(x) \equiv 1$, $Q(xy) \equiv 0$, $R(xy) \equiv f(xy)$.

3. *wypadek:* $st'_y f \geq st'_y g$.
Zapiszmy: $f(xy) \equiv a_0(x) \,.\, y^m + \ldots + a_m(x)$,
$g(xy) \equiv b_0(x) \,.\, y^n + \ldots + b_n(x)$,
$a_0(x) \ldots a_m(x)$, $b_0(x) \ldots b_n(x)$ są wielomianami
$a_0(x) \not\equiv 0$, $b_0(x) \not\equiv 0$, $m \geq n$.

Najpierw:
$b_0(x) \,.\, f(xy) \equiv Q_1(xy)\,g(xy) + R_1(xy)$,
gdzie: $Q_1(xy) \equiv a_0(x) \,.\, y^{m-n}$,
$R_1(xy) \equiv [a_1(x)b_0(x) - a_0(x)b_1(x)]\,y^{m-1} + \ldots$
lub $R_1 \equiv 0$. W każdym razie $R_1(xy)$ jest *niższego* stopnia względem y niż $f(xy)$. Jeżeli $st'_y R_1(xy) \geq st'_y g(xy)$, to kładziemy dalej:
$R_1(xy) \equiv c_0(x)\,y^p + \ldots + c_p(x)$, $c_0(x) \not\equiv 0$.
$b_0(x)\,R_1(xy) \equiv Q_2(xy)\,g(xy) + R_2(xy)$,
gdzie: $Q_2(xy) \equiv c_0(x) \,.\, y^{p-n}$, $R_2(xy) \equiv$
$\equiv [c_1(x)b_0(x) - b_1(x)c_0(x)]\,y^{p-1} + \ldots$

W ten sposób postępujemy dalej, aż będzie:
$st'_y R_\rho(xy) < st'_y g(xy)$ lub $R_\rho(xy) \equiv 0$.

Mnożąc przez odpowiednie czynniki i dodając do siebie powyższe równania, dostaniemy:
$P(x)f(xy) \equiv Q(xy)\,g(xy) + R(xy)$,

[1] p. Umowa na str. 46.

gdzie $R(xy)$ jest względem y stopnia niższego niż $g(xy)$. Widoczne przytem, że $P(x) \not\equiv 0$ i że Q i R są wielomianami.

Tw. Jeżeli $P(x)f(xy) \equiv Q(xy)g(xy) + R(xy)$
i $P(x)/(xy) \equiv \overline{Q}(xy)g(xy) + \overline{R}(xy)$
są rozkładami Euklidesa względem y dla f i g, to: $Q \equiv \overline{Q}$, $R \equiv \overline{R}$.

Dem. Wtedy bowiem: $(Q - \overline{Q})g \equiv R - R$ i jeśliby $Q - \overline{Q} \not\equiv 0$, to $st'_y(Q - \overline{Q})g \geqq st'_y g$, co niemożliwe, gdyż $\overline{R} - R$ niższego stopnia względem y niż g. Zatem $Q \equiv \overline{Q}$ i $R \equiv \overline{R}$.

Uw. Zauważmy, że założono tu identyczność spółczynników-wielomianów przy $f(xy)$ w obu rozkładach!

4. **Dzielenie wielomianów** dwu zmiennych przez wielomiany jednej zmiennej.

Niechaj $f(xy)$ i $\varphi(x)$ będą wielomianami. Założymy przytem, że $f(xy) \not\equiv 0$ i $\varphi(x) \not\equiv 0$. Przedstawmy $f(xy)$ w postaci:

$$f(xy) \equiv a_0(x)y^m + \cdots + a_m(x),$$

[$a_0(x), \ldots a_m(x)$ wielomiany, $a_0(x) \not\equiv 0$, $m \equiv st'_y f$ = stopień *względem* y wielomianu $f(xy)$].

Jeżeli: $\varphi(x) \mid a_0(x), \ldots \varphi(x) \mid a_m(x)$,
to położymy:

$$a_i(x) \equiv b_i(x)\varphi(x)$$
$$g(xy) \equiv b_0(x)y^m + \cdots + b_m(x),$$

wtedy: $g(xy)$ jest wielomianem
i $f(xy) \equiv g(xy) \cdot \varphi(x)$,
zatem: $\varphi(x) \mid f(xy)$.

Załóżmy przeciwnie, że $\varphi(x) \mid f(xy)$,
wtedy: $f(xy) \equiv g(xy) \cdot \varphi(x)$, gdzie:
$g(xy)$ jest wielomianem i gdzie $st'_y f = st'_y g$
zatem: $g(xy) \equiv b_0(x)y^m + \cdots + b_m(x)$
$[b_0(x) \ldots b_m(x)$ wielomiany, $b_0(x) \not\equiv 0]$.

Stąd:
$$a_0(x)y^m + \cdots + a_m(x) \equiv b_0(x)\varphi(x) \cdot y^m + \cdots + b_m(x)\varphi(x).$$

Biorąc pochodne cząstkowe obu stron względem y dla x dowolnego i $y = 0$ aż do rzędu m, otrzymamy:

$$a_0(x) \equiv b_0(x)\varphi(x) \ldots a_m(x) \equiv b_m(x)\varphi(x),$$

więc: $\varphi \mid a_0 \ldots \varphi \mid a_m$. Stąd twierdzenie:

Tw. Warunek konieczny i dostateczny, aby wielomian *niezerowy* $f(xy)$ był *podzielny* przez wielomian *niezerowy* $\varphi(x)$, brzmi:

Wszystkie spółczynniki-wielomiany w rozwinięciu $f(xy)$ wedle potęg y mają być podzielne przez $\varphi(x)$.

Uw. Pojmujemy tu, wedle umowy na str. 58, $\varphi(x)$ jako: $\varphi(x) \cdot y^0$.

Rozważmy teraz w poprzednim wypadku największy wspólny podzielnik wielomianów: $a_0(x) \ldots$ $\ldots a_m(x)$, naprz.:

$h(x) = [a_0(x) \ldots a_m(x)]$ {główny najw. wsp. podz.}

Oczywiście: (1) $h(x) \mid f(xy)$ i (2) gdy $k(x) \mid f(xy)$, to: $k(x) \mid a_0(x), \ldots k(x) \mid a_m(x)$, więc $k(x) \mid h(x)$.

Df. Nazwiemy *największy wspólny podzielnik spółczynników-wielomianów* w rozwinięciu wedle potęg y wielomianu niezerowego $f(xy)$ jego *największym dzielnikiem zależnym tylko od zmiennej* x.

Uw. Widać natychmiast, że gdy $h(x)$ jest takim, to wszystkie inne mają postać:

$$Ah(x),\ A \varepsilon q_2,\ A \neq 0.$$

Uw. Jeżeli $f(xy) \equiv 0$, to każdy wielomian $\varphi(x)$, *niezerowy dzieli* $f(xy)$.

Tw. Jeżeli wielomian $f(xy)$ jest *niezerowy*, $h(x)$ jest jednym z jego największych dzielników zależnych tylko od x i gdy położymy:

$$f(xy) \equiv h(x) \,.\, g(xy),\quad [g(xy) \text{ wielomian}],$$

to $g(xy)$ nie posiada dzielników typu $k(x)$, gdzie: $st' k(x) > 0$.

Dem. Gdyby $k(x) \mid g(xy)$, $k(x) \,.\, t(xy) \equiv g(xy)$, to: $f(xy) \equiv k(x) \,.\, h(x) \,.\, t(xy)$, więc: $k(x) \,.\, h(x) \mid f(xy)$, $k(x)\, h(x) \mid h(x)$. Stąd: $st' k(x) = 0$.

Tw. Jeżeli $\varphi(x) \mid f(xy) \,.\, g(xy)$ i $\varphi(x)$ jest *nierozkładalne*, to $\varphi(x) \mid f(xy)$ lub $\varphi(x) \mid g(xy)$.

Dem. Rozważmy tylko wypadek nietrywjalny: $f \not\equiv 0$, $g \not\equiv 0$ i załóżmy, że $\varphi(x)$ nie dzieli wielomianu $f(xy)$. Napiszmy:

$$f(xy) \equiv a_0(x) y^m + \cdots + a_m(x),$$
$$g(xy) \equiv b_0(x)\, y^n + \cdots + b_n(x),$$
$$a_0(x), \ldots a_m(x),\ b_0(x), \ldots b_n(x)$$

wielomiany, $a_0 \not\equiv 0$, $b_0 \not\equiv 0$.

Nie wszystkie: $a_0(x), \ldots a_n(x)$ są podzielne przez $\varphi(x)$. Naprz. niechaj będzie: $\varphi \mid a_0 \ldots \varphi \mid a_{r-1}$, lecz *nie* $\varphi \mid a_r$. Jeśliby *nie* $\varphi \mid g$, to nie wszystkie $b_0 \ldots b_n$ byłyby podzielne przez φ. Naprz. niechaj:

$$\varphi \mid b_0 \ldots \varphi \mid b_{s-1},\ \text{lecz } \textit{nie}\ \varphi \mid b_s.$$

Rozważmy iloczyn:

$$f(xy)\, g(xy) \equiv c_0(x)\, y^{m+n} + \cdots + c_{m+n}(x),$$

gdzie:

$$c_0(x) \equiv a_0(x)b_0(x), \ldots c_{m+n} = a_m(x)b_n(x).$$

Weźmy pod uwagę spółczynnik:

$$c_{r+s}(x) = a_0(x)b_{r+s}(x) + \cdots + a_{r-1}(x)b_{s+1}(x) + a_r(x)b_s(x) + a_{r+1}(x)b_{s-1}(x) + \cdots + a_{r+s}(x)b_0(x),$$

kładąc, o ile zachodzi potrzeba:

$$a_{m+1}(x) \equiv a_{m+2}(x) \equiv \cdots \equiv 0,$$
$$b_{n+1}(x) \equiv b_{n+2}(x) \equiv \cdots \equiv 0.$$

Widzimy, że *nie prawdą jest,* by: $\varphi \mid c_{r+s}(x)$, bo: *nie* $\varphi(x) \mid a_r(x)b_s(x)$, gdyż:
nie $\varphi \mid a_r$ i *nie* $\varphi \mid b_s$,
przyczem:

$$\varphi \mid a_0b_{r+s} + \cdots + a_{r-1}b_{s+1} + a_{r+1}b_{s-1} + \cdots + a_{r+s}b_0,$$

Tem samem nieprawdą jest, by:

$$\varphi \mid f \,.\, g.$$

Tw. Jeżeli $\varphi(x) \mid f(xy)g(xy)$ i $\varphi(x)$ i $f(xy)$ są *pierwsze względem siebie*, to $\varphi(x) \mid g(xy)$.

Dem. Jeżeli $\varphi(x) \equiv \text{const} \neq 0$, to $\varphi \mid g$. Załóżmy, że $st'\varphi > 0$, wtedy *nie* $\varphi \mid f$. Jeżeli $\varphi(x)$ nie jest nierozkładalne, to rozłożymy je na czynniki stopnia większego niż zero nierozkładalne:

$$\varphi(x) \equiv \varphi_1(x) \ldots \varphi_p(x).$$

Oczywiście: $\varphi_1(x), \ldots \varphi_p(x)$ są pierwsze względem $f(xy)$, dzielą $f(xy)g(xy)$ i nie dzielą $f(xy)$. Zatem: $\varphi_1(x)$ dzieli, wedle tw. poprz. $g(xy)$ i mamy:

$$g(xy) \equiv g_1(xy)\varphi_1(x).$$
$$g(xy).f(xy) \equiv \varphi(x).h(xy) \equiv \varphi_1(x)(\varphi_2(x) \ldots \varphi_p(x)).h(xy),$$
$$f(xy)g_1(xy)\varphi_1(x) \equiv \varphi_2(x) \ldots \varphi_p(x).h(xy).\varphi_1(x),$$
$$(g_1f - \varphi_2 \ldots \varphi_p h)\varphi_1 \equiv 0 \text{ lecz } \varphi_1 \not\equiv 0$$

więc: $g_1f \equiv \varphi_2 \ldots \varphi_p h$. Znów: $[f, \varphi_2] = 1$

i *nie* $\varphi_2 \mid f$, lecz $\varphi_2 \mid g_1 f$, więc $\varphi_2 \mid g_1$,
a więc: $g_1(xy) \equiv g_2(xy)\,\varphi_2(x)$ i t. d.

Ostatecznie:

$$g(xy) \equiv \varphi_1(x)\,\varphi_2(x) \ldots \varphi_p(x) \cdot g_p(xy)$$
$$\equiv \varphi(x)\, g_p(xy),$$

skąd: $\varphi(x) \mid g(xy)$.

5. **Łańcuchowe** dzielenie dla dwu zmiennych.

Założymy, że $f(xy)$ i $g(xy)$ są wielomianami, i że $g(xy) \not\equiv 0$. Prowadźmy łańcuch rozkładów Euklidesa względem y:

$$P_1(x)\, f(xy) \equiv Q_1(xy)\, g(xy) + R_1(xy) \qquad [1]$$
$$P_2(x)\, g(xy) \equiv Q_2(xy)\, R_1(xy) + R_2(xy) \qquad [2]$$
$$P_3(x)\, R_1(xy) \equiv Q_3(xy)\, R_2(xy) + R_3(xy) \qquad [3]$$
$$\vdots$$
$$P_{\rho+1}(x)\, R_{\rho-1}(xy) \equiv Q_{\rho+1}(xy)\, R_\rho(xy) + R_{\rho+1}(xy) \qquad [\rho+1]$$

tak długo, aż będzie:

$$st'_y\, R_{\rho+1}(xy) = 0 \text{ lub } R_{\rho+1}(xy) \equiv 0.$$

Zapisujmy krótko: $R_{\rho+1}(xy) \equiv R_{\rho+1}(x)$.
Mamy jednak jeszcze: $st'_y\, R_\rho(xy) > 0$!

Przypuśćmy teraz, że:

$$h(xy) \mid f(xy) \text{ i } h(xy) \mid g(xy) \text{ i } \mathbf{st'_y\, h > 0}.$$

Wtedy otrzymamy kolejno:

$h \mid R_1$ (dzięki [1]), $h \mid R_2$ (dzięki [2]) ...

$h \mid R_\rho$ (dzięki [ρ]), $h \mid R_{\rho+1}$ (dzięki [ρ+1]).

Mamy tu dwie możliwości:

I. $R_{\rho+1}(x) \not\equiv 0$. Wtedy podzielniki takie jak $h(xy)$, gdzie $st'_y h > 0$ **nie istnieją.** „f i g nie posiadają podzielników wspólnych, zależnych od y".

II. $R_{\rho+1}(x) \equiv 0$. Oddzielmy od $R_\rho(xy)$ najwyższy dzielnik zależny tylko od x. Niechaj nim będzie naprz. $k(x)$:

$$R_\rho(xy) \equiv k(x) \,.\, r(xy).$$

Otrzymamy kolejno:

$r(xy) \mid P_{\rho+1}(x) R_{\rho-1}(xy)$, lecz $[r(xy), P_{\rho+1}(x)] \equiv 1$, stąd: $r(xy) \mid R_{\rho-1}(xy)$.

W dalszym ciągu z równości [ρ]:

$$P_\rho(x) R_{\rho-2}(xy) \equiv Q_\rho(xy) R_{\rho-1}(xy) + R_\rho(xy)$$

otrzymamy:

$$r(xy) \mid R_{\rho-2}(xy) \ldots$$

Ostatecznie:

$$r(xy) \mid g(xy) \text{ i } r(xy) \mid f(xy).$$

Poprzednio widzieliśmy, że jeżeli:

$h(xy) \mid f(xy)$ i $h(xy) \mid g(xy)$ i $st'_y h(xy) > 0$,

to: $h(xy) \mid R_\rho(xy)$, więc $h(xy) \mid r(xy) \,.\, k(x)$.

Załóżmy, że $h(xy)$ nie posiada czynników zależnych od samego x, stopnia dodatniego, to $[h(xy), k(x)] \equiv 1$, skąd:

$$h(xy) \mid r(xy).$$

Wielomian $r(xy)$ możnaby nazwać największym wspólnym podzielnikiem f i g dla dzielników nie zawierających czynników zależnych od samego tylko x, stopnia dodatniego. Oddzielmy teraz od $f(xy)$ najwyższy podzielnik $q(x)$ zależny od x i tak samo od $g(xy)$ najwyższy podzielnik $s(x)$. Niechaj:

$$t(x) \equiv [q(x), s(x)],$$
$$R(xy) \equiv t(x) \,.\, r(xy).$$

Mamy tu:

(1) $t(x) \mid f(xy)$, $t(x) \mid g(xy)$,
$f(xy) = t(x) f'(xy)$, $g(xy) = t(x) g'(xy)$.
$r(xy) \mid f(xy)$, $r(xy) \mid g(xy)$, więc $r(xy) \mid t(x) f'(xy)$,
$r(xy) \mid t(x) g'(xy)$ i $[r(xy), t(x)] = 1$, skąd:
$r(xy) \mid f'(xy)$, $r(xy) \mid g'(xy)$,
$f'(xy) = f''(xy) \cdot r(xy)$, $g'(xy) = g''(xy) r(xy)$,
$f(xy) = t(x) r(xy) f''(xy)$, $g(xy) = t(x) r(xy) g''(xy)$,
$R(xy) \mid f(xy)$, $R(xy) \mid g(xy)$.

(2) Jeżeli $l(xy) \mid f(xy)$ i $l(xy) \mid g(xy)$, to oddzielmy od $l(xy)$ najwyższy podzielnik $m(x)$ tak, że:
$l(xy) = m(x) \cdot l'(xy)$.
Wtedy: $l'(xy) \mid r(xy)$, $r(xy) = l'(xy) \cdot l''(xy)$.
$m(x) \mid f(xy)$, $m(x) \mid g(xy)$, zatem:
$m(x) \mid t(x) r(xy) f''(xy)$, $m(x) \mid t(x) r(xy) g''(xy)$,
$m(x)$ pierwsze względem rf'' i rg'', skąd:
$m(x) \mid t(x)$, $t(x) = m(x) \cdot t'(x)$.
$R(xy) = m(x) t'(x) \cdot l'(xy) \cdot l''(xy)$.
$= l(xy) \cdot t'(x) \cdot l''(xy)$
i ostatecznie: $l(xy) \mid R(xy)$.

Widzimy więc, że $R(xy)$ jest jednym z największych wspólnych podzielników dla $f(xy)$ i $g(xy)$.

Dla $f(xy) = 0$, $g(xy) \neq 0$ widzimy, że $g(xy)$ jest jednym z największych wspólnych podzielników.

Dla $f = 0$ i $g = 0$ największego wspólnego podzielnika brak.

Tw. Jeżeli $R(xy)$ jest największym wspólnym podzielnikiem dla $f(xy)$ i $g(xy)$, to wszystkie inne mają postać: $AR(xy)$, $A \varepsilon q_2$, $A \neq 0$.

Dem. Dowód jak dla jednej zmiennej.

Df. *Głównym największym wspólnym podzielnikiem* dla $f(xy)$ i $g(xy)$ nazwiemy ten, w któ-

rym *główny* wyraz jego postaci zredukowanej ma spółczynnik 1. Ten też oznaczamy przez:

$$[f(xy), g(xy)].$$

Tw. Dla łańcuchowego dzielenia $f(xy)$ i $g(xy)$ względem y otrzymamy jak dla jednej zmiennej: istnieją wielomiany $P(xy)$ i $Q(xy)$ takie, że:

$$P(xy)f(xy) + Q(xy)g(xy) \equiv R_{\rho+1}(x).$$

Dem. Analogicznie jak dla jednej zmiennej.

Tw. Jeżeli $h(xy) \mid f(xy)g(xy)$, $h(xy)$ *nierozkładalne*, to $h \mid f$ lub $h \mid g$.

Dem. Jeżeli $st'_y h(xy) = 0$, to twierdzenie słuszne wedle tw. nr. 4. Jeżeli $st'_y h > 0$ i *nie* $h \mid f$, to $[h, f] = 1$. Wtedy jednak:

$$0 \not\equiv R_{\rho+1}(x) \equiv P(xy)f(xy) + Q(xy)h(xy),$$

$[R_{\rho+1}(x)$ odnośnie do f i $h]$.

Stąd: $h(xy) \mid R_{\rho+1}(x)g(xy)$;

$h(xy)$ nie może zawierać czynników zależnych od samego x stopnia dodatniego, gdyż jest *nierozkładalne* i $st'_y h > 0$, więc $[h, R_{\rho+1}] = 1$.

Z drugiej strony:

$$R_{\rho+1}(x)g(xy) \equiv h(xy) \,.\, l(xy).$$

$R_{\rho+1} \mid h \,.\, l$, więc $R_{\rho+1}(x) \mid l(xy)$,

$$l(xy) = R_{\rho+1}(x) \,.\, l'(xy),$$

$$R_{\rho+1}(x)g(xy) \equiv h(xy) \,.\, R_{\rho+1}(x)l'(xy),$$

$$R_{\rho+1}(x)[g(xy) - h(xy)l'(xy)] \equiv 0,$$

$$R_{\rho+}(x) \not\equiv 0,\ g(xy) - h(xy)l'(xy) \equiv 0,$$

$$g(xy) \equiv h(xy) \,.\, l'(xy),\ h(xy) \mid g(xy).$$

Tw. Jeżeli $h(xy) \mid f(xy)g(xy)$ i $[h, f] \equiv 1$, to $h \mid g$.

Dem. Jeżeli $h(xy)$ *nierozkładalne*, to twier-

dzenie słuszne wedle tw. poprzedniego. Jeżeli nie, to rozłóżmy $h(xy)$ na nierozkładalne rzędu > 0.

$$h(xy) \equiv h_1(xy) \dots h_p(xy).$$

Wtedy: $h_1 \mid fg$, $[h_1, f] \equiv 1$, więc $h_1 \mid g$.

Stąd:
$$g(xy) \equiv h_1(xy) \,.\, g_1(xy),$$
$$fg \equiv h \,.\, l \equiv h_1 h_2 \dots h_p \,.\, l,$$
$$fg_1 h_1 \equiv h_1 h_2 \dots h_p \,.\, l,$$
$$(fg_1 - h_2 \dots h_p l) h_1 \equiv 0, \quad h_1 \not\equiv 0,$$
$$fg_1 \equiv h_2 \dots h_p l, \; h_2 \mid fg_1, \; [h_2, f] \equiv 1, \; h_2 \mid g_1.$$

Stąd znów:
$$g_1 \equiv h_2 \,.\, g_2,$$
$$fg_1 \equiv h_2 h_3 \dots h_p l,$$
$$(fg_2 - h_3 \dots h_p l)\, h_2 \equiv 0, \quad h_2 \not\equiv 0,$$
$$fg_2 \equiv h_3 \dots h_p l, \; h_3 \mid fg_2, \; [h_3, f] \equiv 1, \; h_3 \mid g_2,$$

i t. d. Ostatecznie:

$$g \equiv h_1 h_2 \dots h_p g_p \equiv h \,.\, g_p, \; h \mid g.$$

Każdy wielomian $h(xy)$ *rozkładalny* można przedstawić w postaci iloczynu:

$$h \equiv h_1 \dots h_p,$$

gdzie: $h_1 \dots h_p$ *nierozkładalne* rzędu > 0.

Przypuśćmy, że przedstawiono w ten sposób $h(xy)$ jako:

$$h \equiv h_1 \dots h_p$$
$$h \equiv h'_1 \dots h'_q \,.$$

Widocznie: $h_1 \mid h_1' \dots h'_q$, więc:

$$h_1 \mid h_1' \text{ lub } h_1 \mid h_2' \text{ lub } h_1 \mid h'_q \,.$$

Naprz.: $h_1 \mid h_i'$, lecz h_i' nierozkładalne,

więc: $h_i' \equiv A_1 h_1, \; A_1 \varepsilon q_2, \; A_1 \not\equiv 0,$

$$h_1 \dots h_p \equiv A_1 h_1 \,.\, h_1' \dots h'_{i-1} h'_{i+1} \dots h'_q,$$

$$h_1\{h_2 \ldots h_p - A_1 h_1' \ldots h'_{i-1} h'_{i+1} \ldots h'_q\} \equiv 0,$$
$$h_1 \not\equiv 0,\ h_2 \ldots h_p \equiv A_1 h_1' \ldots h'_{i-1} h'_{i+1} \ldots h'_q.$$

Postępując dalej w ten sposób, zrozumiemy, że: $p = q$ i, że $h_1' \ldots h'_q$ różnią się od $h_1 \ldots h_p$ ew. *porządkiem* i *czynnikami stałemi,* różnemi od zera. Powiemy:

Tw. Rozkład wielomianu $h(xy)$ na czynniki *nierozkładalne* rzędu dodatniego jest możliwy w *jeden* tylko *istotny* sposób.

Czytelnik zechce sam już odtworzyć sobie bieg teorji podzielności i największego wspólnego podzielnika dla więcej niż dwu zmiennych.

Muszę zauważyć, że z pośród różnych metod wykładu teorji podzielności więcej niż jednej zmiennej, wybrałem metodę zbliżoną do wyłożonej w znakomitej książce M. Bôchera: Introduction to the higher Algebra [tłum. niemieckie H. Becka z roku 1910]. Wprowadziłem jednak pewne modyfikacje, pragnąc rzecz przedstawić jeszcze nieco prościej.

Rozdział IV.

Pierwiastki Wielomianów.

§ 1. Zasadnicze twierdzenie Algebry jednej zmiennej.

1. **Df.** Umówimy się nazywać *pierwiastkiem* lub lepiej *miejscem zerowem* funkcji $f(z)$ liczbę zespoloną a, o ile $f(a) = 0$. Jednocześnie miejsca zerowe funkcji f są *pierwiastkami* czy *rozwiązaniami równania:* $f(z) \overset{?}{=} 0$ [czyt. „$f(z)$ kiedy równe zeru"].

Dla nas powstaje niezmiernie ważny problem:

Dany jest wielomian jednej zmiennej $f(z)$. Zapytujemy, czy *istnieje choć jedno miejsce zerowe* (pierwiastek) tego *wielomianu?*

Rozważmy przedewszystkiem dwa wypadki elementarne:

1. *wypadek:* $f(z) = 0$, wtedy *każda liczba zespolona* jest *pierwiastkiem.*

2. *wypadek:* $st'f = 0$, $f(z) = A \neq 0$. Wtedy *żadna liczba nie jest pierwiastkiem.*

Pozostaje nam wypadek: $st'f > 0$.

Tutaj rozstrzyga tak zwane *zasadnicze twierdzenie Algebry*, które brzmi:

Tw. *Każdy wielomian $f(z)$, stopnia większego niż zero posiada choć jedno miejsce zerowe (pierwiastek).*

Dem. Przystępujemy do dowodu tego, tak zasadniczego twierdzenia. Dowód, zresztą elementarny, rozłożymy sobie na kilka części.

Zakładamy zatem, że $f(z)$ jest *wielomianem* i że $st'f > 0$.

I. Zamiast szukać miejsc zerowych dla $f(z)$, szukajmy miejsc zerowych dla $|f(z)|$, co wyjdzie na to samo, gdyż liczba zespolona zeruje się jednocześnie wraz ze swą wartością bezwzględną.

II. Jeżeli pisać będziemy $x = R'z$, $y = I'z$, $z = x + yi$, to każdej parze liczb rzeczywistych x, y odpowiada jedyne $z = x + yi$, a temu z wartość określona $|f(z)|$, tak, że gdy położymy:

$$\varphi(xy) = |f(x + yi)|$$

otrzymamy funkcję *rzeczywistą* $\varphi(xy)$, określoną dla *wszelkich* par *rzeczywistych* (xy), a zadanie nasze polegać będzie na odszukaniu takiej pary

liczb rzeczywistych (x, y), by $\varphi(xy) = 0$, gdyż jeszcze naodwrót:

$$|f(z)| = \varphi\{R'z, I'z\}.$$

III. $\lim_{z|\infty} |f(z)| = \lim_{z|\infty} f(z) = \infty$, gdyż $st' f > 0$ [str. 48].

Obierzmy takie $R_0 (> 0)$, by dla $|z| \geq R_0$ było już: $|f(z)| > 1$, a więc dla:

$$x^2 + y^2 \geq R^2_0 \text{ mieć będziemy:}$$

$$|\varphi(xy)| > 1.$$

Miejsc zerowych, czy to dla $f(z)$ czy $|f(z)|$, czy $\varphi(xy)$ szukać możemy zatem jedynie w obrębie wnętrza koła: $|z| < R_0$ czy $x^2 + y^2 < R_0^2$.

IV. Funkcja $\varphi(xy)$ jest *ciągła* względem (x, y) dla wszelkich x i y rzeczywistych. Rozważmy bowiem dany punkt x_0, y_0 i nb. $z_0 = x_0 + y_0 i$, $\varepsilon > 0$. Ponieważ $f(z)$ jest ciągła w $z = z_0$, więc dobierzemy takie $\delta > 0$, że dla:

$$|z - z_0| < \delta \qquad (1)$$

będzie już: $|f(z) - f(z_0)| < \varepsilon$.

Zatem: dla $|x - x_0| < \sqrt{\tfrac{1}{2}\delta}$, $|y - y_0| < \sqrt{\tfrac{1}{2}\delta}$ będzie:

$$|\varphi(xy) - \varphi(x_0 y_0)| = \big||f(z)| - |f(z_0)|\big| \leq$$
$$\leq |f(z) - f(z_0)| < \varepsilon,$$

przyczem położono tu: $z = x + yi$.

V. W obrębie koła $x^2 + y^2 \leq R_0^2$ funkcja ciągła $\varphi(xy)$ jest *ograniczona* i *przybiera w pewnym* punkcie (x_0, y_0) tego koła swój *kres dolny*, powiedzmy μ.

$$\varphi(x_0 y_0) = \mu, |f(z_0)| = \mu, z_0 = x_0 + y_0 i.$$

VI. Wystarczy udowodnić, że $\mu = 0$. Idea dowodu polegać będzie na tem, że gdyby w jakimś punkcie $(x_0 y_0)$ było $\varphi(x_0 y_0) \neq 0$ (więc > 0), to na pewnym promieniu, wychodzącym z $(x_0 y_0)$ wartości $\varphi(xy)$ byłyby w pobliżu tego punktu mniejsze niż $\varphi(x_0 y_0)$. Zatem $\varphi(x_0 y_0)$ nie byłoby wartością kresu dolnego, nawet w sensie lokalnym.

Uw. Rozważając powierzchnię $Z = \varphi(xy)$ w układzie osi (x, y, Z) moglibyśmy udowodnić, że o ile $\varphi(x_0 y_0) \neq 0$, to powierzchnia przedstawia około tego punktu obraz taki, jak przełęcz w górach z której, w pewną stronę idąc, można zawsze zejść *niżej*.

Niech będzie zatem $0 < \mu = \varphi(x_0 y_0) = |f(z_0)|$, $f(z_0) \neq 0$. Rozważmy $f(z_0 + h)$ dla dowolnych h zespolonych.

Możemy rozwinąć $f(z_0 + h)$ wedle potęg h [str. 42].

$$f(z_0 + h) \equiv f(z_0) + \frac{h}{1!} f'(z_0) + \cdots + \frac{h^n}{n!} f^{(n)}(z_0),$$

gdzie $n = st' f > 0$.

Napewne $f^{(n)}(z_0) \neq 0$, gdyż kładąc:

$$f(z) \equiv a_0 z^n + \cdots + a_n. \quad a_0 \neq 0$$

mamy: $n!\, a_0 = f^{(n)}(z) = f^{(n)}(z_0) \neq 0.$

Może być jednak:

$$f'(z_0) = \cdots = f^{(\lambda-1)}(z_0) = 0, \; f^{(\lambda)}(z_0) \neq 0$$
$$0 \leqq \lambda \leqq n.$$

Zatem napiszemy:

$$f(z_0 + h) = f(z_0) + \frac{f^{(\lambda)}(z_0)}{\lambda!} h^\lambda + \cdots + \frac{f^{(n)}(z_0)}{n!} h^n,$$

skąd:

$$\frac{f(z_0 + h)}{f(z_0)} = 1 + \frac{f^{(\lambda)}(z_0)}{\lambda! f(z_0)} h^\lambda + \cdots + \frac{f^{(n)}(z_0)}{n! f(z_0)} h^n.$$

Położymy: $h = re^{\varphi i}$, $\frac{f^{(s)}(z_0)}{s!\,f(z_0)} = r_s e^{\varphi_s i}$,

$s = \lambda, \ldots n$, $r_\lambda > 0$, $r_n > 0$, $r, r_\lambda \ldots r_n, \varphi, \varphi_\lambda \ldots \varphi_n$ rzeczywiste.

Otrzymamy:

$$\frac{f(z_0+h)}{f(z_0)} = 1 + r^\lambda r_\lambda e^{(\lambda\varphi+\varphi_\lambda i)} + \cdots + r^n r_n e^{(n\varphi+\varphi_n)i}.$$

Kładziemy najpierw: $\lambda\varphi + \varphi_\lambda = \pi$, $\varphi = \frac{\pi - \varphi_\lambda}{\lambda}$, co wyznacza pewien określony promień dla $z_0 + h$. Wtedy:

$$\frac{f(z_0+h)}{f(z_0)} = (1 - r^\lambda r_\lambda) + \cdots + r^n r_n e^{(n\varphi+\varphi_n)i}.$$

Jeżeli $\lambda = n$, to $\frac{f(z_0+h)}{f(z_0)} = 1 - r^\lambda r_\lambda$, więc obierając:

$$0 < r < \frac{1}{\sqrt[\lambda]{r_\lambda}},$$

dostaniemy:

$$\left|\frac{f(z_0+h)}{f(z_0)}\right| < 1,$$

$$|f(z_0+h)| < |f(z_0)|,$$

$$\varphi(xy) < \varphi(x_0 y_0),\ x + yi = z_0 + h.$$

Jeżeli $\lambda < n$, to:

$$\frac{f(z_0+h)}{f(z_0)} = (1 - r^\lambda r_\lambda) + r^{\lambda+1} r_{\lambda+1} e^{[(\lambda+1)\varphi+\varphi_{\lambda+1}]i} + \cdots + r^n r_n e^{(n\varphi+\varphi_n)i}.$$

Kładąc: $m = \max\{r_{\lambda+1}, \ldots r_n\}$

otrzymamy:

$$\left|\frac{f(z_0+h)}{f(z_0)}\right| \leqq |1-r^\lambda r_\lambda| + m\{r^{\lambda+1}+\cdots+r^n\}$$

[pamiętamy, że dla $\sigma \varepsilon q$ mamy $|e^{\sigma i}|=1$!]

Otóż: $r^\lambda r_\lambda$, $r^{\lambda+1},\ldots r^n$ dążą do zera wraz z r, zatem obierając odpowiednie $\delta>0$, mieć będziemy:

$$1-r^\lambda r_\lambda > 0$$

oraz: $$1-r^\lambda r_\lambda + m(r^{\lambda+1}+\cdots+r^n) < 1.$$

Więc dla wszelkich h zespolonych takich, że:

$$h = re^{\varphi i},\ 0<r<\delta,\ \varphi = \frac{\pi-\varphi_\lambda}{\lambda}$$

będzie:

$$\left|\frac{f(z_0+h)}{f(z_0)}\right| < 1$$

czyli:

$$|f(z_0+h)| < |f(z_0)|$$

$$\varphi(x\,y) < \varphi(x_0 y_0),\ x+yi = z_0+h.$$

Ponieważ $\mu = \varphi(x_0 y_0)$ ma być kresem dolnym, więc widzimy, że nie może być $\mu>0$. Zatem $\varphi(x_0 y_0)=0$, $f(z_0)=0$ i odszukaliśmy choć jedno miejsce zerowe dla wielomianu $f(z)$.

2. **Inny dowód twierdzenia zasadniczego.**

Teorja funkcyj analitycznych pozwala nam podać dowód twierdzenia zasadniczego w kilku wierszach. Założymy, że wielomian $f(z)$ jest stale różny od zera i że $sl' f>0$.

Połóżmy $g(z) \equiv -\frac{1}{f(z)}$; byłaby to funkcja określona w *całej* płaszczyźnie, posiadająca *wszędzie* pochodną $g'(z) = -\frac{f'(z)}{f^2(z)}$ zatem funkcja *całkowita* (entière). Ponieważ: $\lim\limits_{z|\infty} f(z) = \infty$, gdyż $sl' f>0$, więc $\lim\limits_{z|\infty} g(z) = 0$, a więc $g(z)$ byłoby *wielomianem identycznie zerowym* [str. 49], co przecież niemożliwe. Zatem choć raz na płaszczyźnie $f'(z)=0$.

3. **Czynniki pierwiastkowe.**

Załóżmy, że $f(z)$ jest wielomianem. Badajmy podzielność $f(z)$ przez $(z-a)$, gdzie $a \varepsilon q_2$. Wedle rozkładu Euklidesa mamy:

$$f(z) \equiv Q(z)(z-a) + R(z),$$

Q i R wielomiany, $R(z)$ stopnia niższego niż $(z-a)$.

Stąd: $R(z) \equiv \text{const.}\ (= \text{lub} \neq 0).$

$$R(z) \equiv R.$$

Kładąc $z = a$, otrzymamy: $f(a) = R$, zatem:

$f(z) \equiv Q(z)(z-a) + f(a)$. Stąd:

Tw. Warunkiem koniecznym i dostatecznym, by $f(z)$ było podzielne przez $(z-a)$ jest $f(a) = 0$, czyli należenie a do pierwiastków wielomianu $f(z)$.

Df. Wielomian $z-a$ nazywa się *czynnikiem* pierwiastkowym dla wielomianu $f(z)$, gdy a jest pierwiastkiem dla $f(z)$.

Wtedy i tylko wtedy: $z-a \mid f(z)$.

Załóżmy, że $st'f = n > 0$. Wielomian $f(z)$ posiada choć jeden pierwiastek a_1, więc $f(z) = Q_1(z).(z-a_1)$, gdzie $Q_1(z)$ jest wielomianem i $st'Q_1 = n-1$. Jeżeli $n-1 > 0$, to $Q_1(z)$ posiada choć jeden pierwiastek a_2 i $Q_1(z) = Q_2(z)\ (z-a_2)$, gdzie Q_2 jest wielomianem i $st'Q_2 = n-2$, $f(z) \equiv Q_2(z)\ (z-a_1)\ (z-a_2)$, $f(a_2) = 0$.

Postępując w ten sposób dalej, otrzymamy ciąg:

$$a_1, a_2 \ldots a_n \qquad (1)$$

taki, że: $a_1, a_2, \ldots a_n$ są pierwiastkami dla $f(z)$ i, że:

$$f(z) \equiv Q_n(z).(z-a_1)\ldots(z-a_n),$$

przyczem: $st'Q_n(z) = 0$ $Q_n(z) \equiv A \neq 0$, gdyż inaczej byłoby $f(z) \equiv 0$.

Df. Ciąg: $a_1, a_2, \ldots a_p$

nazywa się *pełnym ciągiem pierwiastków* wielomianu $f(z)$ *niezerowego*, gdy:

$$f(z) \equiv A(z-a_1)\ldots(z-a_p),\ A \in q_2,\ A \neq 0.$$

Mamy tu zaraz twierdzenia:

Tw. (1) Każdy wielomian $f(z)$ stopnia >0 posiada choć jeden pełny ciąg pierwiastków.

(2) Ilość członów pełnego ciągu pierwiastków

$$a_1, a_2, \ldots a_p$$

jest równa stopniowi wielomianu:

$$st'\, f(z) = p,$$

zatem wszystkie pełne ciągi pierwiastków mają tę samą ilość członów.

(3) Każdy pierwiastek wielomianu $f(z) \not\equiv 0$ figuruje choć raz w każdym pełnym ciągu jego pierwiastków.

(4) Różne ciągi pełne tego samego wielomianu niezerowego różnić się mogą między sobą jedynie *porządkiem* członów.

(5) Każdy pierwiastek a wielomianu niezerowego figuruje w każdym ciągu pełnym jego pierwiastków taką samą ilość razy α (α całkowite, >0) przyczem:

Df. α zwie się *rzędem* pierwiastka a względem $f(z)$.

(6) Wielomian stopnia n posiada *najwyżej* n **różnych** pierwiastków.

Dem. (1) Wynika z przeprowadzonego badania.

(2) Wtedy bowiem:

$$f(z) \equiv A(z-a_1)\ldots(z-a_p),\ A \neq 0,$$

więc:

$$st'f = st'(A\hat{z}^0) + st'(\hat{z} - a_1) + \cdots + st'(\hat{z} - a_p) = \\ = 0 + 1 + \cdots + 1 = p.$$

(3) Jeżeli b jest pierwiastkiem dla f, więc $f(b) = 0$, to:

$$0 = A(b - a_1) \ldots (b - a_p),\ A \neq 0,$$

więc: $b - a_1 = 0$ lub ... lub $b - a_p = 0$,

zatem: $b = a_1$ lub ... lub $b = a_p$.

(4) Jeżeli: $a_1, \ldots a_p$ i $b_1 \ldots b_p$ są pełnemi ciągami dla $f(z)$ $(\not\equiv 0)$, to:

$$f(z) \equiv A(z - a_1) \ldots (z - a_p),\ A \neq 0, \\ \equiv B(z - b_1) \ldots (z - b_p),\ B \neq 0.$$

Ale: $f(b_1) = 0$, więc $b_1 = a_{i_1}$ $1 \leq i_1 \leq p$ całkowite,

$$f(z) \equiv Q_1(z)(z - b_1) \equiv A(z - a_1) \ldots \\ \ldots (z - a_{i_1 - 1}) \cdot (z - a_{i_1 + 1}) \ldots (z - a_p)(z - b_1)$$

$$[Q_1(z) - A(z - a_1) \ldots (z - a_{i_1 - 1})(z - a_{i_1 + 1}) \ldots (z - a_p)] \cdot (z - b_1) \equiv 0,$$

stąd:

$$Q_1(z) \equiv A(z - a_1) \ldots (z - a_{i_1 - 1})(z - a_{i_1 + 1}) \ldots (z - a_p),$$

bo $z - b_1 \not\equiv 0$, więc:

$$Q_1(z) - A(z - a_1) \ldots (z - a_{i_1 - 1})(z - a_{i_1 + 1}) \ldots (z - a_p).$$

nie może mieć stopnia. Z drugiej strony:

$$f(z) \equiv (z - b_1) \cdot Q_1(z) \\ \equiv B(z - b_2) \ldots (z - b_p) \cdot (z - b_1),$$

więc: $Q_1(z) \equiv B(z - b_2) \ldots (z - b_p)$,

gdyż rozkład Euklidesa jest *jedyny*.

Dalej:

$$Q_1(b_2) = 0,\ Q_1(z) \equiv A(z - a_1) \ldots (z - a_{i_1 - 1}) \cdot \\ \cdot (z - a_{i_1 + 1}) \ldots (z - a_p),$$

więc znów: $b_2 = a_{i_2}$, $1 \leq i_2 \leq p$, całkowite i $i_1 \neq i_2$ i t. d.

Postępując w ten sposób, otrzymamy:

$$b_1 = a_{i_1},\ b_2 = a_{i_2} \ldots b_p = a_{i_p}$$

$i_1, i_2, \ldots i_p$ *różne* między sobą, całkowite, $\geqq 1$, $\leqq p$, co dowodzi twierdzenia.

(5) Wynika bezpośrednio z (4).

(6) Wynika z (2) i (3).

Df. Jeżeli $a_1, a_2 \ldots a_p$ jest pełnym ciągiem pierwiastków wielomianu $f(z)$ niezerowego, to rozkład:

$$f(z) \equiv A(z - a_1) \ldots (z - a_p)$$

nazywa się rozkładem $f(z)$ na czynniki *(linjowe pierwiastkowe)*. A jest *stałą rozkładu.*

Tw. Rozkłady wielomianu $f(z)$ niezerowego na czynniki linjowe różnią się co najwyżej porządkiem czynników linjowych (1^{go} stopnia); stałe tych rozkładów są jednakowe.

Dem. Nb. $f(z) \equiv A(z - a_1) \ldots (z - a_p)$, $A \neq 0$

$$\equiv B(z - b_1) \ldots (z - b_p),\ B \neq 0,$$

to wiemy już, że: $a_1 \ldots a_p$ i $b_1 \ldots b_p$
różnią się najwyżej porządkiem,
zatem: $(z - a_1) \ldots (z - a_p) \equiv (z - b_1) \ldots (z - b_p)$,
stąd: $(A - B)(z - a_1) \ldots (z - a_p) \equiv 0$,
co pociąga, że $A = B$, gdyż:

$$z - a_s \neq 0,\ s = 1, 2 \ldots p.$$

Cor. Stała rozkładu A da się wyznaczyć w sposób następujący:

Jeżeli: $f(z) \equiv a_0 z^p + \cdots + a_p$, $a_0 \neq 0$,
to: $A = a_0$, gdyż:

$$a_0 z^p + \cdots + a_p \equiv A(z - a_1) \ldots (z - a_p);$$

dzielimy obie strony przez z^p (dla $z \neq 0$), co da nam:

$$a_0+\frac{a_1}{z}+\cdots+\frac{a_p}{z^p}=A\left(1-\frac{a_1}{z}\right)\cdots\left(1-\frac{a_p}{z}\right)$$

i zdążamy z z do ∞, wtedy w granicy otrzymamy:

$$a_0=A.$$

Uw. Widzieliśmy już, że spółczynnik najwyższej potęgi z wielomianu $f(z)$ w jego postaci zredukowanej równa się $\frac{f^{(p)}(0)}{p!}$, gdzie $p=st'f$.

Uw. Wielomian niezerowy $f(z)$ stopnia p jest *kanonicznym*, gdy $\frac{f^{(p)}(0)}{p!}=1$, gdy zatem jego spółczynnik najwyższej potęgi z w postaci zredukowanej jest *jedynką*. Stałą rozkładu jest wtedy jedność.

Niech będzie $f(z)$ wielomianem stopnia >0; $a_1,\ldots a_p$ pełnym ciągiem jego pierwiastków. Jeżeli:

$$b_1,\ldots b_r$$

są wszystkiemi różnemi wartościami członów tego ciągu, więc wszystkiemi *różnemi* pierwiastkami $f(z)$, a liczby $\alpha_1\ldots\alpha_r$ ich *rzędami*, to widocznie:

$$f(z)\equiv A(z-a_1)\ldots(z-a_p)\equiv$$
$$\equiv A(z-b_1)^{\alpha_1}\ldots(z-b_r)^{\alpha_r}$$

($\alpha_1,\ldots\alpha_r$ całkowite, >0).

Df. Rozkład: $f(z)\equiv A(z-b_1)^{\alpha_1}\ldots(z-b_r)^{\alpha_r}$, $A\neq 0$, gdzie: $b_1\ldots b_r$ są wszystkiemi *różnemi* pierwiastkami $f(z)$ niezerowego, $\alpha_1\ldots\alpha_r$ ich odpowiedniemi rzędami, zwie się *rozkładem* na *dzielniki pierwiastkowe*, A jego *stałą*.

Df. $(z-b)^{\alpha}$ zwie się *dzielnikiem* pierwiastkowym dla $f(z)$ niezerowego, gdy b jest *pierwiastkiem* f i α jego *rzędem*.

Mamy tu twierdzenie:

Tw. (1) Każdy wielomian stopnia dodatniego posiada choć jeden rozkład na dzielniki pierwiastkowe.

(2) Jeżeli $A(z-b_1)^{\alpha_1}\dots(z-b_r)^{\alpha_r}$ jest rozkładem dla $f(z)$, to $r \leq p$, $\alpha_1+\dots+\alpha_r = p$, gdzie $p = st' f(>0)$.

(3) Różne rozkłady tego samego $f(z)$ mogą się różnić jedynie porządkiem dzielników pierwiastkowych; stałe rozkładów są jednakowe.

Dem.

(1) Wynika z przeprowadzonego badania.

(2) Wynika z definicji i porównania stopni obu stron.

(3) Wynika z definicji i analogicznego twierdzenia dla rozkładu na czynniki linjowe.

Uwagi. Niezmiernie często spotyka się jeszcze staromodne przekonanie, jakoby wielomian stopnia p posiadał p pierwiastków, przyczem *„niektóre z nich mogą być równe między sobą“*. Jest to przeżytek z niekrytycznych czasów, gdy niebardzo odróżniano **ciąg** zupełny pierwiastków, posiadający p członów, od *zbioru pierwiastków* posiadającego r elementów, gdzie $r \leq p$.

Df. Pierwiastek a rzędu α nazywają też często pierwiastkiem *wielokrotnym*, o *krotności* α. Nie należy jednak mówić przestarzałym sposobem, że wtedy wielomian „posiada α pierwiastków **równych** a“! Tradycję należy szanować, lecz nie tam, gdzie prowadziłoby to do absurdu!

4. **Rząd pierwiastka** wielomianu jednej zmiennej.

Określiliśmy już pojęcie *rzędu* α pierwiastka a

wielomianu $f(z)$ niezerowego, jak również odnośnego *dzielnika* pierwiastkowego $(z-a)^{\alpha}$.

Niechaj, dla $f(z) \not\equiv 0$, będzie dany rozkład na *dzielniki* pierwiastkowe:

$$f(z) \equiv A(z-a_1)^{\alpha_1} \dots (z-a_r)^{\alpha_r}, \quad A \neq 0,$$
$$r \leqq p, \; a_1 \dots a_r \text{ różne}, \; p = sl' f > 0.$$

Widzimy, że:

$$(z-a_s)^{\alpha_s} \mid f(z), \; s = 1, \dots r, \; \alpha_s > 0$$

całkowite. Tem samem:

$$(z-a_s)^{\beta} \mid f(z), \text{ gdzie } 0 \leqq \beta \leqq \alpha_s$$

całkowite. Przypuśćmy, że:

$$(z-a_s)^{\beta} \mid f(z), \text{ gdzie } \beta > \alpha_s, \text{ całkowite.}$$

Wtedy: $\beta = \alpha_s + h, \; h > 0$, całkowite:

$$f(z) \equiv Q(z)(z-a_s)^{\beta} \quad (Q \text{ jest wielomianem}).$$

Stąd:

$$Q(z).(z-a_s)^h.(z-a_s)^{\alpha_s} \equiv A(z-a_1)^{\alpha_1} \dots (z-a_{s-1})^{\alpha_{s-1}}.$$
$$.(z-a_{s+1})^{\alpha_{s+1}} \dots (z-a_r)^{\alpha_r}(z-a_s)^{\alpha_s}$$

Stąd znów:

$$[Q(z)(z-a_s)^h - A(z-a_1)^{\alpha_1} \dots (z-a_{s-1})^{\alpha_{s-1}}.$$
$$.(z-a_{s+1})^{\alpha_{s+1}} \dots (z-a_r)^{\alpha_r}].(z-a_s)^{\alpha_s} \equiv 0,$$

a więc, skoro $(z-a_s)^{\alpha_s} \not\equiv 0$, otrzymujemy:

$$Q(z)(z-a_s)^h \equiv A(z-a_1)^{\alpha_1} \dots (z-a_{s-1})^{\alpha_{s-1}}.$$
$$.(z-a_{s+1})^{\alpha_{s+1}} \dots (z-a_r)^{\alpha_r}.$$

Kładąc: $z = a_s$ i uwzględniając, że:

$\alpha_1, \dots \alpha_r > 0$, $a_1 \dots a_{s-1}, \; a_{s+1} \dots a_r$ różne od a_s, dostaniemy:

$$0 = A(a_s - a_1)^{\alpha_1} \dots (a_s - a_{s-1})^{\alpha_{s-1}}(a_s - a_{s+1})^{\alpha_{s+1}} \dots$$
$$\dots (a_s - a_r)^{\alpha_r},$$

więc: $a_s = a_1$ lub $\dots a_s = a_{s-1}$ lub $a_s = a_{s+1} \dots$
$\dots$ lub $a_s = a_r$,

co niemożliwe. Mamy zatem twierdzenie:

Tw. *Rząd* α pierwiastka a wielomianu niezerowego $f(z)$ jest największym wykładnikiem β całkowitym takim, że:

$$(z-a)^{\beta} \mid f(z).$$

Dla α mamy: $f(z) \equiv Q(z)(z-a)^{\alpha}$, $Q(a) \neq 0$, Q jest wielomianem.

Inne kryterjum dla rzędu dadzą nam pochodne:

Tw. Warunkiem koniecznym i dostatecznym, by α było *rzędem* pierwiastka a wielomianu niezerowego $f(z)$, jest:

$$f(a) = 0,\ f'(a) = 0 \ldots f^{(\alpha-1)}(a) = 0,\ f^{(\alpha)}(a) \neq 0.$$

Dem. 1. *Dostateczność.*

Rozwińmy $f(z)$, stopnia $p(>0)$, wedle potęg $(z-a)$:

$$f(z) \equiv A_0(z-a)^p + \cdots + A_p,$$

gdzie [str. 48]:

$$A_s = \frac{f^{(p-s)}(a)}{(p-s)!},\ s = 0, 1, \ldots p.$$

Z założenia będzie:

$$A_p = A_{p-1} = \cdots = A_{p-\alpha+1} = 0,\ A_{p-\alpha} \neq 0,$$

więc:

$$\begin{aligned} f(z) &\equiv A_0(z-a)^p + \cdots + A_{p-\alpha}(z-a)^{\alpha} \\ &\equiv (z-a)^{\alpha}\left[A_0(z-a)^{p-\alpha} + \cdots + A_{p-\alpha}\right] \\ &\equiv (z-a)^{\alpha} Q(z), \end{aligned}$$

gdzie: $Q(a) = A_{p-\alpha} \neq 0$, więc:

$(z-a)^{\alpha} \mid f(z)$, lecz *nie* $(z-a)^{\beta} \mid f(z)$, gdy $\beta > \alpha$, całkowite.

2. *Konieczność.*

Gdy α jest rzędem dla a, to:

$f(z) = Q(z)(z-a)^{\alpha}$, $Q(a) \neq 0$, Q jest wielomianem.

$$f(z) \equiv A_0(z-a)^p + \cdots + A_p$$

$$p = sl'f,\ A_s = \frac{f^{p-s}(a)}{(p-s)!},\ s = 0, 1, \ldots p.$$

Stąd: $Q(z)(z-a)^\alpha \equiv A_0(z-a)^p + \cdots + A_p$

Biorąc pochodną obu stron rzędu $s = 0, 1, 2 \ldots \alpha - 1$ i kładąc za każdym razem $z = a$, otrzymamy:

$$A_p = 0,\ A_{p-1} = 0, \ldots A_{p-\alpha+1} = 0;$$

lecz już dla pochodnej rzędu α otrzymamy po podstawieniu $z = a$:

$$Q(a) \,.\, \alpha! = A_{p-\alpha} \,.\, \alpha!,$$

więc: $A_{p-\alpha} \neq 0$. Tem samem:

$$f^{(0)}(a) = \ldots f^{(\alpha-1)}(a) = 0,\ f^{(\alpha)} \neq 0.$$

Uw. Wyższe pochodne dla $Q(z)(z-a)^\alpha$ tworzymy wedle znanego wzoru Leibniza dla pochodnych iloczynu.

5. Interpolacja.

Tw. Przypuśćmy, że wielomiany $f(z)$ i $g(z)$ są stopnia *niższego* lub *równego* m[1] (m całkowite, $\geqq 0$), że następnie ciąg:

$$z_0, z_1, z_2, \ldots z_m$$

składa się z $m+1$ liczb *różnych* i że nakoniec:

$$f(z_i) = g(z_i) \text{ dla } i = 0, 1, \ldots m.$$

Wtedy: $f(z) \equiv g(z)$

Dem. W tych warunkach $\varphi(z) \equiv f(z) - g(z)$ jest wielomianem stopnia niższego lub równego m i przytem $\varphi(z_i) = 0$ $(i = 0, 1, \ldots m)$, zatem $\varphi(z)$

[1] znaczy to, że $f(z)$ czy $g(z)$ *posiadają stopień* $\leqq m$ lub $f(z)$ czy $g(z)$ są *identycznie zerem.*

posiada $m+1$ *różnych* pierwiastków. Dzięki tw. (6) na str. 92 musi być $\varphi(z) \equiv 0$. Stąd: $f(z) \equiv g(z)$.

Uw. Widzimy, że wielomian stopnia $\leq m$ jest jednoznacznie wyznaczony, gdy każemy mu przybierać w $m+1$ miejscach: $z_0, z_1 \ldots z_m$, określone wartości, powiedzmy:

$w_0, w_1, w_2, \ldots w_m$ (niekoniecznie różne),

pod warunkiem, *że wogóle istnieje.*

Tę ostatnią sprawę załatwia twierdzenie:

Tw. interpolacyjne Lagrange'a[1]

Gdy ciąg: $z_0, z_1 \ldots z_m$

składa się z liczb różnych, a ciąg:

$$w_0, w_1 \ldots w_m$$

z liczb zespolonych *(różnych* lub *nie),* to istnieje *jedyny wielomian* stopnia *mniejszego* lub *równego* m (m całkowite, ≥ 0), taki że:

$$f(z_i) = w_i \quad (i = 0, 1, \ldots m).$$

Dem. Zbudujmy następujący ciąg funkcyj:

$$X_s(z) \overset{\text{df}}{=} \frac{(z-z_1)\ldots(z-z_{s-1})(z-z_{s+1})\ldots(z-z_m)}{(z_s-z_1)\ldots(z_s-z_{s-1})(z_s-z_{s+1})\ldots(z_s-z_m)}$$

Są to wielomiany zawsze określone dla $s = 0 \ldots m$, gdyż $z_0, \ldots z_m$ są *różne.*

Zauważmy, że wielomiany te, zwane *wielomianami interpolacyjnemi Lagrange'a,* posiadają własność następującą:

$X_s(z_k) = 0$ dla $k = 0, 1, \ldots m$, lecz $k \neq s$

i $X_s(z_s) = 1. \qquad (s = 0, 1, \ldots m).$

Zbudujmy teraz wielomian:

$$f(z) \overset{\text{df}}{=} X_0(z) w_0 + \cdots + X_m(z) w_m.$$

---

[1] Lagrange: Journal de l'école polytéchnique 7 et 8 cahier (1812).

Widzimy odrazu, że:

$$f(z_s) = X_0(z_s)w_0 + \cdots + X_{s-1}(z_s)w_{s-1} + X_s(z_s)w_s + \\ + X_{s+1}(z_s)w_{s+1} + \cdots + X_m(z_s)w_m = \\ = X_s(z_s)w_s = w_s,\ s = 0, 1, \ldots m.;$$

tem samem wielomian $f(z)$ spełnia żądane wymagania.

Że jednak innych już wielomianów tego rodzaju niema, o tem mówi poprzednie twierdzenie.

Uw. Jeżeli oznaczać będziemy przez $\varphi(z)/\psi(z)$ iloraz wielomianu φ przez wielomian ψ, *o ile* $\psi(z) \mid \varphi(z)$; i jeżeli utworzymy sobie wielomian:

$$\Phi(z) \overset{\text{df}}{=} (z-z_0)\ldots(z-z_m),$$

to łatwo wyrachujemy, że:

$$X_s(z) = \frac{\Phi(z)}{(z-z_s)\Phi'(z_s)}.$$

Albowiem:

$$\Phi'(z) = (z-z_1)\ldots(z-z_m) + (z-z_0)(z-z_2)\ldots \\ \ldots(z-z_m) + \ldots + (z-z_0)\ldots(z-z_{m-1}),$$

stąd:

$$\Phi'(z_s) = (z_s-z_0)\ldots(z_s-z_{s-1})(z_s-z_{s+1})\ldots(z_s-z_m).$$

Formuły Eulera.

Rozważmy wielomiany:

$$f_i(z) = z^{m-i},\ m \text{ całk.} > 0,\ i = 0, 1 \ldots m,$$

jakoteż ciąg: $z_0, z_1 \ldots z_m$ liczb *różnych* między sobą. Starajmy się wyznaczyć $f_i(z)$ przy pomocy formuł Lagrange'a. Mamy tu:

$$w_s = f_i(z_s) = z_s^{m-i},$$

$$X_s(z) = \frac{z^m + a_1^{(s)} z^{m-1} + \cdots + a_m^{(s)}}{\Phi'(z_s)},\ s = 0, 1 \ldots m$$

$$\Phi(z) = (z-z_0)\ldots(z-z_m).$$

Zatem:

$$z^{m-i} \equiv \sum_{s|0}^{m} \frac{z^m + a_1^{(s)} z^{m-1} + \ldots + a_m^{(s)}}{\Phi'(z_s)} \cdot z_s^{m-i}$$

Po lewej stronie mamy wielomian w postaci zredukowanej, po prawej ewentualnie nie zredukowany. Redukując prawą stronę i porównując spółczynniki przy z^m po obu stronach [postać zredukowana jest jedyną!], otrzymamy:

$$\sum_{s|0}^{m} \frac{z_s^{m-i}}{\Phi'(z_s)} = 0 \text{ . dla } i = 1, 2 \ldots m,$$

$$\sum_{s|0}^{m} \frac{z_s^m}{\Phi'(z_s)} = 1.$$

Są to tak zwane formuły *Eulera*.

Uw. Zastosowawszy formułę Lagrange'a do wielomianu $f(z) = 1$, otrzymamy:

$$1 = \sum_{s|0}^{m} X_s(z),$$

gdzie X_s zbudowano przy pomocy ciągu liczb *różnych*:

$$z_0, z_1 \ldots z_m.$$

Metoda Newtona[1] i Gauss'a[2].

Zadajemy sobie znów ciągi:

$z_0, z_1 \ldots z_m$ (liczb *różnych*),

$w_0, w_1 \ldots w_m$ (dowolnych).

Wiemy już, dzięki metodzie Lagrange'a, że istnieje jedyny wielomian $f(z)$ stopnia $\leq m$ taki, że:

$$f(z_s) = w_s \quad (s = 0, 1 \ldots m).$$

---

[1] I. Newton. „Principia". Liber III. Lemma 5. (1687).

[2] K. F. Gauss. „Theoria interpolationis methodo nova tractata". Dzieła t. III.

Próbujmy go przedstawić w postaci:

$$f(z) \equiv c_0 + c_1(z-z_0) + c_2(z-z_0)(z-z_1) + \cdots + c_m(z-z_0)\ldots(z-z_{m-1}).$$

Gdybyśmy znali już $f(z)$, to c_m, $c_{m-1}\ldots c_0$ otrzymalibyśmy, dzieląc kolejno $f(z)$ przez $(z-z_0)\ldots(z-z_{m-1})$, otrzymaną resztę przez $(z-z_0)\ldots(z-z_{m-2})$ i. t. d. Istnienie i jednoznaczność $c_0, c_1, \ldots c_m$ są zatem zapewnione. Postaramy się te liczby odszukać efektywnie:

(1) kładziemy $z = z_0$, stąd:

$$c_0 = f(z_0) = w_0,$$

(2) kładziemy $z = z_1$, stąd:

$$c_1 = \frac{f(z_1) - c_0}{z_1 - z_0} = \frac{w_1 - w_0}{z_1 - z_0},$$

(3) kładziemy $z = z_2$, stąd:

$$c_2 = \frac{f(z_2) - c_0 - c_1(z_2 - z_0)}{(z_2 - z_0)(z_2 - z_1)} =$$

$$= \frac{(w_2 - w_0) - \dfrac{w_1 - w_0}{z_1 - z_0}(z_2 - z_0)}{(z_2 - z_0)(z_2 - z_1)} =$$

$$= \frac{(w_2 - w_0)(z_1 - z_0) - (w_1 - w_0)(z_2 - z_0)}{(z_2 - z_0)(z_2 - z_1)(z_1 - z_0)} \text{ i t. d.}$$

Otrzymamy w ten sposób wszystkie $c_0 \ldots c_m$. Można łatwo obliczyć, że:

$$c_s = \frac{w_0}{(z_0 - z_1)\ldots(z_0 - z_s)} +$$

$$+ \frac{w_1}{(z_1 - z_0)(z_1 - z_2)\ldots(z_1 - z_s)} + \cdots$$

$$\ldots + \frac{w_s}{(z_s - z_0)\ldots(z_s - z_{s-1})}$$

$s = 0, 1, \ldots m.$

Uw. Gauss wyraża c_s przy pomocy nieco innych formuł.

6. **Miejsca zerowe** wielomianów więcej niż jednej zmiennej.

Df. Miejscem zerowem (gorzej: *pierwiastkiem*) wielomianu $f(z_1 \ldots z_k)$ nazywamy każdy układ liczb zespolonych:

$$(a_1 \ldots a_k)$$

taki, że: $$f(a_1 \ldots a_k) = 0.$$

Tw. Każdy wielomian $f(z_1 \ldots z_k)$, gdzie $k > 1$, *rzędu większego niż zero* posiada *nieskończenie wiele miejsc zerowych:*

Dem. Wielomian nasz nie może być stopnia *zero* względem *każdej* ze swych zmiennych. Załóżmy dla prostoty, że naprz. $st'_{z_k} f = p > 0$.

Przedstawmy tedy $f(z_1 \ldots z_k)$ jako:

$f(z_1 \ldots z_k) \equiv A_0(z_1 \ldots z_{k-1})\, z_k^{\,p} + \cdots + A_p(z_1 \ldots z_{k-1})$,

gdzie $A_0, A_1, \ldots A_p$ są wielomianami

i $$A_0(z_1 \ldots z_{k-1}) \not\equiv 0.$$

Obierzmy teraz układ $(a_1 \ldots a_{k-1})$ tak, by:

$$A_0(a_1 \ldots a_{k-1}) \neq 0.$$

i rozważmy:

$$\varphi(\hat{z}_k) \equiv f(a_1 \ldots a_{k-1}, \hat{z}) \equiv A_0(a_1 \ldots a_{k-1})\, \hat{z}_k^{\,p} + \ldots$$
$$\ldots + A_p(a_1 \ldots a_{k-1}).$$

Jest to wielomian zmiennej z_k, stopnia $p > 0$.

Posiada on zatem przynajmniej jeden pierwiastek naprz. a_k; wtedy jednak:

$$0 = \varphi(a_k) = f(a_1 \dots a_k)$$

i $(a_1 \dots a_k)$ jest miejscem zerowem dla f.

Atoli $A_0(z_1 \dots z_k)$ jest funkcją ciągłą, zatem, gdy $\varepsilon > 0$ i dość małe,

$$|b_i - a_i| < \varepsilon \quad , \quad i = 1 \dots k-1,$$

to: $$A_0(b_1 \dots b_{k-1}) \neq 0.$$

Szukamy teraz b_k tak, by:

$$\varphi(b_k) = f(b_1 \dots b_{k-1}, b_k) = 0.$$

Otrzymamy: $$f(b_1 \dots b_k) = 0.$$

W ten sposób otrzymamy widocznie nieskończenie wiele układów:

$$(b_1 \dots b_k),$$

będących miejscami zerowemi dla $f(z_1 \dots z_k)$.

Cor. Można okazać, iż po odszukaniu miejsca $(a_1 \dots a_k)$ jak poprzednio i obraniu dowolnego $\varepsilon > 0$, udałoby się wybrać $\varepsilon \geq \delta > 0$, tak, by nierówności:

$$|b_s - a_s| < \delta, \; s = 1, 2, \dots k-1$$

pozwoliły odszukać potrzebne b_k, spełniające warunek:

$$|b_k - a_k| < \varepsilon.$$

Wielomian f posiada zatem nieskończenie wiele miejsc zerowych w każdem otoczeniu miejsca $(a_1 \dots a_k)$. Dowodu tego twierdzenia podać tu atoli nie możemy; wymaga on użycia silniejszych środków teorji funkcyj analitycznych lub dalszych twierdzeń algebry, których tu jeszcze nie mamy.

Podamy jeszcze dwa twierdzenia:

Tw. Gdy $f(xy)$ i $g(xy)$ są *pierwsze* względem siebie [str. 66], to f i g mają conajwyżej *skończoną ilość wspólnych miejsc zerowych.*

Dem. Pomińmy wypadki trywjalne, gdy $f \equiv 0$ lub $g \equiv 0$ czy też $rz'f = 0$ lub $rz'g = 0$ i załóżmy, że $rz'f > 0$, $rz'g > 0$.

Dzieląc łańcuchowo naprz. względem x [str. 80], otrzymamy związek:

$$P(xy)f(xy) + Q(xy)g(xy) \equiv R_{\rho+1}(y)$$

P, Q, $R_{\rho+1}$ wielomiany, $R_{\rho+1}(y) \not\equiv 0$.

Jeżeli (x_0y_0) jest wspólnem miejscem zerowem dla $f(xy)$ i $g(xy)$, to:

$$0 = R_{\rho+1}(y_0).$$

Miejsca wspólne mogą mieć do dyspozycji zatem tylko takie y, dla których $R_{\rho+1}(y) = 0$, a takich jest skończona ilość.

Analogiczne dzielenie względem y przekona nas o tem, że miejsca zerowe wspólne posiadają do dyspozycji tylko skończoną ilość wartości na x. Stąd twierdzenie:

Tw. Jeżeli $g(xy)$ nierozkładalne, $f(xy)$ i $g(xy)$ zerują się wspólnie dla (x_0y_0) i jeżeli w otoczeniu (x_0y_0) każde miejsce zerowe dla $g(xy)$ jest miejscem zerowem dla $f(xy)$, to $g(xy)$ dzieli $f(xy)$.

Dem. Widocznie $f(xy)$ i $g(xy)$ mają nieskończenie wiele wspólnych miejsc zerowych, zatem nieprawdą jest, by f i g były pierwsze względem siebie, lecz $g(xy)$ nierozkładalne, więc $g(xy) \mid f(xy)$.

§ 2. Równanie dwumienne. Pierwiastki jedności.

1. Pierwiastki jedności.

Df. Równaniem *dwumiennem* nazywa się równanie postaci:

$$z^m - a \overset{?}{=} 0 \text{ lub } z^m \overset{?}{=} a,\ m \text{ całk.} > 0,\ a \in q_2.$$

Rozwiązanie tego równania polega na wyszukaniu pierwiastków (miejsc zerowych) wielomianu $z^m - a$. Szczególnie ważny wypadek przedstawia wielomian:

$$z^m - 1,$$

którego miejsca zerowe nazywają się m-temi *pierwiastkami jedności.*

Przystępujemy do ich oznaczenia.

Tw. *Pełnym ciągiem pierwiastków* m-tych jedności, gdzie m całkowite, dodatnie, jest ciąg:

$$e^{2\pi i \cdot \frac{0}{m}},\ e^{2\pi i \cdot \frac{1}{m}}, \ldots e^{2\pi i \cdot \frac{m-1}{m}}, \qquad (*)$$

a zatem:

$$e^{2\pi i \cdot \frac{s}{m}}, \text{ gdzie } s = 0, 1, \ldots m - 1.$$

Dem. 1. $\left(e^{2\pi i \cdot \frac{s}{m}}\right)^m = e^{2\pi i \cdot s} = 1$ [p. str. 39 i 40], więc wszystkie człony ciągu (*) są pierwiastkami wielomianu: $z^m - 1$.

2. Człony ciągu (*) są różnemi liczbami. Rzeczywiście: równość

$$e^{2\pi i \cdot \frac{s'}{m}} = e^{2\pi i \cdot \frac{s''}{m}},\ s', s'' = 0, 1 \ldots m - 1,\ s' \neq s'',$$

pociągnęłaby, że:

$$e^{2\pi i \cdot \frac{s'-s''}{m}} = 1,$$

więc: $\cos 2\pi \cdot \frac{s' - s''}{m} = 1, \sin 2\pi \cdot \frac{s' - s''}{m} = 0,$

stąd: $2\pi \cdot \frac{s' - s''}{m}$ musiałoby być wielokrotnością całkowitą liczby 2π czyli $\frac{s' - s''}{m}$ całkowite, co niemożliwe.

3. Ilość członów ciągu (*) o wartościach *różnych* wynosi m, ilość pierwiastków wielomianu $z^m - 1$ wynosi conajwyżej m, zatem ciąg (*) jest ciągiem *zupełnym* pierwiastków.

Uw. Każda liczba: $e^{2\pi i \cdot \frac{s}{m}}$, gdzie s całkowite, będzie również pierwiastkiem naszego wielomianu, atoli wydzieliwszy z $\frac{s}{m}$ całości i resztę w postaci:

$$s = m \cdot q + r, \quad 0 \leq r < m, q \text{ całkowite,}$$

otrzymamy:

$$e^{2\pi i \cdot \frac{s}{m}} = e^{2\pi i \cdot \frac{mq+r}{m}} = e^{2\pi i \cdot q} \cdot e^{2\pi i \cdot \frac{r}{m}}$$
$$= 1 \cdot e^{2\pi i \cdot \frac{r}{m}},$$

więc temsamem dostajemy tylko jeden z członów ciągu (*).

Uw. 2. W znakowaniu Żmurki możemy zapisać ciąg (*) w postaci:

$$1_0, \ 1_{\frac{2\pi i}{m}}, \ldots 1_{\frac{2(m-1)\pi i}{m}}.$$

Inaczej jeszcze:

$$e^{2\pi i \cdot \frac{s}{m}} = \cos \frac{2\pi s}{m} + i \sin \frac{2\pi s}{m},$$
$$s = 0, 1 \ldots m - 1.$$

Początkowym członem ciągu (*) jest zawsze $e^0 = 1$.

Df. Pierwiastek m-ty jedności (m całk. > 0) jest *pierwotnym* (dla m), gdy nie jest jednocześnie pierwiastkiem n-tym, gdzieby n było całkowite, dodatnie i $n < m$.

Uw. Zatem nie jest takim nigdy 1, o ile $m > 1$.

Jeżeli m-tym pierwiastkiem jedności jest naprz.:

$$e^{2\pi i \cdot \frac{s}{m}}$$

i jest on jednocześnie pierwiastkiem n-tym, gdzie $n < m$, to zachodzi równość:

$$e^{\frac{2\pi ri}{n}} = e^{\frac{2\pi si}{m}} \qquad 0 \leqq r < n,\ 0 \leqq s < m.$$

Zatem:

$$e^{2\pi i\left(\frac{r}{n} - \frac{s}{m}\right)} = 1, \qquad \frac{r}{n} - \frac{s}{m} \text{ całkowite},$$

co możliwe jedynie, gdy: $\frac{r}{n} = \frac{s}{m}$, a zatem gdy ułamek $\frac{s}{m}$ dał się skrócić. Warunek ten jest też widocznie dostateczny. Stąd:

Tw. Jedynemi i wszystkiemi pierwiastkami *pierwotnemi* jedności, rzędu m są:

$$e^{\frac{2\pi si}{m}}, \quad s = 0, 1, \ldots m-1,$$

gdzie jednak s i m są *pierwsze względem siebie*.

Uw. Ilość liczb *pierwszych* względem m całkowitego i dodatniego i *nie większych* niż m oznaczamy, za przykładem Gaussa, przez $\varphi(m)$.

Zatem: Istnieje dokładnie $\varphi(m)$ pierwotnych pierwiastków m-tych jedności. Gdy m jest liczbą pierwszą (> 1), to $\varphi(m) = m - 1$ i *wszystkie* pier-

wiastki różne od 1 są *pierwotne.* Zawsze pierwotnym jest pierwiastek:

$$e^{\frac{2\pi i}{m}}.$$

Tw. Jeżeli ε jest pierwiastkiem *pierwotnym* m-tym jedności, to ciąg:

$$\varepsilon^0 = 1,\ \varepsilon^1, \ldots \varepsilon^{m-1} \qquad (*)$$

jest zupełnym ciągiem m-tych pierwiastków jedności.

Dem. 1. $(\varepsilon^r)^m = \varepsilon^{mr} = (\varepsilon^m)^r = 1^r = 1$

dla $r = 0, 1, \ldots m-1$,

więc człony $(*)$ są pierwiastkami.

2. Równość:

$$\varepsilon^r = \varepsilon^{r'},\ 0 \leqq r < m,\ 0 \leqq r' < m,\ r \neq r',$$

pociąga:

$$e^{\frac{2\pi s r i}{m}} = e^{\frac{2\pi s r' i}{m}},\ \text{gdy: } \varepsilon = e^{2\pi i \cdot \frac{s}{m}},$$

$$e^{2\pi i s\left(\frac{r-r'}{m}\right)} = 1,\ s \cdot \frac{r-r'}{m} \text{ całkowite,}$$

więc $r - r'$ podzielne przez m, bo s pierwsze względem m. Stąd już $r - r' = 0$, $r = r'$ wbrew przypuszczeniu. W ciągu $(*)$ mamy zatem m różnych członów.

Uw. Twierdzenie powyższe *nie* jest słuszne, gdy ε nie jest pierwotne i gdy temsamem $1 < k =$ najw. wsp. podz. dla s i m $(m > 1)$, gdyż:

$$\varepsilon^{\frac{m}{k}} = e^{\frac{2\pi s i}{m} \cdot \frac{m}{k}} = e^{2\pi i \cdot \frac{s}{k}} = 1,\ \frac{s}{k} \text{ całkowite,}$$

więc w ciągu (*) mamy już dwa człony:

$$\varepsilon^0 \text{ i } \varepsilon^{\frac{m}{k}} \quad \left(\frac{m}{k} < m\right),$$

mające tę samą wartość.

Obecnie odszukamy efektywnie m-te pierwiastki jedności dla $m = 1, 2, 3, 4, 5$.

m = 1.

Pełny ciąg pierwiastków:

$$e^0 = 1.$$

m = 2.

Pełny ciąg:

$$e^0, e^{\pi i},$$

czyli: $1, -1.$

Pierwotnym jest -1.

m = 3.

Pełny ciąg:

$$1 = e^0, \; e^{\frac{2\pi i}{3}}, \; e^{\frac{4\pi i}{3}}.$$

$$(1) \quad \cos\frac{2\pi}{3} = \cos\left(\pi - \frac{\pi}{3}\right) = -\cos\frac{\pi}{3} = -\frac{1}{2},$$

$$\sin\frac{2\pi}{3} = \sin\left(\pi - \frac{\pi}{3}\right) = \sin\frac{\pi}{3} = \frac{\sqrt{3}}{2},$$

$$e^{\frac{2\pi i}{3}} = -\frac{1}{2} + \frac{i}{2}\sqrt{3}.$$

$$(2) \quad e^{\frac{4\pi i}{3}} = \left(e^{\frac{2\pi i}{3}}\right)^2 = \left(-\frac{1}{2} + \frac{i}{2}\sqrt{3}\right)^2 = -\frac{1}{2} - \frac{i}{2}\sqrt{3}.$$

Zatem mamy pierwiastki:

$$1, -\frac{1}{2}+\frac{i}{2}\sqrt{3}, -\frac{1}{2}-\frac{i}{2}\sqrt{3}.$$

Pierwotne są tu wszystkie z wyjątkiem 1.

m = 4.

Pełny ciąg:

$$1, e^{\frac{\pi}{2}i}, e^{\pi i}, e^{\frac{3}{2}\pi i},$$

czyli: $1, i, -1, -i.$

Pierwotne: $i, -i.$

m = 5.

Pełny ciąg:

$$1, e^{\frac{2\pi i}{5}}, \left(e^{\frac{2\pi i}{5}}\right)^2, \left(e^{\frac{2\pi i}{5}}\right)^3, \left(e^{\frac{2\pi i}{5}}\right)^4,$$

gdyż $e^{\frac{2\pi i}{5}}$ jest pierwotnym.

(1) Obliczmy $\cos\frac{2\pi}{5}$ i $\sin\frac{2\pi}{5}$, $\left(\frac{2\pi}{5}=72^0\right)$.

Rozważamy trójkąt równoramienny ABC, gdzie $AB=1$, $\sphericalangle A=\sphericalangle B=72°$, $\sphericalangle C=36°$. Obieramy M na AC tak, że $\sphericalangle MBA=\sphericalangle CBM$ i rozważamy trójkąt AMB. W nim:

$$\sphericalangle A=72°,\ \sphericalangle B=36°,\ \sphericalangle M=72°,$$

więc trójkąty ABC i AMB są *podobne*, Stąd:

$$AB:AC=AM:AB=(AC-MC):AB.$$

Lecz trójkąt MCB jest równoramienny, bo:

$\sphericalangle MBC=\sphericalangle MCB=36°$. Zatem:

$1:AC=(AC-1):1$ $[MC=MB=AB]$

$AC^2-AC=1$

$$AC=\frac{1}{2}+\frac{\sqrt{5}}{2}$$ [odwrotny stosunek „złotego podziału“].

Stąd już:

$$\cos\frac{2\pi}{5}=\frac{1}{2AC}=\frac{1}{1+\sqrt{5}}=\frac{\sqrt{5}-1}{4},$$

$$\sin\frac{2\pi}{5}=\frac{\sqrt{10+2\sqrt{5}}}{4},$$

$$e^{\frac{2\pi i}{5}}=\frac{\sqrt{5}-1}{4}+i\frac{\sqrt{10+2\sqrt{5}}}{4}.$$

Oznaczając na chwilę:

$$a=\sqrt{10+2\sqrt{5}},\ a'=\sqrt{10-2\sqrt{5}},$$

otrzymamy przez potęgowanie z łatwością pełny ciąg:

$$1,\ \frac{1}{4}(-1+\sqrt{5}+ai),\ \frac{1}{4}(-1-\sqrt{5}+a'i),$$

$$\frac{1}{4}(-1-\sqrt{5}-a'i),\ \frac{1}{4}(-1+\sqrt{5}-ai).$$

Uw. Czytelnik obliczy jeszcze z łatwością wypadek $m=6$ czy $m=8$. Dla $m=17$ i $m=19$ formuły podał Gauss (Dzieła t. 1), a dla $m=257$ Richelot (Journal de Crelle t. IX).

Jeżeli dla $m>2$ wypiszemy pełny ciąg m-tych pierwiastków jedności:

$$1,\ e^{\frac{2\pi i}{m}},\ e^{\frac{4\pi i}{m}},\ \ldots e^{\frac{2(m-1)\pi i}{m}}$$

i zauważymy, że na płaszczyźnie Gaussa leżą one wszystkie na kole o środku w początku układu i promieniu $=1$, i dzielą obwód tego koła na m równych części, zrozumiemy, że łącząc punkty

reprezentacyjne odcinkami prostemi, otrzymamy umiarowy wielobok o m bokach i zobaczymy, że problem *konstrukcji* takiego wieloboku i problem *rozwiązania* równania $z^m - 1 \stackrel{?}{=} 0$ *są sobie równoważne.* Równanie powyższe nazywają też często *równaniem podziału koła.* Było ono i jest przedmiotem rozległych studjów algebraików i teoretyków liczb. Klasycznem dziełem jest *Bachmanna* „Die Lehre von der Kreisteilung". Lipsk. 1872.

Równanie podziału koła posiada znany nam pierwiastek 1, więc $(z-1) \mid (z^m - 1)$.

Rzeczywiście:

$$z^m - 1 \equiv (z-1)(z^{m-1} + z^{m-2} + \cdots + 1).$$

Aby odszukać inne niż 1 pierwiastki, należy rozwiązać równanie:

$$z^{m-1} + \cdots + 1 \stackrel{?}{=} 0.$$

Uczyniliśmy to właśnie dla $m = 2, 3, 4, 5$. Gauss[1] okazał, w związku z równaniem podziału koła, że jedynemi wielobokami umiarowemi, gdzie liczba boków m jest liczbą *pierwszą*, konstruowalnemi przy pomocy *linijki* i *cyrkla* są wieloboki odpowiadające wypadkom:

$$m = 2^n + 1 \qquad (n \text{ całkowite}).$$

Są to kolejno wypadki: $m = 3, 5, 17, 257...$

[Rozumiemy dlaczego Richelot podawał formuły dla $m = 257$!]. Czytelnik zechce zwrócić się w tym względzie do pięknego artykułu F. Enriquesa: O równaniach algebraicznie rozwiązalnych zapomocą pier-

[1] K. F. Gauss: „Disquisitiones arithmeticae" 1801, [Dzieła, t. 1]. Art. 365.

wiastków stopnia drugiego... w zbiorze: Enriques „Zagadnienia geometrji elementarnej“, tłum. Kwietniewskiego i Wojtowicza.

2. Ogólne równanie dwumienne.

Rozważmy równanie:

$$z^m \stackrel{?}{=} a, \qquad (*)$$

gdzie m całkowite, > 0 i a zespolone.

Przedstawmy liczbę a w postaci:

$$a = re^{\varphi i},$$

gdzie $r = |a|$, φ jest jedną z amplitud liczby a.

Jeżeli $a = 0$, to widocznie *jedynie* liczba *zero* jest pierwiastkiem równania $(*)$.

Dla $a \neq 0$ $(r > 0)$ mamy inne twierdzenie:

Tw. Gdy $a \neq 0$, m całk. > 0, to ciąg:

$$\sqrt[m]{r} \cdot e^{\left(\frac{\varphi + 2\pi s}{m}\right) i}, \qquad (**)$$

$$s = 0, 1, \ldots m - 1$$

jest *pełnym ciągiem pierwiastków* równania $(*)$.

Dem. (1) $\left[\sqrt[m]{r} \cdot e^{\left(\frac{\varphi + 2\pi s}{m}\right) i}\right]^m = r \cdot e^{(\varphi + 2\pi s) i} =$

$$= r \cdot e^{\varphi i} \cdot e^{2\pi s i} = a \cdot 1 = a.$$

(2) Wyrazy ciągu $(**)$ są różne, gdyż przypuszczenie:

$$\sqrt[m]{r} \cdot e^{\left(\frac{\varphi + 2\pi s}{m}\right) i} = \sqrt[m]{r} \cdot e^{\left(\frac{\varphi + 2\pi s'}{m}\right) i},$$

$0 < s < m$, $0 < s' < m$, $s \neq s'$, prowadzi do wniosku:

$$e^{\left(\frac{\varphi + 2\pi s}{m}\right) i - \left(\frac{\varphi + 2\pi s'}{m}\right) i} = 1$$

Stąd: $e^{2\pi i\left(\frac{s-s'}{m}\right)} = 1$, $\frac{s-s'}{m}$ całkowite,

$s = s'$, wbrew założeniu.

(3) Równanie (*) ma atoli najwyżej m różnych pierwiastków.

Uw. 1. Jeżeli $\varepsilon_0\,\varepsilon_1 \ldots \varepsilon_{m-1}$ oznacza pełny ciąg m-tych pierwiastków jedności, to ciąg (**) dany jest przez:

$$\sqrt[m]{r}\,.\,e^{\frac{\varphi i}{m}}\,\varepsilon_0, \quad \sqrt[m]{r}\,.\,e^{\frac{\varphi i}{m}}\,\varepsilon_1, \ldots \sqrt[m]{r}\,.\,e^{\frac{\varphi i}{m}}\,.\,\varepsilon_{m-1}.$$

Df. Gdy $a \neq 0$, to obierzmy amplitudę φ_0 tak, by $0 \leqq \varphi_0 < 2\pi$, co jest możliwe i to w jedyny sposób. Amplitudę taką nazwiemy *główną*.

Df. Nazwiemy *głównym* pierwiastkiem m-tym liczby a, różnej od zera, liczbę:

$$\sqrt[m]{r}\,.\,e^{\frac{\varphi_0 i}{m}},$$

gdzie $r = |a|$, oraz φ_0 jest *główną* amplitudą liczby a.

Głównym pierwiastkiem m-tym liczby 0 nazwiemy 0.

Oznaczać będziemy *główny* m-ty pierwiastek liczby a (m całk., > 0) znakiem: $\sqrt[m]{a}$.

Przykłady:

(1) $\sqrt{i} = \sqrt{1}\,.\,e^{\frac{\varphi_0 i}{2}} = 1\,.\,e^{\frac{\pi}{4}i} = \left(\frac{1}{2} + \frac{i}{2}\right)\sqrt{2}$, $\varphi_0 = \frac{\pi}{2}$.

(2) $\sqrt[m]{1} = e^{\frac{\varphi_0 i}{m}} = 1$, $\varphi_0 = 0$.

(3) $\sqrt{-a}$, gdzie $a \varepsilon q$ i $a > 0$, wyraża się przez:

$$\sqrt{|a|}.e^{\frac{\pi i}{2}} = i\sqrt{|a|}, \quad \varphi_0 = \pi.$$

[Pozostałym pierwiastkiem jest: $-i\sqrt{|a|}$].

§ 3. Związki między pierwiastkami a spółczynnikami wielomianu jednej zmiennej.

1. Wielomiany kanoniczne i wzory *s.*

Rozważmy dowolny wielomian $f(z)$ niezerowy. Napiszmy go w postaci zredukowanej:

$$f(z) \equiv a_0 z^m + \cdots + a_m, \quad a_0 \neq 0.$$

Dzieląc $f(z)$ przez a_0 otrzymamy wielomian:

$$\varphi(z) \equiv z^m + \frac{a_1}{a_0} z^{m-1} + \cdots + \frac{a_m}{a_0}.$$

Df. Wielomian $f(z)$ *niezerowy* jest *kanonicznym*, gdy spółczynnik przy najwyższej potędze jego *postaci zredukowanej* jest *jednością.*

Wielomian $\varphi(z)$ jest *kanonicznym* wielomianu $f(z)$, gdy $\varphi(z)$ jest kanonicznym, i $f(z) \equiv a_0\varphi(z)$, gdzie a_0 jest spółczynnikiem najwyższej potęgi postaci zredukowanej wielomianu $f(z)$. Definicja odnosi się tylko do wielomianów *niezerowych.*

Niechaj będzie $f(z)$ stopnia $\geqq 1$, $\varphi(z)$ jego kanonicznym oraz: $z_1, z_2, \ldots z_m$ (*)
ciągiem *zupełnym* pierwiastków $f(z)$.

Ponieważ: $f(k) = 0 . \equiv . \varphi(k) = 0$, więc ciąg (*) jest *zupełnym* ciągiem pierwiastków wielomianu $\varphi(z)$, przyczem:

$$f(z) \equiv a_0(z - z_1) \ldots (z - z_m).$$
$$\varphi(z) \equiv (z - z_1) \ldots (z - z_m).$$

Tw. Wielomian $f(z)$ stopnia $\geqq 1$ i jego kanoniczny $\varphi(z)$ mają ten sam ciąg zupełny pierwiastków. Rozkłady $f(z)$ i $\varphi(z)$ na *czynniki* jak i *dzielniki* pierwiastkowe różnić się mogą tylko w *stałej* rozkładu, którą jest dla kanonicznego *jedność*.

Rozważmy wielomian *kanoniczny* $f(z)$, stopnia $m \geqq 1$:

$$f(z) \equiv z^m + a_1 z^{m-1} + \ldots + a_m$$

i ciąg *zupełny* jego pierwiastków:

$$z_1,\ z_2 \ldots z_m .$$

Mamy tu identyczność:

$$z^m + a_1 z^{m-1} + \cdots + a_m \equiv (z - z_1) \ldots (z - z_m).$$

Wymnażając i redukując prawą stronę, a następnie porównując z lewą, dostaniemy związki:

$$\left.\begin{aligned} -a_1 &= z_1 + \cdots + z_m \\ +a_2 &= z_1 z_2 + \cdots + z_{m-1} z_m \\ -a_3 &= z_1 z_2 z_3 + \cdots + z_{m-2} z_{m-1} z_m \\ &\vdots \\ (-1)^m a_m &= z_1 z_2 \ldots z_m \end{aligned}\right\} \quad (1)$$

Należy dobrze rozumieć symbolikę wyrażeń po prawych stronach związków (1). Mamy tu na myśli, że przy związku dla a_s wzięto 1° wszystkie *kombinacje* bez powtórzeń, po s członów ciągu: $z_1, \ldots z_m$, 2° zesumowano odnośne iloczyny razem, co dało w sumie $(-1)^s a_s$.

Symbolika formuł (1) nie jest jasna i subtelna, jak zresztą przeważnie symbolika kombinatoryki; nie opłaca się jednak obciążać książki specjalnie skonstruowanem znakowaniem, zadowolimy się sym-

boliką mniej dokładną, popartą słownem objaśnieniem.

Tw. Jeżeli dla ciągu zupełnego pierwiastków:

$$z_1 \ldots z_m$$

wielomianu $f(z) \equiv z^m + a_1 z^{m-1} + \cdots + a_m$ *kanonicznego,* wprowadzimy znakowania:

$$(s_1)\quad \begin{cases} s_1 = z_1 + \cdots + z_m \\ s_2 = z_1 z_2 + \cdots + z_{m-1} z_m \\ s_3 = z_1 z_2 z_3 + z_1 z_2 z_4 + \cdots + z_{m-2} z_{m-1} z_m \\ \vdots \\ s_m = z_1 z_2 \ldots z_m, \end{cases}$$ to:

$$(s_2)\quad s_k = a_k (-1)^k,\ k = 1, 2 \ldots m.$$

Wprowadzamy jeszcze definicję: $s_0 \overset{df}{=} 1$.

Formuły (s_1) i (s_2) nazywać będziemy *wzorami* s.

Wielomian $f(z)$ możemy zapisać w postaci:

$$f(z) \equiv z^m - s_1 z^{m-1} + s_2 z^{m-2} + \cdots + (-1)^m s_m$$

lub $f(z) \equiv s_0 z^m - s_1 z^{m-1} + \cdots + (-1)^m s_m \equiv$

$$\equiv \sum_{k|0}^{m} (-1)^k . s_k . z^{m-k}$$

Przykład: dla $f(z) \equiv z^2 + a z + b$ mamy:

$$z_1 + z_2 = -a,\ z_1 z_2 = b;$$

dla $f(z) \equiv z^3 + a z^2 + bz + c$ mamy:

$$z_1 + z_2 + z_3 = -a,\ z_1 z_2 + z_2 z_3 + z_3 z_1 = b,$$

$$z_1 z_2 z_3 = -c.$$

Spotkamy się z wzorami s jeszcze w dalszym ciągu.

§ 4. Wielomiany rzeczywiste i ich pierwiastki.

1. **Wielomiany rzeczywiste** jednej zmiennej.

Df. Wielomianem rzeczywistym jednej zmiennej jest wielomian *zerowy* jakoteż każdy wielomian, którego wszystkie spółczynniki formy *zredukowanej* są liczbami *rzeczywistemi*.

$$f(z) \equiv 0, \text{ lub } f(z) \equiv a_0 z^m + \cdots + a_m,$$
$$a_0 \neq 0;\ a_0, a_1 \ldots a_m \varepsilon q$$

Nie każdy wielomian *rzeczywisty* posiada pierwiastki *rzeczywiste*. Typowym przykładem będzie wielomian $z^2 + a$, gdzie $a \varepsilon q$ i $a > 0$. Ta właśnie okoliczność skłoniła algebraików do stworzenia sobie zakresu liczb q_2 i częściowego opuszczenia zakresu q, aby posiadać *zasadnicze twierdzenie algebry*, którego brak w zakresie liczb rzeczywistych.

Mamy atoli twierdzenie:

Tw. Każdy wielomian *rzeczywisty*, stopnia *nieparzystego* posiada choć jeden pierwiastek *rzeczywisty*.

Dem. Niech będzie:

$$f(z) \equiv a_0 z^m + \cdots + a_m,\ a_0 \neq 0.$$
$$a_0 \ldots a_m \varepsilon q,\quad m \text{ całk. } \textit{nieparzyste}.$$

Zamiast $f(z)$ rozważmy jego kanoniczny:

$$\varphi(z) \equiv z^m + \frac{a_1}{a_0} z^{m-1} + \cdots + \frac{a_m}{a_0},$$

który jest również rzeczywisty i tego samego stopnia, a posiada te same pierwiastki co $f(z)$.

Rozważajmy tylko rzeczywiste wartości na z. Dla $z \neq 0$ mamy:

$$\varphi(z) = z^m \left\{ 1 + \frac{a_1}{a_0 z} + \cdots + \frac{a_m}{a_0 z^m} \right\}.$$

W granicy:

$$\lim_{z|\pm\infty} \left(1 + \frac{a_1}{a_0 z} + \cdots + \frac{a_m}{a_0 z^m} \right) = 1$$

$$\lim_{z|+\infty} \varphi(z) = +\infty, \quad \lim_{z|-\infty} \varphi(z) = -\infty.$$

[m nieparzyste!]

Możemy zatem obrać dwie liczby a i b rzeczywiste tak, by:

$$a < b, \ \varphi(a) < 0, \ \varphi(b) > 0.$$

Ponieważ $\varphi(z)$ jest ciągłą funkcją w przedziale rzeczywistym $[a, b]$, więc znajdzie się takie z_0 rzeczywiste, że:

$$a < z_0 < b \ \text{ i } \ \varphi(z_0) = 0, \ \text{ więc i } f(z_0) = 0.$$

2. **Wielomiany sprzężone** jednej zmiennej.

Rozważmy wielomian:

$$f(z) \equiv a_0 z^m + \cdots + a_m, \ a_0 \neq 0, \ m \text{ całk.} \geq 0$$

i wielomian:

$$\bar{f}(z) \equiv \bar{a}_0 z^m + \cdots + \bar{a}_m,$$

gdzie: $\bar{a}_s$ jest liczbą *sprzężoną* do a_s, $s = 0, \ldots m$.

Df. *Sprzężonym* wielomianu $f(z)$ *niezerowego* nazwiemy wielomian $\bar{f}(z)$, który powstał z $f(z)$ w ten sposób, że wszystkie spółczynniki postaci zredukowanej wielomianu $f(z)$ zastąpiono przez ich sprzężone. Sprzężonym wielomianu *zerowego* nazwiemy wielomian zerowy.

Tw. 1. Każdy wielomian posiada określony wielomian sprzężony.

2. Jeżeli w postaci *zredukowanej* wielomianu $f(z)$ zastąpimy spółczynniki przez sprzężone, otrzymamy *zredukowaną* postać wielomianu $f(z)$.

3. Gdy $f(u) = 0$, to $\overline{f}(\overline{u}) = 0$.

4. $\overline{\overline{f}}(z) \equiv f(z)$

5. $\overline{f^{(k)}}(z) \equiv \overline{f^{(k)}(z)}$, $k = 0, 1, 2 \ldots\ldots$

6. Wielomian $f(z)$ jest wtedy i tylko wtedy rzeczywisty, gdy jest równoważny swemu sprzężonemu: $f(z) \equiv \overline{f}(z)$.

Dem. 1. Z badania poprzedniego i definicji.

2. Gdy $f(z) \equiv a_0 z^m + \cdots + a_m$, $a_0 \neq 0$, to: $\overline{a}_0 \neq 0$, więc $\overline{a}_0 z^m + \cdots + \overline{a}_m$ jest postacią zredukowaną dla $\overline{f}(z)$.

3. Widocznie, dzięki twierdzeniom o sprzężonych na str. 32, mamy:

$$\overline{f(u)} = \overline{f}(\overline{u}),$$

zatem $f(u) = 0 \,.\supset.\, \overline{f(u)} = 0 \,.\supset.\, \overline{f}(\overline{u}) = 0$.

4. Dzięki temu, że $a \in q_2 \,.\supset.\, \overline{\overline{a}} = a$.

5. Udowadniamy przez zastosowanie formuł dla pochodnych i powołanie się na określenie.

6. (1) $f(z) \equiv \overline{f}(z)$ pociąga:

$$a_0 = \overline{a}_0, \ldots a_m = \overline{a}_m \text{ (dzięki 2.)}$$

więc: $$a_0, a_1, \ldots a_m \in q.$$

(2) Odwrotnie: $a_0, \ldots a_m \in q$ pociąga:

$$a_0 = \overline{a}_0, \ldots . a_m = \overline{a}_m \text{ i } f(z) \equiv \overline{f}(z).$$

Osobno oddzielimy od poprzednich ważne twierdzenie:

Tw. Jeżeli a jest pierwiastkiem rzędu k [str. 92] wielomianu (niezerowego) $f(z)$, to $\bar{a}$ jest pierwiastkiem *również* rzędu k dla sprzężonego $\bar{f}(z)$.

Dem. Wtedy:

$$f(a) = f'(a) = \cdots = f^{(k-1)}(a) = 0,\ f^{(k)}(a) \neq 0,$$

[str. 98] więc:

$$\bar{f}(\bar{a}) = \bar{f}'(\bar{a}) = \cdots = \bar{f}^{(k-1)}(\bar{a}) = 0,\ \bar{f}^{(k)}(\bar{a}) \neq 0.$$

stąd: $\bar{a}$ jest pierwiastkiem rzędu k dla $\bar{f}(z)$.

Tw. Gdy a jest pierwiastkiem rzędu k wielomianu *rzeczywistego* $f(z)$, to $\bar{a}$ jest *również* pierwiastkiem i to rzędu k tego wielomianu.

Dem. Wtedy: $f(z) \equiv \bar{f}(z)$, więc wystarczy powołać się na twierdzenie poprzednie.

Rozważmy wielomian *rzeczywisty* stopnia $m > 0$

$$f(z) \equiv k_0 z^m + \cdots + k_m$$

i jego *zupełny* ciąg pierwiastków:

$$z_1 \ldots z_m$$

Dzięki twierdzeniu poprzedniemu jasnem się staje, że jeżeli *rzeczywistemi* w ciągu pierwiastków są: $a_1 \ldots a_r$,

to pozostałe rozpadną się na dwie grupy:

$$a_1' \ldots a_s',\ \bar{a}_1' \ldots \bar{a}_s'.$$

$$\{\bar{a}_i' \text{ sprzężone do } a_i'\} \quad i = 1 \ldots s.$$

Napiszmy wtedy rozkład $f(z)$ na czynniki pierwiastkowe w postaci:

$$f(z) \equiv k_0 (z - a_1) \ldots (z - a_r)\ (z - a_1')\ (z - \bar{a}_1') \ldots$$
$$\ldots (z - a_s')\ (z - \bar{a}_s'),\ r + 2s = m.$$

Rozważmy iloczyn:

$$(z - a_i')(z - \overline{a}_i'), \qquad i = 1 \ldots s.$$

Jest on równoważny:

$$z^2 - (a_i' + \overline{a}_i')\, z + a_i' \overline{a}_i'.$$

Lecz: $b_i = -(a_i' + \overline{a}_i')$ i $c_i = a_i' \overline{a}_i'$

są *liczbami rzeczywistemi,* gdyż:

$$I'(a_i' + \overline{a}_i') = I' a_i' + I' \overline{a}_i' = I' a_i' - I' a_i' = 0,$$

$$I'(a_i' \,.\, \overline{a}_i') = I' a_i' \,.\, R' \overline{a}_i' + I' \overline{a}_i' \,.\, R' a_i' =$$

$$= I' a_i' \,.\, R' a_i' - I' a_i' \,.\, R' a_i' = 0.$$

Zatem mamy rozkład:

$$f(z) \equiv k_0 (z - a_1) \ldots (z - a_r)(z^2 + b_1 z + c_1) \ldots$$

$$\ldots (z^2 + b_s z + c_s).$$

na czynniki *linjowe* i *kwadratowe* o spółczynnikach *rzeczywistych.*

Jeżeli teraz rozważymy pełny ciąg *różnych* pierwiastków wielomianu $f(z)$, to znów rozdzielimy je na trzy grupy:

(1) $a_1 \ldots a_p$ rzeczywiste (różne),

(2) $a_1' \ldots a_q'$ } istotnie zespolone

(3) $\overline{a}_1' \ldots \overline{a}_q'$ } $\overline{a}_i'$ sprzężone do a_i'.

Jeżeli $\alpha_1 \ldots \alpha_p$ są odpowiedniemi rzędami pierwiastków pierwszej grupy, $\beta_1 \ldots \beta_q$ rzędami dla drugiej grupy, to $\beta_1 \ldots \beta_q$ są również rzędami dla trzeciej.

Rozkład na *dzielniki pierwiastkowe* da nam [str. 95]:

$$f(z) \equiv k_0 (z - a_1)^{\alpha_1} \ldots (z - a_p)^{\alpha_p} \,.\, (z^2 + b_1 z + c_1)^{\beta_1} \ldots$$

$$\ldots (z^2 + b_q z + c_q)^{\beta_q},$$

gdzie: $b_i = -(a_i' + \overline{a}_i')$, $c_i = a_i' \,.\, \overline{a}_i'$

rzeczywiste $(i = 1, \ldots q)$.

Otrzymaliśmy zatem rozkład typu:

$$f(z) \equiv k_0 \varphi_1(z) \dots \varphi_{p+q}(z),$$

gdzie $\varphi_1 \dots \varphi_{p+q}$ są potęgami całkowitemi dodatniemi wielomianów 1^{go} lub 2^{go} stopnia. Stąd:

Tw. Każdy wielomian niezerowy stopnia dodatniego da się rozłożyć na czynniki *rzeczywiste* stopnia zerowego, pierwszego lub drugiego. Ewentualnie możemy stałą rozkładu włączyć do jednego z czynników.

3. **Kanoniczne i sprzężone** wielomianów wielu zmiennych.

Czytelnik zechce sam przenieść dosłownie określenia z 1 i 2 na wypadek wielu zmiennych i zastanowić się, które z twierdzeń udowodnionych poprzednio zachowują swą moc i nadal.

Wspominam jeszcze o tem, że wedle niektórych autorów wielomian jest *rzeczywistym*, gdy jego *kanoniczny* jest rzeczywisty w sensie nr. 1. Wielomian $f(z_1 \dots z_k)$ ma wtedy postać:

$$f(z_1 \dots z_k) \equiv a \,.\, \varphi(z_1 \dots z_k),$$

gdzie $\varphi(z_1 \dots z_k)$ jest wielomianem rzeczywistym, lecz a może być *istotnie zespolone.*

§5. Przywiedlność wielomianów jednej zmiennej.

1. **Wielomiany całkowite i wymierne** jednej zmiennej.

Df. Wielomian $f(z)$ stopnia $m \geqq 0$ jest *całkowity* względnie *wymierny*, gdy wszystkie spółczynniki jego postaci zredukowanej są *liczbami całkowitemi* względnie *wymiernemi* $\left(\leqq 0\right)$.

Df. Wielomian *niezerowy* $f(z)$ *całkowity* względnie *wymierny* jest *przywiedlny*, jeżeli można go przedstawić w postaci:

$$f(z) \equiv \varphi(z)\,\psi(z),$$

gdzie:

(1) $\varphi(z)$ i $\psi(z)$ są wielomianami *całkowitemi* względnie *wymiernemi*.

(2) $sl'\varphi > 0$, $sl'\psi > 0$.

W przeciwnym wypadku mówimy o *nieprzywiedlności* wielomianu $f(z)$.

Uw. *Przywiedlność* jest szczególnym wypadkiem *rozkładalności*, podczas, gdy jednak kwestja rozkładalności wielomianu jednej zmiennej jest sprawą trywjalną, gdyż dzięki twierdzeniu zasadniczemu algebry, każdy wielomian stopnia większego niż jedność jest rozkładalny, tu przeciwnie możemy łatwo podać przykłady nieprzywiedlności wielomianów dowolnie wysokiego stopnia. Dalsze twierdzenia pozwolą nam naprzykład stwierdzić, że takiemi są, między innemi:

$$z^2 + 5z + 5$$

lub: $$z^3 + 5z^2 + 5z + 5 \quad \text{i t. p.}$$

Zbadamy najpierw sprawę przywiedlności *wymiernej*. Ponieważ wielomian *całkowity* jest też *wymiernym*, więc wyróżniać będziemy przywiedlność *wymierną* wielomianu *całkowitego*, przywiedlność *całkowitą* wielomianu *całkowitego* i t. d.

Tw.[1] Jeżeli wielomian *całkowity* jest *wymiernie* przywiedlny, to jest również *całkowicie* przywiedlny.

[1] Gauss: „Disquisitiones arithmeticae“ § 42 (niezupełnie w tem samem brzmieniu).

Dem. Załóżmy, że:

(1) $f(z) \equiv a_0 z^m + \cdots + a_m$, $a_0 \neq 0$, $a_0 \ldots a_m$ [całkowite.

(2) $f(z) \equiv \varphi(z) . \psi(z)$.

(3) $\varphi(z) \equiv b_0 z^s + \cdots + b_s$, $\psi(z) \equiv c_0 z^t + \cdots + c_t$ | $b_0 \neq 0$, $c_0 \neq 0$, $b_0 \ldots b_s$, $c_0 \ldots c_t$ wymierne, $s > 0$, $t > 0$, $s + t = m$

Niechaj najmniejszym wspólnym mianownikiem dodatnim dla $b_0 \ldots b_s$ będzie b, dla $c_0 \ldots c_t$ zaś $c\,(>0)$ i niechaj:

$$b_i = \frac{k_i}{b},\ i = 0, 1, \ldots s;\quad c_i = \frac{l_i}{c},\ i = 0, 1, \ldots t.$$

$$\varphi(z) = \frac{1}{b}(k_0 z^s + \cdots + k_s) \equiv \frac{1}{b}\Phi(z),$$

$$\psi(z) \equiv \frac{1}{c}(l_0 z^t + \cdots + l_t) \equiv \frac{1}{c}\Psi(z),$$

$$bc\,f(z) \equiv \Phi(z)\,\Psi(z) \equiv m_0 z^{s+t} + m_1 z^{s+t-1} + \cdots + m_{s+t},$$

gdzie: $m_i = k_0 l_i + k_1 l_{i-1} + \cdots + k_i l_0$,

więc: $bc\,a_i = m_i$, $i = 0, 1 \ldots m$,

kładąc, gdy zajdzie potrzeba:

$$k_{s+1} = k_{s+2} = \cdots = 0,\ l_{t+1} = l_{t+2} = \cdots = 0.$$

Przypuśćmy, że liczba *pierwsza* $p\,(>1)$ jest podzielnikiem iloczynu bc, czyli że $p \mid bc$.

Twierdzimy, że:

$$p \mid k_0 \ldots p \mid k_s \text{ lub } p \mid l_0 \ldots p \mid l_t.$$

Gdyby tak nie było, to:

$p \mid k_0 \ldots p \mid k_{q-1}$, lecz *nie* $p \mid k_q$ $(q \leqq s)$

i $p \mid l_0 \ldots p \mid l_{r-1}$, lecz *nie* $p \mid l_r$ $(r \leqq t)$.

Zbadajmy wtedy m_{q+r}:

$$bca_{q+r} = m_{q+r} = k_0 l_{q+r} + \cdots + k_{q-1} l_{r+1} + \\ + k_q l_r + \cdots + k_{q+r} l_0.$$

Otóż:

$p \mid k_0 l_{q+r} + \cdots + k_{q-1} l_{r+1} + k_{q+1} l_{r-1} + \cdots + k_{q+r} l_0$,

lecz: *nie* $p \mid k_q l_r$, gdyż *nie* $p \mid k_q$ i *nie* $p \mid l_r$,

a jednak: $p \mid bca_{q+r}$ czyli $p \mid m_{q+r}$,

co niemożliwe.

A więc naprz. $p \mid k_0, \ldots p \mid k_s$. Kładąc:

$$k_0 / p = k_0', \ldots k_s / p = k_s', \; bc / p = d,$$

otrzymamy:

$$d \,.\, f(z) \equiv (k_0' z^s + \cdots + k_s')(l_0 z_t + \cdots + l_t) \equiv \\ \equiv \Phi'(z) \,.\, \Psi(z), \text{ gdzie } \Phi'(z) \text{ i } \Psi(z)$$

są wielomianami całkowitemi.

Szukamy w dalszym ciągu podzielników pierwszych dla d, o ile jeszcze $d > 1$ i powtarzamy poprzednie postępowanie. Ostatecznie otrzymamy:

$$f(z) \equiv (\overline{k_0} z^s + \cdots + \overline{k_s})(\overline{l_0} z^t + \cdots + \overline{l_t}) \equiv \\ \equiv \overline{\Phi}(z) \,.\, \overline{\Psi}(z), \text{ gdzie } \overline{\Phi}(z) \text{ i } \overline{\Psi}(z)$$

są wielomianami całkowitemi stopni s i t większych niż zero, i stąd rozkład *całkowity dla* $f(z)$, *co dowodzi twierdzenia.*

Przejdźmy teraz do rozkładalności wymiernej wielomianu wymiernego. Niechaj będzie:

$f(z) \equiv a_0 z^m + \cdots + a_m$, $a_0 \neq 0$, $a_0 \ldots a_m$ *wymierne.*

Oznaczmy przez a najmniejszy wspólny mianownik dla $a_0 \ldots a_m$, następnie $b_i = a_i / a$, $i = 0 \ldots m$

i $$F(z) \equiv a f(z).$$

$F(z)$ jest wielomianem całkowitym. Jeżeli $F(z)$ jest całkowicie przywiedlne: $F(z) \equiv \varphi(z)\psi(z)$, gdzie $\varphi(z)$ i $\psi(z)$ całkowite, to:

$$f(z) = \frac{\varphi(z)}{a} \cdot \psi(z),$$

więc $f(z)$ jest *wymiernie* przywiedlne.

Jeżeli teraz $f(z)$ jest *wymiernie* przywiedlne:

$f(z) \equiv \varphi(z)\psi(z)$, $\varphi(z)$ i $\psi(z)$ wymierne;

to: $F(z) \equiv af(z) \equiv a\varphi(z)\psi(z) \equiv \overline{\varphi}(z)\psi(z)$

jest *wymiernie* przywiedlne, a więc jest też i *całkowicie* przywiedlne. Badanie *wymiernej* przywiedlności *wymiernego* $f(z)$ sprowadza się zatem do zbadania *całkowitej przywiedlności całkowitego* $F(z)$.

Pozostaje nam zatem *całkowita przywiedlność całkowitych* wielomianów do zbadania. Mamy tu przedewszystkiem zasadniczego znaczenia wynik badań *L. Kroneckera*:[1]

Tw. Zbadanie całkowitej przywiedlności całkowitego wielomianu może być zawsze uskutecznione przez wykonanie skończonej ilości algebraicznych operacyj.

Metoda Kroneckera.

Niechaj będzie:

$f(z) \equiv a_0 z^m + \cdots + a_m$, $a_0 \neq 0$, $a_0 \ldots a_m$ całk.

Jeżeli $f(z)$ ma być przywiedlne: $f(z) \equiv \varphi(z) . \psi(z)$, $\varphi(z)$ i $\psi(z)$ całkowite, $st'\varphi = s > 0$, $st'\psi = t > 0$, $s + t = m$, to $s \leqq E\left(\frac{m}{2}\right)$ lub $t \leqq E\left(\frac{m}{2}\right)$, gdzie

[1] Grundzüge einer arithmetischen Theorie der algebraischen Grössen. Journal de Crelle, t. 92.

$n = E\left(\frac{m}{2}\right)$ jest *całkowitą* częścią $\frac{m}{2}$. Wystarcza zatem szukać czynników $\varphi(z)$ całkowitych stopnia zawartego między 1 a n. Aby to uczynić, obieramy dowolnie ciąg $n+1$ liczb *całkowitych, różnych* między sobą:

$$z_0, z_1, \ldots z_n.$$

Oznaczmy: $w_i = f(z_i)$, $i = 0, 1 \ldots n$. Są to widocznie liczby *całkowite*. Jeżeli istnieje rozkład całkowity: $f(z) \equiv \varphi(z)\psi(z)$, $0 < st'\varphi \leqq n$, $0 < st'\psi$, to: $w_i = \varphi(z_i)\psi(z_i)$, $i = 0 \ldots n$.

Lecz $\varphi(z)$ i $\psi(z)$ są wielomianami całkowitemi, więc $\varphi(z_i)$ i $\psi(z_i)$ są całkowite i do tego:

$$\varphi(z_i) \mid w_i.$$

Widzimy więc, że wartości:

$$\varphi(z_0), \ldots \varphi(z_n)$$

trzeba szukać wśród podzielników liczb $w_0 \ldots w_n$. Tworzymy zatem tabliczkę podzielników:

	podzielniki
w_0	d_0', d_0'', ...
w_1	d_1', d_1'', ...
⋮	
w_n	d_n', d_n'', ...

Jest to możliwe do wykonania przy pomocy skończonej ilości operacyj algebraicznych na liczbach całkowitych.

Obieramy teraz dowolnie po jednym podzielniku dla każdego w_i:

$$d^{(0)} \ldots d^{(n)},$$

gdzie: $d^{(0)} \mid w_0, \ldots d^{(n)} \mid w_n$.

Wyborów takich jest *skończona ilość.*

Dokonawszy wyboru, szukamy metodą interpolacyjną (naprz. Lagrange'a) wielomianu $\varphi(z)$ stopnia $\leqq n$, takiego, by:

$$\varphi(z_0) = d^{(0)}, \ldots \varphi(z_n) = d^{(n)}.$$

Odszukawszy go, próbujemy dzielić $f(z)$ przez $\varphi(z)$. Odrzucamy φ, gdy *nie* $\varphi(z) \mid f(z)$. W ten sposób otrzymamy, po odrzuceniu nieodpowiednich, wszystkie podzielniki $\varphi(z)$ całkowite wielomianu $f(z)$, a tem samem zbadamy, czy $f(z)$ takowe wogole posiada. Wynik badania powie nam czy $f(z)$ jest całkowicie przywiedlne czy nie.

Uw. Runge i Mandl w pracach zamieszczonych w Journal de Crelle t. 99 i t. 113 starali się wprowadzić pewne uproszczenia do metody Kroneckera, pozwalające zmniejszyć ilość interpolacyj i dzieleń tej metody.

Posiadamy niezliczoną ilość, przeważnie mało ważnych w praktyce, kryterjów *nieprzywiedlności* całkowitej. Z tych cytujemy tylko najbardziej znane:

Tw. Eisensteina[1] (i **Schönemanna**).

Jeżeli wielomian *kanoniczny:*

$$f(z) \equiv z^m + a_1 z^{m-1} + \cdots + a_m$$

jest *całkowity* i znajdzie się taka liczba *pierwsza* p (> 1), że:

$$p \mid a_1 \ldots p \mid a_m, \text{ lecz nie } p^2 \mid a_m,$$

to $f(z)$ jest *nieprzywiedlne.*

[1] Eisenstein (uczeń Gaussa): Journ. de Crelle, t. 39; Schönemann: Journ. de Crelle, t. 32.

Dem. Gdyby:

$f(z) \equiv \varphi(z)\,\psi(z)$,

$\left.\begin{array}{l}\varphi(z) \equiv b_0 z^s + \cdots + b_s \\ \psi(z) \equiv c_0 z^t + \cdots + c_t\end{array}\right\}$ $b_0 \neq 0,\ c_0 \neq 0,\ b_0 \ldots b_s, c_0 \ldots$ ...c_t całk. $s>0, t>0, s+t=m$,

to:

$a_m = b_s c_t,\ a_{m-1} = b_s c_{t-1} + c_t b_{s-1}, \ldots 1 = a_0 = b_0 c_0.$

Ponieważ: $p \mid b_s c_t$ i *nie* $p^2 \mid b_s c_t$, więc naprz. $p \mid b_s$ i *nie* $p \mid c_t$ [lub przeciwnie].

wtedy: $p \mid a_{m-1}$, stąd: $p \mid c_t b_{s-1}$ i *nie* $p \mid c_t$,

a więc: $p \mid b_{s-1}$. Idąc tak dalej otrzymalibyśmy nakoniec, że $p \mid b_0$, więc $p \mid 1$, co niemożliwe. Zatem $f(z)$ nieprzywiedlne.

Przykład: 1. Gdy p jest liczbą pierwszą (>1), to wielomian: $z^m + pz^{m-1} + \cdots + p \quad (m > 0)$ jest nierozkładalny. [W przykładach na początku ustępu niniejszego obraliśmy $p = 5$].

2. Wiadomo nam [str. 114], że:

$$z - 1 \mid z^m - 1 \qquad (m \text{ całk.} > 0),$$

przyczem:

$$z^m - 1 \equiv (z-1)(z^{m-1} + z^{m-2} + \cdots + 1) \quad (m > 1).$$

Oznaczmy: $F(z) \equiv z^{m-1} + \cdots + 1$.

Kładąc $z - 1 = y$, otrzymamy:

$$(1+y)^m - 1 \equiv y\,F(1+y),$$

$$F(1+y) \equiv y^{m-1} + \binom{m}{1} y^{m-2} + \cdots + \binom{m}{m-2} y + \binom{m}{m-1}$$

Niech będzie m liczbą pierwszą (>1). Wtedy:

$$m \mid \binom{m}{1}, \ldots m \mid \binom{m}{m-1}, \text{ lecz } \textit{nie } m^2 \mid \binom{m}{m-1},$$

zatem $F(1+y)$ nie jest całkowicie rozkładalne.

Tem samem $F(z)$ jest też nieprzywiedlne, bo: $F(z) \equiv \varphi(z)\psi(z)$ dałoby: $F(1+y) \equiv \varphi(1+y)\psi(1+y)$.

Zakończymy uwagą o *rozkładalności rzeczywistej* wielomianów rzeczywistych. Powołując się na badania § 4 ust. 2 obecnego rozdziału, zawnioskujemy łatwo:

Tw. Wielomian *rzeczywisty niezerowy* jest *tylko* wtedy *rzeczywiście nierozkładalny,* gdy jest stopnia *zerowego* lub *pierwszego* albo stopnia *drugiego* i *nie posiada* pierwiastków *rzeczywistych.*

Zagadnienia, związane z rozkładalnością wielomianów więcej niż jednej zmiennej, przekraczają ramy niniejszej książeczki.

2. **Pierwiastki wymierne** wielomianu całkowitego.

Niechaj będzie:

$f(z) \equiv a_0 z^m + \cdots + a_m$, $a_0 \neq 0$, $a_0, \ldots a_m$ całkowite.

Jeżeli a jest pierwiastkiem *całkowitym* dla $f(z)$, to:

$$a_0 a^m + a_1 a^{m-1} + \cdots + a_m = 0,$$

skąd: $$a \mid a_m.$$

Jeżeli ułamek *nieskracalny* $\frac{r}{s}$ jest pierwiastkiem dla $f(z)$, to:

$$a_0 \frac{r^m}{s^m} + a_1 \frac{r^{m-1}}{s^{m-1}} + \cdots + a_m = 0,$$

$$a_0 r^m + a_1 r^{m-1} s + \cdots + a_m s^m = 0.$$

Stąd: $r \mid a_m s^m$, lecz $[r, s^m] = 1$, więc $r \mid a_m$

i $s \mid a_0 r^m$, lecz $[s, r^m] = 1$, więc $s \mid a_0$.

Mamy zatem twierdzenia, które jednocześnie dają

nam w rękę metodę szukania pierwiastków całkowitych i wymiernych wielomianu całkowitego.

Tw. 1. Jedynemi pierwiastkami całkowitemi wielomianu całkowitego:

$$f(z) \equiv a_0 z^m + \cdots + a_m, \quad a_0 \neq 0,$$

mogą być *podzielniki* wyrazu a_m.

2. Jedynemi pierwiastkami wymiernemi, typu $\frac{r}{s}$, gdzie $[r, s] = 1$, mogą być takie $\frac{r}{s}$, gdzie $r \mid a_m$ i $s \mid a_0$.

3. Wielomian całkowity kanoniczny może mieć pierwiastki wymierne tylko takie, które są liczbami *całkowitemi* [$s \mid a_0$, $a_0 = 1$, $s = \pm 1$].

Uw. Poszukując pierwiastków wymiernych typu $\frac{r}{s}$, gdzie $[r, s] = 1$, możemy zawsze założyć, że s jest dodatnie.

§ 6. Teorja Sturma.

1. **Problem.** Zagadnienie jakie stawiało sobie wielu algebraików, jak Descartes, Harriot, Budan czy Fourier, polegało na tem, by mając dany wielomian niezerowy *rzeczywisty* i jakiś przedział liczbowy, odszukać *ilość* pierwiastków *rzeczywistych*, zawartych w tym przedziale. Wynikiem ich badań jest szereg twierdzeń, noszących imiona swych twórców, które pozwalają odpowiedzieć na to pytanie w sposób mniej lub więcej dokładny.

Matematyk francuski Ch. Sturm podał metodę, pozwalającą na rozstrzygnięcie tego problemu

przy pomocy skończonej ilość operacyj algebraicznych.[1] Zajmiemy się teraz jej wykładem.

2. Łańcuchy Sturma.

Df. Nazwiemy *łańcuchem Sturma w przedziale liczbowym otwartym* (a, b) *ciąg* skończony wielomianów *rzeczywistych:*

$$f_0(z),\ f_1(z) \ldots, f_p(z)$$

o własnościach:

I. $f_0(a) \neq 0,\ f_0(b) \neq 0.$

II. $f_p(z) \neq 0$ dla $a \leqq z \leqq b.$

III. Gdy $f_s(z_0) = 0,\ a \leqq z_0 \leqq b,\ 1 \leqq s \leqq p-1,$ to: $$f_{s-1}(z_0) \cdot f_{s+1}(z_0) < 0,$$ [a więc $f_{s-1}(z_0) \neq 0,\ f_{s+1}(z_0) \neq 0$; $f_{s-1}(z_0)$ i $f_{s+1}(z_0)$ mają przeciwne znaki].

IV. Gdy $a < z_0 < b$ i $f_0(z_0) = 0$, to:

$$f_1(z_0) \cdot f_0'(z_0) > 0^2 \quad \text{[te same znaki!]}.$$

Df. Jeżeli $f(z)$ jest wielomianem *rzeczywistym,* to łańcuch Sturma: $f_0(z) \ldots f_p(z)$ w przedziale (ab) jest *łańcuchem* **dla** $f(z)$, gdy:

$$f(z) \cdot f_0(z) = 0, \text{ dla } a \leqq z \leqq b,$$

pociąga, że $f(z) = 0$ *i* $f_0(z) = 0$, a więc gdy: $f(z)$ i $f_0(z)$ zerują się *jednocześnie* w przedziale (ab) i $f(a) \neq 0$ oraz $f(b) \neq 0.$

Tw. Jeżeli $f_0(z), \ldots f_p(z)$ jest łańcuchem Sturma w przedziale (ab), to wielomian $f_0(z)$ nie

[1] p. Analyse d'un Mémoire sur la résolutions des équations numériques. Bull. de Ferussac. t. XI, 1829 i Mémoire sur la résolution des équations numeriques. Mém. des Savants Etrangers. Paris. 1835 [tłum. niem. w Ostwald Klassiker, t. 143].

[2] $f_0'(z)$ jest *pochodną* $f_0(z)$!

posiada w przedziale (ab) pierwiastków *rzeczywistych wielokrotnych.*

Dem. Gdyby takim było k, to mielibyśmy:

$$f_0(k) = 0,\ f_0'(k) = 0,\ (a < k < b),$$

co sprzeciwiałoby się warunkowi IV.

Oczywiście musi być $f_0(z) \not\equiv 0$.

Tw. Każdy wielomian *rzeczywisty niezerowy* posiada w *każdym* przedziale (ab) choć jeden łańcuch Sturma, o ile tylko końce przedziału a i b *nie* są jego *pierwiastkami.*

Dem. Niechaj będzie:

$$f(z) \equiv a_0 z^m + \cdots + a_m,\ a_0 \neq 0,\ a_0, \ldots a_m \in q,$$
$$f(a) \neq 0,\ f(b) \neq 0.$$

Jeżeli rozłożymy $f(z)$ na *dzielniki pierwiastkowe* [str. 95] i przedstawimy jako:

$$f(z) \equiv a_0 (z - b_1)^{\beta_1} \ldots (z - b_r)^{\beta_r},$$

gdzie: $b_1 \ldots b_r$ jest pełnym ciągiem *różnych* pierwiastków $f(z)$; $\beta_1 \ldots \beta_r$ są odnośnemi rzędami, to największy wspólny podzielnik dla $f(z)$ i $f'(z)$ ma postać:

$$\bar{f}(z) \equiv [f(z), f'(z)] \equiv (z - b_1)^{\beta_1 - 1} \ldots (z - b_r)^{\beta_r - 1},$$

stąd: dzieląc $f(z)$ przez $\bar{f}(z)$, otrzymamy:

$$\varphi(z) \equiv a_0 (z - b_1) \ldots (z - b_r),$$

więc $\varphi(z)$ posiada dokładnie te same pierwiastki co $f(z)$, lecz wszystkie rzędu *jeden.*

(1) Obierzmy za $f_0(z)$ wielomian $\varphi(z)$, przyczem zważmy, że gdy $f(z)$ rzeczywiste, to $f'(z)$ rzeczywiste i $\bar{f}(z)$, otrzymane drogą łańcuchowego dzielenia, też będzie wielomianem rzeczywistym.

Stąd iloraz $\varphi(z)$ będzie rzeczywisty i nie może się zerować jednocześnie ze swą pochodną $\varphi'(z)$, gdyż posiada jednokrotne tylko pierwiastki. Ponieważ:

$$f(a) \neq 0 \,.\supset.\, \varphi(a) \neq 0 \text{ i } f(b) \neq 0 \,.\supset.\, \varphi(b) \neq 0,$$

więc spełniony będzie warunek I.

(2) Obierzmy za $f_1(z)$ wielomian $f_0'(z)\,(=\varphi'(z))$, przez co spełniamy warunek IV.

(3) Przeprowadźmy łańcuchowe dzielenie $f_0(z)$ przez $f_1(z)$ *zmieniając tylko znaki reszt:*

$$\begin{aligned} f_0(z) &= Q_1(z)\, f_1(z) - R_1(z) \\ f_1(z) &= Q_2(z)\, R_1(z) - R_2(z) \\ &\vdots \\ R_{\rho-1}(z) &= Q_{\rho+1}(z)\, R_\rho(z) - R_{\rho+1}(z) \end{aligned} \qquad (*)$$

$sl' f_1 > sl' R_1 > \cdots > sl' R_{\rho+1}$, $R_{\rho+1}(z) = \text{const} = A$. Ponieważ $f_0(z)$ i $f_1(z)$ są pierwsze względem siebie, więc $R_{\rho+1}(z) = A \neq 0$.

Połóżmy teraz:

$$f_2(z) = R_1(z), \ldots f_{\rho+2}(z) = R_{\rho+1}(z),\ \rho + 2 = p.$$

Otóż $f_p(z) = A \neq 0$ wszędzie, więc i w przedziale (ab) łącznie z końcami. Tem samem czynimy zadość warunkowi II.

Jeżeli: $a < k < b$, $1 \leq s \leq p-1$, $f_s(k) = 0 = R_{s-1}(k)$, to: $f_{s-1}(z) = R_{s-2}(z) = Q_s(z)\, R_{s-1}(z) - R_s(z) =$

$$= Q_s(z) \,.\, f_s(z) - f_{s+1}(z).$$

[dla $s = 1$ trzeba położyć: $R_0 = f_1$, $R_{-1} = f_0$.].

Stąd: $$f_{s-1}(k) = -f_{s+1}(k)$$

Gdyby $f_{s+1}(k) = 0$, to byłoby $R_{s-1}(k) = 0$ i $R_s(k) = 0$, więc dzięki związkom $(*)$ kolejno:

$$R_{s+1}(k) = R_{s+2}(k) = \ldots = R_{\rho+1}(k) = 0$$

co niemożliwe, bo $A \neq 0$.

Zatem: $f_{s+1}(k) \neq 0,\ f_{s-1}(k) \neq 0$

i $f_{s+1}(k) \cdot f_{s-1}(k) < 0,$

przez co już czynimy zadość warunkowi III.

Ciąg: $f_0, f_1, \ldots f_p$ jest więc żądanym łańcuchem Sturma.

Uw. Nie jest to oczywiście jedyny sposób tworzenia łańcucha Sturma. Naprzykład możnaby się natychmiast zatrzymać w ciągu reszt $R_1, R_2 \ldots$, gdyby się pokazało, że pewna reszta nie zeruje się w przedziale (a, b), ani na jego końcach. Rozprawa Sturma z r. 1835, cytowana wyżej, zawiera wiele podobnych praktycznych uwag, upraszczających tworzenie łańcucha.

3. Ilość zmian znaków.

Oznaczmy przez $V(a,b)$, gdzie a i b *rzeczywiste*, $a \neq 0$ i $b \neq 0$, liczbę 1, gdy $a \cdot b < 0$, natomiast liczbę 0, gdy $a \cdot b > 0$.

Niechaj teraz ciąg:

$$a_0, a_1 \ldots a_p$$

składa się z liczb *rzeczywistych różnych od zera*.

Df. Ilością zmian znaków w ciągu liczb *rzeczywistych różnych od zera*:

$$a_0, a_1 \ldots a_p \tag{1}$$

nazwiemy liczbę:

$$V(a_0, a_1, \ldots a_p) \overset{\text{df.}}{=} V(a_0, a_1) + V(a_1, a_2) + \cdots$$
$$\cdots + V(a_{p-1}, a_p).$$

Ilością zmian znaków w ciągu liczb *rzeczywistych*:

$$a_0, a_1 \ldots a_p \tag{2}$$

gdzie *nie wszystkie* człony są *zerem*, lecz gdzie

mogą występować człony zerowe, nazwiemy ilość zmian znaków w ciągu, który powstaje z (2) przez *odrzucenie zer.*

Dla zupełności położymy jeszcze:

$$V(a, 0, \ldots 0) = 0, \quad a \varepsilon q.$$

Przyda nam się bardzo następujący:

Lemmat: Gdy $a, b, c \varepsilon q$, $a \neq 0$, $c \neq 0$

i $$V(a, b, c) = 1,$$

to: $V(a, k, c) = 1$ dla *dowolnego k rzeczywistego.*

Dem. Zastępując, co oczywiście wolno, liczby dodatnie przez $+1$, ujemne przez -1 mamy następujące możliwości:

$$V(a, b, c) = V(+1, +1, -1) = V(+1, -1, -1) = V(+1, 0, -1)$$

lub $$V(a, b, c) = V(-1, +1, +1) = V(-1, -1, +1) = V(-1, 0, +1).$$

Wykluczone są kombinacje:

$V(a, b, c) = V(+1, b, +1)$ i $V(a, b, c) = V(-1, b, -1)$,

co dałoby dla $b \gtrless 0$ zawsze 2 lub 0.

4. Twierdzenie Sturma.

Jeżeli: $f(z)$ jest wielomianem *rzeczywistym niezerowym*, (a, b) przedziałem liczbowym otwartym

$$a < b, \quad f(a) \neq 0, \quad f(b) \neq 0,$$

$$f_0(z), \quad f_1(z) \ldots f_p(z)$$

łańcuchem Sturma dla $f(z)$ w przedziale (ab) i jeżeli oznaczymy:

$$A = V\{f_0(a), f_1(a), \ldots f_p(a)\}$$

$$B = V\{f_0(b), f_1(b), \ldots f_p(b)\},$$

to ilość pierwiastków *rzeczywistych* wielomianu $f(z)$ w przedziale otwartym $(a\,b)$ wynosi:

$$E(a,b) = A - B.$$

Dem. Utwórzmy zbiór (M) złożony z liczb a i b oraz wszystkich pierwiastków *wszystkich* wielomianów: $f_0, f_1 \ldots f_p$, leżących w przedziale domkniętym $[a\,b]$. Będzie to zbiór *skończony*, posiadający przynajmniej dwa elementy. Ustawmy wszystkie elementy zbioru (M) w ciąg *rosnący:*

$$a = a_0 < a_1 < \ldots < a_m = b.$$

Oznaczmy:

$$V(z) = V\{f_0(z), f_1(z), \ldots f_p(z)\}$$

dla $z \in q$ i badajmy przebieg funkcji rzeczywistej $V(z)$, gdy z wędruje od a do b.

(1) $$V(a) = A,\ V(b) = B.$$

(2) Gdy z wędruje wewnątrz przedziału częściowego $(a_s,\ a_{s+1})$, $s = 0, 1, \ldots m-1$, to $V(z)$ nie ulega zmianie ($=$ const.), ze względu na znaną własność funkcyj ciągłych rzeczywistych zmiennych.

(3) $V(z)$ ulegać może zmianie swej wartości jedynie przy przejściu przez człon a_s ciągu:

$$a_0, a_1 \ldots a_m.$$

(4) Jeżeli $f_{k-1}(a_s) \neq 0$, $f_k(a_s) \neq 0$, $f_{k+1}(a_s) \neq 0$, to $$V\{f_{k-1}(z),\ f_k(z),\ f_{k+1}(z)\}$$ *nie ulega zmianie* przy przejściu przez a_s, gdyż nie zmieniają się znaki żadnej z trzech funkcyj:

$$f_{k-1},\ f_k,\ f_{k+1}.$$

(5) Jeżeli $k > 1$ i $f_k(a_s) = 0$, to:

$$f_{k-1}(a_s) \cdot f_{k+1}(a_s) < 0$$

(war. III) z a t e m:

$$V\{f_{k-1}(a_s), f_k(a_s), f_{k+1}(a_s)\} = 1.$$

Funkcje $f_{k-1}(z)$ i $f_{k+1}(z)$ zachowują swe znaki w przedziale (a_{s-1}, a_{s+1}) lub w (a_s, a_{s+1}) gdy $s = 0$, czy też (a_{s-1}, a_s), gdy $s = m$.

W takim przedziale:

$$V\{f_{k-1}(z), f_k(a_s), f_{k+1}(z)\} = 1 = V\{f_{k-1}(z), f_k(z), f_{k+1}(z)\},$$

dzięki L e m m a t o w i poprzedniego ustępu, zatem: $V\{f_{k-1}(z), f_k(z), f_{k+1}(z)\}$ nie ulega zmianie przy przejściu przez a_s.

(6) Nie może być $f_p(a_s) = 0$, gdyż $f_p(z) \neq 0$ w przedziale i na jego końcach.

(7) Gdy $f_0(a_s) = 0$, to $a_s \neq a_0 = a$ i $a_s \neq a_m = b$. Funkcja $f_0(z)$ *zmienia znak* przy przejściu przez a_s, bo gdyby $f_0(z)$ miało ten sam znak w (a_{s-1}, a_s) co w (a_s, a_{s+1}), to $f_0(z)$ miałoby w punkcie a_s extremum, zatem byłoby:

$$f_0'(a_s) = 0, \text{ więc } f_1(a_s) = 0,$$

co wykluczone wedle warunku IV.

$V(f_0(z), f_1(z)) = V(f_0(z), f_0'(z))$ w otoczeniu punktu a_s. [war. IV].

Atoli:

$$f_0(a_s + h) = f_0(a_s) + f_0'(a_s) \cdot h + \cdots + \frac{f_0^{(r)}(a_s)}{r!} h^r$$

$$= f_0'(a_s)\, h + \cdots + \frac{f_0^{(r)}(a_s)}{r!} h^r, \quad r = st' f_0.$$

$$\frac{f_0(a_s + h)}{f_0'(a_s)} = h\left[1 + \frac{f_0''(a_s)}{2! f_0'(a_s)} h + \cdots + \frac{f_0^{(r)}(a_s)}{r! f_0'(a_s)} \cdot h^{-1}\right],$$

zatem lewa strona dla dostatecznie małych $|h|$ jest ujemna przy $h<0$, dodatnia przy $h>0$; $f_1(a_s)$ nie zmienia znaku w przedziałach (a_{s-1}, a_s) i (a_s, a_{s+1}), zatem:

$$V\{f_0(z), f_1(z)\} = +1 \quad \text{w } (a_{s-1}, a_s)$$
$$V\{f_0(z), f_1(z)\} = 0 \quad \text{w } (a_s, a_{s+1})$$

Stąd widać, że $V\{f_0(z), f_1(z)\}$ przy przejściu przez a_s *pomniejsza* się o *jedność*.

(8) Uwzględniając definicję $V\{f_0(z), \dots f_\nu(z)\}$, widzimy, że $V(z)$ pomniejsza się o 1 wtedy i tylko wtedy, gdy a_s jest pierwiastkiem dla $f_0(z)$, a więc dla $f(z)$. Stąd już:

$$E(a,b) = V(a) - V(b) = A - B.$$

5. **Uzupełniające uwagi.**

Jeżeli chcemy zbadać ilość pierwiastków w przedziale *otwartym* (a,b) w wypadku, gdy $f(a)=0$ lub $f(b)=0$, to ponieważ ilość pierwiastków $f(z)$ niezerowego w tym przedziale jest *skończona*, możemy obrać tak małe $\varepsilon>0$, by:

(1) $f(z) \neq 0$ w przedziale $(a, a+\varepsilon)$.

(2) $f(z) \neq 0$ w przedziale $(b-\varepsilon, b)$.

(3) $a+\varepsilon < b-\varepsilon$.

(4) $f(a+\varepsilon) \neq 0$, $f(b-\varepsilon) \neq 0$.

szukamy następnie $E(a+\varepsilon, b-\varepsilon)$ metodą Sturma, co da nam odpowiedź na nasz problem.

Jeżeli chcemy znaleźć ilość pierwiastków w przedziale *zamkniętym* $[a,b]$, to znów obieramy tak $\varepsilon>0$, że:

(1) $f(z) \neq 0$ w $(a-\varepsilon, a)$ i $(b, b+\varepsilon)$,

(2) $f(a-\varepsilon) \neq 0$, $f(b+\varepsilon) \neq 0$.

Szukamy wtedy $E(a-\varepsilon, b+\varepsilon)$.

Ze względu na skończoną wogóle ilość pierwiastków wielomianu niezerowego możemy znaleźć takie $k>0$ i $l<0$, że:

(1) $\quad f(l) \neq 0, \; f(k) \neq 0$

i że (2) wszystkie pierwiastki rzeczywiste dla $f(z)$ znajdą się w przedziale (l, k).

Wtedy, odszukane metodą Sturma:

$$E(l, k), \; E(0, k), E(l, 0),$$

dadzą nam odpowiednio:

$$E(-\infty, +\infty), \; E(0, +\infty), \; E(-\infty, 0)$$

a więc: ilość pierwiastków *rzeczywistych* wogóle, ilość pierwiastków *dodatnich*, ewentualnie ilość pierwiastków *ujemnych*.

Aby odszukać $E(a, +\infty)$ czy $E(-\infty, a)$, trzeba tylko obrać $k>a$ względnie $l<a$ i szukać $E(a, k)$ względnie $E(l, a)$. Analogicznie radzimy sobie w innych jeszcze wypadkach.

W dalszym toku wykładu poznamy sposoby odszukiwania efektywnego liczb takich jak ε, k i l w obecnych rozważaniach.

6. Związek z teorją funkcyj analitycznych.

Teorja funkcyj analitycznych pozwala nam rozwiązać problem obszerniejszy jeszcze niż zagadnienia dotychczasowe, dzięki genjalnym odkryciom A. Cauchy'ego. Tak zwane twierdzenie Cauchy'ego o *residuach*, („pozostałościach", jak tłumaczy J. Sochocki) daje nam w zastosowaniu do wielomianów wynik następujący. Pomyślmy sobie, że na płaszczyźnie Gaussa zatoczono pewną krzywą zamkniętą C, która dzieli tę płaszczyznę na dwie części i załóżmy, że krzywa ta nie przechodzi przez żadne miejsce zerowe wielomianu niezerowego $f(z)$ (rzeczywi-

stego lub nie) oraz, że posiada naprz. w każdym punkcie styczną, zmieniającą się w sposób ciągły wzdłuż krzywej. Oznaczmy przez:

$$a_1, a_2, \ldots a_k$$

ciąg wszystkich *różnych* pierwiastków wielomianu $f(z)$ leżących *wewnątrz* C oraz przez: $\alpha_1, \alpha_2, \ldots \alpha_k$ ich rzędy.

Rozważmy całkę:

$$\int_C \frac{f'(z)}{f(z)}\,dz$$

wziętą wzdłuż krzywej C w kierunku dodatnim.

Otóż twierdzenie Cauchy'ego powiada, że:

$$\frac{1}{2\pi i}\int_C \frac{f'(z)}{f(z)}\,dz = \alpha_1 + \ldots + \alpha_r.$$

Jeżeli wielomian $f(z)$ zastąpimy przez wielomian $\overline{f}(z)$, który posiada dokładnie te same pierwiastki, co $f(z)$, lecz wszystkie rzędu *jeden*, to:

$$\frac{1}{2\pi i}\int \frac{\overline{f}'(z)}{\overline{f}(z)}\,dz$$

daje nam wprost ilość pierwiastków $f(z)$ zawartych w obrębie krzywej C.

Jeżeli teraz $f(z)$ jest wielomianem rzeczywistym i $f(a) \neq 0$, $f(b) \neq 0$, $a < b$, $a, b \varepsilon q$, to szukamy takiego $\varepsilon (> 0)$, by wewnątrz i na brzegu prostokąta o wierzchołkach leżących w punktach:

$$a + \varepsilon i,\ a - \varepsilon i,\ b + \varepsilon i,\ b - \varepsilon i,$$

nie było pierwiastków istotnie zespolonych i za C obieramy obwód tego prostokąta, wtedy:

$$\frac{1}{2\pi i}\int_C \frac{f'(z)}{f(z)}\,dz = E(a, b),$$

Na stronie 105 pozostawiliśmy bez dowodu ważne twierdzenie o miejscach zerowych wielomianów o więcej niż jednej zmiennej. Lukę tę chcemy teraz wypełnić.

Będziemy jednak zmuszeni powołać się na teorję funkcyj analitycznych, a mianowicie na twierdzenia, które przyjęliśmy w poprzednim ustępie.

Przypuśćmy więc, że wielomian:

$$f(z_1 \dots z_k),\ k > 1,$$

posiada stopień *dodatni* względem naprz. z_k i że:

$$f(a_1 \dots a_k) = 0.$$

Obieramy dowolnie liczbę $\varepsilon, > 0$. Widocznie wielomian $\varphi(\hat{z}) \equiv f(a_1 \dots a_{k-1}, \hat{z})$ posiadał pierwiastek a_k i można będzie, wobec tego, obrać $0 < \eta < \varepsilon$ tak, by w otoczeniu: $|z - a_k| < \eta$ *łącznie* z *brzegiem* pierwiastek a_k był *jedynym*. Rzędem jego niech będzie $\alpha\ (\geq 0)$.

Oznaczając przez K ograniczenie powyższego otoczenia dostaniemy wedle ust. 6:

$$\frac{1}{2\pi i}\int_K \frac{\varphi'(z)}{\varphi(z)}\,dz = \alpha > 0.$$

Funkcja $\dfrac{\varphi'(z)}{\varphi(z)}$ ma sens wzdłuż K, atoli wielomiany $f'(z_1 \dots z_{k-1} z_k)$ i $f'_{z_k}(z_1 \dots z_{k-1} z_k)$ są funkcjami *ciągłemi*, więc można będzie dobrać liczbę $\delta > 0$ tak, by *wzdłuż* K i dla $|b_1 - a_1| < \delta \dots |b_{k-1} - a_{k-1}| < \delta$ zachodziły związki:

$$(1)\ f(b_1 \dots b_{k-1} z) \neq 0,\ (2) |\varepsilon(z)| = \left|\frac{f'_{z_k}(b_1 \dots b_{k-1} z)}{f(b_1 \dots b_{k-1} z)} - \frac{\varphi'(z)}{\varphi(z)}\right| < \frac{1}{\eta}.$$

Wtedy:

$$\frac{1}{2\pi i}\int_K \frac{f'_{z_k}(b_1 \dots b_{k-1} z)}{f(b_1 \dots b_{k-1} z)}\,dz = \frac{1}{2\pi i}\int_K \frac{\varphi'(z)}{\varphi(z)}\,dz + \frac{1}{2\pi i}\int_K \varepsilon(z)\,dz$$

$$= \alpha + \frac{1}{2\pi i}\int_K \varepsilon(z)\,dz. \qquad (*)$$

Lecz:

$$\left|\frac{1}{2\pi i}\int_K \varepsilon(z)\,dz\right| \leq \frac{1}{2\pi} \cdot 2\pi\eta \cdot \max \varepsilon(z)$$

$$< \eta \cdot \frac{1}{\eta} = 1.$$

Atoli prawa strona równości (*) musi być liczbą *całkowitą*, więc:

$$\frac{1}{2\pi i}\int_K \varepsilon(z)\,dz = 0$$

i

$$\frac{1}{2\pi i}\int_K \frac{f'_{z_k}(b_1 \dots b_{k-1} z)}{f(b_1 \dots b_{k-1} z)}\,dz = \alpha > 0,$$

co świadczy, że $f(b_1 \dots b_{k-1} z)$ posiada choć jeden pierwiastek, powiedzmy b_k, w otoczeniu $|z - a_k| < \eta < \varepsilon$.

Stąd wnioski:

(1) Do każdego systemu $b_1 \dots b_{k-1}$ takiego, że:

$$|b_1 - a_1| < \delta, \dots |b_{k-1} - a_{k-1}| < \delta$$

można dobrać b_k tak, że:

$$f(b_1 \dots b_{k-1} b_k) = 0 \text{ i } |a_k - b_k| < \varepsilon.$$

(2) Biorąc $\delta' = \min(\delta, \varepsilon)$ i żądając w (1), by:

$$|b_1 - a_1| < \delta' \dots |b_{k-1} - a_{k-1}| < \delta'$$

spostrzeżemy, że w otoczeniu:

$$|b_1 - a_1| < \varepsilon \dots |b_k - a_k| < \varepsilon$$

wielomian $f(z_1 \dots z_k)$ posiada nieskończenie wiele pierwiastków.

(3) Dla każdego układu $b_1 \dots b_{k-1}$ takiego, że:

$$|b_1 - a_1| < \delta \dots |b_{k-1} - a_{k-1}| < \delta,$$

pełny ciąg pierwiastków wielomianu $f(b_1 \dots b_{k-1} z)$, leżących w otoczeniu $|z - a_k| < \eta$ posiada dokładnie α członów.

[Celem zrozumienia wywodów niniejszego i jak i poprzedniego ustępu, zechce czytelnik zaczerpnąć kilka potrzebnych wiadomości z dziedziny całek funkcyj zespolonej zmiennej z cytowanej już książeczki Knoppa: Funktionentheorie].

§ 7. Oddzielanie pierwiastków rzeczywistych wielomianu jednej zmiennej.

1. Kresy pierwiastków rzeczywistych.

Obierzmy wielomian *rzeczywisty, niezerowy,* stopnia dodatniego:

$f(z) \equiv a_0 z^m + \cdots + a_m,\ m > 0,\ a_0 \neq 0,\ a_0 \ldots a_m \in q$

Załóżmy, że:

$a_0, \ldots a_{s-1}$ są *nieujemne*, $a_s < 0,\ 0 < s \leqq m.$

Rozważajmy tylko z rzeczywiste i > 1. Wtedy:

$$|f(z)| \geqq a_0 z^m + \cdots + a_{s-1} z^{m-s+1} - \\ - \{|a_s| z^{m-s} + \cdots + |a_m|\}.$$

Oznaczmy: $K = \max\{|a_s|, \ldots |a_m|\},\ K > 0;$

Otrzymamy:

$$|f(z)| \geqq a_0 z^m - K\{z^{m-s} + \cdots + 1\} \\ = a_0 z^m - K \frac{z^{m-s+1} - 1}{z - 1} \\ = \frac{z^{m-s+1}[a_0(z^s - z^{s-1}) - K] + K}{z - 1}.$$

Obierzmy z tak, by $a_0(z^s - z^{s-1}) > K$. Atoli:

$a_0(z^s - z^{s-1}) = a_0 z^{s-1}(z - 1) > a_0(z - 1)^s$ dla $z > 1$,

więc wystarczy założyć, że $z > 1 + \sqrt[s]{\frac{K}{a_0}}$. Zatem dla tych wartości na z będzie $|f(z)| > 0$. Stąd:

Tw. Gdy w wielomianie *rzeczywistym* stopnia dodatniego:

$f(z) \equiv a_0 z^m + \cdots + a_m,\ a_0 \neq 0,\ a_0 \ldots a_m \in q, m > 0,$

mamy: $a_0, \ldots a_{s-1} \geqq 0,\ a_s < 0 \quad 0 < s \leqq m,$

to liczba dodatnia $1+\sqrt[s]{\frac{K}{a_0}}$, gdzie $K=\max\{|a_s|,\ldots |a_m|\}$, stanowi granicę górną dla pierwiastków *dodatnich*.

Uw. Wielomian $f(z)$ i jego kanoniczny mają te same pierwiastki, często opłaca się rozważać tylko wielomiany kanoniczne, wtedy $a_0=1>0$. Uzyskana granica jest tem lepsza im mniejsze jest K. Gdy wszystkie spółczynniki są $\geqq 0$, to wielomian nie posiada pierwiastków rzeczywistych dodatnich.

Uw. 2. Jeżeli w $f(z)$ zastąpimy z przez $-z$, to wielomian:

$$\varphi(z)\equiv(-1)^m f(-z)\equiv a_0 z^m - a_1 z^{m-1}+\cdots\pm a_m$$

posiada pierwiastki przeciwnego znaku niż $f(z)$, a równe im co do wartości bezwzględnej. Gdy a jest granicą *górną* dla pierwiastków *dodatnich* $\varphi(z)$, to $-a$ będzie granicą *dolną* dla pierwiastków *ujemnych* $f(z)$.

Uw. 3. Warunkiem koniecznym i dostatecznym, by *zero* było pierwiastkiem wielomianu:

$$f(z)\equiv a_0 z^m+\cdots+a_m \qquad (a_0\neq 0),$$

jest oczywiście: $a_m=0$.

Jeżeli ogólniej: $a_s\neq 0$, $a_{s+1}=0\ldots a_m=0$, $0\leqslant s<m$, to wielomian: $\psi(z)\equiv a_0 z^s+\cdots+a_s$, a więc taki, że: $f(z)\equiv\psi(z)\,.\,z^{m-s}$

posiada za pierwiastki jedynie (i wszystkie) pierwiastki wielomianu $f(z)$ *po odrzuceniu zera*. Celem zbadania zatem *dodatnich* i *ujemnych* pierwiastków wielomianu rzeczywistego $f(z)$ możemy zawsze zastąpić $f(z)$ przez $\psi(z)$.

Uw. 4. Jeżeli założymy (co można wobec uw. 3), że wielomian rzeczywisty $f(z) \equiv a_0 z^m + \cdots + a_m$, $a_0 \neq 0$, *nie* posiada pierwiastka *zero*, a więc, że $a_m \neq 0$, to wielomian:

$$\varphi(z) \equiv a_m z^m + a_{m-1} z^{m-1} + \cdots + a_0$$
$$= z^m f\left(\frac{1}{z}\right) \text{ dla } z \neq 0$$

posiada pierwiastki dokładnie równe *odwrotnościom* pierwiastków wielomianu $f(z)$.

Odszukawszy górną granicę $a'\,(>0)$ dla *dodatnich* pierwiastków $\varphi(z)$ widzimy, że $\frac{1}{a'}\,(>0)$ będzie *dolną* granicą *dodatnią* pierwiastków *dodatnich* wielomianu $f(z)$. Analogicznie znajdziemy górną granicę *ujemną* pierwiastków *ujemnych* $f(z)$.

Przykład. Niechaj będzie:

$$f(z) \equiv 3z^5 + 2z^4 + z^3 - 4z^2 + z + 7.$$

Obliczamy: $\max\{4, 1, 7\} = 7$.

Granica górna pierwiastków dodatnich $f(z) =$

$$= 1 + \sqrt[3]{\frac{7}{3}} = 1 + \frac{1}{3}\sqrt[3]{63} = 2{\cdot}326\ldots < 2{\cdot}4.$$

Kładziemy: $\varphi(z) \equiv (-1)^5 f(-z) \equiv$

$$\equiv 3z^5 - 2z^4 + z^3 + 4z^2 + z - 7,$$

$$\max\{2, 1, 4, 1, 7\} = 7,$$

$$1 + \sqrt[1]{\frac{7}{3}} = 3{\cdot}33\ldots, = 3\tfrac{1}{3},$$

granica dolna pierwiastków ujemnych $f(z) =$

$$= -3{\cdot}33\ldots > -3{\cdot}4.$$

Kładziemy: $\psi(z) \equiv 7z^5 + z^4 - 4z^3 + z^2 + 2z + 3$

$$= \frac{1}{z^5} f\left(\frac{1}{z}\right) \text{ dla } z \neq 0.$$

$$\max\{4, 1, 2, 3\} = 4,$$

$$1 + \sqrt[2]{\frac{4}{7}} = 1 + \frac{1}{7}\sqrt{28};$$

granica dolna dodatnia pierwiastków dodatnich $f(z) =$

$$= \frac{1}{1 + \frac{1}{7}\sqrt{28}} = \frac{7}{7 + \sqrt{28}} =$$

$$= \frac{7(7 - \sqrt{28})}{21} = \frac{1}{3}(7 - \sqrt{28})$$

$$= 0{\cdot}569\ldots > 0{\cdot}5.$$

Kładziemy:

$$\chi(z) \equiv (-1)^5 \psi(-z) \equiv 7z^5 - z^4 - 4z^3 - z^2 + 2z - 3,$$

$$\max\{1, 4, 1, 2, 3\} = 4,\ 1 + \sqrt[1]{\frac{4}{7}} = \frac{11}{7},$$

granica górna ujemna pierwiastków ujemnych $f(z) =$

$$= -\frac{7}{11} = -0{\cdot}63\ldots < -0{\cdot}6.$$

A więc ostatecznie wielomian $f(z)$ posiada ewentualne pierwiastki *dodatnie* zawarte w przedziale $(0{\cdot}5,\ 2{\cdot}4)$, *ujemne* w przedziale $(-3{\cdot}4,\ -0{\cdot}6)$. Zero nie jest pierwiastkiem.

Metoda powyższa daje nam możność obliczania mniej lub więcej dobrych granic dla pierwiastków rzeczywistych wielomianu rzeczywistego. Wiele podobnych reguł podano dotychczas. Najbardziej znanemi są jeszcze reguły Newtona, Cauchy'ego i Laguerra, ale w tej kwestji odesłać musimy już czytelnika do obszerniejszych traktatów algebry.

2. Oddzielanie pierwiastków.

Zamknąwszy dodatnie i ujemne pierwiastki wielomianu niezerowego rzeczywistego w odnośnych przedziałach, chcielibyśmy obecnie podzielić te przedziały na drobniejsze podprzedziały tak, by w obrębie każdego z nich (wewnątrz lub na brzegu) znajdować się mógł conajwyżej jeden pierwiastek naszego wielomianu. Wielomian nasz posiada jedynie skończoną liczbę pierwiastków, zatem, oznaczywszy pełny ciąg *różnych* pierwiastków przez:

$$z_1, \ldots z_r$$

widzimy, że:

$$H = \min \{ |z_1 - z_2|, \ldots |z_1 - z_r|, |z_2 - z_3| \ldots |z_3 - z_r| \ldots |z_{r-1} - z_r| \}$$

jest liczbą *dodatnią*. Wystarczyłoby nam znać choć jedną liczbę $h < H$, by przedziały o długości h czyniły już zadość naszemu życzeniu. Zagadnieniem szukania takich liczb jak h zajmowali się nie bylejacy matematycy, bo Cauchy, Lagrange, Kronecker i inni. Atoli nie można powiedzieć, by reguły podane przez nich należały do najwygodniejszych. W rozdziale o rugowniku poznamy jedną z tych reguł, może jeszcze najlepszą w praktyce.

Zauważmy tymczasem, że gdy obierzemy dowolnie liczbę d dodatnią i rozważać będziemy przedziały domknięte:

$$[0, d],\ [d, 2d] \ldots [-d, 0],\ [-2d, -d] \ldots$$

to, o ile jednym z nich jest $[a, b]$ i $f(a) \cdot f(b) < 0$, wtedy wewnątrz $[a, b]$ leży *przynajmniej jeden* pierwiastek wielomianu rzeczywistego $f(z)$. W poszukiwaniu naszem należy się ograniczyć tylko

do takich $[a, b]$, które nie wykraczają poza przedziały dla pierwiastków dodatnich czy ujemnych, jakie można było uzyskać metodami poprzedniego ustępu. Jeżeli w ten sposób znajdziemy n takich przedziałów $[ab]$, gdzie leży choć jeden pierwiastek $f(z)$ i $sl' f = n$, to rozdzieliliśmy już wszystkie pierwiastki rzeczywiste. Skonstatowanie, że $f(a) = 0$ czy $f(b) = 0$ ułatwia nam tylko zadanie. Gdybyśmy nie doszli za pierwszym razem celu, to obierzmy $d' = \frac{d}{2}$ i powtórzmy nasze badanie jeszcze raz. Ostatecznie musimy dojść do liczby mniejszej niż H.

Jednakże wielomian rzeczywisty $f(z)$ stopnia n nie musi mieć n rzeczywistych pierwiastków. Badanie ilości pierwiastków w danym przedziale metodą Sturma będzie tu, wobec wielkiej ilości prób, zwykle zbyt uciążliwe. Znajomość H lub liczby mniejszej niż H byłaby nieodzowną. Przypuśćmy jednak, że $0 < d < H$ i że $[a, b]$ jest jednym z przedziałów:

$$[kd, (k+1)d], \quad k = 0, \pm 1, \pm 2, \ldots$$

Załóżmy też, że $f(a) \neq 0$ i $f(b) \neq 0$.

Możemy zawsze przypuścić, że $f(z)$ posiada jedynie pierwiastki rzędu *jeden*, gdyż umiemy zastąpić dany nam wielomian przez inny o takich samych pierwiastkach, lecz pojedynczych.

Jeżeli: $f(a) \cdot f(b) < 0$, to w (ab) leży jeden jedyny pierwiastek wielomianu $f(z)$.

Jeżeli: $f(a) \cdot f(b) > 0$, to może ich znajdować się jedynie *parzysta* ilość, lecz $d < H$, więc w $[ab]$ nie leży *żaden* pierwiastek dla $f(z)$.

W ten sposób dowiedzielibyśmy się nie tylko o rozmieszczeniu wszystkich pierwiastków rzeczywistych, w czem wypadek $f(a)=0$ lub $f(b)=0$ jeszczeby nam dopomógł, lecz także zbadalibyśmy ich ilość. Tę ostatnią możemy też oznaczyć przy pomocy metody Sturma.

Jeden z późniejszych rozdziałów poświęcimy zarysowi metod obliczania przybliżonego pierwiastków rzeczywistych, przyczem przybliżone z żądaną dokładnością wyrachowanie pierwiastka polega na zamknięciu go w przedziale, którego długość jest dostatecznie mała. Już tu należy jednak zwrócić uwagę, że sprawa to trudna i że poznawszy jedną czy dwie metody, nie nabędziemy jeszcze przez to możności praktycznego obliczania. Jest to zadaniem stosowanej matematyki wynaleźć odpowiednie metody techniki rachunkowej i zagadnieniem tem zajmują się dzieła specjalnie temu poświęcone.

Gdyby teraz wielomian niezerowy $f(z)$ nie był *rzeczywisty*, to moglibyśmy rozważyć wielomian:

$$F(z)=f(z)\,.\,\bar{f}(z),$$

gdzie $\bar{f}(z)$ jest sprzężonym do $f(z)$ [str. 121].

Otóż wielomian $F(z)$ jest *rzeczywisty*, przytem [str. 122] każdy pierwiastek $f(z)$ jest też pierwiastkiem dla $F(z)$, przeciwnie zaś, gdy $F(a)=0$, to $f(a)=0$ lub $f(\bar{a})=0$.

Możemy zatem badać tylko rzeczywiste pierwiastki wielomianu $F(z)$. Nie twierdzimy bynajmniej, że jest to najprostsza droga prowadząca do celu.

§ 8. Równania 2, 3 i 4 stopnia.

1. Równanie drugiego stopnia.

Rozważmy wielomian:

$$f(z) \equiv A z^2 + Bz + C, \quad A \neq 0, \quad A, B, C \varepsilon q_2$$

Równanie: $f(z) \overset{?}{=} 0$ posiada oczywiście te same pierwiastki, co równanie:

$$4A\, f(z) \overset{?}{=} 0.$$

Otóż:

$$\begin{aligned} 4Af(z) &\equiv 4A^2z^2 + 4ABz + 4AC \equiv \\ &\equiv (2Az + B)^2 - (B^2 - 4AC) \\ &\equiv (2Az + B - \sqrt{\Delta})(2Az + B + \sqrt{\Delta}), \end{aligned}$$

gdzie $\Delta \equiv B^2 - 4AC$, $\sqrt{\Delta}$ jest pierwiastkiem *głównym* [str. 116]. Stąd: pełny ciąg pierwiastków wielomianu $f(z)$ dany jest przez:

$$\frac{-B + \sqrt{\Delta}}{2A}, \quad \frac{-B - \sqrt{\Delta}}{2A}.$$

Mamy tu: 1. *dwa* pierwiastki, gdy $\Delta \neq 0$
2. *jeden* pierwiastek, gdy $\Delta = 0$.

2. Równanie trzeciego stopnia.

Rozważymy: $F(z) \equiv Az^3 + Bz^2 + Cz + D$,
$A \neq 0, \quad A, B, C, D \varepsilon q_2.$

Przez podstawienie: $y = z - m$ otrzymamy:

$$\begin{aligned} G(y) \equiv F(y + m) &\equiv A(y + m)^3 + B(y + m)^2 + \\ &C(y + m) + D \equiv \\ &\equiv Ay^3 + (3Am + B)y^2 + (3Am^2 + 2Bm + C)y \\ &+ Am^3 + Bm^2 + Cm + D, \end{aligned}$$

Jeżeli położymy: $m = -\frac{B}{3A}$, to $G(y)$ przybierze postać: $G(y) \equiv Ay^3 + C'y + D'$, zatem wystarcza zająć się wielomianem typu:

$$f(z) \equiv z^3 + pz + q, \quad p \text{ i } q \text{ zespolone.}$$

1. wypadek: $p \neq 0$, $q = 0$. Wtedy $f(z) \equiv z(z^2 + p)$. Pełny ciąg pierwiastków:

$$0, \sqrt{-p}, -\sqrt{-p} \quad \{\sqrt{-p} \text{ pierwiastek główny}\}.$$

Zatem: trzy pierwiastki.

2. wypadek: $p = 0$, $q \neq 0$. Wtedy $f(z) \equiv z^3 + q$. Pełny ciąg pierwiastków:

$$\sqrt[3]{-q}, \sqrt[3]{-q}\left(-\frac{1}{2} + \frac{i}{2}\sqrt{3}\right), \sqrt[3]{-q}\left(-\frac{1}{2} - \frac{i}{2}\sqrt{3}\right)$$

$$\left[\sqrt[3]{-q} \text{ główny, zresztą p. str. 111}\right].$$

Zatem: trzy pierwiastki.

3. wypadek: $p = 0$ i $q = 0$. Wtedy: $f(z) \equiv z^3$. Pełny ciąg pierwiastków: 0.

Zatem: jeden pierwiastek.

4. wypadek: $p \neq 0$ i $q \neq 0$,[1]

Przypuśćmy, że z jest pierwiastkiem i próbujmy przedstawić z jako sumę:

$$z = u + v \tag{1}$$

tak, by:

$$u^3 + v^3 + q = 0. \tag{2}$$

Wtedy byłoby:

$$(u + v)^3 + p(u + v) + q = 0 \text{ i } u^3 + v^3 + q = 0 \tag{3}$$

[1] Rozwiązany przez *Scipione del Ferro* w 1515, ogłoszony przez *Cardano* w 1545. Również *Tartaglia* podał rozwiązanie w r. 1535.

a więc: $(3uv+p)(u+v)=0$ i $u^3+v^3+q=0$ (4)
skąd: $3uv+p=0$ i $u^3+v^3+q=0$ lub
$u+v=0$ i $u^3+v^3+q=0$.

Druga możliwość odpada, bo wtedy $q=0$ wbrew założeniu. Zatem:

$$u^3+v^3+q=0 \text{ i } 3uv+p=0. \quad (5)$$

Ponieważ $p \neq 0$, więc byłoby:

$$u \neq 0, v \neq 0, v=-\frac{p}{3u} \text{ i } u^3+v^3+q=0. \quad (6)$$

Zatem: $$u^3-\frac{p^3}{27u^3}+q=0, \; v=-\frac{p}{3u}. \quad (7)$$

Stąd: $$u^6+qu^3-\frac{p^3}{27}=0, \quad v=-\frac{p}{3u}. \quad (8)$$

Temsamem:

$$u=\varepsilon\sqrt[3]{-\frac{q}{2}+\varepsilon'\sqrt{R}}, \quad v=-\frac{p}{3u} \quad (9)$$

gdzie: ε jest którymkolwiek trzecim pierwiastkiem jedności [str. 111], $\varepsilon'=\pm 1$,

$$R=\frac{q^2}{4}+\frac{p^3}{27}, \quad \sqrt[3]{-\frac{q}{2}+\varepsilon'\sqrt{R}}$$

podobnie jak i $\sqrt{R}$, jest pierwiastkiem głównym.

Aby wartości podyktowane przez (9) miały sens, potrzeba i wystarcza, by:

$$-\frac{q}{2}+\sqrt{R} \neq 0, \; -\frac{q}{2}-\sqrt{R} \neq 0,$$

czyli:

$$\left(-\frac{q}{2}+\sqrt{R}\right)\left(-\frac{q}{2}-\sqrt{R}\right)=\frac{q^2}{4}-R=-\frac{p^3}{27} \neq 0, \; p \neq 0,$$

co rzeczywiście ma miejsce.

Badamy, czy wartości (9) spełniają związki w (5).

Otóż: (1) $3uv + p = 0$ dzięki (9),

$$(2)\quad u^3 + v^3 + q = -\frac{q}{2} + \varepsilon'\sqrt{R} - \frac{p^3}{27\left(-\frac{q}{2} + \varepsilon'\sqrt{R}\right)} + q =$$

$$= \frac{1}{-\frac{q}{2} + \varepsilon'\sqrt{R}}\left[\frac{q^2}{4} + R - q\varepsilon'\sqrt{R} - \frac{p^3}{27} - \frac{q^2}{2} + q\varepsilon'\sqrt{R}\right] =$$

$$= \frac{1}{-\frac{q}{2} + \varepsilon'\sqrt{R}}\left[\frac{q^2}{4} + R - \frac{p^3}{27} - \frac{q^2}{2}\right] = 0.$$

Stąd już widzimy, że związki (4) i (3) są spełnione, zatem $u + v$, podyktowane przez (9) spełnia równanie: $z^3 + pz + q = 0$.

Atoli:

$$v = -\frac{p}{3\varepsilon\sqrt[3]{-\frac{q}{2} + \varepsilon'\sqrt{R}}} = \frac{-p\varepsilon\sqrt[3]{-\frac{q}{2} - \varepsilon'\sqrt{R}}}{3\varepsilon^2\sqrt[3]{+\frac{q^2}{4} - R}} =$$

$$= \varepsilon^2\sqrt[3]{-\frac{q}{2} - \varepsilon'\sqrt{R}},$$

zatem mamy pełny ciąg pierwiastków dla $f(z)$:

$$\varepsilon\left(\sqrt[3]{-\frac{q}{2} + \sqrt{R}} + \varepsilon\sqrt[3]{-\frac{q}{2} - \sqrt{R}}\right), \text{ gdzie:}$$

$$\varepsilon = 1,\ -\frac{1}{2} + \frac{i}{2}\sqrt{3},\ -\frac{1}{2} - \frac{i}{2}\sqrt{3}.$$

[Formuły Cardana].

Badając, przy pomocy łańcuchowego dzielenia $f(z)$ i $f'(z)$, wyrachujemy, że f i f' są pierwsze względem siebie lub nie zależnie od tego czy $R \neq 0$ czy $R = 0$. Trzykrotny pierwiastek wystąpi zatem

wtedy i tylko wtedy, gdy $R=0$ i $f''(z)=0$, a więc gdy $z=0$ jest pierwiastkiem i $R=0$, co pociąga, że $q=0$ i $R=\frac{q^2}{4}+\frac{p^3}{27}=0$, więc $p=q=0$.

Mamy zatem wypadki:

1.	$R\neq 0$	3 pierwiastki.
2.	$R=0,\ q\neq 0$	2 pierwiastki.
3.	$R=0,\ q=0$ (więc i $p=0$)	1 pierwiastek.

3. **Równanie 3go stopnia** rzeczywiste.

Gdy teraz założymy, że w $f(z)=z^3+pz+q$ liczby p i q są rzeczywiste, to gdy:

(1) $R\neq 0$, mamy 3 pierwiastki różne, wiec *jeden* rzeczywisty i *dwa* zespolone sprzężone lub wszystkie *trzy* rzeczywiste [str. 123]; gdy:

(2) $R=0,\ q\neq 0$, mamy dwa pierwiastki rzeczywiste (jeden pojedynczy i jeden podwójny); gdy:

(3) $R=0,\ p=0,\ q=0$, mamy jeden pierwiastek rzeczywisty *zero* (potrójny).

Musimy jeszcze zbadać wypadek (1) nieco dokładniej.

(α) Gdy $p=0$ i $R\neq 0$, to $R=\frac{q^2}{4}>0$ i mamy, wedle ustępu poprzedniego, *jeden* pierwiastek rzeczywisty.

(β) Gdy $p\neq 0$ i $R\neq 0$, to zbadamy pochodną:

$$f'(z)=3z^2+p.$$

(β_1) Gdy $p>0$, to $R>0$, $f'(z)>0$ dla wszelkich z rzeczywistych, zatem $f(z)$ stale rosnąca, więc posiada *jeden* pierwiastek rzeczywisty.

(β_2) Gdy $p<0$, to $f'(z)=0$ dla $+\sqrt{-\frac{p}{3}}$

i $-\sqrt{-\frac{p}{3}}$, przyczem $-\sqrt{-\frac{p}{3}} < +\sqrt{-\frac{p}{3}}$, $f(z)$ rośnie dla $z \leqq -\sqrt{-\frac{p}{3}}$, maleje dla $-\sqrt{-\frac{p}{3}} \leqq z \leqq \sqrt{-\frac{p}{3}}$ i znowu rośnie dla $z \geqq +\sqrt{-\frac{p}{3}}$. Wielomian $f(z)$ posiada zatem dla $z = -\sqrt{\frac{-p}{3}}$ maximum, a dla $z = +\sqrt{\frac{-p}{3}}$ minimum. Otóż:

$$f\left(\pm\sqrt{\frac{-p}{3}}\right) = q \pm \frac{2p}{3}\sqrt{\frac{-p}{3}},$$

$$R = \left(\frac{q}{2} + \frac{p}{3}\sqrt{\frac{-p}{3}}\right)\left(\frac{q}{2} - \frac{p}{3}\sqrt{\frac{-p}{3}}\right).$$

Zatem: gdy $R>0$, to $f\left(-\sqrt{\frac{-p}{3}}\right)<0$ i $f\left(+\sqrt{\frac{-p}{3}}\right)<0$ lub $f\left(-\sqrt{\frac{-p}{3}}\right)>0$ i $f\left(+\sqrt{\frac{-p}{3}}\right)>0$, więc $f(z)$ posiada *jeden* pierwiastek rzeczywisty, gdyż $\lim_{z|-\infty} f(z) = -\infty$, $\lim_{z|+\infty} f(z) = +\infty$;

gdy: $R<0$, to $0 \leqq |q| < -\frac{2p}{3}\sqrt{\frac{-p}{3}}$,

$q + \frac{2p}{3}\sqrt{\frac{-p}{3}} < 0$, $q - \frac{2p}{3}\sqrt{\frac{-p}{3}} > 0$, zatem $f\left(-\sqrt{\frac{-p}{3}}\right)>0$, $f\left(+\sqrt{\frac{-p}{3}}\right)<0$, więc $f(z)$

przechodzi od $-\infty$ do $f\left(-\sqrt{\frac{-p}{3}}\right)>0$, stąd do $f\left(+\sqrt{\frac{-p}{3}}\right)<0$ i znowu do $+\infty$, tem samem posiada *trzy* pierwiastki rzeczywiste.

Ostatecznie: $R>0$ 1 pierwiastek rzeczywisty.
$R<0$ 3 pierwiastki rzeczywiste.

Wypadek $R<0$ nazywają starzy algebraicy „*casus irreducibilis*“ z tego powodu, że formuły Cardana dają nam pierwiastki rzeczywiste w postaci:

$$\varepsilon\left[\sqrt[3]{-\frac{q}{2}+\sqrt{R}}+\varepsilon\sqrt[3]{-\frac{q}{2}-\sqrt{R}}\right]$$

pozornie zespolonej, jednakże udowodniono, iż żadna skończona ilość operacyj algebraicznych nie zdoła nadać tym wzorom postaci efektywnie rzeczywistej.

4. Równanie stopnia czwartego.

Rozważmy wielomian:

$$F(z)\equiv Az^4+Bz^3+Cz^2+Dz+E,$$
$$A\neq 0,\ A, B, C, D, E\,\varepsilon\, q_2.$$

Przez podstawienie analogiczne jak ust. 1:

$$z=y-\frac{B}{4A}$$

otrzymamy wielomian $G(y)\equiv F\left(y-\frac{B}{4A}\right)$ kształtu:

$$Ay^4+C'y^2+D'y+E'.$$

Wystarcza zatem badać wielomian typu:

$$f(z)\equiv z^4+pz^2+qz+r,\quad p, q, r\,\varepsilon\, q_2.$$

Oznaczmy przez: z_1, z_2, z_3, z_4 pełny ciąg jego pierwiastków. Wzory (s), rozważane na str. 119, powiedzą nam, że:

$$z_1 + z_2 + z_3 + z_4 = 0.$$

Połóżmy: $a = z_1 + z_2 = -(z_3 + z_4)$,

$$b = z_1 z_2, \quad c = z_3 z_4,$$

to: $f(z) \equiv (z - z_1)(z - z_2)(z - z_3)(z - z_4) \equiv$

$$\equiv (z^2 - az + b) \cdot (z^2 + az + c); \qquad (1)$$

a równanie: $f(z) \overset{?}{=} 0$ jest równoważne alternatywom:

$$z^2 - az + b \overset{?}{=} 0 \ \textit{lub} \ z^2 + az + c \overset{?}{=} 0.$$

Widzimy, że byleby można było odszukać a, b i c, to rozwiązanie równania 4^{go} stopnia sprowadzimy do rozwiązania dwu równań 2^{go} stopnia.

Porównując spółczynniki obu stron (1) po wymnożeniu i zredukowaniu, otrzymamy układ związków:

$$bc = r, \ ab - ac = q, \ b + c - a^2 = p. \qquad (2)$$

Gdy: $q = 0$, to $f(z) \equiv z^4 + pz^2 + r$,

zatem przez podstawienie $z^2 = w$ trudność sprowadza się do rozwiązania równania:

$$w^2 + pw + r \overset{?}{=} 0.$$

Załóżmy zatem, że $q \neq 0$. Wtedy $a \neq 0$, gdyż $a(b - c) = q$.

W tym wypadku otrzymamy z (2)

$$b + c = a^2 + p$$

$$b - c = \frac{q}{a}. \qquad (3)$$

Stąd:
$$b = \frac{1}{2}\left\{a^2 + p + \frac{q}{a}\right\}$$
$$c = \frac{1}{2}\left\{a^2 + p - \frac{q}{a}\right\}. \qquad (4)$$

Podstawienie w $bc = r$ da nam:
$$(a^2 + p)^2 - \frac{q^2}{a^2} = 4r. \qquad (5)$$

Kładąc $s = a^2$ otrzymamy:
$$s(s + p)^2 - q^2 - 4rs = 0. \qquad (6)$$

Jest to równanie stopnia 3^{go}, rozwiązane poprzednio. Wyznaczymy stąd s, a tem samem a i następnie ze związków (4) otrzymamy wprost już b i c.

Ze względu na dość małe *praktyczne* znaczenie tego rozwiązania, pomijamy dyskusję szczegółową.

Równanie 4^{go} stopnia rozwiązał pierwszy Ferrari, uczeń Cardana.[1]

3. **Algebraiczne** rozwiązywanie równań.

Równania aż do stopnia czwartego włącznie nauczyliśmy się rozwiązywać *algebraicznie*. Rozumiemy przez to, że w każdym z tych wypadków udało się nam wyrazić pierwiastki równania przy pomocy skończonej ilości działań: *dodawania, odejmowania; mnożenia, dzielenia i pierwiastkowania*, zastosowanych do spółczynników równania i liczb zespolonych stałych. Możność ta kończy się atoli od stopnia *piątego* począwszy. Dla równania stopnia piątego udowodnił to *Niels Abel*, a wogóle dla rów-

[1] H. Cardano ogłosił ten wynik w „Artis magnae seu de regulis algebraicis liber unus“ [Norymberga 1545].

nań stopnia $n > 4$, *Évariste Galois*. Nie znaczy to wcale, aby przy pomocy *innych* niż wymienione działań, nie dało się to uskutecznić. Tak naprzykład Ch. Hermite rozwiązał ogólne równanie stopnia piątego przy pomocy funkcyj eliptycznych w r. 1859. W dalszych rozdziałach tej książeczki poznamy metodę rozwiązywania równania stopnia 3^{go} względnie 4^{go} przy pomocy formuł gonjometrycznych, co praktycznie jedynie prowadzi do celu.

Metoda rozwiązywania algebraicznego nie jest, jak widać, jedyną w wypadku równań algebraicznych, nawet stopni niższych niż piąty. Fakt niemożności algebraicznego rozwiązania równań ogólnych stopnia wyższego niż 4 posiada atoli wielkie znaczenie w dziejach algebry, gdyż spowodował stworzenie tak zwanej teorji Galois, a wraz z nią nowoczesnej algebry grup, ciał i liczb algebraicznych.

Rozdział V.

Rugownik i Wyróżnik.

§ 1. Rugownik wielomianów jednej zmiennej.

1. Określenie i główne własności.

Rozważmy dwa wielomiany *niezerowe* o stopniach *dodatnich:*

$$f(z) \equiv a_0 z^m + \cdots + a_m,\ a_0 \neq 0,\ m > 0,$$
$$g(z) \equiv b_0 z^n + \cdots + b_n,\ b_0 \neq 0,\ n > 0.$$

Niechaj pełnemi ciągami pierwiastków będą:

$$u_1 \cdots u_m \quad \text{dla } f(z),$$
$$v_1 \cdots v_n \quad \text{dla } g(z).$$

Warunek konieczny i dostateczny, by $f(z)$ i $g(z)$ posiadały choć jeden pierwiastek wspólny, brzmi oczywiście:

$$g(u_1)\dots g(u_m)=0$$

lub: $$f(v_1)\dots f(v_n)=0.$$

Otóż: $$f(z)\equiv a_0(z-u_1)\dots(z-u_m)$$
$$g(z)\equiv b_0(z-v_1)\dots(z-v_n),$$

więc: $$g(u_1)\dots g(u_m)=b_0^m\prod_{i|1}^{m}\prod_{k|1}^{n}(u_i-v_k),$$

$$f(v_1)\dots f(v_n)=a_0^n\prod_{k|1}^{n}\prod_{i|1}^{m}(v_k-u_i).$$

Df. Wprowadzamy ze względów na symetrję wyrażenie:

$$R(f,g)=a_0^n\,b_0^m\prod_{i|1}^{m}\prod_{k|1}^{n}(u_i-v_k)$$

i nazwiemy *rugownikiem* wielomianów *niezerowych*, o stopniach *dodatnich*, $f(z)$ i $g(z)$.

Widzimy wtedy, że:

$$a_0^n g(u_1)\dots g(u_m)=R(f,g),$$
$$b_0^m f(v_1)\dots f(v_n)=R(g,f)=(-1)^{m\,n}R(f,g).$$

Mamy już zatem twierdzenia:

Tw. Warunkiem koniecznym i dostatecznym, by wielomiany $f(z)$ i $g(z)$, gdzie $st'f>0$, $st'g>0$, posiadały choć jeden wspólny pierwiastek, jest:

$$R(f,g)=0.$$

Tw. Gdy $m=st'f(z)>0$, $n=st'g(z)>0$, to:

$$R(f,g)=(-1)^{m\,n}R(g,f).$$

[Twierdzenie o odwróceniu].

Udowodnimy kilka dalszych twierdzeń.

Tw. Gdy $sł' f(z) > 0$, $sł' g(z) > 0$, $sł' h(z) > 0$, to: $$R(f.g, h) = R(f, h).R(g, h).$$

[Twierdzenie o iloczynie].

Dem. Niech będzie c_0 najwyższym spółczynnikiem[1] dla $h(z)$, ciąg: $\alpha_1 \ldots \alpha_p$ niech przedstawia pełny ciąg pierwiastków dla $h(z)$. Wtedy:

$$\begin{cases} R(f, h) = (-1)^{mp} c_0^m f(\alpha_1) \ldots f(\alpha_p), \\ R(g, h) = (-1)^{np} c_0^n g(\alpha_1) \ldots g(\alpha_p), \\ R(fg, h) = (-1)^{(m+n)p} c_0^{m+n} f(\alpha_1) g(\alpha_1) \ldots f(\alpha_p) g(\alpha_p), \end{cases}$$

co dowodzi twierdzenia.

Tw. Gdy $m = sł' f > 0$, $p = sł' g > 0$, $sł' h + sł' g < sł' f$, to:

$$R(f + h.g, g) = R(f, g).$$

[Twierdzenie o redukcji].

Dem. Niech będzie: b_0 najwyższym spółczynnikiem oraz $\alpha_1 \ldots \alpha_p$ pełnym ciągiem pierwiastków $g(z)$. Wtedy: $sł'(f + h.g) = m$,

$$R(f + h.g, g) = (-1)^{mn} b_0^m \prod_{i|1}^{p} [f(\alpha_i) + h(\alpha_i) g(\alpha_i)] =$$

$$= (-1)^{mn} b_0^m \prod_{i|1}^{p} f(\alpha_i) = R(f, g), \quad \text{gdyż} \quad g(\alpha_i) = 0,$$

$$i = 1, 2 \ldots p.$$

Cor. Twierdzenie słuszne jeszcze dla wypadku: $sł' h + sł' g = sł' f$, gdy tylko $sł'(f + hg) = m$,

a więc gdy $a_0 + b_0 c_0 \neq 0$, gdzie c_0 jest najwyższym spółczynnikiem w $h(z)$.

---

[1] tak nazwiemy krótko spółczynnik najwyższej potęgi postaci zredukowanej wielomianu.

Tw. Gdy $m = st'f > 0$, $n = st'g > 0$, $A \varepsilon q_2$, $A \neq 0$, to:

$$R(Af, g) = A^n R(f, g),$$
$$R(f, Ag) = A^m R(f, g).$$

[Twierdzenie o wyłączaniu stałej].

Dem. Gdy $\alpha_1 \ldots \alpha_m$ jest pełnym ciągiem pierwiastków dla $f(z)$, a_0 najwyższym spółczynnikiem $f(z)$, to:

$$R(Af, g) = A^n \cdot a^n g(\alpha_1) \ldots g(\alpha_m) =$$
$$= A^n R(f, g).$$

Analogicznie obliczymy $R(f, Ag)$.

2. Rugownik jako wyznacznik.

Spółczynniki postaci zredukowanej wielomianu wyznaczają jego pierwiastki, tem samem podanie spółczynników wielomianów $f(z)$ i $g(z)$ powinno dać już możność rozstrzygnięcia, czy $f(z)$ i $g(z)$ posiadają wspólne pierwiastki czy nie. Nasuwa to podejrzenie, że rugownik $R(f, g)$ da się wyrazić algebraicznie przy pomocy samych tylko spółczynników $f(z)$ i $g(z)$. Zobaczymy teraz, że tak jest rzeczywiście.

Rozważamy najpierw wielomiany:

$$f(z) \equiv z - k, \; g(z) \equiv b_0 z^n + \cdots + b_n,$$
$$b_0 \neq 0, \; n > 0, \; k \varepsilon q_2 \ldots$$

oraz wyznacznik stopnia $n + 1 = st'g + st'f$

$$\Delta = \begin{vmatrix} 1, & -k, & 0 \ldots 0 \\ 0, & 1, & -k, \ldots 0 \\ \cdots & \cdots & \cdots \\ 0, & 0, & \ldots 1, -k \\ b_0, & b_1, & \ldots b_{n-1}, b_n \end{vmatrix}.$$

Przekształcajmy go w następujący sposób:

(1) Pierwszą kolumnę, pomnożoną przez k dodajmy do drugiej.

(2) W otrzymanym wyznaczniku, drugą kolumnę, pomnożoną przez k dodajmy do trzeciej.

. . . . . .

(n) W otrzymanym wyznaczniku n-tą kolumnę, pomnożoną przez k dodajmy do $(n+1)$-ej. Otrzymamy wtedy:

$$\Delta = \begin{vmatrix} 1, 0, \ldots\ldots 0 \\ 0, 1, \ldots\ldots 0 \\ \ldots\ldots\ldots\ldots \\ 0, 0, \ldots\ldots, 1, 0 \\ b_0, b_1 + k b_0, \ldots, g(k) \end{vmatrix} = g(k) = R(z - k, g).$$

Jeżeli teraz: $f(z) \equiv a_0 z + a_1$, $g(z) \equiv b_0 z^n + \cdots + b_n$, $a_0 \neq 0$, $b_0 \neq 0$, $n > 0$,

to:

$$R(f,g) = a_0^n R\left(z + \frac{a_1}{a_0}, g\right) = a_0^n \begin{vmatrix} 1, \frac{a_1}{a_0}, 0 \ldots\ldots 0 \\ \ldots\ldots\ldots\ldots \\ 0, 0, 0 \ldots 1, \frac{a_1}{a_0} \\ b_0, b_1, b_2 \ldots b_{n-1}, b_n \end{vmatrix}$$

$$= \begin{vmatrix} a_0, a_1, 0 \ldots\ldots 0 \\ 0, a_0, a_1, \ldots\ldots 0 \\ \ldots\ldots\ldots\ldots \\ 0, 0, 0 \ldots a_0, a_1 \\ b_0, b_1, b_2, \ldots b_{n-1}, b_n \end{vmatrix}.$$

Twierdzimy, że ogólnie:

Tw.

Jeżeli $st' f > 0$, $st' g > 0$, $f(z) \equiv a_0 z^m + \cdots + a_m$, $g(z) \equiv b_0 z^n + \cdots + b_n$, $a_0 \neq 0$, $b_0 \neq 0$, to:

$$R(f,g)=\begin{vmatrix} a_0, a_1, \ldots a_m, 0, \ldots 0 \\ 0, a_0, a_1 \ldots a_m, 0 \ldots 0 \\ \vdots \\ 0, 0, \ldots a_0, a_1 \ldots a_m \\ b_0, b_1, \ldots b_n, 0 \ldots 0 \\ 0, b_0, \ldots b_n, 0 \ldots 0 \\ \vdots \\ 0, 0 \ldots b_0, b_1, \ldots b_n \end{vmatrix},$$

przyczem wyznacznik jest stopnia $n+m$.

Dem. 1. Gdy $st'f=1$, to twierdzenie słuszne, jak to wykazuje przeprowadzone powyżej badanie.

2. Przypuśćmy, że twierdzenie słuszne dla danego całkowitego i dodatniego m; okażemy jego słuszność jeszcze dla $m+1$.

Tworzymy wyznacznik stopnia $n+m+1$:

$$\Delta=\begin{vmatrix} a_0', a_1' \ldots a'_{m+1}, 0 \ldots 0 \\ \vdots \\ 0, 0, \ldots a_0', a_1' \ldots a'_{m+1} \\ b_0, b_1 \ldots b_n, 0 \ldots 0 \\ \vdots \\ 0, 0 \ldots b_0, b_1, \ldots b_n \end{vmatrix},$$

gdzie: $F(z)\equiv a_0' z^{m+1}+\cdots+a'_{m+1}\equiv f(z)(z-k)\equiv$
$\equiv(z-k)(a_0 z^m+\cdots+a_m)$.

Mamy tu związki:

$a_0'=a_0,\ a_1'=a_1-ka_0,\ a_2'=a_2-ka_1,\ldots$
$\ldots a_m'=a_m-ka_{m-1},\ a'_{m+1}=-ka_m;$

więc: $a_0k+a_1'=a_1,\ a_1k+a_2'=a_2,\ldots$
$\ldots a_{m-1}k+a_m'=a_m,\ a_mk+a'_{m+1}=0.$

Aby zaoszczędzić miejsca, opisujemy słowami przekształcenia, które przeprowadzimy na Δ.

(1) Pierwszą kolumnę w Δ, pomnożoną przez k dodajemy do drugiej.

(2) W otrzymanym wyznaczniku drugą kolumnę, pomnożoną przez k dodajemy do trzeciej.

$(n+m)$ W otrzymanym wyznaczniku $n+m$-tą kolumnę, pomnożoną przez k dodajemy do $(n+m+1)$-ej.

Otrzymamy w ten sposób:

$$\Delta = \begin{vmatrix} a_0, a_1, \ldots a_m, 0 \ldots\ldots 0 \\ 0, 0, \ldots a_0, a_1, \ldots a_m, 0 \\ b_0, b_1+kb_0, \ldots g(k), \ldots 0 \\ 0, 0, \ldots b_0, b_1+kb_0, \ldots g(k) \end{vmatrix} \begin{matrix} \} (n) \\ \\ \} (m+1) \end{matrix}$$

A teraz:

$(n+2)$ — wiersz, pomnożony przez k odejmujemy od $(n+1)$-go.

W otrzymanym wyznaczniku;

$(n+3)$ — wiersz, pomnożony przez k odejmu-
[jemy od $(n+2)$-go.

W otrzymanym wyznaczniku:

$(n+m+1)$ — wiersz, pomnożony przez k odejmujemy od $(n+m)$-go.

Ostatecznie dostajemy:

$$\Delta = \begin{vmatrix} a_0, a_1, \ldots\ldots a_m, 0 \ldots\ldots 0 \\ \vdots \\ 0, 0, \ldots a_0, a_1 \ldots\ldots a_m 0 \\ b_0, b_1, \ldots\ldots b_n, 0 \ldots\ldots 0 \\ \vdots \\ 0 \ldots b_0, b_1 \ldots\ldots\ldots b_n 0 \\ 0, 0, \ldots b_0, b_1+kb_0, \ldots g(k) \end{vmatrix} \begin{matrix} \} (n) \\ \\ \} (m+1) \end{matrix} =$$

$$= g(k) \cdot \begin{vmatrix} a_0, a_1, \ldots\ldots a_m, 0 \ldots 0 \\ \vdots \\ 0\ , 0\ , \ldots a_0\ , a_1, \ldots a_m \\ b_0, b_1 \ldots\ldots\ldots b_n, \ldots 0 \\ \vdots \\ 0\ , 0\ , \ldots b_0, b_1 \ldots\ldots b_n \end{vmatrix} \begin{matrix} \\ \\ \}(n) \\ \\ \\ \}(m) \end{matrix} = g(k) \cdot R(f, g).$$

Stąd:

$$\Delta = g(k) \cdot R(f, g) = R(z - k,\ g) \cdot R(f, g) =$$
$$= R[(z - k) \cdot f,\ g] = R(F, g).$$

Zatem twierdzenie słuszne jeszcze dla $m + 1$.

3. Dzięki zasadzie indukcji matematycznej twierdzenie będzie słuszne dla każdego n i m naturalnego.

Przykład.

$$f(z) \equiv Az^2 + Bz + C,\ g(z) \equiv az^2 + bz + c,$$
$$A \neq 0,\ a \neq 0.$$

$$R(f, g) = \begin{vmatrix} A, B, C, 0 \\ 0\ , A, B, C \\ a\ , b\ , c\ , 0 \\ 0\ , a\ , b\ , c \end{vmatrix} = \frac{1}{Aa} \begin{vmatrix} 1, \frac{B}{A}, \frac{C}{A}, 0 \\ 0, A, B, C \\ 1, \frac{b}{a}, \frac{c}{a}, 0 \\ 0, a, b, c \end{vmatrix} =$$

$$= \frac{1}{Aa} \begin{vmatrix} 1, & \frac{B}{A}, & \frac{C}{A}, & 0 \\ 0, & A, & B, & C \\ 0, & \frac{b}{a} - \frac{B}{A}, & \frac{c}{a} - \frac{C}{A}, & 0 \\ 0, & a, & b, & c \end{vmatrix} = \frac{1}{Aa} \begin{vmatrix} A, & B, & C \\ \frac{b}{a} - \frac{B}{A}, & \frac{c}{a} - \frac{C}{A}, & 0 \\ a, & b, & c \end{vmatrix} =$$

$$= \begin{vmatrix} A, & B, & C \\ Ab - aB, & Ac - aC, & 0 \\ a, & b, & c \end{vmatrix} =$$

$$= ACb^2 - BCab + C^2a^2 - 2ACac + A^2c^2 + B^2ac - ABbc$$

$$= (Ac - Ca)^2 - (Ab - Ba)(Bc - Cb) =$$

$$= \begin{vmatrix} Ac - Ca , & Ab - Ba \\ Bc - Cb , & Ac - Ca \end{vmatrix}.$$

Znikanie tego wyrażenia jest warunkiem koniecznym i dostatecznym, by wielomiany $f(z)$ i $g(z)$ stopnia drugiego posiadały choć jeden wspólny pierwiastek.

Rozważając rugownik $R(f, g)$ jako funkcję spółczynników postaci zredukowanej wielomianów $f(z) \equiv a_0 z^m + \cdots + a_m$, $g(z) \equiv b_0 z^n + \cdots + b_n$ widzimy, że:

Tw. Rugownik wielomianów stopni dodatnich jest *wielomianem* spółczynników postaci zredukowanej obu wielomianów.

Dem. Wynika to stąd, że wyznacznik jest wielomianem swych elementów.

Tw. Rugownik wielomianów $f(z)$ i $g(z)$ stopni dodatnich m i n jest wielomianem jednorodnym rzędu n spółczynników wielomianu $f(z)$, a rzędu m spółczynników wielomianu $g(z)$ [spółczynniki postaci zredukowanej].

Dem.

Gdy $f(z) \equiv a_0 z^m + \cdots + a_m$, $g(z) \equiv b_0 z^n + \cdots + b_n$, $a_0 \neq 0$, $b_0 \neq 0$, $m > 0$, $n > 0$ i napiszemy rugownik jako:

$$R(f, g) \equiv F(a_0, \ldots a_m, b_0, \ldots b_n),$$

to związki:

$$R(\lambda f, g) = \lambda^n R(f, g) \text{ i } R(f, \lambda g) = \lambda^m R(f, g)$$

powiedzą nam, że:

$$F(\lambda a_0, \ldots \lambda a_m; b_0, \ldots b_n) \equiv \lambda^n F(a_0 \ldots a_m, b_0 \ldots b_n),$$
$$F(a_0 \ldots a_m; \lambda b_0 \ldots \lambda b_n) \equiv \lambda^m F(a_0 \ldots a_m, b_0 \ldots b_n),$$

co wedle twierdzenia na [str. 64] dowodzi słuszności naszej tezy.

Uw. Mamy jeszcze:

$$R(\lambda f, \lambda g) \equiv \lambda^{m+n} R(f, g),$$

więc rugownik jest wielomianem jednorodnym rzędu $m + n$ *wszystkich* spółczynników.

§2. Wyróżnik wielomianu jednej zmiennej.

Wiemy już [str. 98], że warunkiem koniecznym i dostatecznym, by wielomian:

$$f(z) \equiv a_0 z^m + \cdots + a_m, \quad a_0 \neq 0, \quad m > 1,$$

posiadał choć jeden pierwiastek wielokrotny jest: $[f(z), f'(z)] \not\equiv 1$, a więc, by $f(z)$ i $f'(z)$ posiadały choć jeden pierwiastek wspólny, tem samem by:

$$R(f, f') = 0.$$

Df. *Wyróżnikiem* wielomianu $f(z) \equiv a_0 z^m + \cdots + a_m$, $a_0 \neq 0$, $m > 1$, nazwiemy wyrażenie:

$$D(f) = \frac{1}{a_0} R(f, f').$$

Uw. Czynniki $\frac{1}{a_0}$, nie mające żadnego wpływu na zerowanie się $D(f)$ wprowadziliśmy celem uzyskania lepszej symetrji wzorów. U niektórych autorów mamy jeszcze czynnik: $(-1)^{\frac{m(m-1)}{2}}$.

Tw. Warunkiem koniecznym i dostatecznym, by wielomian $f(z)$ stopnia >1 posiadał choć jeden pierwiastek wielokrotny, jest: $D(f)=0$.

Przykłady: 1. $f(z)\equiv Az^2+Bz+C$, $A\neq 0$,

Mamy tu: $f'(z)\equiv 2Az+B$.

$$D(f)=\frac{1}{A}\cdot\begin{vmatrix} A, & B, & C \\ 2A, & B, & 0 \\ 0, & 2A, & B \end{vmatrix}=4AC-B^2$$

$D(f)=0$ równoważne zatem: $B^2-4AC=0$.

2. $f(z)\equiv z^3+pz+q$, $f'(z)=3z^2+p$.

$$D(f)=\begin{vmatrix} 1, & 0, & p, & q, & 0 \\ 0, & 1, & 0, & p, & q \\ 3, & 0, & p, & 0, & 0 \\ 0, & 3, & 0, & p, & 0 \\ 0, & 0, & 3, & 0, & p \end{vmatrix}=4p^3+27q^2$$

$D(f)=0$ równoważne zatem:

$$\frac{p^3}{27}+\frac{q^2}{4}=0. \qquad \text{[p. str. 156].}$$

Tw. Jeżeli $z_1 \ldots z_m$ jest pełnym ciągiem pierwiastków $f(z)\equiv a_0 z^m+\cdots+a_m$, $a_0\neq 0$ i $stf>1$,

to: $D(f)=(-1)^{\frac{m(m-1)}{2}}\cdot a_0^{2m-2}\prod_{i=1}^{m-1}\prod_{k=i+1}^{m}(z_i-z_k)^2$.

Dem. Wystarczy zastosować formułę na str. 164. do naszego wypadku i przypomnieć sobie, że:

$$f'(z_s)=a_0(z_s-z_1)\ldots(z_s-z_{s-1})(z_s-z_{s+1})\ldots(z_s-z_m),$$

$$s=1,2\ldots m.$$

co otrzymamy rozkładając $f(z)$ na czynniki linjowe, różniczkując i podstawiając $z = z_s$, $s = 1, 2 \ldots m$.

Tw. Gdy $f(z) \equiv a_0 z^m + \cdots + a_m$, $g(z) \equiv b_0 z^n + \cdots + b_n$, $a_0 \neq 0$, $b_0 \neq 0$, $m > 1$, $n > 1$, to:

$$D(f.g) = (-1)^{mn} . D(f) . D(g) . R(f,g)^2.$$

Dem. $D(f.g) = \frac{1}{a_0 b_0} R(f.g, f'g + g'f) =$

$$= \frac{1}{a_0 b_0} R(f, f'g + g'f) . R(g, f'g + g'f)$$

$$= \frac{1}{a_0 b_0} R(f, f'g) . R(g, g'f) =$$

$$= \frac{1}{a_0 b_0} R(f, f') . R(g, g') . R(f, g) . R(g, f) =$$

$$= D(f) . D(g) . (-1)^{mn} R(f, g)^2.$$

Zastosowano tu *Corr.* do twierdzenia o *redukcji*, gdyż najwyższy spółczynnik w $f'g + g'f$ wynosi:

$$(n + m)\, a_0 b_0 \neq 0, \quad st'(f'g + g'f) = st'(f'g) =$$
$$= st'(g'f) = m + n - 1.$$

§ 3. Równanie różnic pierwiastków.

Rozważmy wielomian $f(z) \equiv a_0 z^m + \cdots + a_m$, $a_0 \neq 0$, $m > 1$. Aby zachodziły *jednocześnie* $f(z) = 0$ i $f(z + u) = 0$, potrzeba i wystarcza, by z i $z + u$ były pierwiastkami, a więc by: z było pierwiastkiem i u *różnicą pierwiastków wielomianu* $f(z)$.

Otóż:

$$f(z+u)-f(z)\equiv u f'(z)+\frac{u^2}{2!}f''(z)+\cdots+$$

$$+\frac{u^m}{m!}f^{(m)}(z)\equiv u\,.\,M(z,u),$$

gdzie $M(z,u)$ jest wielomianem zmiennych z i u.

1° Jeżeli z_0 jest pierwiastkiem $f(z)$ i u_0 jest *różnicą różnych* pierwiastków $f(z)$, a więc:

$$u_0\neq 0,\ \text{to:}\ M(z_0,u_0)=0.$$

Naodwrót: gdy z_0 jest pierwiastkiem $f(z)$ i $u\neq 0$ oraz $M(z_0,u_0)=0$, to $f(z_0)=0$ i $f(z_0+u_0)=0$, a więc u_0 jest *różnicą różnych* pierwiastków wielomianu $f(z)$.

2° Dla żadnej wartości stałej $u_0\neq 0$ wielomian $M(\hat{z},u_0)$ nie jest *identycznie* zerem. Pociągnęło by to bowiem za sobą, że $f(z+u_0)-f(z)\equiv 0$.

Otóż: $f(u_0+z)-f(z)\equiv f(u_0)+f'(u_0)z+\cdots+$

$$+\frac{f^{(m)}(u_0)}{m!}z^m-f(z)\equiv(f(u_0)-a_m)+\cdots+$$

$$+\left(\frac{f^{(m-1)}(u_0)}{(m-1)!}-a_1\right)z^{m-1}$$

Zatem byłoby:

$$\frac{f^{(m-1)}(u_0)}{(m-1)!}-a_1=m\,a_0u_0+a_1-a_1=m\,a_0u_0=0,$$

skąd: $u_0=0$.

Widzimy też, że $sł'_z\{f(\hat{z}+u_0)-f(\hat{z})\}=m-1$, więc również: $sł'_z M(\hat{z},u_0)=m-1>0$.

Dla $u = 0$ mamy: $M(z, 0) = f'(z)$, więc: $st'M(z, 0) = m - 1$.

3° Utworzymy rugownik wielomianów $f(\hat{z})$ i $M(\hat{z}, u)$ dla u stałego, $\neq 0$.

Rugownik ten jest wielomianem $F(u)$ zmiennej u.

4° Zerowanie się wielomianu $F(u)$ dla $u_0 \neq 0$ jest warunkiem koniecznym i dostatecznym, by $f(z)$ i $f(z + u_0)$ posiadały wspólne miejsce zerowe, a więc by u_0 było *różnicą różnych pierwiastków* wielomianu $f(z)$.

Df. Równanie $F(u) \overset{?}{=} 0$, utworzone w powyższy sposób nazywamy *równaniem różnic pierwiastków* wielomianu $f(z)$ stopnia > 1.

Uw. Ściśle biorąc jest to równanie różnic *niezerowych*.

W paragrafie 7. rozdziału poprzedniego podaliśmy sposób obliczania górnych i dolnych granic pierwiastków wielomianu rzeczywistego. Jeżeli $f(z)$ jest wielomianem rzeczywistym, to $F(u)$ jest również rzeczywistym; zatem, gdy obliczymy dolną granicę bezwzględnych wartości pierwiastków niezerowych rzeczywistych wielomianu $F(u)$, otrzymamy w ten sposób dolną granicę bezwzględnych wartości *różnic różnych pierwiastków rzeczywistych* wielomianu $f(z)$, która była nam potrzebna w rozważaniach na str. 151.

Uw. 1. Zauważmy, że $M(z, 0) = f'(z) \neq 0$. $st'M(z, 0) = m - 1 > 0$, więc:

$$F(0) = R\{f(z), M(z, 0)\} = R(f, f') = a_0 D(f),$$

zatem $F(0) = 0$ wyraża warunek konieczny i dostateczny, by $f(z)$ posiadało *wielokrotne* pierwiastki.

Gdy $[f, f'] \equiv 1$, to $F(0) \neq 0$, zatem *różnica* $u = 0$ *jednakowych* pierwiastków $f(z)$ *nie* spełnia warunku: $F(u) = 0$.

Metoda Cauchy'ego obliczania granicy różnic pierwiastków.

Niechaj:

$$f(z) \equiv z^m + a_1 z^{m-1} + \cdots + a_m,\ m > 2$$

posiada pełny ciąg *różnych* pierwiastków:

$$z_1,\ z_2 \ldots z_m \qquad [m \text{ różnych}]$$

[możemy się zawsze ograniczyć do rozważania tego jedynie wypadku].

Rozważamy wyróżnik $D(f)$, oraz granicę górną λ wartości bezwzględnych pierwiastków $f(z)$, którą umielibyśmy obliczyć metodą, wyłożoną na str. 147.

$$\lambda > \max \{ |z_1|, \ldots |z_m| \}$$

$$0 < |D(f)| = \left| \prod_{i<k} (z_i - z_k)^2 \right| < (z_s - z_t)^2 . (2\lambda)^{m(m-1)-2}$$

$$s, t = 1, 2 \ldots m,\ s \neq t.$$

Stąd: $$|z_s - z_t| < \frac{1}{(2\lambda)^{\frac{m(m-1)}{2} - 1}} \cdot |D(f)|^{\frac{1}{2}},$$

Zatem: $$\sqrt{|(Df)|} . (2\lambda)^{1 - \frac{m(m-1)}{2}}$$

przedstawia dolną granicę bezwzględnych *różnic, różnych* między sobą pierwiastków wielomianu $f(z)$.

Gdy $f(z)$ jest wielomianem całkowitym, możemy za wartość granicy przyjąć:

$$(2\lambda)^{1-\frac{m(m-1)}{2}},$$

gdyż wtedy $|D(f)|$ jest liczbą całkowitą $\geqq 1$.

W praktyce, granice obliczone powyższą metodą, wypadają najczęściej zanadto małe, co przy oddzielaniu pierwiastków zmusza do zbyt wielu rachunków.

KONIEC CZĘŚCI I.

SPIS RZECZY:

WYDAWNICTWA BIBLJOTECZKI
KÓŁKA MAT.-FIZ. U. U. J.

Nr. 1. Prof. dr. W. Wł
liczb całkow
Nr. 2. — Teorja mno
Nr. 3. Prof. dr. A. Hob
różniczkowa
cz. I. . . .
Nr. 4. — cz. II. . . .
Nr. 5. Prof. dr. W. Wilkosz: Zarys algebry
cz. I. . . . .
Nr. 6. — cz. II. (w druk

Kółko Mat.-Fiz. U. U. J. po

Prof. dr. J. Sleszyński
tom I. Nakładem Kó
— tom II. Nakładem K
— Teorja wyznaczników

Prof. dr. A. Hoborski: Zbiór zadań z wyższej matematyki cz. I. Nakł. Kółka 1928 12·00
— Geometrja różniczkowa. Teorja powierzchni (litogr.) Nakł. Kółka . 1928 9·00
— Teorja ciągłych i skończonych grup przekształceń Lie'go (litogr.). Nakładem Kółka 1930 8.00
— Wyższa matematyka cz. I. Nakładem autora . . . . . 1928 9·90
— cz. II. Nakładem autora . . . 1923 5·00
Prof. dr. A. Rosenblatt: Geometrja analityczna na płaszczyźnie, Nakładem Polskiej Akademji Umiejętności . 1926 6·00
— Geometrja analityczna trzywymiarowa (litogr.). Nakładem Kółka . . . 1931 12·00
Prof. dr. S. Zaremba: Mechanika teoretyczna (Litogr.). Nakładem Kółka 1926 3·00
— Teorja całek wielokrotnych (Litogr.). Nakładem Kółka . . . . . 1923 3·00

Ostatnie Kółka Mat.-Fiz. U. U. J. mają znaczne zniżki.