ARTYKUŁ PIĄTY.

O równaniach algiebraicznych rozwiązalnych za pomocą pierwiastków stopnia drugiego i o możliwości wykreślania wielokątów foremnych.

napisał

Federigo Enriques z Bolonji.

Sprawa rozstrzygnięcia, czy zadanie gieometryczne konstrukcyjne może być rozwiązane sposobem elementarnym, to znaczy, przez wykonywanie nad elementami danemi działań linjałem i cyrklem, sprowadza się za pośrednictwem gieometrji analitycznej do pytania algiebraicznego.

O sposobie, w jaki to sprowadzenie się dokonywa, i o uwagach, związanych z tym przedmiotem, mówi Castelnuovo w artykule IV. Dla nas wystarczy tutaj przypomnieć rezultat podstawowy:

Niech będzie dane zadanie gieometryczne oznaczone, prowadzące do poszukiwania punktów płaszczyzny, któreby były w żądanych zależnościach od pewnych punktów, danych na tej samej płaszczyźnie; ażeby punkty szukane mogły być skonstruowane przez wykonywanie nad punktami danemi (oraz, jeśli zechcemy, nad punktami, prostemi i kołami dowolnemi) działań za pomocą linjału i cyrkla, jest warunkiem koniecznym i wystarczającym, żeby spółrzędne kartezjańskie punktów poszukiwanych można było otrzymać przez wykonywanie nad spółrzędnemi punktów danych działań wymiernych oraz kolejnego wyciągania pierwiastków stopnia drugiego (w liczbie skończonej).

Oznaczmy w krótkości nazwą „wyrażeń pierwiastkowych (niewymiernych) stopnia drugiego“ wyrażenia utworzone przez wy-

konywanie nad wielkościami danemi działań wymiernych i wyciągania pierwiastków stopnia drugiego; możemy wtedy wyrazić powyższy warunek rozwiązalności zadania, mówiąc, że spółrzędne punktów szukanych muszą być wyrażeniami pierwiastkowemi stopnia drugiego, utworzonemi ze spółrzędnych punktów danych.

Dowiedziemy nieco później, że każde wyrażenie pierwiastkowe stopnia drugiego czyni zadość jakiemuś równaniu algiebraicznemu, którego spółczynniki są wyrażeniami wymiernemi względem wielkości danych, czyli są wymierne w danym obszarze wymierności. Wskutek tego sprawa rozstrzygnięcia, czy dane zadanie może być rozwiązane elementarnie, sprowadza się do dwuch pytań następujących:

1° rozstrzygnąć, czy to zadanie (po uprzednim sprowadzeniu do omawianej wyżej postaci) jest algiebraiczne, to znaczy, czy zależy od równania algiebraicznego o spółczynnikach wymiernych w danym obszarze;

2° rozstrzygnąć, czy dane równanie algiebraiczne może być rozwiązane za pomocą działań wymiernych i wyciągania pierwiastków stopnia drugiego w danym obszarze wymierności, do którego należą spółczynniki równania.

Co się tyczy pytania pierwszego, to zaznaczymy, że gieometrja analityczna uczy przekształcać zależności gieometryczne na zależności analityczne; jeżeli te ostatnie zależności przedstawiają się pod postacią algiebraiczną, wtedy otrzymujemy od razu na powyższe pytanie odpowiedź potwierdzającą. Natomiast rozstrzygnięcie pytania staje się o wiele trudniejszym, jeżeli się otrzymuje zależności analityczne, nie występujące pod postacią algiebraiczną, gdyż wtedy trzeba się przekonać, czy te zależności analityczne (jeżeli chodzi o znalezienie niewiadomych w oznaczonym przypadku) mogą być oddane przez zależności algiebraiczne; takie badania prowadzą w rzeczywistości do najwyższych zagadnień analizy (por. art. VIII).

Zajmiemy się tu drugim pytaniem i podamy w tym celu twierdzenie ogólne o stopniu równań algiebraicznych, które można rozwiązać za pomocą pierwiastków stopnia drugiego. Pytanie nie będzie przez to wyczerpane (ażeby je wyczerpać potrzebnyby był wykład obszerniejszy); ale rezultat osiągnięty wystarcza do tych zastosowań w zakresie gieometrji elementarnej, które właśnie mamy na widoku.

Pomiędzy temi zastosowaniami występują przedewszystkim konstrukcje wielokątów foremnych, rozpatrywane w tym artykule, oraz zastosowania do zadań o podwojeniu sześcianu i o podziale kąta na trzy części równe, o czym będzie mowa w artykule VII.

Starożytni przekazali nam konstrukcje elementarne wielokąta foremnego o liczbie boków 2^n, trójkąta równobocznego i pięciokąta foremnego,

jak również wielokątów foremnych o liczbie boków $2^n.3$, $2^n.5$, 3.5, $2^n.3.5$, zależnych od poprzednich.

Otóż możnaby było np. poszukiwać konstrukcji elementarnych siedmiokąta albo dziewięciokąta foremnego i trudnoby było zdać sobie sprawę z trudności, którebyśmy przytym napotkali, gdyby nie poddano w wątpliwość rozwiązalności takich zadań. Gromadziłyby się w ten sposób daremne wysiłki, a z niepowodzenia nie możnaby nawet było nauczyć się czegokolwiek o charakterze rozpatrywanych zagadnień.

Gdyby jednak kto doszedł do przekonania, że tu chodzi o zagadnienia nierozwiązalne, to czyby się odważył na próby w następnych przypadkach, w których trudności, sądząc z pozoru, muszą wzrastać? Po stwierdzeniu, albo przypuszczeniu, że nie można zbudować elementarnie wielokątów foremnych o 7, 9, 11, 13, 14 bokach, czy mogłoby przyjść na myśl poszukiwanie konstrukcji wielokąta foremnego o 17 bokach? A jednak jest faktem, że konstrukcja siedemnastokąta jest możliwa, natomiast są niemożliwe konstrukcje (linjałem i cyrklem) wielokątów foremnych o 7, 9, 11, 13, 14 bokach.

O tym poucza bardzo piękna teorja równań dwumiennych Gaussa.

Konstrukcja wielokąta foremnego, mającego n boków, zależy od rozwiązania równania dwumiennego

$$z^n = 1,$$

które, po opuszczeniu pierwiastka $z = 1$, sprowadza się do postaci

$$z^{n-1} + z^{n-2} + \ldots + 1 = 0.$$

Ażeby n-kąt można było zbudować elementarnie, trzeba żeby równanie powyższe było rozwiązalne za pomocą pierwiastków stopnia drugiego (w bezwzględnym obszarze wymierności [1]). Otóż ta rozwiązalność zależy od postaci liczby n; a mianowicie równanie jest rozwiązalne, jeżeli n po rozłożeniu na czynniki pierwsze otrzymuje postać:

$$n = 2^{\nu}(2^{2^{\nu_1}} + 1)(2^{2^{\nu_2}} + 1)\ldots(2^{2^{\nu_s}} + 1),$$

gdzie $\nu_1, \nu_2, \ldots \nu_s$ są wszystkie różne od siebie.

We wzorze tym są przeto zawarte wszystkie wielokąty foremne, które można zbudować elementarnie*).

Niektóre wiadomości szczegółowe o takich wielokątach podamy w § 9 tego artykułu i zakończymy wzmianką o zagadnieniu siedmiokąta.

---

*) Co do przyrządów, któremi się trzeba posługiwać w konstrukcji, Hilbert zauważył, że użycie cyrkla można zastąpić użyciem przenośnika odcinków (por. art. IV, § 11).

Odsyłamy do art. VI w sprawie rozmaitych konstrukcji siedemnastokąta; natomiast tutaj poprzestaniemy na zaznaczeniu możliwości teoretycznej, wynikającej z powyższego twierdzenia ogólnego.

Załączamy na zakończenie tytuły głównych prac, w których są wyłożone teorje, będące przedmiotem tego artykułu, a któremi posiłkowaliśmy się w tej pracy.

1°. Co do równań algiebraicznych, rozwiązalnych za pomocą wyrażeń pierwiastkowych stopnia drugiego:

J. Petersen, *Theorie der algebraischen Gleichungen*, Kopenhagen 1878.—F. Klein, *Vorträge über ausgewählte Fragen der Elementargeometrie*, Leipzig 1895.—A. Capelli, *Lezioni di algebra complementare*, Pallerano, Napoli 1895.

2°. Co do teorji równań dwumiennych w związku z zagadnieniem wielokątów foremnych:

F. Gauss, *Disquisitiones arithmeticae, sectio VII* (1801), Werke Bd. I.—P. Bachmann, *Die Lehre von der Kreisteilung*, Leipzig 1872.—F. Klein, l. c.—L. Bianchi, *Lezioni sulla teoria delle sostituzioni e delle equazioni algebriche secondo Galois*, Pisa, Nistri, 1896.

I.

§ 1. Sprowadzanie wyrażeń niewymiernych stopnia drugiego do postaci normalnej. — Weźmy pod uwagę wyrażenie (pierwiastkowe stopnia drugiego) x, utworzone za pomocą działań wymiernych i kolejnego wyciągania pierwiastków z pewnych wielkości danych $1, \alpha, \beta, \ldots$, które wyznaczają obszar wymierności $[1, \alpha, \beta, \ldots]$. W tym wyrażeniu mieszczą się wyrazy, z których każdy zawiera pewną liczbę znaków pierwiastków, położonych jeden nad drugim; całe wyrażenie składa się z tych wyrazów w sposób wymierny. Nazywać będziemy wyrazem rzędu m taki wyraz, w którym pod jednym znakiem pierwiastka mieści się jeszcze $m-1$ znaków pierwiastka. Tak np.

$$\sqrt{a+\sqrt{b}}, \quad \sqrt{\sqrt{a}+\sqrt{b}}, \quad \sqrt{\sqrt{a}+\sqrt{b+\sqrt{c}}},$$

gdzie a, b, c przedstawiają wyrażenia wymierne, są wyrazami rzędu 2, 3 i 4.

Wyraz rzędu m można oznaczyć przez $\sqrt{X}$, gdzie X jest wyrażeniem pierwiastkowym stopnia drugiego, złożonym z wyrazów rzędu niższego i równego $m-1$.

W wyrażeniu x mogą się znajdować takie wyrazy rzędu m-tego, które się dadzą wyrazić wymiernie przez pozostałe wyrazy rzędu m-tego i przez wyrazy rzędów niższych; wtedy, zastępując te wyrazy tego rodzaju wyrażeniami, można zredukować liczbę wyrazów, występujących w x.

Wyobraźmy sobie, że wykonaliśmy kilkakrotnie, dopóki to było możliwe, wszystkie redukcje, do których dają sposobność wyrazy rzędu m-tego, zawarte w x; następnie wszystkie redukcje, dotyczące wyrazów rzędu $m-1$, i t. d.; dostaniemy wtedy wyrażenie x w takiej postaci, że liczba wyrazów już nie może być zmniejszona, gdyż żaden wyraz nie może być wyrażony wymiernie za pomocą pozostałych wyrazów tego samego rzędu i wyrazów rzędu niższego. Rozpatrzmy z osobna każdy wyraz $\sqrt{X}$ wyrażenia x i sprowadźmy analogicznie X do jaknajmniejszej liczby wyrazów. W ten sam sposób postąpimy z każdym wyrażeniem, zawartym pod znakiem pierwiastka każdego wyrazu w wyrażeniu X i t. d. Wykonawszy wszystkie możliwe redukcje, otrzymamy w końcu dla x takie wyrażenie, w którym wszystkie p i e r w i a s t k i są n i e z a l e ż n e, tak że ich liczba nie może już być zmniejszona w sposób wskazany wyżej.

Ażeby tę rzecz lepiej wyjaśnić, weźmy jako przykład:

$$x = \sqrt{\sqrt{a} + \sqrt{b} + \sqrt{ab}} + \sqrt{c} + \sqrt{d} + \sqrt{\frac{c}{d}}.$$

Możemy zastąpić pod pierwszym znakiem pierwiastka

$$\sqrt{ab} \text{ przez } \sqrt{a}.\sqrt{b};$$

możemy też zastąpić wyraz ostatni

$$\sqrt{\frac{c}{d}} \text{ przez } \frac{\sqrt{c}}{\sqrt{d}};$$

po wykonaniu tych redukcji dostajemy wyrażenie

$$x = \sqrt{\sqrt{a} + \sqrt{b} + \sqrt{a}.\sqrt{b}} + \sqrt{c} + \sqrt{d} + \frac{\sqrt{c}}{\sqrt{d}},$$

w którym wszystkie pierwiastki są od siebie niezależne.

Po sprowadzeniu wyrażenia x do postaci, zawierającej tylko pierwiastki niezależne, weźmy pod uwagę wyraz najwyższego rzędu m; tym wyrazem niech będzie $\sqrt{X}$. Wyrażenie x można uważać jako wyrażenie wymierne względem $\sqrt{X}$, w którym spółczynniki $a_1, a_2, \ldots b_1, b_2, \ldots$ są utworzone wymiernie z wyrazów pozostałych; a więc

$$x = \frac{a_1 + a_2\sqrt{X} + a_3(\sqrt{X})^2 + \ldots + a_{n+1}(\sqrt{X})^n}{b_1 + b_2\sqrt{X} + b_3(\sqrt{X})^2 + \ldots + b_{\nu+1}(\sqrt{X})^\nu}.$$

Ponieważ zaś

$$(\sqrt{X})^2 = X,\ (\sqrt{X})^4 = X^2, \ldots$$

przeto można napisać

$$x = \frac{p + q\sqrt{X}}{r + s\sqrt{X}},$$

gdzie p, q, r, s zależą wymiernie od wyrazów rzędu m różnych od $\sqrt{X}$, oraz od wyrazów rzędów niższych. A ponieważ

$$x = \frac{p + q\sqrt{X}}{r + s\sqrt{X}} = \frac{(p + q\sqrt{X})(r - s\sqrt{X})}{(r + s\sqrt{X})(r - s\sqrt{X})} = \frac{pr - qsX}{r^2 - s^2X} + \frac{qr - ps}{r^2 - s^2X}\sqrt{X},$$

przeto

$$x = A + B\sqrt{X},$$

gdzie A i B zależą wymiernie od wyrazów $\sqrt{Y}$, $\sqrt{Z}, \ldots$ m-go rzędu oraz od wyrazów rzędów niższych.

Zajmijmy się kolejnym rozpatrzeniem wyrażeń A i B. Każde z nich, np. A, może być przedstawione względem $\sqrt{Y}$ podobnie jak x względem $\sqrt{X}$:

$$A = A_1 + A_2\sqrt{Y},$$

gdzie A_1 i A_2 są złożone wymiernie z $\sqrt{Z}, \ldots$ i z wyrazów rzędu niższego od m.

Postępując w taki sam sposób z nowemi wyrażeniami A_1, $A_2, \ldots$ dojdziemy w końcu do przedstawienia x pod postacią wyrażenia całkowitego względem wyrazów rzędu m

$$\sqrt{X},\ \sqrt{Y},\ \sqrt{Z}, \ldots;$$

wyrazy te występują tylko pomnożone przez siebie, ale nie podniesione do potęgi; spółczynniki tego wyrażenia zależą wymiernie od wyrazów rzędu niższego od m.

Redukcja tego rodzaju, jaką wykonaliśmy względem wyrazów rzędu m, może być oczywiście wykonywana stopniowo względem wyrazów rzędu $m-1$, występujących w x albo w wyrażeniach X, Y, $Z, \ldots$; następnie względem wyrazów rzędu $m-2$ i t. d. Dojdziem w końcu do wyrażenia x pod postacią, którą nazwiemy p o s t a c i ą n o r m a l n ą, a która jest utworzona (na podstawie wielkości wymiernych w obszarze danym) tylko za pomocą działań dodawania, mnożenia i wyciągania pierwiastka stopnia drugiego, przyczym każdy pierwiastek stopnia drugiego występuje tylko w potędze pierwszej.

Dalsze nasze rozumowania nad wyrażeniami pierwiastkowemi stopnia drugiego opierać się będą na założeniu, że te wyrażenia zostały sprowadzone do pierwiastków niezależnych pod postacią normalną; liczbę tych pierwiastków możemy wtedy nazywać rzędem wyrażenia pierwiastkowego.

§ 2. Układanie równania algiebraicznego, któremu wyrażenie pierwiastkowe czyni zadość. Wyrażenie pierwiastkowe stopnia drugiego x rzędu n czyni zadość równaniu algiebraicznemu stopnia 2^n o spółczynnikach wymiernych (w obszarze wymierności).

Wyobraźmy sobie, że n pierwiastkom, występującym w wyrażeniu x nadajemy wszystkie wartości (dodatnie i ujemne), jakie te pierwiastki mogą przyjmować; dostaniemy w ten sposób 2^n wartości x, a mianowicie $x_1, x_2, x_3, \ldots x_i, \ldots x_{2^n}$, między któremi mogą być pierwiastki równe (jak o tym się później przekonamy).

Utwórzmy równanie

$$f(x)=(x-x_1)(x-x_2)\ldots(x-x_{2^n})=x^{2^n}+p_1x^{2^n-1}+\ldots+p_{2^n}=0,$$

którego pierwiastkami są wielkości x_i.

Spółczynniki tego równania wyrażają się przez funkcje symetryczne elementarne wielkości x_i za pomocą wzorów:

$$p_1=-\Sigma x_i$$

$$p_2=\Sigma x_i x_k$$

$$\ldots\ldots\ldots$$

$$p_2=x_1x_2\ldots x_{2^n}.$$

Trzeba dowieść, że te spółczynniki są wymierne.

Własność ta jest wynikiem faktu podstawowego, że p_r są funkcjami symetrycznemi wielkości x_i, czyli że pozostają bez zmiany, jeżeli porządek tych wielkości x_i zostaje w jakikolwiek sposób zmieniony (np.

$$p_1=-(x_1+x_2+\ldots+x_{2^n})=-(x_2+x_1+x_3+\ldots+x_{2^n})\ldots).$$

Przedewszystkim, ponieważ p_r są funkcjami symetrycznemi wielkości x_i, przeto nie powinny się zmieniać, jeżeli zostaną zmienione w jakikolwiek oznaczony sposób znaki pierwiastków występujących w x_i, gdyż zmiana taka wywołuje jedynie przestawienia w uporządkowaniu tych wielkości. Jeżeli np.

$$x=\sqrt{a+\sqrt{b}},$$

to możemy oznaczyć wartości wyrażenia x przez

$$x_1 = +\sqrt{a+\sqrt{b}}$$

$$x_2 = -\sqrt{a+\sqrt{b}}$$

$$x_3 = +\sqrt{a-\sqrt{b}}$$

$$x_4 = -\sqrt{a-\sqrt{b}};$$

widzimy teraz, że zmieniając znak przy $\sqrt{b}$, przestawiamy wartości x_1, x_3 i x_2, x_4; jeżeli natomiast zmienimy znaki obu pierwiastków, to przestawimy wartości x_1, x_4 i x_2, x_3; jeżeli wreszcie zmienimy znak pierwiastka zewnętrznego $\sqrt{a+\sqrt{b}}$, to przestawimy x_1, x_2 i x_3, x_4.

Rozpatrzmy teraz p_r jako wyrażenie pierwiastkowe utworzone z pierwiastków występujących w x i przypuśćmy, że to wyrażenie zostało sprowadzone do postaci normalnej. W założeniu, że to wyrażenie zawiera wyrazy $\sqrt{X}$, $\sqrt{Y}$, $\sqrt{Z}$, ... rzędu m, uwydatnijmy wyraz $\sqrt{X}$, pisząc

$$p_r = P + Q\sqrt{X}.$$

Ponieważ p_r pozostaje bez zmiany, jeżeli zmienimy znak przy $\sqrt{X}$, przeto

$$P + Q\sqrt{X} = P - Q\sqrt{X},$$

czyli

$$Q\sqrt{X} = 0,$$

a więc

$$Q = 0.$$

A zatym p_r nie zależy od $\sqrt{X}$. W sposób podobny znaleźlibyśmy, że p_r nie zależy od $\sqrt{Y}$, $\sqrt{Z}$, ..., a więc występują w nim wyrazy, zawierające co najwyżej pierwiastki rzędu $m-1$.

Ale powtarzając to samo rozumowanie w zastosowaniu do wyrazów rzędu $m-1$, widzimy, że p_r nie może też od nich zależeć. Postępując tak dalej dowodzi się, że p_r nie zależy od żadnego wyrazu pierwiastkowego, czyli że p_r jest wyrażeniem wymiernym (w danym obszarze). Zostało więc stwierdzone, że $f(x)=0$ jest równaniem o spółczynnikach wymiernych, c. b. d. d.

Zaznaczyliśmy, że pomiędzy wartościami x_1, x_2, ... wyrażenia x mogą być niektóre równe sobie; jeżeli np.

$$x = \sqrt{a+\sqrt{b}} + \sqrt{a-\sqrt{b}},$$

to wartości równe otrzymamy dla x, zmieniając znak przy $\sqrt{b}$.

Przypuśćmy, że z pośród 2^n wartości niewiadomej x wybieramy

wszystkie wartości różne; niech to będą np. $x_1, x_2, x_3, \ldots x_r$. Wtedy, równanie stopnia r

$$\varphi(x) = (x - x_1)(x - x_2) \ldots (x - x_r) = 0$$

ma również spółczynniki wymierne, czego się dowodzi tak samo, jak dla $f(x) = 0$.

Porównywając dwa równania

$$f(x) = 0, \quad \varphi(x) = 0,$$

widzimy, że wszystkie pierwiastki drugiego równania są zarazem pierwiastkami pierwszego, a więc równanie pierwsze jest przywiedlne, jeżeli $r < 2^n$; jest więc

$$f(x) = \varphi(x) \cdot \psi(x),$$

gdzie $\psi(x)$ oznacza wielomian o spółczynnikach wymiernych.

§ 3. O stopniu równań nieprzywiedlnych, dających się rozwiązać za pomocą wyrażeń pierwiastkowych stopnia drugiego. Dowiedziemy przedewszystkim twierdzenia: jeżeli równaniu algiebraicznemu o spółczynnikach wymiernych (w danym obszarze) czyni zadość pewna wartość wyrażenia pierwiastkowego stopnia drugiego x, to czynią mu zadość wszystkie wartości x, otrzymane przez zmiany znaków przy pierwiastkach.

Niech będzie

$$F(x) = 0$$

równaniem danym.

Przypuśćmy, że x zostało sprowadzone do pierwiastków niezależnych i do postaci normalnej, i uwydatnijmy wyraz rzędu najwyższego m, $\sqrt{X}$

$$x = A + B\sqrt{X}.$$

Podstawmy to wyrażenie w F i sprowadźmy F do postaci normalnej względem $\sqrt{X}$, pisząc:

$$F(x) = L + M\sqrt{X};$$

L i M zależą wymiernie od pozostałych wyrazów rzędu m: $\sqrt{Y}$, $\sqrt{Z}$, ... od wyrazów rzędu niższego, występujących w x.

Mamy teraz (podług założenia)

$$F(x) = L + M\sqrt{X} = 0;$$

przeto

$$L = M = 0,$$

albo też

$$\sqrt{X} = -\frac{L}{M};$$

ale ta ostatnia zależność sprzeciwia się założeniu, że wszystkie pierwiastki zawarte w x są niezależne; zostało więc dowiedzione, że

$$L = M = 0,$$

a wskutek tego

$$L - M\sqrt{X} = 0;$$

przeto równaniu

$$F(x) = 0$$

czyni zadość nietylko

$$x = A + B\sqrt{X},$$

ale także

$$x = A - B\sqrt{X}.$$

W sposób analogiczny dowodzi się, że równaniu $F(x)=0$ czynią zadość wartości, które się otrzymuje, zmieniając w wyrażeniu x jakkolwiek znaki wyrazów rzędu m: $\sqrt{Y}$, $\sqrt{Z}$,...

Przypuśćmy dla uproszczenia rozumowania, że w x występują tylko dwa wyrazy rzędu m:

$$\sqrt{X} \text{ i } \sqrt{Y};$$

będziemy mieli

$$F(x) = L + M\sqrt{X},$$

gdzie

$$L = L_1 + L_2\sqrt{Y}$$

$$M = M_1 + M_2\sqrt{Y};$$

a ponieważ $F(x)=0$, przeto wnosimy, że

$$L_1 = L_2 = M_1 = M_2 = 0.$$

Wyrażenia L_1, L_2, M_1, M_2 zawierają jedynie wyrazy, w których występują pierwiastki co najwyżej $(m-1)$-go rzędu; za pomocą poprzedniego rozumowania dowodzi się, że te wyrażenia pozostają zerami, jeżeli w x wykonane będą jakiekolwiek zmiany znaków przy pierwiastkach wyrazów rzędu $(m-1)$; stąd wynika, że równanie $F(x)=0$ jest spełnione, jeżeli w wyrażeniu x zostaną pozmieniane znaki pierwiastków, tworzących wyrazy rzędu $(m-1)$.

Widzimy już, jak można to rozumowanie prowadzić dalej i dojść w ten sposób do rezultatu, że jeżeli równaniu

$$F(x) = 0$$

czyni zadość jakieś wyrażenie pierwiastkowe stopnia drugiego x, wtedy czynią mu również zadość te wszystkie wartości, które się otrzymuje z wyrażenia danego przez dowolną zmianę znaków przy pierwiastkach, występujących w wyrazach rzędów

$$m,\ m-1,\ m-2, \ldots 1.$$

Pozostaje do okazania, że równanie $F(x)=0$ jest jeszcze spełnione, jeżeli się zmienia znaki pierwiastków, występujących pod innym pierwiastkiem, np. pierwiastków, tworzących wyrazy wyrażenia X, występującego w $\sqrt{X}$. Ale to już zostało pośrednio dowiedzione, gdyż jeżeli

$$F(x)=L+M\sqrt{X},$$

gdzie

$$L=M=0,$$

to zawsze

$$F(x)=0,$$

jakkolwiek się zmienia znaki pierwiastków, występujących w X.

Twierdzenie więc zostało całkowicie dowiedzione.

To twierdzenie prowadzi bezpośrednio do wniosku:

Jeżeli równaniu algiebraicznemu

$$F(x)=0$$

o spółczynnikach wymiernych czyni zadość pewna wartość wyrażenia pierwiastkowego stopnia drugiego x, i jeżeli przez

$$\varphi(x)=0$$

oznaczymy takie równanie (o spółczynnikach wymiernych), któremu czynią zadość wszystkie wartości, jakie x może otrzymać przez zmianę znaków przy pierwiastkach w tym wyrażeniu x zawartych, wtedy

$$F(x)=\varphi(x).\vartheta(x),$$

gdzie ϑ jest wielomianem o spółczynnikach wymiernych.

Jeżeli $F(x)=0$ jest równaniem nieprzywiedlnym, wtedy wielomian ϑ musi się więc sprowadzać do czynnika stałego.

Wróćmy teraz do równania $f(x)=0$ rozpatrywanego wyżej, a więc do równania stopnia 2^n, mającego za pierwiastki 2^n wartości wyrażenia pierwiastkowego x.

Zaznaczyliśmy już, że jeżeli $r<2^n$, to

$$f(x)=\varphi(x)\psi(x),$$

gdzie ψ jest wielomianem o spółczynnikach wymiernych. Otóż równanie $\psi(x)=0$ ma za pierwiastki niektóre wartości wyrażenia pierwiastkowego x, a więc i wszystkie jego wartości; mamy więc jeszcze:

$$\psi(x)=\varphi(x)\,.\,\psi_1(x) \quad \text{i} \quad f(x)=\varphi^2(x)\,.\,\psi_1(x),$$

gdzie ψ_1 jest nowym wielomianem o spółczynnikach wymiernych, albo też wielkością stałą. Zastosujmy do ψ_1 (w założeniu, że to nie jest wielkość stała) rozumowanie, wyłożone powyżej dla ψ, i t. d.; ostatecznie będziemy musieli znaleźć iloraz, który się sprowadza do wielkości stałej c, będziemy więc mieli

$$f(x)=c\varphi^s(x);$$

istotnie, dzielenie nie może być prowadzone do nieskończoności, gdyż f jest funkcją stopnia skończonego.

Ponieważ, jak mówiliśmy, $f(x)=c\varphi^s(x)$, a r jest stopniem funkcji φ, zaś 2^n stopniem funkcji f, przeto:

$$rs=2^n,$$

tak że zarówno r jak s nie zawierają żadnego czynnika pierwszego różnego od 2; w rezultacie więc stopień równania

$$\varphi(x)=0$$

będzie

$$r=2^\nu.$$

Stąd, pamiętając o rezultatach poprzednich, wyprowadzamy twierdzenie podstawowe:

Jeżeli równanie algiebraiczne nieprzywiedlne jest rozwiązalne za pomocą samych pierwiastków stopnia drugiego (w danym obszarze wymierności, do którego należą jego spółczynniki), wtedy jego stopień jest potęgą dwuch.

Ten warunek konieczny nie jest jednak wystarczającym; tak np. równanie ogólne stopnia czwartego nie jest rozwiązalne za pomocą pierwiastków stopnia drugiego.

Warunki, którym musi czynić zadość równanie stopnia 2^ν, ażeby mogło być rozwiązane za pomocą pierwiastków stopnia drugiego, oraz sposoby postępowania, któremi w ogólności trzeba się posługiwać w celu istotnego rozwiązania, badał wyczerpująco Julius Petersen w rozmaitych pracach (por. np. cytowaną „*Theorie der algebraischen Gleichungen*“).

II.

§ 4. Sprowadzenie zagadnienia wielokątów foremnych do równań dwumiennych. Zamierzamy zastosować powyższe rezultaty, o równaniach rozwiązalnych za pomocą pierwiastków stopnia drugiego, do zagadnienia o konstrukcji wielokątów foremnych.

Musimy przedewszystkim nadać zagadnieniu postać analityczną. W tym celu zaczniemy od sprowadzenia zadania do takiej postaci, ażeby dane były punkty i ażeby poszukiwane były punkty, mające z tamtemi punktami związki z góry ustalone.

Do tego celu wystarczają następujące bardzo proste uwagi:

a) Wszystkie n-kąty foremne są do siebie podobne; a więc zadanie zbudowania n-kąta foremnego, mającego bok dany, sprowadza się od razu do zadania zbudowania jakiegokolwiek n-kąta foremnego. Niewiadomą jest kąt wielokąta, albo, jeśli kto woli, kąt środkowy, opierający się na boku; bok występuje w zadaniu jako parametr dowolny.

b) Jeżeli potrafimy zbudować n-kąt foremny, wtedy możemy też zbudować n-kąt foremny wpisany w koło dane i mający jeden wierzchołek dany, można więc podzielić koło na n łuków równych, począwszy od danego punktu, jako jednego z punktów podziału; i odwrotnie.

A więc zagadnienie wielokątów foremnych jest w zupełności równoważne z zagadnieniem podziału koła na n części równych, jeżeli tylko można przyjąć, że jest dany środek O koła i jeden z punktów podziału A. Można przytym odległość obu punktów danych, czyli promień koła, przyjąć za jednostkę.

Pod tą postacią zadanie, w którym danemi są punkty, sprowadza się do poszukiwania $(n-1)$ punktów (podziału), które wraz z A stanowią wierzchołki n-kąta foremnego.

Każdy z tych punktów wyznacza wraz z A (w którymkolwiek z dwóch zwrotów) łuk, który pomnożony przez n daje wielokrotność całego okręgu koła, a więc łuk

$$\frac{2\pi m}{n}$$

(przyczym można przyjąć $m < n$).

Odwołajmy się do dwuch osi spółrzędnych prostokątnych, przyjmując O za początek i OA za oś odciętych x. Punkt A mieć będzie za spółrzędne 1, 0; punkty poszukiwane będą miały pewne spółrzędne

$$x_1,\ y_1;\ x_2,\ y_2;\ \ldots;\ x_{n-1},\ y_{n-1}$$

(czyniące zadość równaniu koła

$$x^2+y^2=1).$$

Te spółrzędne właśnie trzeba wyznaczyć, opierając się jedynie na danych wielkościach 0, 1, określających obszar wymierności bezwzględny [1].

Wyobraźmy sobie przedstawione na płaszczyźnie wartości zmiennej zespolonej

$$z=x+iy$$

(odwzorowanie podług Arganda i Gaussa). Każdej wartości z odpowiada (jak wiadomo) moduł

$$\rho=|\sqrt{x^2+y^2}|$$

i argument

$$\vartheta=\operatorname{arc\,tg}\frac{y}{x};$$

są to spółrzędne biegunowe punktu (x, y), przedstawiającego z, tak że

$$z=\rho(\cos\vartheta+i\sin\vartheta).$$

Moduł jest odległością bezwzględną punktu (x, y) od początku spółrzędnych (promień wodzący); argument jest kątem (anomalją), który prosta, łącząca ten punkt z początkiem spółrzędnych, tworzy z osią x.

Mnożenie dwuch liczb zespolonych

$$z=x+iy,\ z'=x'+iy'$$

można wykonać: algiebraicznie, podług zwykłych zasad rachunku, kładąc

$$Z=zz'=(xx'-yy')+i(xy'+x'y);$$

lub też gieometrycznie, wyznaczając punkt, który ma za spółrzędne biegunowe

$$P=\rho\rho'=|\sqrt{x^2+y^2}|\cdot|\sqrt{x'^2+y'^2}|$$

$$\Theta=\vartheta+\vartheta'=\operatorname{arc\,tg}\frac{y}{x}+\operatorname{arc\,tg}\frac{y'}{x'},$$

czyli tworząc iloczyn modułów i sumę argumentów.

Stosując tę zasadę gieometryczną, utworzymy kolejne potęgi liczb zespolonych

$$z_s=x_s+iy_s,$$

mające za obrazy punkty poszukiwane

$$(x_1, y_1), \ldots (x_{n-1}, y_{n-1}).$$

Modułem jest

$$\sqrt{x_s^2 + y_s^2} = 1,$$

a argumentem

$$\frac{2\pi m}{n}$$

$$\left(\text{skąd } z_s = \cos\frac{2\pi m}{n} + i\sin\frac{2\pi m}{n}\right);$$

a więc moduł potęgi z_s^n będzie zawsze $=1$, natomiast jej argument będzie

$$\frac{2\pi mh}{n}.$$

W szczególności dla $h=n$ punkt z_s^n znajdzie się na części dodatniej osi x, a więc pokryje się z punktem

$$A \equiv (1,\ 0);$$

wskutek tego

$$z_s^n = 1.$$

Odwrotnie, niech będzie $(x,\ y)$ takim punktem różnym od A, że

$$z^n = (x+iy)^n = 1;$$

ten punkt musi mieć moduł ρ taki, że $\rho^n = 1$, musi więc mieć moduł $=1$; oprócz tego musi mieć taki argument ϑ, który pomnożony przez n różni się od 0 o wielokrotność 2π, a więc

$$\vartheta = \frac{2\pi m}{n}.$$

Punkt taki jest przeto jednym z punktów

$$(x_1,\ y_1), \ldots (x_{n-1},\ y_{n-1}),$$

czyniących zadość zagadnieniu.

Dochodzimy więc do wniosku:

Zagadnienie budowy n-kąta foremnego zależy od rozwiązania równania dwumiennego

$$z^n = 1,$$

a mianowicie od wynalezienia pierwiastków tego równania różnych od $z=1$; zależy więc od rozwiązania równania

$$\frac{z^n - 1}{z-1} = z^{n-1} + z^{n-2} + \ldots + 1 = 0.$$

To równanie można rozłożyć na dwa inne, z których jedno zawierałoby x, drugie y; ale to nie jest konieczne ani pożyteczne. Jeżeli powyższe równanie dla z może być rozwiązane za pomocą pierwiastków stopnia drugiego (w obszarze wymierności [1], wyznaczonym przez spółczynniki), wtedy i spółrzędne x, y punktów szukanych wyrażą się za pomocą pierwiastków stopnia drugiego, gdyż

$$\sqrt{a+ib}=\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}}+i\sqrt{\frac{\sqrt{a^2+b^2}-a}{2}};$$

a więc n-kąt może być w takim razie zbudowany linjałem i cyrklem. Odwrotnie, jeżeli n-kąt może być zbudowany, wtedy x, y są wyrażeniami pierwiastkowemi stopnia drugiego, a więc i pierwiastki

$$z=x+iy$$

równania dwumiennego dadzą się wyrazić za pomocą pierwiastków stopnia drugiego.

Zagadnienie o konstrukcji elementarnej wielokątów foremnych zostało tym sposobem sprowadzone do rozwiązania (jeżeli to możliwe), za pomocą pierwiastków stopnia drugiego, równania dwumiennego

$$z^n=1.$$

§ 5. Nieprzywiedlność równania $\frac{z^p-1}{z-1}=0$, jeżeli p jest liczbą pierwszą. Weźmy pod rozwagę równanie

$$z^p-1=0$$

w założeniu, że p jest liczbą pierwszą. Po usunięciu czynnika linjowego $z-1$, równanie to sprowadza się do postaci

$$F(z)=\frac{z^p-1}{z-1}=z^{p-1}+z^{p-2}+\ldots+z+1=0.$$

Chcemy dowieść, że to równanie jest nieprzywiedlne w obszarze bezwzględnym wymierności [1], czyli że $F(z)$ nie można rozłożyć na iloczyn dwuch wielomianów o spółczynnikach (liczbowych) wymiernych.

W tym celu musimy przedewszystkim podać twierdzenie przybrane o rozkładalności wielomianów; twierdzenie to zawdzięczamy Gaussowi.

Niech będzie wielomian

$$f(z)=a_0z^n+a_1z^{n-1}+\ldots+a_n,$$

którego spółczynniki niech będą liczbami całkowitemi; mówimy, że ten

wielomian jest p i e r w o t n y, jeżeli liczby $a_0, a_1, \ldots a_n$ nie mają żadnego czynnika wspólnego różnego od jedności.

Niech teraz będą

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

dwoma wielomianami pierwotnemi o spółczynnikach całkowitych. Utwórzmy iloczyn

$$F(z) = f(z) \cdot \varphi(z) = c_0 z^{m+n} + c_1 z^{m+n-1} + \ldots + c_{m+n},$$

gdzie

$$c_0 = a_0 b_0$$
$$c_1 = a_0 b_1 + a_1 b_0$$

i wogóle

$$c_h = a_0 b_h + a_1 b_{h-1} + \ldots + a_h b_0,$$

z tym zastrzeżeniem, że

$$a_r = 0 \text{ dla } r > n,$$
$$b_s = 0 \text{ dla } s > m.$$

Dowiedziemy, że wielomian $F(z)$ jest pierwotny, czyli że nie istnieje żadna liczba pierwsza $p(>1)$, która byłaby dzielnikiem wszystkich liczb $c_0, c_1, \ldots c_{m+n}$.

Niech będzie dana liczba pierwsza $p(>1)$; ta liczba nie może być dzielnikiem wszystkich spółczynników a wielomianu f, ani też wszystkich spółczynników b wielomianu φ; można więc znaleźć pierwszy spółczynnik a_r

$$(\text{przyczym } r \leqq n)$$

i tak samo pierwszy spółczynnik b_s

$$(\text{przyczym } s \leqq m),$$

które nie są podzielne przez p. Rozpatrzmy teraz spółczynnik

$$c_{r+s} = a_0 b_{r+s} + \ldots + a_{r-1} b_{s+1} + a_r b_s + a_{r+1} b_{s-1} + \ldots + a_{r+s} b_0.$$

Wszystkie wyrazy tej sumy są podzielne przez p, z wyjątkiem wyrazu $a_r b_s$; a więc c_{r+s} nie jest podzielne przez p.

Powyższa uwaga pozwala nam dowieść twierdzenia następującego.

Twierdzenie przybrane Gaussa. J e ż e l i w i e l o m i a n o s p ó ł c z y n n i k a c h c a ł k o w i t y c h $F(z)$ j e s t p r z y w i e d l n y, w t e d y m o ż e b y ć r o z ł o ż o n y n a i l o c z y n d w u c h w i e l o m i a n ó w o s p ó ł c z y n n i k a c h c a ł k o w i t y c h.

Możemy założyć, nie sprawiając przez to ograniczenia, że F jest wie-

lomianem pierwotnym, gdyż w razie przeciwnym możnaby było przedstawić F pod postacią $\mu F'$, gdzie F' jest wielomianem pierwotnym, a μ liczbą całkowitą (dzielnikiem wspólnym spółczynników wielomianu F); wystarczyłoby więc oczywiście dowieść twierdzenia dla F'.

Przypuśćmy więc, że $F(z)$ rozkłada się na iloczyn dwuch wielomianów $f(z)$ i $\varphi(z)$ o spółczynnikach wymiernych; chcemy dowieść, że F jest wtedy również iloczynem wielomianów o spółczynnikach całkowitych.

Sprowadźmy wszystkie spółczynniki wielomianu f do najmniejszego mianownika wspólnego a; liczniki będą wtedy miały największy dzielnik wspólny α, pierwszy względem a. Postąpmy w taki sam sposób ze spółczynnikami wielomianu φ, sprowadzając je do najmniejszego mianownika wspólnego b; niech będzie β największym czynnikiem wspólnym liczników w tak przekształconych spółczynnikach. Wtedy wielomiany $\frac{af}{\alpha}$ i $\frac{b\varphi}{\beta}$ będą miały spółczynniki całkowite i będą wielomianami pierwotnemi; ich iloczyn

$$\frac{ab}{\alpha\beta} f\varphi = \frac{ab}{\alpha\beta} F$$

będzie więc wielomianem o spółczynnikach całkowitych i będzie pierwotnym.

Wskutek pierwszego warunku, ponieważ spółczynniki wielomianu F nie mają żadnego czynnika wspólnego, przeto każdy czynnik pierwszy zawarty w $\alpha\beta$ musi być dzielnikiem iloczynu ab, a więc $\alpha\beta$ mieści się w ab bez reszty; wskutek drugiego iloraz $\frac{ab}{\alpha\beta} = c$ (który, jak już mówiliśmy, jest liczbą całkowitą) musi być równy 1, gdyż inaczej wszystkie spółczynniki w cF byłyby podzielne przez $c > 1$.

Ostatecznie więc $F(z)$ jest iloczynem dwuch wielomianów pierwotnych o spółczynnikach całkowitych $\frac{a}{\alpha} f$ i $\frac{b}{\beta}\varphi$, c. b. d. d.

Na zasadzie twierdzenia Gaussa można łatwo dowieść, stosując rozumowanie Eisensteina*), że:

Równanie $\frac{z^p - 1}{z - 1} = 0$, w którym p jest liczbą pierwszą, jest nieprzywiedlne.

Jeżeli założymy

$$z = x + 1,$$

*) Journal für Mathematik, Bd. 39, str. 167. Dwa inne dowodzenia tego samego twierdzenia były dane przez Kroneckera, Journ. f. Math. Bd. 29 i Journal de mathématiques 12, vol. 1. Por. Bachmann, l. c.

to równanie powyższe przyjmie postać

$$F(x) \equiv x^{p-1} + px^{p-2} + \frac{p(p-1)}{1.2} x^{p-3} + \ldots + \binom{p}{r} x^{p-r-1} + \ldots + p = 0 .$$

Wystarcza oczywiście dowieść nieprzywiedlności równania $F(x) = 0$, gdyż jeżeli

$$\frac{z^p - 1}{z - 1} = \varphi_1(z) . f_1(z),$$

gdzie φ_1, f_1 są dwoma wielomianami, to:

$$F(x) = \varphi_1(x+1) . f_1(x+1) = \varphi(x) . f(x),$$

gdzie φ i f są dwoma wielomianami względem x.

Przypuśćmy więc, że równanie $F(x) = 0$ jest przywiedlne, wtedy będzie

$$F(x) = \varphi(x) . f(x),$$

gdzie φ i f są dwoma wielomianami o zmiennej x i o spółczynnikach całkowitych:

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n$$
$$\varphi(x) = b_0 x^m + b_1 x^{m-1} + \ldots + b_m .$$

Po wykonaniu iloczynu φf otrzymamy wielomian równy tożsamościowo F:

$$c_0 x^{n+m} + c_1 x^{n+m-1} + \ldots + c_{n+m},$$

w którym stopień $n + m = p$.

Będziemy więc mieli wzory:

$$c_0 = a_0 b_0 = 1$$
$$c_1 = a_0 b_1 + a_1 b_0 = p$$
$$c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0 = \frac{p(p-1)}{2}$$
$$\ldots \ldots \ldots \ldots \ldots \ldots$$
$$c_{n+m-1} = a_{n-1} b_m + a_n b_{m-1} = \frac{p(p-1)}{2}$$
$$c_{n+m} = a_n b_m = p.$$

A zatym wszystkie spółczynniki c, z wyjątkiem c_0, są podzielne przez liczbę pierwszą p.

Otóż ostatni z wypisanych wzorów, właśnie dlatego, że p jest liczbą pierwszą, pociąga za sobą to, że jedna z liczb a_n, b_m równa się ± 1, a druga $\pm p$; niech np. będzie

$$a_n = 1, \quad b_m = p.$$

Podstawiając te wartości we wzorze przedostatnim, znajdziemy

$$c_{n+m-1} = a_{n-1}p + b_{m-1};$$

a ponieważ p mieści się w c_{n+m-1} bez reszty, przeto b_{m-1} musi być podzielne przez p, czyli:

$$b_{m-1} = pb'_{m-1}.$$

Postępując podobnie przy rozpatrywaniu wyrażenia c_{n+m-2}, znajdziemy:

$$c_{n+m-2} = a_{n-2} \cdot p + a_{n-1}b'_{m-1} \cdot p + b_{m-2},$$

a zatym b_{m-2} jest podzielne przez p, czyli

$$b_{m-2} = p \cdot b'_{m-2}.$$

Z wyrażeń $c_{n+m-3}, \ldots c_n$ znajduje się stopniowo, że wszystkie spółczynniki $b_{m-3}, \ldots b_0$ są podzielne przez p; ale ten rezultat w stosunku do b_0 okazuje się niedorzecznym, gdyż równość

$$c_0 = a_0 b_0 = 1$$

daje

$$a_0 = \pm 1, \quad b_0 = \pm 1.$$

Niedorzeczność, do której prowadzi założenie, że wielomian F daje się rozłożyć, dowodzi, że równanie $F = 0$, a więc

$$\frac{z^p - 1}{z - 1} = 0$$

jest nieprzywiedlne, c. b. d. d.

§ 6. Niemożliwość konstrukcji elementarnej wielokątów foremnych, których liczba boków p jest pierwsza i nie ma postaci $2^n + 1$. Pamiętając o rezultacie podstawowym § 3, wnosimy:

Jeżeli równanie $\frac{z^p - 1}{z - 1} = 0$, w którym p jest liczbą pierwszą, może być rozwiązane za pomocą pierwiastków stopnia drugiego, to $p - 1$ musi być potęgą dwuch, a zatym

$$p = 2^n + 1.$$

Wskutek tego:

Wielokąta foremnego, którego liczba boków p jest pierwsza, nie można zbudować linjałem i cyrklem jeżeli p nie ma postaci $2^n + 1$.

Tak np. wielokątów foremnych, mających 7, 11, 13, 19,... boków, nie można zbudować w sposób elementarny.

§ 7. Możliwość konstrukcji wielokątów foremnych, których liczba boków p jest liczbą pierwszą, mającą postać $2^n + 1$. Powyższemu rezultatowi przeczącemu przeciwstawia się następujący rezultat twierdzący:

Wielokąt foremny, którego liczba boków p jest liczbą pierwszą postaci 2^{n+1}, może być zbudowany linjałem i cyrklem.

Ażeby dowieść tego twierdzenia, należy okazać, że równanie (nieprzywiedlne)

$$\frac{z^p-1}{z-1}=z^{p-1}+z^{p-2}+\ldots+z+1=0$$

może być rozwiązane za pomocą kolejnego wyciągania pierwiastków stopnia drugiego, jeżeli p jest liczbą pierwszą postaci 2^n+1.

Pierwiastki tego równania, czyli różne od jedności pierwiastki stopnia p z jedności są:

$$\varepsilon_1=\cos\frac{2\pi}{p}+i\sin\frac{2\pi}{p}$$

. . . . . .

$$\varepsilon_m=\cos\frac{2\pi m}{p}+i\sin\frac{2\pi m}{p}$$

. . . . . .

$$\varepsilon_{p-1}=\cos\frac{2\pi(p-1)}{p}+i\sin\frac{2\pi(p-1)}{p}.$$

Wszystkie te pierwiastki można otrzymać, tworząc kolejne potęgi któregokolwiek z nich ε. Obierając np. pierwiastek $\varepsilon=\varepsilon_1$, dostaniemy istotnie $\varepsilon_m=\varepsilon^m$.

Poczynając od pierwiastka $\varepsilon=\varepsilon_2$, mieć będziemy:

$$\varepsilon_2=\varepsilon,\ \varepsilon_4=\varepsilon^2,\ \varepsilon_6=\varepsilon^3,\ \ldots\ \varepsilon_{p-1}=\varepsilon^{\frac{p-1}{2}},$$

$$\varepsilon_1=\varepsilon^{\frac{p-1}{2}+1},\ \varepsilon_3=\varepsilon^{\frac{p-1}{2}+2},\ \varepsilon_5=\varepsilon^{\frac{p-1}{2}+3},\ \ldots\ \varepsilon_{p-2}=\varepsilon^{p-1}.$$

W podobny sposób potęgi kolejne któregokolwiek $\varepsilon=\varepsilon_m$ z wykładnikami $1, 2, \ldots, (p-1)$ są wszystkie różne od siebie, odtwarzają więc (w innym porządku) pierwiastki $\varepsilon_1, \varepsilon_2, \ldots \varepsilon_{p-1}$. W rzeczy samej, nie mogłoby być dla $h<p$, $k<p$,

$$\varepsilon_m^h=\varepsilon_m^k,$$

gdyby nie było

$$\varepsilon_m^{h-k}=1,$$

czyli

$$\cos\frac{2\pi m(h-k)}{p}+i\sin\frac{2\pi m(h-k)}{p}=1,$$

skądby wypadło:

$$2\pi\frac{m(h-k)}{p}=2\pi s,$$

gdzie s jest liczbą całkowitą; ale ta równość jest niedorzeczna, gdyż jeżeli p jest liczbą pierwszą, a $m<p$, to p nie może być dzielnikiem iloczynu $m(h-k)$, nie będąc dzielnikiem liczby $h-k$.

Zauważmy jeszcze, że zawsze zachodzi równość

$$\varepsilon^{l+mp}=\varepsilon^{l},$$

gdyż

$$\varepsilon^{mp}=1.$$

Jeżeli teraz chcemy pogłębić badanie pierwiastków naszego równania, to musimy wziąć z teorji liczb twierdzenie następujące*):

Jeżeli jest dana liczba pierwsza p, to zawsze pomiędzy liczbami $1, 2, \ldots, p-1$ istnieje taka liczba g, że potęgi

$$g, g^2, \ldots, g^{p-1},$$

podzielone przez p, dają jako reszty liczby

$$1, 2, \ldots, p-1,$$

wzięte w innym porządku.

Taka liczba g nazywa się pierwiastkiem pierwotnym modułu p.

Jeżeli np. $p=5$, i zaczynamy od rozpatrywania liczby 2, to mamy

$$2^1=2,\ 2^2=4,\ 2^3=8,\ 2^4=16;$$

te liczby podzielone przez 5 dają odpowiednio jako reszty:

$$2, 4, 3, 1;$$

a więc 2 jest pierwiastkiem pierwotnym modułu 5.

W przypadku $p=7$, tworząc kolejne potęgi liczby 2, otrzymujemy liczby

$$2^1=2,\ 2^2=4,\ 2^3=8,\ 2^4=16,\ 2^5=32,\ 2^6=64,$$

które po podzieleniu przez 7 dają jako reszty

$$2, 4, 1, 2, 4, 1;$$

a więc 2 nie jest pierwiastkiem pierwotnym modułu 7. Natomiast kolejne potęgi liczby 3:

$$3^1=3,\ 3^2=9,\ 3^3=27,\ 3^4=81,\ 3^5=243,\ 3^6=729,$$

podzielone przez 7, dają jako reszty:

$$3, 2, 6, 4, 5, 1;$$

a zatym liczba 3 jest pierwiastkiem pierwotnym modułu 7.

---

*) Por. np. U. Scarpis, *Primi elementi della teoria dei numeri.* Hoepli 1897.

Zwracając się do ogólnego przypadku jakiejkolwiek liczby pierwszej p postaci 2^n+1, przypuśćmy, żeśmy wyznaczyli pierwiastek pierwotny g modułu p, i weźmy znowu pod uwagę jeden z pierwiastków ε równania

$$\frac{z^p-1}{z-1}=0.$$

Tworząc kolejne potęgi

$$\varepsilon^g,\ \varepsilon^{g^2},\ \varepsilon^{g^3},\ \ldots,\ \varepsilon^{g^{p-1}},$$

widzimy, że te potęgi odtwarzają w innym porządku pierwiastki

$$\varepsilon,\ \varepsilon^2,\ \ldots,\ \varepsilon^{p-1}.$$

W rzeczy samej, jeżeli oznaczymy przez s_r resztę z podzielenia g^r przez p, jeżeli więc

$$g^r=ph+s_r,$$

to będziemy mieli

$$\varepsilon^{g^r}=\varepsilon^{s_r},$$

gdyż

$$\varepsilon^{ph}=1;$$

s_r przyjmuje tutaj (w innym porządku) wszystkie wartości $1, 2, \ldots, p-1$, jeżeli r otrzymuje kolejne wartości $1, 2, \ldots, p-1$.

Podzielmy teraz pierwiastki

$$\varepsilon^g,\ \varepsilon^{g^2},\ \ldots,\ \varepsilon^{g^{p-1}}$$

na dwie grupy

$$\varepsilon^g,\ \varepsilon^{g^3},\ \ldots,\ \varepsilon^{g^{p-2}}$$

$$\varepsilon^{g^2},\ \varepsilon^{g^4},\ \ldots,\ \varepsilon^{g^{p-1}}$$

i załóżmy

$$\eta_1=\varepsilon^g+\varepsilon^{g^3}+\ldots+\varepsilon^{g^{p-2}}$$

$$\eta_2=\varepsilon^{g^2}+\varepsilon^{g^4}+\ldots+\varepsilon^{g^{p-1}}.$$

Podzielmy każdą z poprzednio utworzonych grup na dwie inne, zakładając:

$$\left.\begin{aligned}\eta_{11}&=\varepsilon^g+\varepsilon^{g^5}+\ldots+\varepsilon^{g^{p-4}}\\ \eta_{12}&=\varepsilon^{g^3}+\varepsilon^{g^7}+\ldots+\varepsilon^{g^{p-2}}\end{aligned}\right\}\ \eta_{11}+\eta_{12}=\eta_1$$

$$\left.\begin{aligned}\eta_{21}&=\varepsilon^{g^2}+\varepsilon^{g^6}+\ldots+\varepsilon^{g^{p-3}}\\ \eta_{22}&=\varepsilon^{g^4}+\varepsilon^{g^8}+\ldots+\varepsilon^{g^{p-1}}\end{aligned}\right\}\ \eta_{21}+\eta_{22}=\eta_2.$$

Można tym sposobem postępować dalej, tworząc stopniowo sumy o liczbach wyrazów

$$\frac{p-1}{4},\ \frac{p-1}{8},\ \ldots,$$

i dojść w końcu (ponieważ $p-1$ jest potęgą liczby 2) do sum o jednym tylko wyrazie, czyli do pierwiastków danego równania. Sumy wskazane wyżej otrzymują nazwę „okresów Gaussa". Okażemy, w jaki sposób te okresy dadzą się obliczać przez kolejne wyciąganie pierwiastków stopnia drugiego.

Zauważmy przedewszystkim, że suma

$$\eta_1 + \eta_2 = \eta = \varepsilon^g + \varepsilon^{g^2} + \ldots + \varepsilon^{g^{p-1}} = -1,$$

gdyż η, pominąwszy znak, jest spółczynnikiem przy z^{p-2} w równaniu

$$z^{p-1} + z^{p-2} + \ldots + 1 = 0,$$

dla którego liczby ε są pierwiastkami.

Weźmy pod uwagę iloczyn $\eta_1\eta_2$.

Po wykonaniu mnożenia dwuch sum, stanowiących η_1 i η_2, otrzymuje się sumę wyrazów postaci

$$\varepsilon^{g^r} . \varepsilon^{g^s} = \varepsilon^{g^r + g^s} = \varepsilon^h = \varepsilon^{g^t},$$

a więc sumę wyrazów, z których każdy zawiera się w jednej z dwuch grup, stanowiących η_1 i η_2.

Wyrażenie

$$\eta_1\eta_2 = \Sigma\varepsilon^{g^t}$$

nie zmienia się, jeżeli w nim zastąpić ε przez ε^g, ponieważ takie podstawienie wywołuje jedynie (jak to łatwo sprawdzić) zamianę

$$\eta_1 \text{ na } \eta_2 \text{ i } \eta_2 \text{ na } \eta_1.$$

Ten fakt zasadniczy pociąga za sobą, że suma $\Sigma\varepsilon^{g^t}$ zawiera jednakową liczbę razy ρ każdy pierwiastek równania

$$\frac{z^p - 1}{z - 1} = 0;$$

mamy przeto:

$$\eta_1\eta_2 = \Sigma\varepsilon^{g^t} = \rho\eta = -\rho.$$

Ażeby się jasno przekonać, jak się dochodzi do tego wyniku, zacznijmy od grupowania wyrazów podobnych sumy $\Sigma\varepsilon^{g^t}$; napiszemy więc:

$$\eta_1\eta_2 = \varkappa\varepsilon^{g^r} + \lambda\varepsilon^{g^s} + \ldots$$

i dowiedziemy, że spółczynniki całkowite $\varkappa$, λ, ... są wszystkie sobie równe; w tym celu wystarczy dowieść, że żaden z nich nie może być mniejszy od innego dowolnie obranego.

Jeżeli np. w powyższej sumie występuje wyraz $\rho\varepsilon^g$, to zastępując w nim ε przez ε^g, otrzymamy wyraz $\rho\varepsilon^{g^2}$, a z tego wyrazu dostaniemy ko-

lejno wyrazy $\rho\varepsilon^{g^3}$, $\rho\varepsilon^{g^4}$, ..., które muszą wszystkie występować w tej sumie. Jeżeli w sumie występuje wyraz $\rho\varepsilon^{g^3}$, to zastępując w nim ε przez ε^g i wykonywając to samo podstawienie w wyrazach kolejno otrzymywanych, dostaniemy wyrazy

$$\rho\varepsilon^{g^3},\ \rho\varepsilon^{g^4},\ \ldots,\ \rho\varepsilon^{g^{p-1}},\ (\rho\varepsilon^{g^p}=\rho\varepsilon^g),$$

które również muszą wszystkie występować w tej sumie.

I w ogóle z istnienia wyrazu $\rho\varepsilon^{g^t}$, można wnosić, że suma musi zawierać wszystkie wyrazy

$$\rho\varepsilon^{g^{t+1}},\ \rho^{g^{t+2}},\ \ldots,\ \rho\varepsilon^{g^{t+p-1}},$$

które przedstawiają w innym porządku wyrazy

$$\rho\varepsilon^g,\ \rho\varepsilon^{g^3},\ \ldots,\ \rho\varepsilon^{g^{p-1}}.$$

Widzimy więc, że $\eta_1+\eta_2$ i $\eta_1\eta_2$ są liczbami całkowitemi, a więc η_1, η_2 czynią zadość równaniu stopnia drugiego

$$x^2+x-\rho=0$$

o spółczynnikach całkowitych.

To równanie rozwiązuje się za pomocą pierwiastka $\sqrt{1+4\rho}$, przez który wyrażają się η_1 i η_2.

Przechodzimy teraz do obliczenia okresów, z których każdy zawiera $\frac{p-1}{4}$ wyrazów:

$$\eta_{11},\ \eta_{12},\ \eta_{21},\ \eta_{22}.$$

Mamy przedewszystkim:

$$\eta_{11}+\eta_{12}=\eta_1,\ \eta_{21}+\eta_{22}=\eta_2.$$

Utwórzmy teraz iloczyny

$$\eta_{11}\eta_{12},\ \eta_{21}\eta_{22}.$$

Rozpatrując np. pierwszy z tych iloczynów widzimy, że można go sprowadzić do sumy wyrazów postaci ε^{g^t}, a mianowicie do sumy, która się nie zmienia, jeżeli w każdym jej wyrazie zastąpimy ε przez ε^{g^2}; w rzeczy samej, wskutek takiego podstawienia okresy η_{11} i η_{12} zamieniają się tylko jeden na drugi. Stąd wnosimy (jak i poprzednio), że jeżeli wyrażenie $\eta_{11}\eta_{12}$ zawiera pewną liczbę razy ρ_1 jakiś wyraz sumy η_1, to zawiera tyleż razy i inne wyrazy tej samej sumy (jeżeli np. $\eta_{11}\eta_{12}$ zawiera wyraz $\rho_1\varepsilon^g$, to zawiera też $\rho_1\varepsilon^{g^3}$, $\rho_1\varepsilon^{g^5}$, ...); podobnie, jeżeli omawiane wyrażenie zawiera ρ_2 razy jakiś wyraz sumy η_2, to zawiera także ρ_2 razy wszystkie wyrazy pozostałe; a więc:

$$\eta_{11}\eta_{12} = \rho_1\eta_1 + \rho_2\eta_2,$$

gdzie ρ_1 i ρ_2 są liczbami całkowitemi.

Przeto η_{11}, η_{12} są pierwiastkami równania stopnia drugiego

$$x^2 - \eta_1 x + (\rho_1\eta_1 + \rho_2\eta_2) = 0.$$

A więc η_{11}, η_{12} można obliczyć przez wyciąganie pierwiastka stopnia drugiego, mając już η_1, η_2. Podobnie znajduje się η_{21}, η_{22}.

Teraz widać, jak można dojść stopniowo do obliczenia okresów o liczbie wyrazów $\frac{p-1}{8}$.

Weźmy np. pod uwagę η_{111} i η_{112}; ich suma jest

$$\eta_{111} + \eta_{112} = \eta_{11},$$

a ich iloczyn wyraża się przez połączenie linjowe o spółczynnikach całkowitych wyrażeń η_{11}, η_{12}, η_{21}, η_{22}; tak więc η_{111}, η_{112} otrzymuje się przez wyciągnięcie nowego pierwiastka stopnia drugiego, obejmującego okresy otrzymane przedtym.

Postępując dalej tym samym sposobem, można utworzyć okresy o liczbie wyrazów

$$\frac{p-1}{16}, \quad \frac{p-1}{32}, \ldots,$$

a wreszcie okresy o jednym wyrazie

$$\left(\frac{p-1}{2^n} = 1\right),$$

czyli pierwiastki ε równania danego.

Możemy więc wnioskować: Jeżeli p jest liczbą pierwszą postaci 2^n+1, wtedy równanie

$$\frac{z^p - 1}{z - 1} = 0$$

może być rozwiązane przez kolejne wyciąganie pierwiastków stopnia drugiego, a więc wielokąt foremny o liczbie boków p może być zbudowany linjałem i cyrklem.

Uwaga. W rozumowaniu powyższym nie braliśmy w rachubę dwuznaczności, występującej w wyborze znaków, które trzeba nadawać wprowadzanym stopniowo pierwiastkom stopnia drugiego. Rzeczywiście nie potrzeba się zajmować tą dwuznacznością, jeżeli mamy jedynie na widoku wykazanie, że okresy η mogą być wyrażone za pomocą pierwiastków

stopnia drugiego, że więc dane równanie $\frac{z^p-1}{z-1}=0$ jest rozwiązalne za pomocą takich pierwiastków. Jeżeli, przystępując do istotnego rozwiązania, uwzględnimy dwojakie znaki tych pierwiastków, to znajdziemy wszystkie pierwiastki ε danego równania. Ale gdyby do utworzenia okresu η był z góry dany którykolwiek poszczególny pierwiastek ε, to chcąc obliczyć η trzebaby było stopniowo dobierać znaki w sposób odpowiedni. Odpowiednie reguły, które przytym występują, będą rozważane w przypadku $p=17$ w artykule VI, gdzie nabierają znaczenia przy faktycznym wykreślaniu siedemnastokąta.

§ 8. O liczbach pierwszych postaci 2^n+1. Otrzymane rezultaty uwydatnia uwaga następująca:

Każda liczba pierwsza postaci 2^n+1 jest liczbą postaci $2^{2^\nu}+1$, to znaczy, że jeżeli 2^n+1 jest liczbą pierwszą, to n musi być potęgą dwuch.

Ażeby tego twierdzenia dowieść, wystarczy zauważyć, że jeżeli n ma jakiś dzielnik nieparzysty >1

$$2k+1,$$

a więc

$$n=h(2k+1),$$

wtedy liczba

$$2^n+1=2^{h(2k+1)}+1$$

nie może być liczbą pierwszą.

Łatwo się przekonać, że $2^{h(2k+1)}+1$ nie może być liczbą pierwszą, gdyż jest podzielna przez 2^h+1. W rzeczy samej, dwumian

$$x^{2k+1}+1$$

staje się zerem dla $x=-1$, jest więc podzielny przez $x+1$:

$$x^{2k+1}+1=(x+1)[x^{2k}-x^{2k-1}+\ldots+(-1)^r x^{2k-r}+\ldots+1];$$

jeżeli uczynimy

$$x=2^h,$$

to znajdziemy właśnie, że $2^{h(2k+1)}+1$ jest podzielne przez 2^h+1.

Możemy teraz rezultaty paragrafów poprzednich wypowiedzieć w taki sposób:

Wielokąty foremne, których liczba boków p jest liczbą pierwszą, a które można zbudować linjałem i cyrklem, są to te wielokąty, dla których p ma postać

$$p=2^{2^\nu}+1.$$

Ażeby okazać doniosłość tego rezultatu, przyjmijmy dla ν wielkości

$$\nu = 0,\ 1,\ 2,\ 3,\ 4;$$

otrzymamy wtedy z wzoru

$$p = 2^{2^\nu} + 1$$

liczby pierwsze

$$3,\ 5,\ 17,\ 257,\ 65537.$$

Wartości $p = 3,\ 5$ odpowiadają dobrze znanym przypadkom trójkąta równobocznego i pięciokąta foremnego; natomiast następne wartości prowadzą do trzech nowych wielokątów foremnych, które można zbudować, a między któremi szczególnie godnym uwagi jest przypadek $p = 17$. Rozwiązanie równania dwumiennego $z^{17} = 1$ podał Gauss, a konstrukcjom gieometrycznym siedemnastokąta poświęcono dalsze prace (Legendre, Grunert, Staudt, Serret, Schröter, Gérard), które będą omówione w artykule VI.

Przypadek $p = 257$ badał Richelot*); rezultaty tych badań interpretowali gieometrycznie Affolter i Pascal**).

Przypadek $p = 65537$ był przedmiotem bardzo starannej pracy Hermesa***).

Ale co się stanie, jeżeli $\nu > 4$? Czy otrzyma się jeszcze liczby pierwsze

$$p = 2^{2^\nu} + 1,$$

a więc nowe wielokąty foremne, które możnaby było zbudować?

Przypadki zbadane dotychczas odnoszą się do liczb, odpowiadających

$$\nu = 5,\ 6,\ 7,$$

czyli do liczb

$$2^{2^5} + 1,\ 2^{2^6} + 1,\ 2^{2^7} + 1,$$

które są liczbami złożonemi.

Jest więc jeszcze wątpliwe, czy szereg liczb

$$2^{2^\nu} + 1$$

zawiera inne liczby pierwsze, oprócz tych, które odpowiadają wartościom

$$\nu = 0,\ 1,\ 2,\ 3,\ 4.$$

§ 9. Zastosowanie metody Gaussa do przypadku pięciokąta foremnego. Podamy w końcu, jako przykład, zastosowanie metody wyłożonej do rozwiązania równania

$$z^5 = 1,$$

---

*) Journ. f. Math., Bd. 9 (1832).
**) Rendic. della R. Accademia di Napoli, 1887.
***) Göttinger Nachrichten, 1894.

od którego zależy konstrukcja pięciokąta foremnego.

Pierwiastki tego równania są:

$$1,\ \varepsilon,\ \varepsilon^2,\ \varepsilon^3,\ \varepsilon^4,$$

gdzie

$$\varepsilon = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}.$$

Wybierzmy pierwiastek pierwotny modułu 5, np. $g=2$; wtedy wielkości ε uporządkują się w sposób następujący:

$$\varepsilon^2,\ \varepsilon^4,\ \varepsilon^8=\varepsilon^3,\ \varepsilon^{16}=\varepsilon.$$

Okresy dwumienne są dane przez

$$\eta_1=\varepsilon^2+\varepsilon^3,\ \eta_2=\varepsilon^4+\varepsilon,$$

przyczym:

$$\eta_1+\eta_2=\eta=-1$$

$$\eta_1\eta_2=(\varepsilon^2+\varepsilon^3)(\varepsilon^4+\varepsilon)=\varepsilon^6+\varepsilon^3+\varepsilon^7+\varepsilon^4=\eta=-1,$$

a więc η_1 i η_2 są pierwiastkami równania

$$x^2+x-1=0,$$

czyli

$$\eta_1=-\tfrac{1}{2}\pm\tfrac{1}{2}\sqrt{5}$$

$$\eta_2=-\tfrac{1}{2}\mp\tfrac{1}{2}\sqrt{5}.$$

Rozpatrzmy okresy o jednym wyrazie

$$\eta_{21}=\varepsilon^4,\ \eta_{22}=\varepsilon$$

gdzie

$$\eta_{21}+\eta_{22}=\eta_2$$

$$\eta_{21}\cdot\eta_{22}=\varepsilon^5=1;$$

ułóżmy równanie stopnia drugiego

$$x^2-\eta_2 x+1=0.$$

Rozwiązując to równanie, dostaniemy:

$$\varepsilon=\tfrac{1}{4}\{-1\mp\sqrt{5}\pm\sqrt{-10\pm 2\sqrt{5}}\},$$

czyli

$$\varepsilon=\tfrac{1}{4}\{-1\mp\sqrt{5}\pm i\sqrt{10\mp 2\sqrt{5}}\}.$$

Cztery pierwiastki ε równania dwumiennego otrzymamy z tego wzoru, jeżeli przed pierwiastkami nadamy znaki + i −. Można się przekonać gieometrycznie (w sposób bardzo łatwy), że pierwiastek

$$\varepsilon=\cos\frac{2\pi}{5}+i\sin\frac{2\pi}{5}$$

dostaniemy, przyjmując wszystkie znaki dodatnie, a więc zakładając:

$$\varepsilon = \tfrac{1}{4}\{-1+\sqrt{5}+i\sqrt{10+2\sqrt{5}}\}.$$

Wzór

$$\eta_2 = 2\cos\frac{2\pi}{5} = -(\tfrac{1}{2}+\sqrt{5})$$

prowadzi do bardzo prostej konstrukcji pięciokąta foremnego.

§ 10. Wielokąty foremne o liczbie boków złożonej. Pomówimy teraz o rozwiązalności wielokątów foremnych mających n boków, jeżeli n jest liczbą złożoną. Zauważmy przedewszystkim, że jeżeli n rozkłada się na iloczyn dwuch liczb całkowitych p, q:

$$n = p \cdot q,$$

to mając n-kąt foremny, można odrazu zbudować p-kąt i q-kąt. W rzeczy samej, jeżeli jest dany łuk koła $\frac{2\pi}{n}$ (którego cięciwa jest bokiem n-kąta), lub, jeśli kto woli, jeżeli jest dany odpowiedni kąt środkowy, wtedy, mnożąc go przez q, otrzymamy łuk lub kąt

$$\frac{2\pi q}{n} = \frac{2\pi}{p},$$

za pomocą którego można zbudować p-kąt.

Przypuśćmy teraz, że liczba n została rozłożona na czynniki pierwsze $p_1, p_2, \ldots p_r$, czyli że

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}.$$

Ażeby konstrukcja n-kąta była możliwa, powinna być możliwa konstrukcja wielokątów foremnych o liczbie boków $p_1^{\alpha_1}$, $p_2^{\alpha_2}, \ldots, p_r^{\alpha_r}$.

Konstrukcja wielokąta foremnego o liczbie boków p^α $(\alpha > 1)$ zależy od rozwiązania równania dwumiennego

$$z^{p^\alpha} = 1,$$

które (jak to widać również gieometrycznie) sprawdza się przez wszystkie pierwiastki równania

$$z^{p^{\alpha-1}} = 1.$$

Równanie

$$\frac{z^{p^\alpha}-1}{z^{p^{\alpha-1}}-1} = 0$$

jest nieprzywiedlne.

Tego twierdzenia dowodzi się za pomocą rozumowania Eisensteina, które już stosowaliśmy w przypadku $\alpha = 1$ (§ 5).

Z twierdzenia powyższego wypływa wniosek, że równanie rozpatrywane jest rozwiązalne za pomocą pierwiastków stopnia drugiego tylko wtedy, jeżeli jego stopień $p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$ jest potęgą liczby 2. Ale liczba $p^{\alpha-1}$, jeżeli $\alpha > 1$, nie może być potęgą dwuch, o ile nie jest $p=2$.

Stąd widzimy, że żaden wielokąt foremny o liczbie boków p^α nie da się wykreślić, jeżeli

$$\alpha > 1, \quad p > 2.$$

Jeżeli więc n-kąt foremny może być zbudowany, to liczba

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$$

musi zawierać, oprócz pewnej potęgi liczby 2, tylko czynniki pierwsze różne od siebie (podniesione do potęgi 1), a każdy z tych czynników p musi mieć postać $2^{2^\nu}+1$, tak że wielokąt foremny o liczbie boków p powinien się dać zbudować (§ 8); ostatecznie więc liczba n powinna mieć postać

$$n = 2^\nu (2^{2^{\nu_1}}+1)(2^{2^{\nu_2}}+1)\dots(2^{2^{\nu_s}}+1),$$

gdzie $\nu_1, \nu_2, \dots \nu_s$ są wszystkie od siebie różne, a

$$p_1 = 2^{2^{\nu_1}}+1, \quad p_2 = 2^{2^{\nu_2}}+1, \dots$$

są liczbami pierwszemi.

Dowiedziemy wreszcie, że jeżeli n jest liczbą tej postaci, to konstrukcja n-kąta foremnego jest wykonalna.

W tym celu wystarczy okazać, jak „mając wielokąty foremne o liczbie boków r, s, jeżeli r, s są liczbami pierwszemi względem siebie, można zbudować wielokąt foremny o liczbie boków $n = rs$".

Jeżeli są dane wielokąty foremne o liczbie boków r i s, to są dane odpowiednie kąty środkowe

$$a = \frac{2\pi}{r}, \quad b = \frac{2\pi}{s}.$$

Jeżeli r i s są liczbami pierwszemi względem siebie, to można rozwiązać równanie nieoznaczone

$$sx - ry = 1,$$

znajdując dwie liczby całkowite x, y które mu czynią zadość; będziemy mieli

$$ax - by = 2\pi\left(\frac{x}{r} - \frac{y}{s}\right) = \frac{2\pi}{rs} = \frac{2\pi}{n},$$

a więc otrzymamy konstrukcję kąta środkowego n-kąta (a przeto i konstrukcję samego n-kąta), tworząc różnicę kątów ax i by.

Jako przykład rozpatrzymy przypadek piętnastokąta foremnego

($n=15$), którego konstrukcję można wyprowadzić z konstrukcji trójkąta równobocznego i pięciokąta foremnego. Rozwiążmy równanie nieoznaczone

$$3x-5y=1,$$

czyniąc

$$x=2,\ y=1.$$

Kąt środkowy piętnastokąta buduje się więc, tworząc różnicę pomiędzy podwójnym kątem środkowym pięciokąta i kątem środkowym trójkąta foremnego

$$\frac{2\pi}{15}=2\cdot\frac{2\pi}{5}-\frac{2\pi}{3}.$$

Ta konstrukcja nie różni się istotnie od konstrukcji Euklidesa, w której kąt

$$\frac{2\pi}{3}-\frac{2\pi}{5}=\frac{4\pi}{15}$$

dzieli się na dwie części równe.

Streszczając wreszcie osiągnięte rezultaty, możemy wypowiedzieć twierdzenie:

n-kąty foremne, dające się zbudować linjałem i cyrklem, są to te wszystkie, ale tylko te, dla których liczba n, rozłożona na czynniki pierwsze, ma postać

$$n=2^{\nu}.(2^{2^{\nu_1}}+1).(2^{2^{\nu_2}}+1)\ldots(2^{2^{\nu_s}}+1),$$

gdzie $\nu_1, \nu_2, \ldots, \nu_s$ są od siebie różne.

§ 11. Uwagi o wyznaczaniu wielokątów foremnych, których konstrukcja nie jest wykonalna elementarnie. Zakończymy ten artykuł niektóremi uwagami o wyznaczaniu wielokątów foremnych, których konstrukcja nie da się wykonać linjałem i cyrklem. Zwracając się do najprostszego przypadku wielokąta foremnego o liczbie boków p, gdzie p jest liczbą pierwszą, objaśnimy na przykładzie, czego nas uczy w tym względzie metoda Gaussa rozwiązywania równań dwumiennych

$$z^p=1.$$

Załóżmy więc $p=7$ i rozpatrzmy pierwiastki równania $z^7=1$ (opuszczając $z=1$):

$$\varepsilon,\ \varepsilon^2,\ \varepsilon^3,\ \varepsilon^4,\ \varepsilon^5,\ \varepsilon^6$$

gdzie

$$\varepsilon=\cos\frac{2\pi\nu}{7}+i\sin\frac{2\pi\nu}{7}.$$

Wybierzmy pierwiastek pierwotny modułu 7; niech będzie $g=3$. Dzięki temu możemy uporządkować pierwiastki ε w sposób następujący:

$$\varepsilon^3,\ \varepsilon^{3^2}=\varepsilon^2,\ \varepsilon^{3^3}=\varepsilon^6,\ \varepsilon^{3^4}=\varepsilon^4,\ \varepsilon^{3^5}=\varepsilon^5,\ \varepsilon^{3^6}=\varepsilon.$$

Utwórzmy okresy o trzech wyrazach

$$\eta_1=\varepsilon^3+\varepsilon^{3^3}+\varepsilon^{3^5}=\varepsilon^3+\varepsilon^6+\varepsilon^5$$

$$\eta_2=\varepsilon^{3^2}+\varepsilon^{3^4}+\varepsilon^{3^6}=\varepsilon^2+\varepsilon^4+\varepsilon;$$

dostaniemy wtedy:

$$\eta_1+\eta_2=\eta=-1$$

$$\eta_1\eta_2=(\varepsilon^3+\varepsilon^6+\varepsilon^5)(\varepsilon^2+\varepsilon^4+\varepsilon)=\varepsilon^5+\varepsilon^7+\varepsilon^4+\varepsilon^8+\varepsilon^{10}+\varepsilon^7+\varepsilon^7+\varepsilon^9+\varepsilon^6=\eta+3=2,$$

a więc η_1, η_2 czynią zadość równaniu stopnia drugiego

$$x^2+x+2=0.$$

Jeżeli η_1, η_2 zostaną obliczone, to wyznaczenie pierwiastków ε zależeć będzie od równania stopnia trzeciego; w rzeczy samej, mamy np.

$$\varepsilon^2+\varepsilon^4+\varepsilon=\eta_2$$

$$\varepsilon^2.\varepsilon^4+\varepsilon^2.\varepsilon+\varepsilon^4.\varepsilon=\eta_1$$

$$\varepsilon^2.\varepsilon^4.\varepsilon=1,$$

a więc ε^2, ε^4, ε są pierwiastkami równania

$$x^3-\eta_2x^2+\eta_1x-1=0.$$

Od wykonania tej redukcji zależy możność sprowadzenia konstrukcji siedmiokąta foremnego do podziału kąta na trzy części równe (por. art. VII).

Zadanie ogólne równania dwumiennego $z^p=1$, gdzie p jest jakąkolwiek liczbą pierwszą, pozwala zawsze na redukcję (jak dla $p=7$), gdyż może być sprowadzone do rozwiązania szeregu równań stopnia niższego. Jeżeli $p-1$, rozłożone na czynniki pierwsze, ma postać

$$p-1=2^{\alpha_1}.3^{\alpha_2}.5^{\alpha_3}\ldots,$$

wtedy trzeba będzie rozwiązać kolejno

α_1 równań stopnia 2-go

α_2 równań stopnia 3-go

α_3 równań stopnia 5-go it. d.

Taką redukcję umożliwia metoda Gaussa, prowadząca do kolejnego tworzenia okresów o liczbie wyrazów

$$\frac{p-1}{2},\ \frac{p-1}{4},\ \ldots\ \frac{p-1}{2^{\alpha_1}},$$

następnie do okresów o liczbie wyrazów

$$\frac{p-1}{2^{\alpha_1}.3}, \cdots \frac{p-1}{2^{\alpha_1}.3^{\alpha_2}},$$

do okresów o liczbie wyrazów

$$\frac{p-1}{2^{\alpha_1}.3^{\alpha_2}.5}, \cdots \frac{p-1}{2^{\alpha_1}.3^{\alpha_2}.5^{\alpha_3}} \text{ i t. d.*)}$$

Ze stanowiska gieometrycznego zajmują nas pierwsze przypadki, w których $p-1$ ma jedynie czynniki pierwsze równe 2 i 3, gdyż wtedy można podać proste konstrukcje p-kąta, odwołując się do przyrządu, dzielącego kąty na trzy części równe (trysektor), albo do paraboli stałej; za pomocą tych środków, w połączeniu z linjałem i cyrklem, można rozwiązywać wszystkie zadania stopnia trzeciego (por. art. VII).

Ograniczymy się tutaj do przytoczenia następujących prac, roztrząsających najprostsze przypadki: dla $p=7$, 13, 97 E. Pascal, Giornale di Matematiche di Battaglini, vol. XXV; dla $p=19$, 37 U. Amaldi, tamże, vol. XXX.

*) Por. Bachmann l. c., Bianchi l. c., gdzie też są podane wzory, służące do faktycznego rozwiązania.