CZĘŚĆ II

ZASTOSOWANIE DO RÓWNAŃ ALGEBRAICZNYCH

§ 11. Redukcja grupy G przy rozszerzaniu ciała K.

Zasadniczy wynik teorii, wyłożonej w Części I, może być krótko scharakteryzowany, jak następuje: korzystając z pojęcia grupy Galois, przeprowadziliśmy klasyfikację wszystkich ciał zawartych w Σ i zawierających K. Klasyfikacja ta ma doniosłe znaczenie dla problemu rozwiązywania równań. Rozwiązywanie ich polega bowiem na kolejnych rozszerzeniach ciała K, doprowadzających wreszcie do ciała Σ lub do jeszcze obszerniejszego ciała (por. § 5 Rozdziału XIII, str. 235). Jest więc rzeczą naturalną rozważyć, jak zmienią się własności równania $f(x)=0$, gdy ciało K rozszerzymy do jednego z ciał Δ_H, i jakie równanie należy rozwiązać, aby otrzymać liczbę, której dołączenie do K daje ciało Δ_H.

Odpowiedź na pierwsze pytanie daje

Twierdzenie 20. *Jeśli Θ jest liczbą ciała Σ, to grupą równania $f(x)=0$ w ciele $K(\Theta)$ jest H_Θ.*

Dowód. Niech G' oznacza grupę równania $f(x)=0$ w ciele $K(\Theta)$. Jest to więc grupa tych podstawień pierwiastków $x_1,x_2,\ldots,x_n$, względem których niezmiennicze są wszystkie relacje wymierne w $K(\Theta)$.

Z § 5 (lemat 3, str. 384) wiemy, że Θ może być przedstawione jako wielomian względem $x_1,x_2,\ldots,x_n$ o współczynnikach należących do K:

$$\Theta = W(x_1,x_2,\ldots,x_n).$$

Związek ten jest pewną relacją między $x_1,x_2,\ldots,x_n$, wymierną w $K(\Theta)$. Dla każdego podstawienia π z grupy G' musi być zatem $\Theta = W(\pi(x_1),\pi(x_2),\ldots,\pi(x_n))$, t. j. $\pi(\Theta)=\Theta$. Grupa G' jest więc zawarta w H_Θ.

Na odwrót, każda relacja wymierna w $K(\Theta)$, zachodząca między $x_1,x_2,\ldots,x_n$, ma postać $V(\Theta,x_1,x_2,\ldots,x_n)=0$, gdzie V jest symbolem wielomianu o współczynnikach z K. Dla każdego podstawienia π, należącego do grupy H_Θ, mamy zatem (por. twierdzenie 3):

$$V(\Theta,\pi(x_1),\pi(x_2),\ldots,\pi(x_n))=0,$$

co dowodzi, że π należy do G'. Grupy G' i H_Θ są więc równe, c. b. d. o.

Twierdzenie 20 wyrażamy krótko, mówiąc, że dołączenie do K liczby Θ powoduje *redukcję* grupy G do grupy H_Θ.

PRZYKŁADY. 1. Jeśli $f(x)=0$ jest równaniem stopnia 3, którego grupa zawiera wszystkie podstawienia liczb x_1,x_2,x_3, to dołączenie któregokolwiek pierwiastka równania

$$a_0^4t^2 = a_1^2a_2^2 + 18a_0a_1a_2a_3 - 4a_0a_2^3 - 4a_1^3a_3 - 27a_0^2a_3^2$$

powoduje redukcję grupy G do grupy C (por. § 7, str. 390, przykład). W § 18 poznamy sposób rozwiązywania równań o grupie G cyklicznej.

2. Załóżmy, że $f(x)=0$ jest równaniem stopnia 4, nieprzywiedlnym w K, i dołączmy do K trzy pierwiastki:

$$\Theta_1 = x_1x_2 + x_3x_4, \quad \Theta_2 = x_1x_4 + x_2x_3, \quad \Theta_3 = x_1x_3 + x_2x_4$$

równania $F(t)=0$ (por. § 6, str. 387, przykład). Grupa równania $f(x)=0$ w ciele $K(\Theta_1)$ pokrywa się z grupą G_8 lub z jedną z jej podgrup. Dołączenie Θ_2 powoduje redukcję grupy do

$$V = \{1, (x_1,x_2)(x_3,x_4), (x_1,x_3)(x_2,x_4), (x_1,x_4)(x_2,x_3)\},$$

ewentualnie do jednej z jej podgrup, gdyż spośród permutacyj grupy G_8 tylko permutacje należące do V przekształcają Θ_2 w siebie. Dołączenie Θ_3 nie powoduje już dalszej redukcji, gdyż suma $\Theta_1+\Theta_2+\Theta_3$ należy do K.

Grupa V nazywa się *grupą czwórkową*.

Sposób rozwiązywania równań o grupie czwórkowej podamy w § 14 (przykład 3, str. 407-408).

ĆWICZENIA. 1. Jeżeli D oznacza wyróżnik wielomianu $f(x)$, to dołączenie któregokolwiek pierwiastka kwadratowego z D do ciała K powoduje redukcję G do podgrupy podstawień parzystych zawartych w G.

2. Jeśli wszystkie podstawienia grupy H_Θ przekształcają x_1 w siebie, to x_1 wyraża się wymiernie przez Θ.

3. Znaleźć grupę równania $x^4+x^3+x^2+x+1=0$ w ciele $\mathcal{R}(\sqrt{5})$, gdzie $\mathcal{R}$ oznacza ciało liczb wymiernych.

[Oprzeć się na równości $e^{\frac{2\pi i}{5}} + e^{-\frac{2\pi i}{5}} = \frac{1}{2}(-1+\sqrt{5})$].

§ 12. Grupa równania, któremu czyni zadość Θ.

Twierdzenie 20 przynosi korzyść w rozwiązywaniu równania $f(x)=0$ tylko wtedy, gdy wyznaczenie liczby Θ jest łatwiejsze niż rozwiązanie tego równania. Zbadamy zatem, jaka jest grupa równania nieprzywiedlnego w K, któremu czyni zadość Θ (por. § 7, str. 389, twierdzenie 11).

Twierdzenie 21. *Grupa G^* nieprzywiedlnego w ciele K równania $P(t)=0$, którego pierwiastkiem jest liczba Θ należąca do ciała Σ, jest homomorficzna z G.*

Jądrem J tego homomorfizmu [1]) *jest część wspólna wszystkich grup sprzężonych z H_Θ; grupy G^* i G/J są więc izomorficzne.*

Dowód. Pierwiastkami równania $P(t)=0$ są liczby:

$$\Theta_1=\pi_1(\Theta),\quad \Theta_2=\pi_2(\Theta),\quad \ldots,\quad \Theta_k=\pi_k(\Theta),$$

sprzężone z Θ. Oznaczmy przez Δ ciało $K(\Theta_1,\Theta_2,\ldots,\Theta_k)$ i niech Z będzie liczbą pierwotną ciała Δ. W § 5 udowodniliśmy (lemat 3, str. 384), że Z może być przedstawione w postaci wielomianu względem $\Theta_1,\Theta_2,\ldots,\Theta_k$ o współczynnikach z K:

$$Z=R(\Theta_1,\Theta_2,\ldots,\Theta_k).$$

Ponieważ liczby $\Theta_1,\Theta_2,\ldots,\Theta_k$ należą do ciała Σ, więc i Z należy do tego ciała. Dla każdego podstawienia π z grupy G jest zatem określona liczba

$$\pi(Z)=R(\pi(\Theta_1),\pi(\Theta_2),\ldots,\pi(\Theta_k)),$$

sprzężona z Z w ciele K. Z drugiej strony każde podstawienie

$$\sigma=\begin{pmatrix}\Theta_1, & \Theta_2, & \ldots, & \Theta_k\\ \Theta_{\alpha_1}, & \Theta_{\alpha_2}, & \ldots, & \Theta_{\alpha_k}\end{pmatrix}$$

powoduje przejście liczby Z na liczbę sprzężoną z nią w ciele Δ:

$$\sigma(Z)=R(\Theta_{\alpha_1},\Theta_{\alpha_2},\ldots,\Theta_{\alpha_k}).$$

Aby zrozumieć dalsze rozumowanie, należy dobrze rozróżniać znaczenie symbolu $\pi(Z)$, gdzie π jest podstawieniem pierwiastków $x_1,x_2,\ldots,x_n$, od znaczenia symbolu $\sigma(Z)$, gdzie σ jest podstawieniem pierwiastków $\Theta_1,\Theta_2,\ldots,\Theta_k$. Podstawienia pierwiastków $x_1,x_2,\ldots,x_n$ oznaczać będziemy literami π, ϱ, ν, opatrując je ewentualnie wskaźnikami, podstawienia zaś liczb $\Theta_1,\Theta_2,\ldots,\Theta_k$ oznaczać będziemy literą σ, ewentualnie również ze wskaźnikami.

[1]) *Jądrem* homomorfizmu grupy G z grupą G^* nazywamy zbiór tych elementów grupy G, którym przyporządkowana jest jedność grupy G^*.

Załóżmy, że grupa G^* równania $P(t)=0$ w ciele K składa się z podstawień $\sigma_1,\sigma_2,\ldots,\sigma_l$. W myśl twierdzenia 12 iloczyn

$$[t-\sigma_1(Z)]\,[t-\sigma_2(Z)]\ldots[t-\sigma_l(Z)] \tag{12}$$

jest wielomianem nieprzywiedlnym w K o współczynnikach należących do K, równym 0 dla $t=Z$.

Oznaczmy przez N grupę tych podstawień π, należących do G, dla których $\pi(Z)=Z$ (grupę symetrii liczby Z). Zgodnie z twierdzeniem 11 możemy powiedzieć, że jeśli $G=\varrho_1N+\varrho_2N+\ldots+\varrho_hN$ oznacza rozkład G na warstwy względem N, to iloczyn

$$[t-\varrho_1(Z)]\,[t-\varrho_2(Z)]\ldots[t-\varrho_h(Z)] \tag{13}$$

jest wielomianem nieprzywiedlnym w K o współczynnikach należących do K, równym 0 dla $t=Z$. Wielomiany (12) i (13) są zatem identyczne.

Wnosimy stąd przede wszystkim, że $l=h$. Elementowi π grupy G przyporządkować teraz możemy element σ_π grupy G^* w następujący sposób: istnieje dokładnie jedno takie $j\leqslant h$, że π należy do kompleksu ϱ_jN; za σ_π przyjmiemy to z podstawień σ_i $(i=1,2,\ldots,h)$, dla którego $\sigma_i(Z)=\varrho_j(Z)$. Każdemu podstawieniu π grupy G odpowiada więc dokładnie jedno podstawienie σ_π grupy G^* i przy tym każde σ należące do grupy G^* jest przyporządkowane co najmniej jednemu π należącemu do grupy G. Jeśli π należy do kompleksu ϱ_jN, to istnieje w N takie podstawienie ν, że $\pi=\varrho_j\nu$, skąd wynika, że $\pi(Z)=\varrho_j(\nu(Z))=\varrho_j(Z)=\sigma_\pi(Z)$. Dla każdego podstawienia π należącego do G mamy więc

$$\pi(Z)=\sigma_\pi(Z). \tag{14}$$

Wykażemy, że przyporządkowanie $\pi\to\sigma_\pi$ ustala homomorfizm grup G i G^*, t. j. że $\sigma_{\pi_1}\cdot\sigma_{\pi_2}=\sigma_{\pi_1\pi_2}$.

Istotnie, z (14) wynika, że $\sigma_{\pi_2}(Z)=\pi_2(Z)$; oznaczmy tę liczbę przez Z':

$$Z'=\pi_2(Z)=\sigma_{\pi_2}(Z).$$

Z' jest liczbą ciała Δ, może więc być przedstawione jako wielomian względem Z o współczynnikach należących do K:

$$Z'=W(Z) \tag{15}$$

(por. twierdzenie 15). Wzór (15) przedstawia pewną zależność wymierną w K, zachodzącą między pierwiastkami $\Theta_1,\Theta_2,\ldots,\Theta_k$. W myśl więc definicji grupy G^* związek (15) musi być niezmienniczy względem podstawienia σ_{π_1}:

$$\sigma_{\pi_1}(Z')=W(\sigma_{\pi_1}(Z)). \tag{16}$$

Wzór (15) przedstawia jednak także pewną zależność wymierną w K, zachodzącą między pierwiastkami $x_1,x_2,\ldots,x_n$, gdyż liczby Z' i Z należą do ciała Σ. Wnosimy stąd, że

$$\pi_1(Z')=W(\pi_1(Z)). \tag{17}$$

Z (14) wynika, że $\pi_1(Z)=\sigma_{\pi_1}(Z)$. Wzory (16) i (17) dają zatem $\sigma_{\pi_1}(Z')=\pi_1(Z')$, a więc $\sigma_{\pi_1}(\sigma_{\pi_2}(Z))=\pi_1(\pi_2(Z))$, czyli $\sigma_{\pi_1}\sigma_{\pi_2}(Z)=\pi_1\pi_2(Z)=\sigma_{\pi_1\pi_2}(Z)$, co możemy jeszcze napisać w postaci $\sigma^{-1}_{\pi_1\pi_2}\sigma_{\pi_1}\sigma_{\pi_2}(Z)=Z$. Ponieważ Z jest liczbą pierwotną ciała Δ, więc równość ta daje $\sigma^{-1}_{\pi_1\pi_2}\cdot\sigma_{\pi_1}\cdot\sigma_{\pi_2}=1$, t. j. $\sigma_{\pi_1}\sigma_{\pi_2}=\sigma_{\pi_1\pi_2}$. Grupy G i G^* są więc homomorficzne.

Wyznaczymy jeszcze jądro J tego homomorfizmu czyli zbiór tych π grupy G, dla których $\sigma_\pi=1$.

Warunek ten jest równoważny równości $\sigma_\pi(Z)=Z$, t. j. $\pi(Z)=Z$, i zachodzi napewno, jeżeli $\pi(\Theta_1)=\Theta_1,\pi(\Theta_2)=\Theta_2,\ldots,\pi(\Theta_k)=\Theta_k$. Na odwrót, jeśli choć jedna z równości $\pi(\Theta_j)=\Theta_j$ nie zachodzi, to podstawienie σ_π nie jest tożsamościowe i $\sigma_\pi(Z)\neq Z$. Na to więc, aby π należało do jądra J, potrzeba i wystarcza, by zachodziły równości:

$$\pi(\Theta_1)=\Theta_1,\quad \pi(\Theta_2)=\Theta_2,\quad \ldots,\quad \pi(\Theta_k)=\Theta_k,$$

t. j. by π należało do grupy symetrii każdej z liczb $\Theta_1,\Theta_2,\ldots,\Theta_k$. Jak wiemy (ob. § 3, ćwiczenie 1) grupą symetrii liczby $\Theta_j=\pi_j(\Theta)$ sprzężonej z Θ jest grupa $\pi_jH_\Theta\pi_j^{-1}$ sprzężona z H_Θ. Jądro J jest więc częścią wspólną wszystkich grup, sprzężonych z H_Θ, c. b. d. o.

Z twierdzenia 21 widoczne jest, że szczególną rolę odgrywają liczby Θ ciała Σ, dla których grupa H_Θ pokrywa się ze swymi grupami sprzężonymi czyli jest dzielnikiem normalnym.

Liczby takie nazywamy *normalnymi* w ciele K, a odpowiadające im równania $P(t)=0$ *równaniami normalnymi* lub *równaniami Galois*.

ĆWICZENIA. 1. Liczba Θ jest normalna w K wtedy i tylko wtedy, gdy każda liczba z nią sprzężona wyraża się jako wielomian $W(\Theta)$ względem Θ o współczynnikach należących do K.

[Grupą symetrii liczby $W(\Theta)$ jest H_Θ na mocy twierdzenia 2. Na odwrót, jeśli $\pi H_{\pi(\Theta)}\pi^{-1}=H_{\pi(\Theta)}$, to $\pi(\Theta)$ ma grupę symetrii H_Θ i wyraża się jako wielomian względem Θ na mocy twierdzenia 14].

2. Równanie $x^{p-1}+x^{p-2}+\ldots+x+1=0$, gdzie p jest liczbą pierwszą, jest normalne w ciele $\mathcal{R}$ liczb wymiernych.

[Jeśli ε jest jednym z pierwiastków, to pozostałymi są potęgi ε].

3. Równanie $x^3-2=0$ nie jest normalne w $\mathcal{R}$, ale jest normalne w ciele $\mathcal{R}(\sqrt{-3})$.

[Pierwiastki zespolone nie wyrażają się w postaci $W(\sqrt[3]{2})$. W ciele $\mathcal{R}(\sqrt{-3})$ mamy dla $x_1=\sqrt[3]{2}$ równości $x_2=\frac{1}{2}(-1-\sqrt{-3})x_1$ i $x_3=\frac{1}{2}(-1+\sqrt{-3})x_1$].

§ 13. Sprowadzenie równania $f(x)=0$ do równań prostych. Możemy teraz wyjaśnić bliżej znaczenie grupy Galois dla problemu rozwiązywania równań. Twierdzenie 21 pokazuje, że dla wyznaczenia liczby Θ ciała Σ musimy rozwiązać równanie $P(t)=0$, którego grupa jest izomorficzna z G/J. Z twierdzenia 20 widzimy, że po znalezieniu liczby Θ rozwiązanie równania $f(x)=0$ sprowadza się do rozwiązania równania o grupie H_Θ. Ostatecznie więc rozwiązanie równania $f(x)=0$ sprowadza się do rozwiązania układu dwu równań, których grupy są izomorficzne z H_Θ i z G/J.

Jeżeli J nie jest grupą jednostkową, to G/J ma mniej elementów niż G. Rozwiązanie równania, którego grupa jest izomorficzna z G/J, jest więc problemem prostszym niż rozwiązanie równania $f(x)=0$.

Takie sprowadzenie równania $f(x)=0$ do układu dwu równań o grupach prostszych jest możliwe zawsze, gdy grupa G zawiera dzielnik normalny N różny od G i od grupy jednostkowej. Za Θ możemy wtedy obrać liczbę, której grupą symetrii jest N, i rozwiązanie równania $f(x)=0$ sprowadzi się do rozwiązania układu dwu równań, których grupy są izomorficzne z G/N i N.

Grupę G, która nie posiada żadnego dzielnika normalnego różnego od G i od grupy jednostkowej, nazywamy *prostą*.

Można udowodnić, że *jeśli N jest maksymalnym dzielnikiem normalnym grupy G*, t. zn. takim, który nie jest zawarty w żadnym różnym od G dzielniku normalnym, *to grupa G/N jest prosta* (por. dalej str. 405, ćwiczenie 1).

Opierając się na tym twierdzeniu, możemy sprowadzić w następujący sposób równanie $f(x)=0$ do ciągu równań o grupach prostych.

Niech G_1 oznacza którykolwiek z maksymalnych dzielników normalnych grupy G, zaś Θ_1 — liczbę, dla której G_1 jest grupą symetrii. Dla znalezienia liczby Θ_1 rozwiązać musimy równanie, którego grupa jest izomorficzna z G/G_1; w ciele $K(\Theta_1)$ równanie $f(x)=0$ ma grupę G_1. Oznaczamy przez G_2 którykolwiek z maksymalnych dzielników normalnych grupy G_1, a przez Θ_2 liczbę, dla której G_2 jest grupą symetrii. Dla znalezienia Θ_2 rozwiązać musimy równanie, którego grupa w ciele $K(\Theta_1)$ jest izomorficzna z G_1/G_2; grupa równania $f(x)=0$ w ciele $K(\Theta_1,\Theta_2)$ jest równa G_2. Postępując tak dalej, dojdziemy do ciągu zstępującego grup, zakończonego grupą jednostkową:

$$G_0=G, \quad G_1, \quad G_2, \quad \ldots, \quad G_k, \tag{18}$$

i ciągu wstępującego ciał:

$$K, \quad K(\Theta_1), \quad K(\Theta_1,\Theta_2), \quad \ldots, \quad K(\Theta_1,\Theta_2,\ldots,\Theta_k),$$

o następujących własnościach:

1° każda z grup ciągu (18) jest maksymalnym dzielnikiem normalnym poprzedzającej;

2° Θ_l jest pierwiastkiem równania $P_l(t)=0$, nieprzywiedlnego w ciele $K(\Theta_1,\Theta_2,\ldots,\Theta_{l-1})$ i którego grupa w tym ciele jest izomorficzna z G_l/G_{l-1};

3° grupą równania $f(x)=0$ w ciele $K(\Theta_1,\Theta_2,\ldots,\Theta_l)$ jest G_l $(l=1,2,\ldots,k)$.

Z własności 3° wynika, że grupa równania $f(x)=0$ w ciele $K(\Theta_1,\Theta_2,\ldots,\Theta_k)$ jest grupą jednostkową. Wszystkie pierwiastki $x_1,x_2,\ldots,x_n$ leżą więc w ciele $K(\Theta_1,\Theta_2,\ldots,\Theta_k)$ (por. § 11, ćwiczenie 2), co moglibyśmy wyrazić równością $K(\Theta_1,\Theta_2,\ldots,\Theta_k)=\Sigma$. Po rozwiązaniu równań

$$P_1(t)=0, \quad P_2(t)=0, \quad \ldots, \quad P_k(t)=0$$

znalezienie pierwiastków $x_1,x_2,\ldots,x_n$ wymaga już tylko operacyj wymiernych.

W ten sposób sprowadziliśmy rozwiązanie równania $f(x)=0$ do rozwiązania układu k równań o grupach prostych.

Wynik ten posiada dla Algebry doniosłe znaczenie. Okazuje się, że istotną trudność przy rozwiązywaniu sprawiają tylko równania o grupach prostych; dalsze badania algebraiczne powinny więc iść w kierunku badania i klasyfikowania równań o takich grupach.

Wspomnimy tu jeszcze bez dowodu o pewnym wyniku, związanym z wyżej teorią:

Ciąg (18) o własności 1° nazywa się *ciągiem składaniowym* grupy G.

Grupa może mieć kilka ciągów składaniowych, jeśli jednak $G_0,G_1',G_2',\ldots,G_l'$ jest drugim, różnym od (18), ciągiem składaniowym grupy G, to $l=k$ i ciągi grup ilorazowych:

$$G_0/G_1, \quad G_1/G_2, \quad G_2/G_3, \quad \ldots, \quad G_{k-1}/G_k,$$
$$G_0'/G_1', \quad G_1'/G_2', \quad G_2'/G_3', \quad \ldots, \quad G_{k-1}'/G_k'$$

różnią się co najwyżej porządkiem (o ile grupy izomorficzne będziemy uważali za identyczne).

Jest to t. zw. *twierdzenie Jordana-Höldera*[1]).

Zauważmy jeszcze, że G_{l+1} jest dzielnikiem normalnym grupy G_l, ale nie jest na ogół dzielnikiem normalnym grupy G.

ĆWICZENIA. 1. Jeżeli grupa G jest homomorficzna z G^* i N^* jest dzielnikiem normalnym grupy G^*, to zbiór N tych elementów grupy G, które przy homomorfizmie przechodzą na elementy grupy N^*, jest dzielnikiem normalnym grupy G.

2. Podać ciągi składaniowe grupy wszystkich podstawień 4 przedmiotów.

[Jeśli S_4 oznacza grupę symetryczną, A_4 — naprzemienną i V — grupę czwórkową, to każdy ciąg składaniowy grupy S_4 ma postać:

$$S_4, \quad A_4, \quad V, \quad C, \quad \{1\},$$

gdzie C oznacza jedną z podgrup rzędu 2 grupy V].

3. Grupa cykliczna jest prosta wtedy i tylko wtedy, gdy jej rząd jest liczbą pierwszą.

[Jeśli rząd grupy jest liczbą pierwszą, to nie ma ona żadnej podgrupy właściwej poza jednostkową. Jeśli $G=\{1,\pi,\pi^2,\ldots,\pi^m\}$ i $m+1=e\cdot f$, to grupa $\{1,\pi^e,\pi^{2e},\ldots,\pi^{(f-1)e}\}$ tworzy dzielnik normalny G].

4. Grupa cykliczna G rzędu $2m$ posiada dzielnik normalny rzędu m. Wywnioskować stąd, że grupa cykliczna rzędu 2^m posiada ciąg składaniowy, którego wszystkie grupy ilorazowe są rzędu 2.

§ 14. Przykłady. 1. Niech $f(x)=x^6+x^5+x^4+x^3+x^2+x+1$ i niech ciało K będzie ciałem $\mathcal{R}$ liczb wymiernych. Jeśli ε jest jednym z pierwiastków, to pozostałe są potęgami ε. Wyznaczymy grupę G tego równania. Ponieważ wielomian $f(x)$ jest nieprzywiedlny w $\mathcal{R}$, więc G jest grupą przechodnią. Niech π_l oznacza którekolwiek podstawienie należące do G i takie, że $\pi_l(\varepsilon)=\varepsilon^l$ $(l=1,2,3,4,5,6)$. Istnieje dokładnie jedno takie podstawienie π_l, gdyż z $\pi_l(\varepsilon)=\varepsilon^l$ wynika, że $\pi_l(\varepsilon^j)=[\pi_l(\varepsilon)]^j=\varepsilon^{lj}$, co dowodzi, że warunek $\pi(\varepsilon)=\varepsilon^l$ wy-

[1]) Dowód tego twierdzenia znaleźć można w każdym obszerniejszym kursie Algebry (por. np. cytowaną na str. 375 książkę van der Waerdena, str. 152).

znacza całkowicie podstawienie π. Grupa G składa się więc z sześciu podstawień: $\pi_1, \pi_2, \pi_3, \pi_4, \pi_5, \pi_6$. Prawo mnożenia tych podstawień odczytujemy ze wzoru $\pi_i(\pi_j(\varepsilon)) = \pi_i(\varepsilon^j) = \varepsilon^{ij} = \pi_{ij}(\varepsilon)$, przy czym iloczyn ij należy zredukować modulo 7. Grupa G jest więc izomorficzna z grupą utworzoną z liczb $1, 2, 3, 4, 5, 6$, której działaniem jest mnożenie zredukowane modulo 7. Grupa ta jest cykliczna. Wiadomo bowiem z Teorii liczb, że istnieje *pierwiastek pierwotny kongruencji* $x^6 \equiv 1 \pmod 7$, t. zn. liczba g taka, że każda z liczb $1, 2, \ldots, 6$ przystaje według modułu 7 do dokładnie jednej z potęg $g, g^2, \ldots, g^6$. Liczby $1, 2, 3, \ldots, 6$ można więc przedstawić jako reszty z dzielenia potęg $g, g^2, \ldots, g^6$ przez 7, skąd wynika, że grupa G jest izomorficzna z grupą cykliczną $\{g, g^2, \ldots, g^6\}$, w której działaniem jest zwykłe mnożenie z tym, że wykładniki potęg są zredukowane modulo 6 (za g przyjąć można 3).

Grupa G ma dwa dzielniki normalne, różne od G i od grupy jednostkowej; odpowiadają one dzielnikom $\{g^3, g^6\}$ i $\{g^2, g^4, g^6\}$ grupy $\{g, g^2, \ldots, g^6\}$ (por. § 13, ćwiczenie 3). Są to więc dzielniki:

$$N_1 = \{1, \pi_6\} \quad \text{i} \quad N_2 = \{1, \pi_2, \pi_4\},$$

gdyż $3^3 \equiv 6 \pmod 7$, $3^2 \equiv 2 \pmod 7$ i $3^4 \equiv 4 \pmod 7$.

Grupa G/N_1 jest izomorficzna z grupą cykliczną rzędu 3, zaś G/N_2 — z grupą cykliczną rzędu 2. Ciągami składaniowymi grupy G są ciągi:

$$G,\ N_1,\ \{1\}, \qquad G,\ N_2,\ \{1\}.$$

Obu tym ciągom odpowiadają dwa różne sposoby rozwiązania równania $f(x) = 0$.

Jeśli wychodzimy z ciągu G, N_1, $\{1\}$, to szukać musimy liczby Θ, dla której N_1 jest grupą symetrii. Liczbą taką jest np. $\Theta = \varepsilon + \varepsilon^6$, gdyż $\pi_6(\Theta) = \pi_6(\varepsilon) + \pi_6(\varepsilon^6) = \varepsilon^6 + \varepsilon^{36} = \varepsilon^6 + \varepsilon$. Sprzężonymi z Θ są liczby $\pi_2(\Theta) = \varepsilon^2 + \varepsilon^5$ i $\pi_3(\varepsilon) = \varepsilon^3 + \varepsilon^4$. Wynika stąd, że Θ jest pierwiastkiem równania

$$[t - (\varepsilon + \varepsilon^6)]\,[t - (\varepsilon^2 + \varepsilon^5)][t - (\varepsilon^3 + \varepsilon^4)] = 0,$$

czyli po pomnożeniu (w myśl tożsamości $\varepsilon + \varepsilon^2 + \ldots + \varepsilon^6 = -1$):

$$P_1(t) = t^3 + t^2 - 2t - 1 = 0.$$

Równanie to jest normalne, gdyż pierwiastki $\varepsilon^2 + \varepsilon^5$ i $\varepsilon^3 + \varepsilon^4$ wyrażają się przez $\Theta = \varepsilon + \varepsilon^6$ wzorami $\varepsilon^2 + \varepsilon^5 = \Theta^2 - 2$ i $\varepsilon^3 + \varepsilon^4 = 1 - \Theta - \Theta^2$; podobnie można wyrazić każde dwa pierwiastki jako wielomiany względem trzeciego.

Równanie $P_1(t) = 0$ rozwiązać możemy np. wzorami Cardano (Rozdział X, § 3, str. 177). Dołączmy pierwiastek Θ tego równania do ciała $\mathcal{R}$. Grupa G redukuje się w ciele $\mathcal{R}(\Theta)$ do $N_1 = \{1, \pi_6\} = \{1, (\varepsilon, \varepsilon^6)(\varepsilon^2, \varepsilon^5)(\varepsilon^3, \varepsilon^4)\}$. Grupa ta jest nieprzechodnia, wielomian $f(x) = 0$ musi więc być przywiedlny w ciele $R(\Theta)$. Istotnie:

$$f(x) = [(x - \varepsilon)(x - \varepsilon^6)][(x - \varepsilon^2)(x - \varepsilon^5)][(x - \varepsilon^3)(x - \varepsilon^4)] =$$
$$= (x^2 - \Theta x + 1)[x^2 - (\Theta^2 - 2)x + 1][x^2 - (1 - \Theta - \Theta^2)x + 1].$$

Pierwiastki równania $f(x) = 0$ uzyskujemy teraz przez rozwiązanie układu trzech równań kwadratowych. Warto przy tym zaznaczyć, że taki sam będzie rozkład wielomianu $f(x)$ w ciałach $\mathcal{R}(\Theta_1)$ i $\mathcal{R}(\Theta_2)$, gdzie Θ_1 i Θ_2 oznaczają pozostałe dwa pierwiastki równania $P_1(t) = 0$, gdyż Θ wyraża się wymiernie zarówno przez Θ_1 jak przez Θ_2.

Jeżeli wychodzimy z ciągu składaniowego $G, N_2, \{1\}$, to szukamy najpierw liczby Z, dla której N_2 jest grupą symetrii. Liczbą taką jest $Z = \varepsilon + \varepsilon^2 + \varepsilon^4$, liczbą sprzężoną z Z jest $\pi_3(Z) = \varepsilon^3 + \varepsilon^6 + \varepsilon^5 = -Z - 1$. Równanie $P_2(t) = 0$, któremu czyni zadość Z jest

$$([t - (\varepsilon + \varepsilon^2 + \varepsilon^4)][t - (\varepsilon^3 + \varepsilon^5 + \varepsilon^6)] = 0,$$

czyli $t^2 + t + 2 = 0$, skąd dla Z wynika jedna z dwu wartości $\frac{1}{2}[-1 \mp \sqrt{-7}]$. Dołączmy Z do ciała $\mathcal{R}$; w nowym ciele grupą równania $f(x) = 0$ jest

$$N_2 = \{1, \pi_2, \pi_4\} = \{1, (\varepsilon, \varepsilon^2, \varepsilon^4)(\varepsilon^3, \varepsilon^6, \varepsilon^5), (\varepsilon, \varepsilon^4, \varepsilon^2)(\varepsilon^3, \varepsilon^5, \varepsilon^6)\}.$$

Ponieważ grupa N_2 nie jest przechodnia, więc wielomian $f(x)$ musi być przywiedlny w ciele $\mathcal{R}(Z)$. Istotnie:

$$f(x) = [(x - \varepsilon)(x - \varepsilon^2)(x - \varepsilon^4)][(x - \varepsilon^3)(x - \varepsilon^5)(x - \varepsilon^6)] =$$
$$= [x^3 - Zx^2 - (Z+1)x - 1][x^3 + (Z+1)x^2 + Zx - 1].$$

Pierwiastki równania $f(x) = 0$ otrzymamy teraz, rozwiązując układ dwu równań stopnia 3.

2. Zupełnie podobne stosunki napotykamy przy dyskusji równań podziału koła $x^{p-1} + x^{p-2} + \ldots + x + 1 = 0$, gdzie p jest liczbą pierwszą. Grupa G takiego równania jest izomorficzna z grupą utworzoną z liczb $1, 2, \ldots, p-1$, której działaniem jest mnożenie zredukowane modulo p. Jest to grupa cykliczna, gdyż jest izomorficzna z grupą $\{g, g^2, \ldots, g^{p-1}\}$, gdzie g jest pierwiastkiem pierwotnym kongruencji $x^{p-1} \equiv 1 \pmod p$, przy czym działaniem grupowym jest mnożenie, a wykładniki potęg są zredukowane modulo $p-1$. Jeżeli $p - 1 = e \cdot f$, to grupa G ma dzielnik normalny N, odpowiadający grupie $\{g^e, g^{2e}, \ldots, g^{(f-1)e}, g^{fe}\}$; liczbą o grupie symetrii N jest

$$\eta = \varepsilon^{g^e} + \varepsilon^{g^{2e}} + \ldots + \varepsilon^{g^{fe}}.$$

Jest to t.zw. *f-członowy okres Gaussa*.

Gauss podał wzory, pozwalające wyznaczyć równanie, którego pierwiastkiem jest η [1]).

3. Rozpatrzymy tu jeszcze równania stopnia 4 o grupie czwórkowej.

Załóżmy, że $f(x)$ jest wielomianem stopnia 4 nieprzywiedlnym w K i że grupą równania $f(x) = 0$ w K jest V (por. § 11, przykład 2). Wynika stąd, że liczby

$$\Theta_1 = x_1x_2 + x_3x_4, \qquad \Theta_2 = x_1x_4 + x_2x_3, \qquad \Theta_3 = x_1x_3 + x_2x_4$$

[1]) Zob. np. książkę van der Waerdena cytowaną na str. 375, § 54, lub Czebotarewa, cytowaną na str. 395, Wydanie 1, Rozdział III, § 2.

należą do K. Grupa V ma ciąg składaniowy $V, C, \{1\}$, gdzie

$$C=\{1,(x_1,x_2)(x_3,x_4)\}.$$

Jeśli więc dołączymy do K liczbę, dla której C jest grupą symetrii, to grupa równania zredukuje się do C i równanie $f(x)=0$ będzie przywiedlne w nowym ciele. Za taką liczbę obrać możemy np. $Z=x_1+x_2$. Liczba ta jest pierwiastkiem równania

$$a_0t^2+a_1t+a_2-a_0\Theta_1=0.$$

Aby znaleźć rozkład wielomianu $f(x)$ w ciele $K(Z)$, opieramy się na tożsamościach:

$$x_3+x_4=-\frac{a_1}{a_0}-Z,$$

$$x_1x_2=\frac{a_0Z\Theta_1+a_3}{2a_0Z+a_1}, \qquad x_3x_4=\frac{a_1(2a_0Z+a_1)}{(a_0Z\Theta_1+a_3)a_0}$$

i otrzymujemy

$$f(x)=a_0[(x-x_1)(x-x_2)][(x-x_3)(x-x_4)]=$$

$$=a_0\left(x^2-Zx+\frac{a_0Z\Theta_1+a_3}{2a_0Z+a_1}\right)\left(x^2+\frac{a_0Z+a_1}{a_0}x+\frac{a_1(2a_0Z+a_1)}{(a_0Z\Theta_1+a_3)a_0}\right).$$

Równanie $f(x)=0$ rozwiążemy teraz, rozwiązując układ dwu równań kwadratowych.

Wyłożona tu teoria (wraz z § 11, przykład 2) pozwala rozwiązać każde równanie stopnia 4.

ĆWICZENIA. 1. Równanie $x^{10}+x^9+x^8+\ldots+x+1=0$ rozkłada się w ciele $\mathcal{R}(\sqrt{-11})$ na iloczyn

$$\left(x^5+\frac{1+\sqrt{-11}}{2}x^4-x^3+x^2+\frac{-1+\sqrt{-11}}{2}x-1\right)\cdot$$

$$\cdot\left(x^5+\frac{1-\sqrt{-11}}{2}x^4-x^3+x^2-\frac{1+\sqrt{-11}}{2}x-1\right)=0.$$

Grupa każdego z równań stojących w nawiasach jest w ciele $\mathcal{R}(\sqrt{-11})$ cykliczna rzędu 5.

2. Rozwiązać równanie

$$x^{12}+x^{11}+x^{10}+\ldots+x+1=0.$$

[Rozwiązanie sprowadza się do rozwiązania układu dwu równań kwadratowych i jednego równania sześciennego, gdyż $12=2\cdot2\cdot3$].

3. Jeśli $2^m+1=p$ jest liczbą pierwszą, to równanie

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

można rozwiązać przez pierwiastniki kwadratowe.

4. Wyróżnik równania $x^{p-1}+x^{p-2}+\ldots+x+1=0$ jest równy

$$(-1)^{\frac{p(p-1)}{2}}p^{p-2}.$$

[Oznaczając lewą stronę równania przez $f(x)$, mamy $D=(-1)^{\frac{p(p-1)}{2}}\prod_{j=1}^{p-1}f'(x_j)$. Ponieważ $f(x)=\frac{x^p-1}{x-1}$, więc $f'(x)=\frac{(p-1)x^p-px^{p-1}+1}{(x-1)^2}$. Wobec $x_j^p=1$ otrzymamy stąd $f'(x_j)=p\frac{1-x_j^{p-1}}{(1-x_j)^2}$, a ponieważ liczby $x_1^{p-1}, x_2^{p-1}, \ldots, x_{p-1}^{p-1}$ różnią się co najwyżej porządkiem od $x_1, x_2, \ldots, x_{p-1}$, więc

$$D=(-1)^{\frac{p(p-1)}{2}}\cdot p^{p-1}\cdot\frac{1}{(1-x_1)(1-x_2)\ldots(1-x_{p-1})}=$$

$$=(-1)^{\frac{p(p-1)}{2}}\cdot p^{p-1}\cdot\frac{1}{f(1)}=(-1)^{\frac{p(p-1)}{2}}\cdot p^{p-2}].$$

§ 15. Prostota grupy naprzemiennej. Z teorii wyłożonej w § 13 wynika, że w Algebrze doniosłą rolę grają grupy proste, t. j. takie, które nie mają żadnego dzielnika normalnego różnego od całej grupy i grupy jednostkowej. Ważnego przykładu grup prostych dostarcza

Twierdzenie 22. *Grupa naprzemienna stopnia n, t. j. grupa wszystkich podstawień parzystych n przedmiotów, jest prosta, o ile $n\neq4$.*

Dowód. Możemy założyć, że permutowanymi przedmiotami są liczby $1,2,\ldots,n$ i że $n>4$, gdyż przypadek $n=3$ nie sprawia trudności. Oznaczmy przez A_n grupę naprzemienną stopnia n, a przez N jakikolwiek jej dzielnik normalny różny od grupy jednostkowej. Dla każdego τ należącego do N oznaczmy przez f_τ ilość tych $x\leqslant n$, dla których $\tau(x)=x$. Wzór $f_\tau=n$ oznacza zatem, że $\tau=1$. Niech π oznacza którekolwiek z należących do N podstawień, dla którego f_π ma możliwie największą wartość, ale jest różne od n.

(i) *Cykle, na które rozkłada się π, są równej długości.*

Istotnie, jeśli k jest ilością cyfr w najkrótszym cyklu podstawienia π, to $f_{\pi^k}>f_\pi$, a więc $\pi^k=1$, t. zn. że każdy cykl podstawienia π ma k cyfr.

(ii) *Każdy cykl podstawienia π ma co najwyżej 3 cyfry.*

Istotnie, przypuśćmy, że π zawiera cykl a-cyfrowy $(u_1,u_2,\ldots,u_a)$, gdzie $a\geqslant3$. Ponieważ N jest dzielnikiem normalnym grupy A_n, a (u_1,u_2,u_a) należy do A_n, więc A_n zawiera podstawienia $\tau=(u_1,u_a,u_2)\,\pi(u_1,u_2,u_a)$ oraz $\sigma=\tau^{-1}\pi$. Jest jasne, że z $\pi(x)=x$ wynika $\tau(x)=x$, a więc też $\sigma(x)=x$, co dowodzi, że $f_\sigma\geqslant f_\pi$. Ponieważ zaś $\sigma(u_a)=u_a$, więc $f_\sigma>f_\pi$, skąd $\sigma=1$, czyli $\pi=\tau$. Ponieważ $\tau(u_2)=u_a$, więc cykl $(u_1,u_2,\ldots,u_a)$ sprowadza się do (u_1,u_2,u_a), czyli $a=3$.

(iii) *π jest albo cyklem trójczłonowym, albo iloczynem dwu cyklów dwuczłonowych.*

Istotnie, przypuśćmy, że cykle podstawienia π są trójczłonowe i że jest ich co najmniej 2. Niech to będą cykle (a,b,c), (d,e,f), ... Ponieważ podstawienie $\tau=(a,d)(b,e)$ jest parzyste, więc $\tau^{-1}\pi\tau$ należy do N; iloczyn $\pi^{-1}\tau^{-1}\pi\tau=\sigma$ też należy zatem do N. Ale $\sigma(a)=a$, a ponadto z $\pi(x)=x$ wynika $\sigma(x)=x$, co dowodzi, że $f_\sigma>f_\pi$, a więc $\sigma=1$. Wynik ten nie jest możliwy, gdyż $\sigma(c)=f$.

Jeśli cykle podstawienia π są dwuczłonowe i jest ich więcej niż 2, to musi ich być co najmniej 4, gdyż podstawienie π jest parzyste. Przypuśćmy, że są to cykle (a,b), (c,d), (e,f) i (g,h). Przyjmując znów $\tau=(a,d)(b,e)$, wnosimy jak poprzednio, że permutacja $\sigma=\pi^{-1}\tau^{-1}\pi\tau$ należy do N, co nie jest możliwe, gdyż $\sigma(g)=g$ a $\sigma(a)=d$.

Dotychczas nie czyniliśmy użytku z założenia, że $n>4$. Opierając się na nim, możemy wykazać, że

(iv) *π jest cyklem trójczłonowym.*

Gdyby bowiem było $\pi=(a,b)(c,d)$, to oznaczając przez e którąkolwiek z liczb $1,2,\ldots,n$ różną od a,b,c,d i przyjmując $\tau=(a,e)(c,d)$, wywnioskowalibyśmy, że podstawienie $\sigma=\pi\tau^{-1}\pi\tau=(a,b,e)$ należy do N, mimo że $f_\sigma>f_\pi$ i $\sigma\neq 1$.

Udowodnimy dalej, że

(v) *N zawiera wszystkie cykle trójczłonowe.*

Zgodnie z (iv) wystarczy w tym celu pokazać, że jeśli N zawiera cykl (a,b,c), to zawiera też cykle (a,b,d), (a,d,c) i (d,b,c), gdzie d jest dowolną liczbą różną od a,b i c. Z założenia wynika, że N zawiera każde podstawienie postaci $\tau^{-1}(a,b,c)\tau$, gdzie τ jest podstawieniem parzystym. Przyjmując tu kolejno $\tau=(c,e,d)$, (b,e,d), (a,e,d) przy czym e oznacza dowolną liczbę różną od a,b,c i d, otrzymamy żądany wynik.

Z (v) wynika łatwo, że N zawiera wszystkie podstawienia parzyste. Istotnie:

$$(p,q)(p,r)=(p,r,q) \quad \text{i} \quad (p,q)(r,s)=(r,p,s)(r,p,q).$$

N zawiera więc iloczyn dowolnych dwu transpozycyj, zatem także iloczyn dowolnej parzystej ich liczby, t. zn. każde podstawienie parzyste. Każdy dzielnik normalny grupy A_n różny od grupy jednostkowej jest więc równy A_n, t. zn. że grupa A_n jest prosta, c. b. d. o.

Ze względu na duże znaczenie grup prostych poświęcono im wiele uwagi. Stwierdzono, że poza grupami A_n (dla $n\neq 4$) i grupami cyklicznymi, których rząd jest liczbą pierwszą (por. § 13, ćwiczenie 3), istnieje nieskończenie wiele grup prostych. Wśród grup rzędu poniżej 1000 występują tylko 3 takie grupy: są one rzędów 167, 504 i 660. Pierwsza z nich ma znaczenie w teorii równań stopnia 7 [1]).

Z twierdzenia 22 wynika jako łatwy wniosek

Twierdzenie 23. *Jedynym dzielnikiem normalnym grupy symetrycznej S_n (gdzie $n\neq 4$), różnym od S_n i od grupy jednostkowej, jest grupa naprzemienna A_n.*

Dowód. Niech N oznacza dzielnik normalny grupy S_n, różny od S_n i od grupy jednostkowej. Część wspólna N i A_n jest oczywiście dzielnikiem normalnym A_n. Zgodnie z twierdzeniem 22 zajść więc musi jedna z następujących możliwości:

[1]) Zob. R. Fricke, *Lehrbuch der Algebra*, Tom 2, Brunświk 1926, str. 211 i nast. Tablicę znanych dotąd 53 niecyklicznych grup prostych, których rząd nie przekracza 1000000, podaje L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, Lipsk 1901, str. 309.

1° N zawiera wszystkie podstawienia parzyste;

2° N nie zawiera żadnego podstawienia parzystego.

W przypadku 1° jest $N=A_n$ lub $N=S_n$ w zależności od tego, czy N nie zawiera żadnego podstawienia nieparzystego, czy zawiera choć jedno takie podstawienie.

W przypadku 2° N zawierać może tylko jedno podstawienie i to podstawienie rzędu 2, gdyż iloczyn dwu podstawień nieparzystych jest parzysty. N ma więc postać $\{1,(u_1,u_2)(u_3,u_4)\ldots\}$, przy czym ilość cykli (u_l,u_{l+1}) jest nieparzysta. Stwierdzamy od razu, że grupa taka nie jest dzielnikiem normalnym grupy S_n; przypadek 2° jest więc niemożliwy.

ĆWICZENIA. 1. Wykazać, że jeśli $n=4$, to podstawienie π, o którym mowa w dowodzie twierdzenia 22, może być iloczynem dwu cykli dwucyfrowych i że N jest wtedy grupą czwórkową.

2. Podać elementy różnych rzędów grupy A_5 i zbadać, które z nich są z sobą sprzężone.

[Grupa ta zawiera 1 element rzędu 1, 15 podstawień rzędu 2 postaci $(i,j)(k,l)$, 20 podstawień rzędu 3 postaci (i,j,k) i 24 podstawienia rzędu 5 postaci (i,j,k,l,m). Wszystkie podstawienia rzędu 2 i wszystkie podstawienia rzędu 3 są między sobą sprzężone; podstawienia rzędu 5 rozpadają się na dwie klasy po 12 elementów i tylko podstawienia należące do tej samej klasy są z sobą sprzężone].

3. Udowodnić, że grupa A_5 jest prosta, opierając się na wynikach ćwiczenia 2.

[Jeśli dzielnik normalny N zawiera choć jedno podstawienie rzędu 2, to zawiera ich 15, jeśli zawiera choć jedno podstawienie rzędu 3, to zawiera ich 20 i jeśli zawiera choć jedno podstawienie rzędu 5, to zawiera ich 12 lub 24. Ponieważ N musi zawierać podstawienie tożsamościowe, więc rząd N może być tylko jedną z liczb 1, $1+15$, $1+20$, $1+12$, $1+24$, $1+15+20$, $1+15+12$, $1+15+24$, $1+20+12$, $1+20+24$, $1+15+20+12$ i $1+15+20+24$. Możliwe są tylko przypadki pierwszy i ostatni, gdyż rząd N musi być dzielnikiem liczby 60].

§ 16. Niewymierności naturalne i uboczne.

W rozważaniach, dotyczących rozwiązania równania $f(x)=0$, liczby ciała K nazywamy nieraz *wymiernymi*.

Liczby nie należące do K nazywamy *niewymiernościami*.

Niewymierności Θ należące do ciała Σ, t. j. dające się przedstawić jako wielomiany względem $x_1,x_2,\ldots,x_n$ o współczynnikach z K, nazywamy *niewymiernościami naturalnymi*.

Inne niewymierności nazywamy *ubocznymi*.

Podział liczb na wymierne, niewymierności naturalne i uboczne zależy oczywiście od ciała K.

W § 11 zbadaliśmy, jaki wpływ na grupę równania $f(x)=0$ wywiera rozszerzenie ciała K przez dołączenie niewymierności naturalnej. Zbadamy obecnie, jaki wpływ wywiera dołączenie do K dowolnej niewymierności.

Twierdzenie 24. *Jeśli A jest ciałem, zawierającym K, to grupa G^* równania $f(x)=0$ w ciele A jest podgrupą grupy G.*

Dołączenie do K dowolnej niewymierności naturalnej Θ, dla której G^* jest grupą symetrii, powoduje redukcję grupy równania $f(x)=0$ do G^*.

Każda liczba Θ o wymienionej własności należy przy tym do A.

Dowód. Grupa G^* równania $f(x)=0$ w ciele A jest podgrupą grupy G (por. § 2, ćwiczenie 2). Jeśli Θ jest liczbą, której grupą symetrii jest G^*, to w myśl twierdzenia 20 grupa równania $f(x)=0$ w ciele $K(\Theta)$ jest równa G^*, co dowodzi pierwszej części twierdzenia 24.

Dla dowodu drugiej jego części załóżmy, że Θ jest niewymiernością naturalną, której grupą symetrii jest G^*. Liczba Θ jest zatem funkcją wymierną pierwiastków $x_1, x_2, \ldots, x_n$, nie zmieniającą swej wartości przy podstawieniach grupy Galois równania $f(x)=0$ w ciele A. W myśl twierdzenia 8 Θ należy do A, c. b. d. o.

Zgodnie z udowodnionym twierdzeniem 24 *każda możliwa redukcja grupy G może być uzyskana przez dołączenie niewymierności naturalnej.*

Wynik ten nosi nazwę *twierdzenia Kroneckera.*

Dokładniejsze wyniki uzyskać można w przypadku, gdy A powstaje z K przez dołączenie liczby, algebraicznej względem K.

Twierdzenie 25. *Jeśli λ jest liczbą algebraiczną względem K stopnia q, to stopień s każdej takiej niewymierności naturalnej Θ, że grupy równania $f(x)=0$ w ciałach $K(\Theta)$ i $K(\lambda)$ są identyczne, jest dzielnikiem stopnia q. Na to, żeby λ było niewymiernością naturalną, potrzeba i wystarcza, by $s=q$.*

Dowód. Jeśli grupa równania $f(x)=0$ w ciele $K(\Theta)$ jest równa grupie tego równania w $K(\lambda)$, to Θ należy do $K(\lambda)$ (twierdzenie 24), a więc stopień Θ jest dzielnikiem stopnia λ (por. § 10, wniosek 2). Jeśli $s=q$, to $K(\Theta)=K(\lambda)$ (§ 10, wniosek 3), a więc λ jest niewymiernością naturalną. Na odwrót, jeśli λ jest niewymiernością naturalną, to grupy symetrii liczb λ i Θ są równe (twierdzenie 20), a więc $s=q$ (twierdzenie 13).

Jako łatwy wniosek otrzymujemy

Twierdzenie 26. *Jeśli λ jest liczbą algebraiczną, której stopień q jest liczbą pierwszą, i grupa G^* równania $f(x)=0$ w ciele $K(\lambda)$ jest różna od G, to λ jest niewymiernością naturalną.*

Dowód. Istotnie, z twierdzeń 24 i 25 wynika, że wskaźnik grupy G^* w G jest dzielnikiem stopnia liczby λ, a więc może być równy 1 lub q. Pierwszy przypadek jest niemożliwy wobec $G^* \neq G$; wskaźnik G^* w G jest więc równy q. Wnosimy stąd, że jeśli Θ jest niewymiernością naturalną o grupie symetrii G^*, to stopień Θ jest równy q (por. twierdzenie 13), a więc λ jest niewymiernością naturalną na mocy twierdzenia 25.

Jeżeli λ jest niewymiernością naturalną, to umiemy wyznaczyć grupę Γ równania $F(x)=0$ nieprzywiedlnego w K, któremu czyni zadość λ (zob. twierdzenie 21). W przypadku, gdy λ jest niewymiernością dowolną, można wypowiedzieć tylko takie twierdzenie: Grupa Γ zawiera dzielnik normalny Γ_1, zaś grupa G — dzielnik normalny G_1 taki, że grupy Γ/Γ_1 i G/G_1 są izomorficzne. G_1 oznacza przy tym grupę, do jakiej redukuje się G przez dołączenie do K wszystkich pierwiastków równania $F(x)=0$, zaś Γ_1 — grupę, do jakiej redukuje się Γ przez dołączenie do K wszystkich pierwiastków równania $f(x)=0$ [1]).

Jeśli λ jest niewymiernością naturalną, to Γ_1 jest grupą jednostkową i twierdzenie powyższe pokrywa się z twierdzeniem 21.

ĆWICZENIA. 1. Jeśli K jest ciałem $\mathcal{R}$ liczb wymiernych, to liczba $\lambda=(1+i):\sqrt{2}$ jest niewymiernością uboczną dla równania x^2+1.

[λ jest jedną z wartości $\sqrt{i}$. W ciele $\mathcal{R}(\lambda)$ grupa równania $x^2+1=0$ jest jednostkowa, tak samo jak w ciele $\mathcal{R}(i)$; λ jest liczbą algebraiczną stopnia 4, a i — stopnia 2].

2. Jeśli K jest ciałem $\mathcal{R}$ liczb wymiernych, to liczba $\theta=\sqrt[3]{2}$ jest niewymiernością naturalną dla równania $x^3-2=0$, a $\lambda=\sqrt[6]{2}$ — niewymiernością uboczną.

§ 17. Równania czyste.

Końcowe §§ poświęcimy zastosowaniu Teorii Galois do rozwiązywania równań przy pomocy pierwiastników. Problem ten był, jak wiadomo, przez wiele stuleci centralnym zagadnieniem Algebry. Teoria Galois stworzona została w związku z tym właśnie zagadnieniem i przyniosła ostateczne jego rozwiązanie.

---

[1]) Fakt, że rzędy grup Γ/Γ_1 i G/G_1 są równe, odkrył C. Jordan, *Traité des substitutions*, Paryż 1870, str. 268. Izomorfizm grup Γ/Γ_1 i G/G_1 wykazał O. Hölder, Mathematische Annalen, Tom 34 (1889), str. 47. Prosty dowód znaleźć można w książce: G. A. Miller, H. F. Blichfeldt i L. E. Dickson, *Theory and Applications of Finite Groups*, New York 1916, § 167.

W § 19 podamy kryteria rozwiązalności przez pierwiastniki, w § 20 zajmować się będziemy rozwiązalnością przez pierwiastniki kwadratowe, a w § 21 — przez pierwiastniki rzeczywiste. Niezbędnym przygotowaniem jest teoria równań czystych i cyklicznych, którą podajemy w niniejszym § 17 i w § 18.

Równaniem czystym w ciele K nazywamy równanie postaci $x^m - a = 0$, gdzie a jest liczbą należącą do ciała K.

Twierdzenie 27. *Jeśli p jest liczbą pierwszą i ciało K zawiera p-te pierwiastki z jedności oraz a nie jest p-tą potęgą żadnej liczby należącej do K, to grupa G równania $x^p - a = 0$ w ciele K jest cykliczna rzędu p.*

Dowód. Niech $\varepsilon = e^{2\pi i/p}$ i niech Θ_0 oznacza jakikolwiek pierwiastek równania $x^p - a = 0$. Pozostałymi jego pierwiastkami są liczby

$$\Theta_1 = \varepsilon\Theta_0, \quad \Theta_2 = \varepsilon^2\Theta_0, \quad \ldots, \quad \Theta_{p-1} = \varepsilon^{p-1}\Theta_0.$$

Ponieważ wielomian $x^p - a$ jest nieprzywiedlny w K (por. Rozdział XIII, § 3, str. 229, twierdzenie 7), więc grupa G jest przechodnia, zawiera zatem dla każdego $k = 0,1,2,\ldots,p-1$ co najmniej jedno takie podstawienie π_k, że $\pi_k(\Theta_0) = \Theta_k$. Warunek ten wyznacza całkowicie podstawienie π_k, gdyż wynika zeń, iż

$$\pi_k(\Theta_j) = \pi_k(\varepsilon^j\Theta_0) = \varepsilon^j\pi_k(\Theta_0) = \varepsilon^j\Theta_k = \varepsilon^{j+k}\Theta_0.$$

Grupa G składa się więc z p podstawień $\pi_0, \pi_1, \ldots, \pi_{p-1}$, czyli jest rzędu p. Ponieważ p jest liczbą pierwszą, więc wynika stąd, że G jest grupą cykliczną, c. b. d. o.

Jeśli ciało K nie zawiera pierwiastków stopnia p z jedności, to grupa równania $x^p - a = 0$ nie jest cykliczna (por. podane dalej ćwiczenia 3, 4 i 5).

Znaczenie równań czystych pochodzi stąd, że przy ich pomocy określa się rozwiązalność równań przez pierwiastniki.

Mówimy mianowicie, że równanie $f(x) = 0$ jest *w ciele K rozwiązalne przez pierwiastniki stopnia co najwyżej m*, jeśli istnieje ciąg wstępujący ciał

$$K, \quad K(\Theta_1), \quad K(\Theta_1,\Theta_2), \quad \ldots, \quad K(\Theta_1,\Theta_2,\ldots,\Theta_k)$$

o następujących własnościach:

1° Ciało $K(\Theta_1,\Theta_2,\ldots,\Theta_l)$ powstaje z ciała $K(\Theta_1,\Theta_2,\ldots,\Theta_{l-1})$ przez dołączenie pierwiastka Θ_l równania czystego $x^{p_l} - a_l = 0$, nieprzywiedlnego w ciele $K(\Theta_1,\Theta_2,\ldots,\Theta_{l-1})$ i którego stopień p_l jest liczbą pierwszą nie większą od m, wyraz zaś wolny a_l należy do ciała $K(\Theta_1,\Theta_2,\ldots,\Theta_{l-1})$;

2° Wszystkie pierwiastki równania $f(x) = 0$ należą do ciała $K(\Theta_1,\Theta_2,\ldots,\Theta_k)$.

Można wykazać, że *jeśli wielomian $f(x)$ jest nieprzywiedlny w K i choć jeden pierwiastek równania $f(x) = 0$ należy do ciała $K(\Theta_1,\Theta_2,\ldots,\Theta_k)$, to wszystkie pierwiastki równania $f(x) = 0$ należą do tego ciała.*

Jest to t. zw. *twierdzenie Abela*, którego dowodzić tu nie będziemy [1]).

ĆWICZENIA. 1. Udowodnić, że w definicji rozwiązalności przez pierwiastniki można we własności 1° pominąć warunek, że p_l jest liczbą pierwszą. [Por. Rozdział XIII, § 5, str. 235].

2. Jeśli równanie $f(x) = 0$ jest rozwiązalne przez pierwiastniki stopnia co najwyżej m w $K(\Theta)$, gdzie Θ oznacza pierwiastek równania rozwiązalnego w K przez pierwiastniki stopnia co najwyżej q, to równanie $f(x) = 0$ jest rozwiązalne w K przez pierwiastniki stopnia co najwyżej $\max(m,q)$.

3. Jeśli grupa równania czystego $x^p - a = 0$, nieprzywiedlnego w ciele K, jest cykliczna, to K zawiera pierwiastki stopnia p z jedności.

[Przypuśćmy, że G składa się z potęg permutacji π. Gdyby π nie składało się z jednego cyklu, zawierającego wszystkie pierwiastki, to grupa G nie byłaby przechodnią. Zatem $\pi = (x_{k_1}, x_{k_2}, \ldots, x_{k_p})$, gdzie $k_1\, k_2 \ldots k_p$ jest permutacją liczb $1,2,\ldots,p$. Możemy przyjąć $k_1 = 1$ i $k_2 = 2$, gdyż zamiast permutacji π można rozpatrywać odpowiednią potęgę tej permutacji. Niech $\varepsilon = x_2 : x_1$ oraz $x_j = \varepsilon^{j-1}x_1$. Z zależności $x_{k_j} = (x_2/x_1)^{k_j - 1} \cdot x_1$ wynika $\pi(x_{k_j}) = \left[\frac{\pi(x_2)}{\pi(x_1)}\right]^{k_j - 1} \cdot \pi(x_1)$ czyli

$$\varepsilon^{k_{j+1}-1} = \varepsilon^{(k_3-2)(k_j-1)+1} \quad \text{i} \quad k_{j+1} - 1 \equiv (k_3-2)(k_j-1)+1 \pmod p.$$

Pisząc tę kongruencję dla dwu kolejnych wartości j i odejmując, otrzymamy $k_{j+1} - k_j \equiv (k_3-2)(k_j - k_{j-1}) \pmod p$, skąd indukcyjnie

$$k_{j+1} - k_1 \equiv (k_3-2)^{j-1} \pmod p,$$

a więc

$$k_{j+1} - k_1 = (k_{j+1} - k_j) + (k_j - k_{j-1}) + \ldots + (k_2 - k_1) \equiv \sum_{\nu=0}^{j-1} (k_3-2)^\nu \pmod p.$$

Wzór ten jest słuszny dla dowolnego $j \geqslant 1$ z tym, że $k_{j+p} = k_j$. Jeśli $k_3 \neq 3$, to otrzymamy stąd $k_{j+1} \equiv \frac{(k_3-2)^j - 1}{k_3 - 3} + 1 \pmod p$, a więc dla $j = p$ otrzymamy kongruencję $\frac{(k_3-2)^p - 1}{k_3 - 3} \equiv 0 \pmod p$. Ale $(k_3-2)^p \equiv (k_3-2) \pmod p$, otrzymujemy zatem $\frac{k_3 - 3}{k_3 - 3} \equiv 0 \pmod p$ czyli $1 \equiv 0 \pmod p$, co nie jest możliwe. Zatem $k_3 = 3$ i $k_{j+1} - k_1 = j$, t. zn. $k_{j+1} = j+1$ i $\pi = (x_1, x_2, \ldots, x_p)$. Wnosimy stąd, że iloraz $\frac{x_2}{x_1} = \varepsilon$ należy do K, gdyż $\pi\left(\frac{x_2}{x_1}\right) = \frac{x_3}{x_2} = \frac{x_2}{x_1}$].

[1]) Zob. np. B. L. van der Waerden, *Moderne Algebra*, § 56.

4. Jeśli K nie zawiera pierwiastków p-tego stopnia z jedności, to grupa nieprzywiedlnego równania czystego jest izomorficzna z pewną podgrupą pełnej grupy metacyklicznej stopnia p (zob. § 1, str. 372, przykład 3).

[Jeśli $\pi(x_1)=x_a$ i $\pi(x_2)=x_b$, to

$$\pi(x_m)=\pi\left(\left(\frac{x_2}{x_1}\right)^{m-1}x_1\right)=\left(\frac{\pi(x_2)}{\pi(x_1)}\right)^{m-1}\pi(x_1)=\left(\frac{x_b}{x_a}\right)^{m-1}x_a=\varepsilon^{(b-a)(m-1)+a-1}\cdot x_1.$$

Podstawieniu π odpowiada więc podstawienie

$$m'\equiv(b-a)(m-1)+a-1 \pmod p$$

należące do pełnej grupy metacyklicznej. Sprawdzamy z łatwością, że przyporządkowanie to jest izomorfizmem].

5. Jeśli K jest ciałem $\mathcal{R}$ liczb wymiernych, to grupa G nieprzywiedlnego równania czystego $x^p-a=0$ w ciele $\mathcal{R}$ jest izomorficzna z całą pełną grupą metacykliczną.

[Wystarczy udowodnić, że rząd G równa się $p(p-1)$. W ciele $\mathcal{R}(e^{\frac{2\pi i}{p}})$ grupa G redukuje się do grupy cyklicznej rzędu p, rząd G jest więc podzielny przez p. W ciele $\mathcal{R}(x_1)$ wielomian x^p-a rozkłada się na iloczyn $(x-x_1)\cdot x_1^{p-1}\cdot g(t)$, gdzie $t=x:x_1$ i $g(t)=t^{p-1}+t^{p-2}+\ldots+t+1$. W ciele $\mathcal{R}$ grupą równania $g(t)=0$ jest grupa cykliczna rzędu $p-1$ (por. § 14, przykład 2). Gdyby dołączenie x_1 redukowało tę grupę, to x_1 byłoby niewymiernością naturalną (twierdzenie 26), a więc stopień x_1 byłby dzielnikiem $p-1$, co jest niedorzeczne. Zatem grupa równania $g(t)=0$ w ciele $\mathcal{R}(x_1)$ ma rząd $p-1$ i taki sam jest rząd grupy równania $x^p-a=0$ w ciele $\mathcal{R}(x_1)$. Rząd G jest więc podzielny przez $p-1$, a zatem wynosi co najmniej $p(p-1)$. Z twierdzenia, dowiedzionego w ćwiczeniu 4, wynika z drugiej strony, że rząd grupy G nie przekracza $p(p-1)$].

§ 18. Równania cykliczne.

Równanie $f(x)=0$ nazywa się *cykliczne* w ciele K, jeśli jego grupa w K jest cykliczna.

PRZYKŁADY. 1. Równania stopnia 3, których wyróżnik jest kwadratem liczby należącej do K (por. § 8, str. 390, przykład), są cykliczne.

2. Równanie $x^{p-1}+x^{p-2}+\ldots+x+1=0$ w ciele $\mathcal{R}$ liczb wymiernych, gdzie p jest liczbą pierwszą (por. § 14, str. 407, przykład 2) jest cykliczne.

3. Uogólniając przykład 2, wykażemy, że jeśli p jest liczbą pierwszą, zaś α dowolną liczbą naturalną, to równanie

$$x^{p^{\alpha-1}(p-1)}+x^{p^{\alpha-1}(p-2)}+\ldots+x^{p^{\alpha-1}}+1=0$$

jest cykliczne w ciele $\mathcal{R}$ liczb wymiernych.

Lewa strona tego równania jest równa $\dfrac{x^{p^\alpha}-1}{x^{p^{\alpha-1}}-1}=f(x)$. Gdyby wielomian ten był przywiedlny w $\mathcal{R}$, to przywiedlny byłby też wielomian

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

Zarówno w liczniku jak w mianowniku współczynniki z wyjątkiem współczynników przy najwyższych potęgach x są podzielne przez p. Na mocy algorytmu dzielenia wnosimy stąd łatwo, że współczynniki wielomianu $f(x+1)$ są podzielne przez p z wyjątkiem pierwszego, który jest równy 1. Aby znaleźć wyraz wolny, skracamy licznik i mianownik przez x i przyjmujemy $x=0$, otrzymując $g(0)=\dfrac{p^\alpha}{p^{\alpha-1}}=p$. Wielomian $g(x)$ jest więc nieprzywiedlny na mocy kryterium Eisensteina (Rozdział VIII, § 14, str. 134).

Pierwiastkami równania $f(x)=0$ są liczby $x_k=e^{2\pi i\cdot\frac{k}{p^\alpha}}$, gdzie k jest względnie pierwsze z p^α. Grupa G tego równania musi więc zawierać takie podstawienie π_k, że $\pi_k(x_1)=x_k$. Warunek ten wyznacza w zupełności podstawienie π_k, gdyż $\pi_k(x_m)=[\pi_k(x_1)]^m=e^{2\pi i\frac{km}{p^\alpha}}=x_{k\cdot m}$, przy czym km należy zredukować modulo p^α. W podobny sposób wykażemy, że $\pi_k\pi_m(x_1)=\pi_{km}(x_1)$, t. j. $\pi_k\cdot\pi_m=\pi_{km}$. Grupa G jest więc izomorficzna z grupą utworzoną z liczb mniejszych niż p^α i pierwszych względem p^α, w której działaniem jest mnożenie zredukowane modulo p^α. Grupa ta jest cykliczna, gdyż z Teorii liczb wiadomo, że istnieje liczba g (t. zw. *liczba pierwotna według modułu* p^α) taka, że reszty z dzielenia liczb $g,g^2,\ldots,g^{p^{\alpha-1}(p-1)}$ przez p^α przebiegają wszystkie liczby mniejsze od p^α i pierwsze względem p^α [1]). Grupa G jest więc izomorficzna z grupą $\{g,g^2,g^3,\ldots,g^{p^{\alpha-1}(p-1)}\}$, w której działaniem grupowym jest mnożenie, a wykładniki potęg redukujemy modulo $p^{\alpha-1}(p-1)$.

Twierdzenie 28. *Jeżeli równanie $f(x)=0$, nieprzywiedlne w ciele K, ma w tym ciele grupę cykliczną rzędu m, a ciało K zawiera m-te pierwiastki z jedności, to równanie $f(x)=0$ jest w ciele K rozwiązalne przez pierwiastniki stopnia co najwyżej m.*

Dowód. Udowodnimy to twierdzenie najpierw dla przypadku, gdy m jest liczbą pierwszą, a następnie pokażemy, że jeśli zachodzi ono dla liczby m, to zachodzi też dla liczby $p\cdot m$, gdzie p jest liczbą pierwszą. Przez indukcję wynikać stąd będzie słuszność twierdzenia dla każdego m.

1° m jest liczbą pierwszą. Grupa G składa się z m potęg pewnego podstawienia π:

$$G=\{1,\pi,\pi^2,\ldots,\pi^{m-1}\}.$$

Podstawienie π nie może zawierać dwu ani więcej cykli i wszystkie pierwiastki $x_1,x_2,\ldots,x_n$ równania $f(x)=0$ muszą wchodzić do π, gdyż w przeciwnym razie grupa G nie mogłaby być prze-

[1]) Zob. np. W. Sierpiński, *Teoria liczb*, Wyd. II, Warszawa 1925, Rozdział VIII, § 2, str. 132.

chodnia. Wynika stąd, że ilość n pierwiastków równania $f(x)=0$ musi być równa m. Możemy zatem tak ponumerować pierwiastki równania $f(x)=0$, żeby było $\pi=(x_1,x_2,\ldots,x_m)$.

Oznaczmy przez ε pierwiastek pierwotny stopnia m z jedności, należący w myśl założenia do ciała K i przyjmijmy dla $j=1,2,\ldots,m-1$

$$\Theta_j=x_1+\varepsilon^j x_2+\varepsilon^{2j}x_3+\ldots+\varepsilon^{(m-1)j}x_m.$$

Liczby te nazywają się *rozwiązującymi Lagrange'a*.

Nie wszystkie rozwiązujące są równe 0. Istotnie, suma ich równa się

$$\sum_{j=1}^{m-1}\Theta_j=(m-1)x_1+\sum_{k=2}^{m}x_k\cdot\sum_{j=1}^{m-1}\varepsilon^{(k-1)j}=mx_1-(x_1+x_2+\ldots+x_m),$$

gdyż $\sum_{j=1}^{m-1}\varepsilon^{(k-1)j}$ jest sumą wszystkich różnych od 1 pierwiastków stopnia m z jedności, a więc równa się -1. Ponieważ suma $x_1+x_2+\ldots+x_m$ należy do ciała K, więc wnosimy stąd, że gdyby wszystkie liczby Θ_j były równe 0, to mx_1, a więc i x_1, należałoby do ciała K wbrew założeniu, że równanie $f(x)=0$ jest nieprzywiedlne w K.

Przyjmijmy, że $\Theta_j\neq 0$. Mamy

$$\pi(\Theta_j)=\sum_{\nu=0}^{m-1}\varepsilon^{\nu j}\cdot\pi(x_{\nu+1})=x_2+\varepsilon^j x_3+\varepsilon^{2j}x_4+\ldots+\varepsilon^{(m-2)j}x_m+\varepsilon^{(m-1)j}x_1=$$
$$=\varepsilon^{(m-1)j}(x_1+\varepsilon^j x_2+\varepsilon^{2j}x_3+\ldots+\varepsilon^{(m-1)j}x_m)=\varepsilon^{-j}\Theta_j,$$

skąd przez indukcję wyprowadzamy, że

$$\pi^k(\Theta_j)=\varepsilon^{-kj}\Theta_j \quad \text{dla } k=0,1,2,\ldots,m-1. \tag{19}$$

Równość $\pi^k(\Theta_j)=\Theta_j$ zachodzi więc tylko dla $k=0$, co dowodzi, że grupa symetrii liczby Θ_j składa się tylko z podstawienia tożsamościowego. Θ_j jest więc liczbą pierwotną ciała $K(x_1,x_2,\ldots,x_m)$, skąd wynika, że wszystkie pierwiastki $x_1,x_2,\ldots,x_m$ należą do ciała $K(\Theta_j)$ (por. twierdzenie 15).

Przyjmijmy $a=\Theta_j^m$. Z (19) wynika, że $\pi^k(a)=a$ dla $k=0,1,2,\ldots,m-1$, t. zn. że a jest niezmiennicze względem wszystkich podstawień grupy G. W myśl twierdzenia 8 liczba a należy więc do K, przy czym nie jest ono m-tą potęgą żadnej liczby należącej do K, gdyż w przeciwnym razie Θ_j, a więc i wszystkie pierwiastki

$x_1,x_2,\ldots,x_m$, należałyby do K. Liczba Θ_j jest więc pierwiastkiem równania czystego $x^m-a=0$, nieprzywiedlnego w K. Wnosimy stąd, że ciąg składający się z dwu ciał K i $K(\Theta_j)$ spełnia warunki 1^0 i 2^0, podane w definicji rozwiązalności równania, t. zn. że równanie $f(x)=0$ jest rozwiązalne przez pierwiastniki stopnia co najwyżej m.

2^0 Załóżmy, że twierdzenie jest słuszne dla liczby m, a p jest liczbą pierwszą, i przypuśćmy, że równanie $f(x)=0$ jest nieprzywiedlne w K i ma w tym ciele grupę G cykliczną rzędu mp. Przypuśćmy wreszcie, że K zawiera pierwiastki stopnia mp z jedności. Wynika stąd, że K zawiera wszystkie pierwiastki stopnia m i wszystkie pierwiastki stopnia p z jedności.

Grupa G ma postać $\{1,\pi,\pi^2,\ldots,\pi^{mp-1}\}$. Podstawienia $1,\pi^p,\pi^{2p},\ldots,\pi^{(m-1)p}$ tworzą dzielnik normalny H grupy G, który jest grupą cykliczną rzędu m; grupa ilorazowa G/H jest izomorficzna z grupą cykliczną rzędu p.

Niech Θ oznacza jakąkolwiek liczbę ciała $\Sigma=K(x_1,x_2,\ldots,x_{mp})$, której grupą symetrii jest H. W ciele $K(\Theta)$ grupą równania $f(x)=0$ jest H, w myśl więc założenia równanie $f(x)=0$ jest w ciele $K(\Theta)$ rozwiązalne przez pierwiastniki stopnia co najwyżej m. Liczba Θ jest pierwiastkiem równania, którego grupa w K jest izomorficzna z G/H, a więc — jak wykazaliśmy w przypadku 1^0 — pierwiastkiem równania rozwiązalnego w K przez pierwiastniki stopnia co najwyżej p. Wynika stąd z łatwością (por. § 17, ćwiczenie 2), że równanie $f(x)=0$ jest rozwiązalne w K przez pierwiastniki stopnia co najwyżej $\max(m,p)\leqslant mp$, c. b. d. o.

ĆWICZENIA. 1. Wykazać, że metodą, wyłożoną w punkcie 1^0 dowodu twierdzenia 28 można rozwiązać równanie cykliczne także w przypadku, gdy m nie jest liczbą pierwszą, o ile choć jedna z rozwiązujących Lagrange'a Θ_j jest różna od 0 [1]).

2. Jeśli $\Theta_j\neq 0$ i ε^j jest pierwotnym pierwiastkiem stopnia m z jedności, to iloraz $\Theta_k:\Theta_j^q=c_k$ należy do ciała K, jeżeli $jq\equiv k \pmod m$.

[Zauważyć, że $\pi(\Theta_k/\Theta_j^q)=\varepsilon^{-k}\Theta_k/\varepsilon^{-jq}\Theta_j^q=\Theta_k/\Theta_j^q$].

[1]) Można też zmodyfikować to rozumowanie tak, aby stosowało się ono do przypadku, gdy wszystkie Θ_j są równe 0. Zob. H. Weber, *Lehrbuch der Algebra*, Tom I, Wydanie 2-e, Brunświk 1912, str. 589, oraz G. B. Mathews, *Algebraic Equations*, Cambridge Tracts in Mathematics and Mathematical Physics No 6 (1915), str. 32-34.

3. Zakładając w ćwiczeniu 2, że $j=1$, wyprowadzić wzory

$$x_k=\frac{1}{m}\sum_{h=1}^{m-1}\varepsilon^{-(k-1)h}\cdot c_h\cdot\Theta_1^h \qquad \text{dla } k=1,2,\ldots,m.$$

[Oprzeć się na wzorach $\sum_{h=1}^{m}\varepsilon^{lh}=0$ dla $l\neq 0$ i $\sum_{h=1}^{m}\varepsilon^{lh}=m$ dla $l=0$].

4. Udowodnić, że równanie $x^{p-1}+x^{p-2}+\ldots+x+1=0$ jest rozwiązalne w ciele $\mathcal{R}$ przez pierwiastniki stopnia co najwyżej $p-1$, gdy p jest liczbą pierwszą.

[Dla $p=2$ twierdzenie jest słuszne. Załóżmy, że jest ono słuszne dla $p<q$, i dołączmy do $\mathcal{R}$ pierwiastki stopni $2,3,\ldots,q-1$ z jedności. W nowym ciele równanie $x^{q-1}+x^{q-2}+\ldots+x+1=0$ ma grupę cykliczną rzędu $q-1$, a więc jest rozwiązalne przez pierwiastniki stopnia co najwyżej $q-1$. Następnie stosujemy ćwiczenie 2 z § 17].

5. Rozwiązać równanie cykliczne $x^{18}+x^9+1=0$.

§ 19. Równania rozwiązalne przez pierwiastniki. Możemy obecnie podać teorio-grupowe kryterium rozwiązalności równania przez pierwiastniki.

Twierdzenie 29. *Jeśli ciało K zawiera wszystkie pierwiastki z jedności, to równanie $f(x)=0$ jest wtedy i tylko wtedy rozwiązalne w K przez pierwiastniki stopnia co najwyżej m, gdy istnieje ciąg skończony grup*

$$G=G_0, \quad G_1, \quad G_2, \quad \ldots, \quad G_k=\{1\}$$

rozpoczynający się od grupy Galois równania $f(x)=0$ w ciele K, zakończony grupą jednostkową i posiadający następujące dwie własności:

1° G_{j+1} jest dzielnikiem normalnym G_j $(j=0,1,2,\ldots,k-1)$,

2° Grupy ilorazowe G_j/G_{j+1} są cykliczne rzędu co najmniej 2 i co najwyżej m.

Dowód. Załóżmy najpierw, że równanie $f(x)=0$ jest w ciele K rozwiązalne przez pierwiastniki stopnia co najwyżej m, t. j. że istnieje ciąg ciał

$$K, \quad K(\Theta_1), \quad K(\Theta_1,\Theta_2), \quad \ldots, \quad K(\Theta_1,\Theta_2,\ldots,\Theta_r)$$

taki, że wszystkie pierwiastki równania $f(x)=0$ należą do ciała $K(\Theta_1,\Theta_2,\ldots,\Theta_r)$ i Θ_j jest pierwiastkiem równania czystego nieprzywiedlnego w $K(\Theta_1,\Theta_2,\ldots,\Theta_{j-1})$, którego stopień jest liczbą pierwszą nie większą od m $(j=1,2,\ldots,r)$.

Przyjmijmy $\Gamma_0=G$ i oznaczmy przez Γ_j grupę równania $f(x)=0$ w ciele $K(\Theta_1,\Theta_2,\ldots,\Theta_j)$ dla $j=1,2,\ldots,r$. Γ_r jest więc grupą jednostkową, zaś Γ_{j+1} — podgrupą Γ_j dla $j=0,1,2,\ldots,r-1$. Zajść mogą dwa przypadki: albo Θ_{j+1} jest niewymiernością uboczną dla równania $f(x)=0$ w ciele $K(\Theta_1,\Theta_2,\ldots,\Theta_j)$, albo niewymiernością naturalną. W pierwszym przypadku $\Gamma_{j+1}=\Gamma_j$ na mocy twierdzenia 26. W drugim przypadku Γ_{j+1} jest grupą symetrii liczby Θ_{j+1} czyli, dokładniej, grupą tych podstawień π należących do Γ_j, dla których $\pi(\Theta_{j+1})=\Theta_{j+1}$. Liczby sprzężone z Θ_{j+1} są pierwiastkami tego samego równania czystego, któremu czyni zadość Θ_{j+1}, czyli mają postać $\varepsilon\Theta_{j+1}$, gdzie ε jest pierwiastkiem z jedności. Grupą symetrii takiej liczby jest oczywiście znów Γ_{j+1}. Grupy sprzężone z Γ_{j+1} pokrywają się więc z Γ_{j+1} (por. § 3, str. 379, ćwiczenie 1), t. zn. że Γ_{j+1} jest dzielnikiem normalnym grupy Γ_j.

Zgodnie z twierdzeniem 21 liczba Θ_{j+1} jest pierwiastkiem nieprzywiedlnego w ciele $K(\Theta_1,\Theta_2,\ldots,\Theta_j)$ równania, którego grupa w tym ciele jest izomorficzna z Γ_j/Γ_{j+1}. Równanie to musi pokrywać się z równaniem czystym, któremu czyni zadość Θ_{j+1}, skąd na mocy twierdzenia 27 wnosimy, że Γ_j/Γ_{j+1} jest grupą cykliczną rzędu co najwyżej m.

Jeżeli teraz usuniemy z ciągu $\Gamma_0,\Gamma_1,\ldots,\Gamma_r$ wyrazy równe wyrazom je poprzedzającym, to otrzymamy ciąg zstępujący grup $G_0,G_1,\ldots,G_k$, spełniający wymienione w twierdzeniu warunki 1° i 2°. Warunki te są więc konieczne dla rozwiązalności równania przez pierwiastniki rzędu co najwyżej m.

Załóżmy teraz, że istnieje ciąg grup $G_0,G_1,\ldots,G_k$, spełniający warunki twierdzenia. Aby wykazać rozwiązalność równania, zastosujemy indukcję względem k.

Jeśli $k=1$, to $G_1=G_k=\{1\}$ i grupy G oraz G_0/G_1 są izomorficzne, co dowodzi, że G jest grupą cykliczną rzędu co najwyżej m. W tym więc przypadku twierdzenie wynika z twierdzenia 28.

Załóżmy słuszność twierdzenia dla przypadku, gdy omawiany ciąg grup ma co najwyżej $k-1$ wyrazów, i dołączmy do K jakąkolwiek liczbę Θ, której grupą symetrii jest G_1. W ciele $K(\Theta)$ równanie $f(x)=0$ ma grupę G_1, w myśl więc założenia jest rozwiązalne w $K(\Theta)$ przez pierwiastniki stopnia co najwyżej m. Grupa równania nieprzywiedlnego w K, któremu czyni zadość Θ, jest izomorficzna z G/G_1; jest to więc grupa cykliczna rzędu co najwyżej m. Z twierdzenia 28 wynika zatem, że Θ jest pierwiastkiem równania rozwiązalnego w K przez pierwiastniki stopnia co najwyżej m, co dowodzi (por. § 17, ćwiczenie 2), że i równanie $f(x)=0$ jest rozwiązalne w K przez takie pierwiastniki. Warunki 1° i 2° są więc dostateczne, c. b. d. o.

Założenie, że ciało K zawiera wszystkie pierwiastki z jedności, nie jest istotne dla słuszności twierdzenia 29, wiemy bowiem, że równania podziału koła są rozwiązalne przez pierwiastniki (por. § 18, ćwiczenie 4).

Korzystając z pojęcia ciągu składaniowego (§ 13, str. 405), można nieco uprościć wysłowienie twierdzenia 29. Równanie $f(x)=0$ jest mianowicie rozwiązalne w K przez pierwiastniki stopnia co najwyżej m wtedy i tylko wtedy, gdy istnieje ciąg składaniowy $G=G_0, G_1, \ldots, G_k=\{1\}$ grupy G, którego grupy ilorazowe G_j/G_{j+1} są cykliczne rzędu co najwyżej m. Ciąg $G_0, G_1, \ldots, G_k$, o którym mowa w twierdzeniu 29, można bowiem zawsze uzupełnić przez ewentualne dołączenie nowych wyrazów do ciągu składaniowego [1]).

Twierdzenie 29 rozstrzyga całkowicie kwestię rozwiązalności równań przez pierwiastniki, przynajmniej w przypadku takich ciał K, dla których umiemy wyznaczać grupę Galois dowolnego równania o współczynnikach z K (por. § 6). Wyznaczywszy bowiem grupę G, możemy zawsze sprawdzić (przez skończoną liczbę prób), czy istnieje ciąg $G_0, G_1, \ldots, G_k$ posiadający własności 1^0 i 2^0 wymienione w twierdzeniu 29.

Jako zastosowanie twierdzenia 29 udowodnimy

Twierdzenie 30. *Równanie nieprzywiedlne o współczynnikach wymiernych, którego stopień n jest liczbą pierwszą większą od 3 i które ma dokładnie 2 pierwiastki zespolone, nie jest rozwiązalne przez pierwiastniki.*

Dowód. Grupą równania, spełniającego założenia twierdzenia, jest S_n (por. twierdzenie 18). W myśl twierdzenia 23 jedynymi ciągami podgrup S_n, jakie spełniają warunek 1^0 twierdzenia 29, są ciągi

$$S_n,\ A_n,\ \{1\} \qquad \text{i} \qquad S_n,\ \{1\}.$$

Ciągi te nie spełniają jednak warunku 2^0 twierdzenia 29, gdyż ani grupa S_n, ani grupa A_n nie są cykliczne.

Twierdzenie 30 dowodzi, że równania stopnia wyższego niż 4 nie są na ogół rozwiązalne przez pierwiastniki [2]). Opierając się na wyniku Hilberta, o którym wspominaliśmy przy końcu § 9 (str. 395), można dowieść, że *dla każdej liczby naturalnej $n>4$ istnieje równanie stopnia n o współczynnikach wymiernych, nierozwiązalne przez pierwiastniki.*

[1]) Por. B. L. van der Waerden, *Moderne Algebra*, Wyd. 2-e, Tom I, Berlin 1937, str. 151.

[2]) Pierwszy ścisły dowód tego twierdzenia dla równań stopnia 5 podał N. H. Abel w r. 1826, kładąc przez to kres długoletnim i bezowocnym próbom rozwiązania ogólnego równania stopnia 5 przez pierwiastniki.

ĆWICZENIA. 1. Wyprowadzić teorio-grupowo rozwiązalność równań stopni 2, 3 i 4.

2. Równanie $x^5-10x+2=0$ nie jest rozwiązalne przez pierwiastniki w ciele $\mathcal{R}$ liczb wymiernych.

[Por. § 9, str. 395, ćwiczenie 1].

3. Jeśli grupa G jest przemienna, to równanie $f(x)=0$ jest rozwiązalne przez pierwiastniki.

[Jeśli N oznacza maksymalny dzielnik normalny grupy G, to G/N jest grupą prostą i przemienną, a więc cykliczną].

Równania o grupach przemiennych nazywamy *abelowymi*.

4. Jeśli każdy pierwiastek równania $f(x)=0$ jest potęgą liczby x_1, to równanie $f(x)=0$ jest abelowe.

[Niech $x_k=x_1^{\alpha_k}$, $\pi(x_1)=x_p$ i $\sigma(x_1)=x_q$. Wtedy:

$$\sigma\pi(x_k)=\sigma([\pi(x_1)]^{\alpha_k})=\sigma(x_p^{\alpha_k})=\sigma(x_1^{\alpha_k p^{\alpha_k}})=x_1^{\alpha_k q^{\alpha_k} p^{\alpha_k}},$$

$$\pi\sigma(x_k)=\pi([\sigma(x_1)]^{\alpha_k})=\pi(x_q^{\alpha_k})=\pi(x_1^{\alpha_k q^{\alpha_k}})=x_1^{\alpha_k p^{\alpha_k} q^{\alpha_k}},$$

a więc $\pi\sigma=\sigma\pi$].

5. Wykazać, że równanie $x^8-x^7+x^5-x^4+x^3-x+1=0$ jest abelowe w ciele $\mathcal{R}$ liczb wymiernych.

[Lewa strona równania jest równa $\frac{(x^{15}-1)(x-1)}{(x^3-1)(x^5-1)}$. Jeśli więc jednym pierwiastkiem jest ε, to pozostałymi są $\varepsilon^2, \varepsilon^4, \varepsilon^7, \varepsilon^8, \varepsilon^{11}, \varepsilon^{13}, \varepsilon^{14}$].

6. Można udowodnić, że lewa strona równania z ćwiczenia 5 jest nieprzywiedlna w ciele $\mathcal{R}$. Opierając się na tym, pokazać, że grupa G tego równania w ciele $\mathcal{R}$ jest izomorficzna z grupą, utworzoną z liczb mniejszych od 15 i względnie pierwszych z 15, w której działaniem jest mnożenie i iloczyn redukuje się zawsze modulo 15. Grupa ta jest przemienna, ale nie jest cykliczna.

Równanie z ćwiczenia 5 jest szczególnym przypadkiem *równań podziału koła*, pojmowanych tu jako równania, których pierwiastkami są pierwiastki pierwotne z jedności (por. Rozdział XI, str. 199). Więcej szczegółów o tych równaniach znaleźć można np. w książkach van der Waerdena i Czebotarewa, cytowanych na str. 375 i 395.

§ 20. Konstrukcje przy pomocy cyrkla i liniału.

Z twierdzenia 29 wynika łatwo następujący warunek konieczny rozwiązalności równania przez pierwiastniki kwadratowe:

Twierdzenie 31. *Jeśli równanie $f(x)=0$ jest w ciele K rozwiązalne przez pierwiastniki kwadratowe, to rząd grupy tego równania w ciele K jest potęgą liczby 2.*

Dowód. Zgodnie z twierdzeniem 29 istnieje ciąg grup

$$G_0=G, \quad G_1, \quad G_2, \quad \ldots, \quad G_k=\{1\}$$

taki, że grupy ilorazowe G_j/G_{j+1} są rzędu 2. Rząd grupy G jest równy iloczynowi rzędów grup G_j/G_{j+1}, jest więc potęgą liczby 2, c. b. d. o.

Można pokazać, że warunek wymieniony w tezie twierdzenia 31 jest nie tylko konieczny, ale i dostateczny dla rozwiązalności równania przez pierwiastniki kwadratowe, każda bowiem grupa, której rząd jest potęgą liczby 2, posiada ciąg składaniowy, którego grupy ilorazowe są rzędu 2 [1]).

Rozwiązalność przez pierwiastniki kwadratowe jest — jak wiemy z Rozdziału XI, § 5, str. 208-209 — związana z *konstruowalnością przy pomocy cyrkla i liniału*. Na to mianowicie, żeby punkt A był konstruowalny przy pomocy cyrkla i liniału z innych danych punktów $A_1, A_2, \ldots, A_k$, potrzeba i wystarcza, by współrzędne x, y punktu A (w dowolnym układzie współrzędnych) były pierwiastkami równań rozwiązalnych przez pierwiastniki kwadratowe w ciele $\mathcal{R}(x_1, y_1, x_2, y_2, \ldots, x_k, y_k)$, gdzie x_j, y_j oznaczają współrzędne punktu A_j dla $j = 1, 2, \ldots, k$. Kryterium pozostaje bez zmiany, gdy dwie współrzędne rzeczywiste x, y zastąpimy jedną współrzędną zespoloną $z = x + iy$.

PRZYKŁADY. 1. Podział kąta na nieparzystą liczbę równych części. Udowodnimy

Twierdzenie 32. *Jeśli p jest liczbą pierwszą nieparzystą, a φ — liczbą rzeczywistą taką, że $e^{i\varphi}$ jest liczbą przestępną, to kąt φ/p radianów nie jest konstruowalny przy pomocy cyrkla i liniału, o ile dane są tylko jednostka miary i kąt φ.*

Dowód. Gdyby kąt φ/p był konstruowalny przy pomocy cyrkla i liniału, to możnaby też znaleźć przy pomocy cyrkla i liniału punkt $e^{i\varphi/p}$, wychodząc z danej jednostki miary i punktu $e^{i\varphi}$. Równanie

$$x^p - e^{i\varphi} = 0 \tag{20}$$

byłoby więc rozwiązalne przez pierwiastniki kwadratowe w ciele $\mathcal{R}(e^{i\varphi})$ i tymbardziej w ciele $\mathcal{R}(e^{i\varphi}, e^{2\pi i/p})$.

Aby dowieść, że przypuszczenie to prowadzi do sprzeczności, wykażemy najpierw, że równanie (20) jest nieprzywiedlne w ciele $\mathcal{R}(e^{i\varphi}, e^{2\pi i/p})$. Istotnie, w przeciwnym razie $e^{i\varphi}$ byłoby p-tą potęgą pewnego elementu a ciała $\mathcal{R}(e^{i\varphi}, e^{2\pi i/p})$ (por. Rozdział XIII, § 3, str. 229, twierdzenie 7). Ponieważ a może być przedstawione w postaci $\frac{P(e^{i\varphi})}{Q(e^{i\varphi})}$, gdzie P i Q są wielomianami jednej zmiennej o współczynnikach należących do $\mathcal{R}(e^{2\pi i/p})$, więc wynikłoby stąd, że

$$[Q(e^{i\varphi})]^p \cdot e^{i\varphi} - [P(e^{i\varphi})]^p = 0. \tag{21}$$

Wielomian $[Q(\xi)]^p \cdot \xi - [P(\xi)]^p$ nie jest tożsamościowo równy 0. Istotnie, jeśli $P(\xi)$ jest wielomianem stopnia μ, a $Q(\xi)$ — wielomianem stopnia ν, to $[Q(\xi)]^p \xi - [P(\xi)]^p$ ma stopień $p\nu + 1$, o ile $\nu \geqslant \mu$, zaś stopień $p\mu$, o ile $\mu > \nu$. Stopień tego wielomianu jest przeto zawsze dodatni. Z (21) wynika więc, że $e^{i\varphi}$

[1]) Zob. np. A. Speiser, *Theorie der Gruppen von endlicher Ordnung*, Wyd. 2-e, Berlin 1927, str. 69.

jest liczbą algebraiczną w ciele $\mathcal{R}(e^{2\pi i/p})$, a więc też w ciele $\mathcal{R}$ (por. Rozdział XII, § 4, str. 217, twierdzenie 4) wbrew założeniu. Wielomian $x^p - e^{i\varphi}$ jest zatem nieprzywiedlny w ciele $\mathcal{R}(e^{i\varphi}, e^{2\pi i/p})$.

Zgodnie z twierdzeniem 27 grupa równania (20) w ciele $R(e^{i\varphi}, e^{2\pi i/p})$ jest cykliczna rzędu p, skąd na mocy twierdzenia 31 wnosimy od razu, że równanie (20) nie jest w tym ciele rozwiązalne przez pierwiastniki kwadratowe, c. b. d. o.

Jest jasne, że istnieją liczby rzeczywiste φ, dla których $e^{i\varphi}$ jest liczbą przestępną [1]). Na mocy twierdzenia 32 możemy stąd wnosić, że podział dowolnego kąta φ na nieparzystą ilość równych części nie da się przeprowadzić przy pomocy samego cyrkla i liniału. Nie wynika stąd oczywiście niemożliwość podziału pewnych specjalnych kątów φ na nieparzystą ilość równych części, jak to zaraz wykażemy dla przypadku $\varphi = 2\pi$.

2. Konstruowalność wielokątów foremnych. Zagadnienie podziału kąta 2π na n równych części jest oczywiście równoważne konstrukcji n-kąta foremnego. Można je też sformułować i tak, że chodzi o skonstruowanie punktu o współrzędnych rzeczywistych $\cos\frac{2\pi}{n}$, $\sin\frac{2\pi}{n}$ czyli punktu o współrzędnej zespolonej $z = x + iy = \varepsilon$, gdzie ε jest którymkolwiek z pierwiastków pierwotnych stopnia n z jedności.

Twierdzenie 33. *Na to, aby n-kąt foremny był konstruowalny przy pomocy cyrkla i liniału, potrzeba i wystarcza, by n miało postać $2^k \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_r$, gdzie $p_1, p_2, \ldots, p_r$ oznaczają różne liczby pierwsze postaci $2^m + 1$.*

Dowód. Załóżmy najpierw, że n jest potęgą liczby pierwszej p:

$$n = p^\alpha.$$

Pierwiastki pierwotne stopnia p^α z jedności są pierwiastkami równania

$$x^{p^{\alpha-1}(p-1)} + x^{p^{\alpha-1}(p-2)} + \ldots + x^{p^{\alpha-1}} + 1 = 0, \tag{22}$$

którego grupa w ciele $\mathcal{R}$ jest cykliczna rzędu $p^{\alpha-1}(p-1)$ (por. § 18, przykład 3). Liczba $p^{\alpha-1}(p-1)$ jest potęgą liczby 2 w dwu przypadkach: gdy $p = 2$ oraz gdy $\alpha = 1$, a p ma postać $2^m + 1$. W tych więc tylko przypadkach równanie (22) może być rozwiązalne przez pierwiastniki kwadratowe. Na odwrót, jeśli warunki te są spełnione, to rząd grupy równania (22) w ciele $\mathcal{R}$ jest potęgą liczby 2, skąd z łatwością wynika, że grupa ta posiada ciąg składaniowy, którego grupy ilorazowe mają rząd 2 (por. § 13, ćwiczenie 4). W myśl twierdzenia 29 równanie (22) jest więc rozwiązalne przez pierwiastniki kwadratowe, czyli n-kąt foremny jest konstruowalny przy pomocy cyrkla i liniału. Twierdzenie 33 jest więc słuszne w przypadku, gdy n jest potęgą liczby pierwszej.

[1]) Wynika to choćby z uwagi, że zbiór liczb algebraicznych jest przeliczalny, a zbiór liczb postaci $e^{i\varphi}$ — nieprzeliczalny. Można udowodnić, że jeśli φ jest liczbą algebraiczną różną od 0 (rzeczywistą lub zespoloną), to $e^{i\varphi}$ jest liczbą przestępną. Zob. F. Lindemann, Mathematische Annalen, Tom 20 (1882), str. 213. Dowód Lindemanna jest dokładnie opracowany w książce G. Hessenberg, *Transzendenz von e und π*, Lipsk-Berlin 1912.

Załóżmy teraz, że n jest iloczynem pewnej ilości czynników pierwszych i że p jest jednym z nich. Przypuśćmy, że $n=p^\alpha h$, gdzie h jest liczbą niepodzielną przez p. Jeśli n-kąt foremny jest konstruowalny przy pomocy cyrkla i liniału, to konstruowalny jest też p^α-kąt foremny, gdyż możemy go otrzymać z n-kąta foremnego, łącząc co h-ty jego wierzchołek. Na mocy udowodnionej już części twierdzenia musi więc być bądź $p=2$, bądź $\alpha=1$ i $p=2^m+1$, co dowodzi, że warunek twierdzenia 33 jest konieczny.

Dla dowodu dostateczności wystarczy zauważyć, że jeśli przy pomocy cyrkla i liniału konstruowalne są punkty o współrzędnych (zespolonych)

$$e^{2\pi i/2^k}, \quad e^{2\pi i/p_1}, \quad \ldots, \quad e^{2\pi i/p_r},$$

to — jak wynika z geometrycznej interpretacji mnożenia liczb zespolonych (Rozdział VI, § 6, str. 92) — konstruowalny jest też punkt o współrzędnej

$$\varepsilon = e^{2\pi i\left[\frac{1}{2^k}+\frac{1}{p_1}+\ldots+\frac{1}{p_r}\right]}.$$

Ponieważ ε jest pierwiastkiem pierwotnym stopnia $n=2^k p_1 p_2 \ldots p_r$ z jedności, więc wynika stąd konstruowalność n-kąta foremnego.

Udowodnione w ten sposób twierdzenie 33 może być jeszcze wypowiedziane w następującej formie, w której objawia się ciekawy związek między Geometrią a Arytmetyką:

Na to, by n-kąt foremny był konstruowalny przy pomocy cyrkla i liniału, potrzeba i wystarcza, żeby ilość liczb pierwszych względem n i mniejszych od n była potęgą liczby 2.

Dla dowodu wystarczy przypomnieć, że ilość liczb pierwszych względem n i mniejszych od n, czyli t. zw. w Teorii liczb *funkcja Gauss'a* (ob. Rozdział VI, § 8, str. 95) jest dana wzorem

$$\varphi(n)=p_1^{\alpha_1-1}(p_1-1)\cdot p_2^{\alpha_2-1}(p_2-1)\ldots p_r^{\alpha_r-1}(p_r-1),$$

gdzie $n=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\ldots p_r^{\alpha_r}$ oznacza rozkład liczby n na czynniki pierwsze [1]).

Można też wyprowadzić w podobny sposób kryterium (czyli warunek konieczny i dostateczny) konstruowalności n-kąta foremnego przy pomocy liniału, cyrkla i cyrkla stożkowego, t. j. przyrządu, pozwalającego kreślić stożkową przez 5 danych punktów. Liczba n musi mieć wówczas postać $2^k 3^l p_1 p_2 \ldots p_r$, gdzie $p_1, p_2, \ldots, p_r$ są to różne liczby pierwsze postaci $2^\alpha 3^\beta + 1$, zaś $\alpha \geqslant 0$ i $\beta \geqslant 0$ [2]).

ĆWICZENIE. Jeśli 2^m+1 jest liczbą pierwszą, to m jest potęgą liczby 2.

[Jeśli q jest liczbą nieparzystą, to x^q+1 jest podzielne przez $x+1$, a więc $2^{2^r q}+1$ jest podzielne przez $2^{2^r}+1$].

[1]) Zob. W. Sierpiński, *Teoria liczb*, Wyd. 2-e, Warszawa 1925, Rozdział VI, str. 93.

[2]) Zob. J. Pierpont, Bulletin of the American Mathematical Society, Tom 2 (1895), str. 77-86.

§ 21. Pierwiastniki rzeczywiste. Załóżmy, że ciało K składa się wyłącznie z liczb rzeczywistych.

Jeśli istnieje ciąg rosnący ciał

$$K, \quad K(\Theta_1), \quad K(\Theta_1,\Theta_2), \quad \ldots, \quad K(\Theta_1,\Theta_2,\ldots,\Theta_k), \tag{23}$$

spełniający warunki 1° i 2° podane w definicji rozwiązalności (§ 17, str. 414-415), w którym nadto liczby $\Theta_1,\Theta_2,\ldots,\Theta_k$ są rzeczywiste, to mówimy, że równanie $f(x)=0$ jest *w ciele K rozwiązalne przez pierwiastniki rzeczywiste.*

Uogólniając wyniki dotyczące t. zw. *casus irreducibilis* dla równań stopnia 3 (ob. Rozdział X, § 5, str. 184), wypowiedzieć możemy

Twierdzenie 34. *Niech ciało K składa się z liczb rzeczywistych i niech równanie $f(x)=0$ ma wszystkie pierwiastki rzeczywiste; jeśli rząd grupy G tego równania w ciele K jest podzielny przez liczbę nieparzystą większą od 1, to równanie $f(x)=0$ nie jest w ciele K rozwiązalne przez pierwiastniki rzeczywiste.*

Dowód. Załóżmy, że istnieje ciąg ciał (23) spełniający warunki 1° i 2° definicji rozwiązalności (str. 414-415), w którym liczby $\Theta_1,\Theta_2,\ldots,\Theta_k$ są rzeczywiste. Niech G_j oznacza grupę równania $f(x)=0$ w ciele $K(\Theta_1,\Theta_2,\ldots,\Theta_j)$ dla $j=1,2,\ldots,k$ i przyjmijmy $G_0=G$. Grupa G_{j+1} jest oczywiście podgrupą grupy G_j dla $j=0,1,2,\ldots,k-1$, przy czym $G_k=\{1\}$. Niech r_j oznacza wskaźnik G_{j+1} w G_j dla $j=0,1,2,\ldots,k-1$. Rząd grupy G jest więc równy $r_0 r_1 \ldots r_{k-1}$, skąd wnosimy, że co najmniej jedna z liczb $r_0, r_1, \ldots, r_{k-1}$, np. liczba r_j, jest podzielna przez liczbę nieparzystą większą od 1. Dołączenie Θ_{j+1} do ciała $K_j=K(\Theta_1,\Theta_2,\ldots,\Theta_j)$ powoduje redukcję grupy równania $f(x)=0$ z G_j do podgrupy właściwej G_{j+1}. Z twierdzenia 26 wynika więc, że Θ_{j+1} jest niewymiernością naturalną, t. zn. daje się przedstawić jako wielomian względem $x_1, x_2, \ldots, x_n$ o współczynnikach należących do K_j:

$$\Theta_{j+1}=W(x_1,x_2,\ldots,x_n).$$

Liczby sprzężone z Θ_{j+1} mają postać $W(\pi(x_1),\pi(x_2),\ldots,\pi(x_n))$, gdzie π przebiega grupę G_j. Liczby te są zatem wszystkie rzeczywiste. Z twierdzenia 11 wiemy, że wszystkie liczby sprzężone z Θ_{j+1} są pierwiastkami jednego i tego samego wielomianu stopnia r_j o współczynnikach należących do K_j i nieprzywiedlnego w K_j. Z drugiej strony, Θ_{j+1} jest pierwiastkiem równania czystego, nieprzywiedlnego w K_j. Dochodzimy w ten sposób do wniosku, że

istnieje równanie czyste stopnia r_j, nieprzywiedlne w K_j, którego wszystkie pierwiastki są rzeczywiste. Wniosek ten jest oczywiście niedorzeczny, gdyż wynikłoby stąd, że i ilorazy dwu dowolnych pierwiastków równania czystego są rzeczywiste, t. zn. wszystkie pierwiastki z jedności stopnia r_j byłyby rzeczywiste, wbrew założeniu, że $r_j > 2$. Twierdzenie 34 jest w ten sposób udowodnione.

ĆWICZENIE. Jeśli K zawiera wyłącznie liczby rzeczywiste, pierwiastki równania $f(x) = 0$ są rzeczywiste i grupa G tego równania w ciele K posiada ciąg składaniowy, którego grupy ilorazowe są rzędu 2, to równanie $f(x) = 0$ jest rozwiązalne przez pierwiastniki rzeczywiste.

[Zastosować takie rozumowanie, jak w dowodzie twierdzenia 29].