Bouquet, (§§ 1 i 2. Dla równania tego dowodzę twierdzenia, analogicznego do twierdzenia Briot i Bouquet, dotyczącego granicy stosunku (§ 2)

$$\sqrt[n]{A_n} : \sqrt[n]{1.2.3\ldots(n-1)}.$$

Badam szereg, czyniący formalnie zadość równaniu powyższemu, wykazując, iż jego rozbieżność zachodzi dzięki obecności pewnych liczb całkowitych, które nazywam czynnikami rozbieżności, i które wyłaniają się w rachunku pochodnych kolejnych. Z rozważań tych wynika interesujące twierdzenie dotyczące szybkości rozbieżności rzeczonego szeregu, które usprawiedliwia zdanie wielu matematyków, iż równanie (2) nie posiada naogół całki holormorficznej.

K. ABRAMOWICZ.

O przekształceniu funkcji automorficznej, należącej do grupy (0, 3; 2, 4, 5).

Sur la transformation d'une fonction automorphe appartenant au groupe (0, 3; 2, 4, 5).

Pierwsze badania nad przekształceniem funkcyj automorficznych znajdujemy u Frickego[1]); dotyczą one przekształcenia 3-go stopnia funkcji automorficznej, należącej do grupy, oznaczonej przez Kleina znakiem (0, 3; 2, 4, 5). Po za tym przypadkiem przekształcenia 3-go stopnia, zbadanym szczegółowo przez Frickego, i dwoma, podanemi przez niego, przypadkami specjalnemi[2]), dającemi grupy G_{60} i G_{168}, dalszych badań w zakresie przekształcenia funkcyj automorficznych nie posiadamy. Przedmiotem pracy niniejszej są pewne spostrzeżenia ogólne, dotyczące przekształcenia p-go stopnia funkcji automorficznej, należącej do grupy (0, 3; 2, 4, 5). Wynik, otrzymany przez nas, możemy sformułować w sposób następujący:

Jeżeli liczba naturalna p ma jednę z postaci:

$$20k+1,\ 20k+3,\ 20k+7,\ 20k+9$$

i jest przytem liczbą pierwszą w ciele kwadratowem $K(j)$, wyznaczonem przez pierwiastek dodatni j równania $j^2+j-1=0$, to przy przekształceniu p-go stopnia funkcji automorficznej $\varphi(z)$, należącej do grupy (0, 3; 2, 4, 5), funkcja przekształcona $\varphi(Tz)$ jest pierwiastkiem równania algebraicznego stopnia p^2+1.

§ 1.

Zauważymy uprzednio, że grupa automorficzna (0, 3; 2, 4, 5) określa się, jako zbiór wszystkich podstawień postaci:

[1]) Anhang w „Vorlesungen über die Theorie der automorphen Functionen" Bd. 2 str. 345.

[2]) Fricke: „Entwicklungen zur Transformation fünfter und siebenter Ordnung einiger spezieller automorpher Functionen" (Acta math., t. 17, str. 345).

$$z' = \frac{(a + b\sqrt{j})z + c + d\sqrt{j}}{(-c + d\sqrt{j})z + a - b\sqrt{j}}, \qquad (1)$$

w ktorych j oznacza pierwiastek dodatni równania $j^2 + j - 1 = 0$, liczby a, b, c, d są liczbami całkowitemi ciała kwadratowego $K(j)$, a wyznacznik: $a^2 + c^2 - j(b^2 + d^2)$ podstawień jest równy 4 albo 2.

Jeżeli dalej $T(z)$ oznacza podstawienie postaci (1), mające wyznacznik

$$a^2 + c^2 - j(b^2 + d^2) = p,$$

gdzie liczba naturalna p jest różna od 4 i 2, to według Poincarégo[1]) przez przekształcenie stopnia p funkcji automorficznej $\varphi(z)$, należącej do grupy (0, 3; 2, 4, 5), rozumiemy wyrażenie funkcji przekształconej $\varphi(Tz)$ przez funkcję początkową $\varphi(z)$.

Zgodnie z powyższem do przekształcenia stopnia p funkcji automorficznej może być użyte każde podstawienie T postaci (1), mające wyznacznik równy liczbie p; w dalszym ciągu zakładamy, że liczba p jest pierwszą w ciele $K(j)$.

Stopień równania algebraicznego, któremu czyni wtedy zadość funkcja przekształcona $\varphi(Tz)$, równa się wskaźnikowi najobszerniejszej wspólnej podgrupy grup:

$$(0, 3; 2, 4, 5), \quad T^{-1}(0, 3; 2, 4, 5)T.$$

Wyznaczenie tego wskaźnika jest celem pracy niniejszej.

§ 2.

Dowolność przy wyborze podstawienia T o wyznaczniku p może być szeroka. Ograniczymy jednak zakres możliwych podstawień (1) przez warunek:

$$b = d = 0.$$

Mieć będziemy wtedy podstawienia postaci:

$$T(z) = \frac{Mz + N}{-Nz + M}$$

o wyznaczniku $M^2 + N^2 = p$ i liczbach M i N całkowitych w ciele $K(j)$; obierzemy jedno z takich podstawień.

Zadanie nasze będzie polegało na wyznaczeniu:

1°, wspólnej podgrupy grup:

[1]) Oeuvres, t. II, p. 463.

$$(0, 3; 2, 4, 5) \text{ i } T^{-1}(0, 3; 2, 4, 5)T,$$

2°, jej wskaźnika względem grupy (0, 3; 2, 4, 5).

Sposób rozwiązania zadania 1° będzie przedstawiał uogólnienie sposobu, użytego przez Frickego przy przekształceniu 3-go stopnia; zadanie 2° będzie rozwiązane w sposób zupełnie odmienny od sposobu stosowanego przez Frickego.

§ 3.

Oznaczając dla krótkości podstawienia grupy (0, 3; 2, 4, 5) przez (a, b, c, d), mieć będziemy na podstawienie T symbol:

$$T = (M, 0, N, 0).$$

Obliczymy podstawienia (A, B, C, D) grupy przekształconej $T^{-1}(0, 3; 2, 4, 5)T$. Korzystając w tym celu z wzorów:

$$\alpha' = mq\alpha - np\delta + pq\beta - mn\gamma,$$
$$\beta' = nq(\alpha - \beta) + q^2\beta - n^2\gamma,$$
$$\gamma' = mp(\delta - \alpha) - p^2\beta + m^2\gamma,$$
$$\delta' = mq\delta - np\alpha - pq\beta + mn\gamma,$$

wyznaczających spółczynniki $\alpha', \beta', \gamma', \delta'$ podstawienia, wynikającego z przekształcenia podstawienia

$$\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \text{ przez } \begin{pmatrix} m, & n \\ p, & q \end{pmatrix},$$

znajdziemy na spółczynniki A, B, C, D podstawień (A, B, C, D) grupy przekształconej $T^{-1}(0, 3; 2, 4, 5)T$ wyrażenia:

$$A = pa, \quad B = b(M^2 - N^2) - 2MNd,$$
$$C = pc, \quad D = d(M^2 - N^2) + 2MNb.$$

Lemmat I: W skład szukanej wspólnej podgrupy grup (0,3; 2, 4, 5) i $T^{-1}(0, 3; 2, 4, 5)T$ wejdą tylko te podstawienia grupy $T^{-1}(0, 3; 2, 4, 5)T$, które powstały z podstawień (a, b, c, d), spełniających kongruencję:

$$2MNd \equiv (M^2 - N^2)b \pmod{p}. \qquad (2)$$

W samej rzeczy, wyznacznik podstawienia (A, B, C, D) jest:

$$A^2 + C^2 - j(B^2 + D^2) = p^2\{a^2 + c^2 - j(b^2 + d^2)\};$$

aby więc podstawienie to mogło należeć do grupy $(0, 3; 2, 4, 5)$, t. j. mieć wyznacznik równy 4 albo 2, muszą liczby A, B, C, D być podzielne przez p, t. j. ilorazy:

$$a' = \frac{A}{p} = a, \quad b' = \frac{B}{p} = \frac{1}{p}\{b(M^2 - N^2) - 2MNd\},$$
$$c' = \frac{C}{p} = c, \quad d' = \frac{D}{p} = \frac{1}{p}\{d(M^2 - N^2) + 2MNb\} \tag{3}$$

muszą być liczbami całkowitemi. Liczba b' jest całkowita, jeżeli jest spełniony warunek (2); lecz z (2) otrzymujemy dalej:

$$2MNd(M^2 - N^2) \equiv b(M^4 + N^4 - 2M^2N^2) \equiv b[(M^2 + N^2)^2 - 4M^2N^2],$$

skąd, ze względu na $M^2 + N^2 = p$, mamy [1])

$$d(M^2 - N^2) \equiv -2MNb \pmod{p},$$

i otrzymana kongruencja wskazuje, że przy spełnieniu (2) liczba d' jest też całkowita.

Lemmat II: Podstawienia (a', b', c', d') grupy $T^{-1}(0, 3; 2, 4, 5)\,T$, mogące wejść w skład grupy $(0, 3; 2, 4, 5)$, spełniać muszą warunek:

$$Md' \equiv Nb' \pmod{p}.$$

W samej rzeczy, na mocy lemmatu I każde takie podstawienie (a', b', c', d') musiało powstać drogą przekształcenia z takiego podstawienia (a, b, c, d), w którem wartości na a, b, c, d otrzymamy, rozwiązując kongruencje (3) co do a, b, c, d; będą to liczby:

$$a = a', \quad b = \frac{1}{p}\{(M^2 - N^2)b' + 2MNd'\},$$
$$c = c', \quad d = \frac{1}{p}\{(M^2 - N^2)d' - 2MNb'\}; \tag{4}$$

ale żeby liczby b i d były całkowite, musi się spełniać kongruencja:

$$(M^2 - N^2)d' \equiv 2MNb' \pmod{p},$$

którą ze względu na $M^2 + N^2 = p$, możemy zamienić na:

$$(2M^2 - p)d' \equiv 2MNb' \pmod{p},$$

stąd wynika:

[1]) Możemy skrócić $2MN$, ponieważ wszystkie ideały ciała $K(j)$ są główne; również liczba $M^2 - N^2$ jest niepodzielna przez p.

$$Md' \equiv Nb' \pmod{p}.$$

Otrzymujemy teraz twierdzenie:

Twierdzenie I: Najobszerniejsza wspólna podgrupa grup

$$(0, 3; 2, 4, 5) \text{ i } T^{-1}(0, 3; 2, 4, 5)\,T$$

składa się z podstawień (a, b, c, d), spełniających kongruencję;

$$Md \equiv Nb \pmod{p}.$$

W samej rzeczy, podstawienia te wchodzą w skład grupy $(0, 3; 2, 4, 5)$: lecz na zasadzie lemmatu II są to zarazem jedyne podstawienia grupy $T^{-1}(0, 3; 2, 4, 5)\,T$, które mogą wejść w skład szukanej wspólnej podgrupy.

§ 4.

Przechodząc obecnie do wyznaczenia wskaźnika podgrupy, wyznaczonej przez kongruencję:

$$Md \equiv Nb \pmod{p},$$

względem grupy $(0, 3; 2, 4, 5)$, możemy napisaną kongruencję zamienić na inną.

W samej rzeczy, jeżeli wyznaczymy liczbę $R + Sj$, spełniającą kongruencję:

$$(R + Sj)^2 \equiv -1 \pmod{p},$$

to będzie miała zawsze miejsce jedna z kongruencyj:

$$M(R + Sj) - N \equiv 0,$$
$$M(R + Sj) + N \equiv 0,$$

ponieważ wtedy iloczyn ich lewych stron

$$M^2(R + Sj)^2 - N^2$$

będzie, ze względu na warunek $M^2 + N^2 = p$, liczbą podzielną przez p.

Możemy przeto wypowiedzieć twierdzenie:

Twierdzenie II: Jeżeli istnieje liczba $R + Sj$, spełniająca kongruencję:

$$(R + Sj)^2 + 1 \equiv 0 \pmod{p}, \tag{5}$$

to przy przekształceniu grupy $(0, 3; 2, 4, 5)$ za pomocą dowolnego podstawienia:

$$T = \frac{Mz + N}{-Nz + M}$$

o wyznaczniku $M^2+N^2=p$ wspólną podgrupę grup $(0,3;2,4,5)$ i $T^{-1}(0,3;2,4,5)T$ wyznacza zawsze jedna z kongruencyj

$$\pm d \equiv (R+Sj)b \pmod{p}.$$

Zbiór przeto podstawień T o wyznaczniku p zawiera 2 klasy: dla jednej klasy wspólną podgrupę grup $(0,3;2,4,5)$ i $T^{-1}(0,3;2,4,5)T$ wyznacza kongruencja:

$$d \equiv (R+Sj)b \pmod{p},$$

dla drugiej klasy — wspólną podgrupę wyznacza kongruencja:

$$-d \equiv (R+Sj)b \pmod{p}.$$

§ 5.

Wszędzie wyżej zakładaliśmy istnienie liczby $R+Sj$, spełniającej kongruencję (5). Kongruencja ta jest równoważna następującym kongruencjom:

$$R^2+S^2 \equiv -1, \quad 2R \equiv S \pmod{p},$$

skąd otrzymujemy

$$5R^2+1 \equiv 0 \pmod{p}.$$

Liczba zatem $R+Sj$ istnieje tylko wtedy, jeżeli liczba pierwsza p spełnia warunek:

$$\left(\frac{-5}{p}\right)=1.$$

Jak widzimy, liczba pierwsza p musi mieć jednę z postaci:

$$20k+1, \quad 20k+3, \quad 20k+7, \quad 20k+9.$$

Mamy twierdzenie:

Twierdzenie III: Jeżeli przy przekształceniu p-go stopnia funkcji automorficznej $\varphi(z)$, należącej do grupy $(0,3;2,4,5)$, liczba pierwsza p spełnia warunek:

$$\left(\frac{-5}{p}\right)=1,$$

to funkcja przekształcona $\varphi(Tz)$ jest pierwiastkiem równania algebraicznego, którego stopień równa się wskaźnikowi podgrupy wyznaczonej przez kongruencję:

$$d \equiv (R+Sj)b \pmod{p},$$

w której liczbę $R+Sj$ wyznacza warunek: $(R+Sj)^2+1 \equiv 0 \pmod{p}$.

§ 6.

Mając teraz na celu wyznaczenie tego wskaźnika, zauważymy, że przy przekształceniu 3-go stopnia metoda Frickego polegała na wyznaczeniu obszaru zasadniczego rozważanej podgrupy. Liczba trójkątów, składających otrzymany obszar zasadniczy, wyznaczała wtedy wskaźnik rozważanej podgrupy. Zdaje się, że użycie tego sposobu w przypadku ogólnym byłoby niezwykle trudnem do przeprowadzenia.

Sposób nasz zasadzać się będzie na pewnej własności grupy skończonej G rzędu $\frac{1}{2}p^2(p^4-1)$, do której redukuje się grupa $(0,3;2,4,5)$ względem modułu p. Własność o której mówimy, polegać będzie na istnieniu u grupy G pewnej podgrupy rzędu $\frac{1}{2}p^2(p^2-1)$.

Podstawienia grupy skończonej G będziemy oznaczali symbolem (a,b,c,d); grupę G będziemy uważali, jako zbiór symboli (a,b,c,d), w których spółczynniki a,b,c,d przebiegać będą układ zupełny liczb całkowitych ciała $K(j)$, nieprzystających do siebie względem modułu p, i spełniać warunek:

$$a^2+c^2-j(b^2+d^2) \equiv 1 \pmod{p}.$$

§ 7.

Weźmiemy najprzód pod uwagę podstawienie

$$S=(1,1,0,R+Sj),$$

mające ostatni wyraz $R+Sj$; podstawienie to posiada własność:

$$S^p \equiv 1 \pmod{p},$$

ponieważ łatwo się przekonać, że wogóle każde podstawienie postaci $U=(1,b,c,d)$ ma okres p; w samej rzeczy, korzystając z wzorów:

$$\begin{aligned} A &= a\alpha+jb\beta-c\gamma+jd\delta,\\ B &= a\beta+\beta\alpha+c\delta-\gamma d,\\ C &= a\gamma+jb\delta+c\alpha-jd\beta,\\ D &= a\delta+d\alpha+b\gamma-c\beta \end{aligned} \tag{6}$$

na iloczyn

$$(A,B,C,D)=(a,b,c,d)(\alpha,\beta,\gamma,\delta),$$

znajdziemy kolejno:

$$U^2 \equiv (1,2b,2c,2d),$$

$$U^3 \equiv (1,3b,3c,3d),$$

$$\cdots\cdots\cdots$$

$$U^p \equiv (1,pb,pc,pd) \equiv (1,0,0,0) \equiv 1;$$

podstawienie S ma przytem wyznacznik $\equiv 1 \pmod p$, ponieważ $(R+Sj)^2 \equiv -1 \pmod p$.

Podstawienie to daje początek grupie cyklicznej:

$$G_p = (1, 1, 0, R+Sj)^k, \quad k = 0, 1, 2, \ldots p-1.$$

Ważnem będzie dla dalszego wyznaczenie wszystkich podstawień (a, b, c, d) grupy G, które przekształcałyby grupę G_p samą w siebie; zbiór tych podstawień będzie najobszerniejszą grupą, dla której grupa G_p będzie dzielnikiem normalnym.

Mamy przeto warunek:

$$(-a, b, c, d)(1, 1, 0, R+Sj)(a, b, c, d) \equiv (1, 1, 0, R+Sj),$$

ponieważ podstawienie $(-a, b, c, d)$ jest odwrotnością podstawienia (a, b, c, d).

Jeżeli lewą stronę tej kongruencji oznaczymy przez (a', b', c', d'), to korzystając z wzorów (6) i mając na uwadze warunek:

$$a^2 + c^2 - j(b^2 + d^2) \equiv 1 \pmod p, \tag{7}$$

znajdziemy:

$$\begin{aligned} a' &\equiv -1, \\ b' &\equiv -2a^2 + 2jb^2 + 1 + 2(R+Sj)(ca + bdj), \\ c' &\equiv -2adj + 2j(R+Sj)(dc + ab), \\ d' &\equiv -2ac + 2jbd + (R+Sj)(1 + 2d^2j - 2a^2); \end{aligned}$$

będziemy przeto (po skróceniu 2) mieli kongruencje:

$$\begin{aligned} c^2 - jd^2 + (R+Sj)(ca + bdj) &\equiv 0, \\ ad - (R+Sj)(ab + dc) &\equiv 0, \\ jbd - ac + (R+Sj)(c^2 - b^2j) &\equiv 0. \end{aligned} \tag{8}$$

Mnożąc pierwszą z tych kongruencyj przez b, a trzecią przez d, i dodając, otrzymamy:

$$bc^2 + c[(R+Sj)(ab + dc) - ad] \equiv 0 \pmod p,$$

co, ze względu na kongruencję drugą, zamieni się na:

$$bc^2 \equiv 0 \pmod p,$$

stąd albo 1°, $b \equiv 0$, albo 2°, $c \equiv 0$.

Warunek $b \equiv 0$ jest niemożliwy, ponieważ przy nim trzecia z kongruencyj (8) zamieni się na

$$c[-a + c(R+Sj)] \equiv 0,$$

i da warunek: $a \equiv c(R+Sj)$; lecz przy tym warunku pierwsza z kongruencyj (8) przejdzie na $-jd^2 \equiv 0$, co pociągnie za sobą $d \equiv 0$; ale otrzymane w ten sposób wartości:

$$b \equiv 0, \quad a \equiv c(R+Sj), \quad d \equiv 0$$

nie spełniają kongruencji (7).

Pozostaje możliwość $c \equiv 0$; wtedy trzecia z kongruencyj (8) przechodzi na

$$jb[d - b(R+Sj)] \equiv 0 \pmod p,$$

co daje

$$d \equiv b(R+Sj).$$

Wtedy i pierwsza z kongruencyj (8) spełnia się; z warunku zaś (7) otrzymujemy na a wartość $\equiv \pm 1$.

Poszukiwane podstawienia, przekształcające grupę G_p samą w siebie, będą zatem postaci:

$$(1, b, 0, (R+Sj)b); \tag{9}$$

liczba b, która pozostała niewyznaczona, przybierać będzie wszystkie wartości, nieprzystające do siebie względem modułu p.

Możemy przeto wypowiedzieć twierdzenie:

Twierdzenie IV: Zbiór p^2 podstawień postaci (9), w których b przebiega układ zupełny liczb całkowitych ciała $K(j)$, nieprzystających do siebie względem modułu p, tworzy najobszerniejszą grupę G_{p^2}, dla której grupa cykliczna G_p:

$$(1, 1, 0, R+Sj)^k, \; k = 0, 1, 2, \ldots p-1$$

jest dzielnikiem normalnym.

§ 8.

Możemy dalej przekonać się o istnieniu conajmniej $p^2 + 1$ grup powyższego typu.

W samej rzeczy, liczba[1]) podstawień (a, b, c, d) ze spółczynnikiem $a \equiv 1$, po odrzuceniu podstawienia $(1, 0, 0, 0)$, wynosi $p^4 - 1$. Jeżeli grupę G_{p^2} przekształcimy za pomocą dowolnego podstawienia U o okresie p, wziętego z liczby powyższych $p^4 - 1$ podstawień, to otrzymamy nową grupę rzędu p^2, złożoną wyłącznie z podstawień o okresie p.

Każde podstawienie o okresie p wchodzić będzie tylko raz jeden do pewnej określonej grupy typu G_{p^2}.

[1]) Liczba ta jest wyznaczona w pracy naszej: Przyczynek do przekształcenia 7-go stopnia pewnej funkcji automorficznej (Prace Komisji Mat.-Przyrod. Poz. Tow. Nauk., serja D, t. I, str. 28).

W samej rzeczy, jeżeliby S_1 i S_2 były dwoma podstawieniami grupy G_{p^2}, z których jedno, np., S_1 mogłoby wejść w skład nowej grupy, otrzymanej z G_{p^2} drogą przekształcenia przy pomocy podstawienia V, to musiałoby być:

$$S_1 = V^{-1} S_2 V,$$

skąd wynikałoby: $VS_1 = S_2 V$, co jest jednak niemożliwe, ponieważ grupa G_{p^2}, zgodnie z definicją, jest zbiorem wszystkich podstawień o okresie p przemiennych ze sobą.

Jeżeli przeto każde podstawienie o okresie p z ogólnej ich liczby p^4-1 wejdzie tylko raz jeden do pewnej określonej grupy rzędu p^2, zawierającej p^2-1 podstawień, różnych od 1, to liczba otrzymanych grup będzie wynosiła $(p^4-1):(p^2-1) = p^2+1$.

§ 9.

Okażemy teraz, że grupa G_{p^2} jest dzielnikiem normalnym o wskaźniku $\frac{1}{2}(p^2-1)$ pewnej grupy rzędu $\frac{1}{2}p^2(p^2-1)$.

Dołączymy w tym celu do p^2 podstawień:

$$(1, b, 0, (R + Sj)\, b)$$

wszystkie podstawienia postaci:

$$(a, b, c, (R + Sj)\, b).$$

Będziemy mieli $\frac{1}{2}(p^2-1)$ układów po p^2 takich podstawień; w samej rzeczy, ze względu na warunek (7), mieć będziemy:

$$a^2 + c^2 - jb^2\,[1 + (R + Sj)^2] \equiv 1 \pmod p,$$

skąd, zważając na kongruencję:

$$(R + Sj)^2 + 1 \equiv 0 \pmod p,$$

otrzymamy na wyznaczenie a i c zależność: $a^2 + c^2 \equiv 1 \pmod p$; otrzymamy w ten sposób $\frac{1}{2}(p^2-1)$ par (a, c) wartości [1]) na a i c. Dalszych układów postaci:

$$(-a, b, -c, (R + Sj)\, b)$$

brać pod uwagę nie będzie trzeba, gdyż podstawienia takie mogą być napisane w postaci:

$$(a, -b, c, -(R + Sj)\, b),$$

i, jak widać odrazu, nie przedstawiają nowych podstawień (mod p).

Po tych uwagach udowodnimy twierdzenie, które da możność wyznaczenia poszukiwanego przez nas wskaźnika.

[1]) P. pracę naszą wyżej cytowaną, str. 29.

Twierdzenie V: Zbiór $\frac{1}{2}p^2(p^2-1)$ podstawień postaci:

$$(a, b, c, (R + Sj)\, b),$$

w których b przebiega układ zupełny liczb nieprzystających do siebie względem modułu p, a liczby a i c spełniają kongruencję

$$a^2 + c^2 \equiv 1 \pmod p,$$

tworzy grupę, dla której grupa G_{p^2} jest dzielnikiem normalnym.

Wystarczy napisać iloczyn:

$$(a, b, c, (R + Sj)\, b) \cdot (a_1, b_1, c_1, (R + Sj)\, b_1)$$

dwóch podstawień

$$(a, b, c, (R + Sj)\, b) \text{ i } (a_1, b_1, c_1, (R + Sj)\, b_1),$$

spełniających warunki:

$$a^2 + c^2 \equiv 1, \quad a_1^2 + c_1^2 \equiv 1 \pmod p.$$

Oznaczając go przez (A, B, C, D), mieć będziemy:

$$A \equiv aa_1 - cc_1,$$

$$B \equiv ab_1 + ba_1 + (R + Sj)(cb_1 - c_1 b),$$

$$C \equiv ac_1 + ca_1,$$

$$D \equiv bc_1 - cb_1 + (R + Sj)(ab_1 + ba_1).$$

Mając dalej na uwadzę kongruencję:

$$(R + Sj)^2 \equiv -1 \pmod p,$$

sprawdzimy natychmiast zależność:

$$D \equiv (R + Sj)\, B \pmod p. \tag{9}$$

Mamy także dalej:

$$A^2 + C^2 \equiv a^2 a_1^2 + c^2 c_1^2 + a^2 c_1^2 + c^2 a_1^2 \equiv$$

$$\equiv (a^2 + c^2)\, a_1^2 + c^2 c_1^2 + c_1^2 (1 - c^2) \equiv a_1^2 + c_1^2 \equiv 1,$$

co w związku z (9) dowodzi, że zbiór wymienionych w twierdzeniu podstawień rzeczywiście tworzy grupę.

Aby okazać, że grupa G_{p^2} jest dzielnikiem normalnym tej grupy, zauważymy najwpierw, że grupa ta, zgodnie z definicją, zawiera w sobie

tylko p^2 podstawień o pierwszym wyrazie $a \equiv 1$; są niemi wszystkie podstawienia grupy G_{p^2}. Jeżeli teraz przekształcimy grupę G_{p^2} za pomocą jakiegokolwiek podstawienia

$$U = (a', b', c', d'),$$

to z łatwością obliczymy na zasadzie wzorów § 3, że pierwszy wyraz a u podstawień grupy $U^{-1} G_{p^2} U$ będzie liczbą:

$$a'^2 + c'^2 - j(b'^2 + d'^2) \equiv 1 \pmod{p},$$

przystającą względem modułu p do 1.

Zgodnie przeto z wyżej powiedzianem będzie musiało być:

$$U^{-1} G_{p^2} U = G_{p^2}$$

dla wszelkiego U.

§ 10.

Wyznaczenie grupy rzędu $\frac{1}{2}p^2(p^2-1)$ daje nam teraz możność udowodnienia następującego twierdzenia:

Twierdzenie VI: Jeżeli liczbę $R + Sj$ wyznacza kongruencja:

$$(R + Sj)^2 + 1 \equiv 0 \pmod{p},$$

to zbiór wszystkich podstawień:

$$\frac{(a + b\sqrt{j})\, z + c + d\sqrt{j}}{(-c + d\sqrt{j})\, z + a - b\sqrt{j}} \qquad (10)$$

grupy $(0, 3;\ 2, 4, 5)$, spełniających warunek:

$$d \equiv (R + Sj)\, b \pmod{p}, \qquad (11)$$

tworzy podgrupę grupy $(0, 3;\ 2, 4, 5)$ o wskaźniku $p^2 + 1$.

Oznaczymy początkowo wskaźnik literą μ, a rozważaną podgrupę podstawień (10), spełniających warunek (11), literą Γ_μ; grupę $(0, 3;\ 2, 4, 5)$ można będzie wtedy przedstawić w postaci:

$$(0, 3;\ 2, 4, 5) = (\Gamma_\mu, S_2\, \Gamma_\mu, \ldots\ldots S_\mu\, \Gamma_\mu),$$

gdzie litery S_i oznaczać będą pewne, różne między sobą, podstawienia (10), nie spełniające kongruencji (11).

Jeżeli teraz zwrócimy uwagę na grupę skończoną G rzędu $\frac{1}{2}p^2(p^4-1)$, do której redukuje się względem modułu p grupa $(0, 3;\ 2, 4, 5)$, to spostrzeżemy, że względem modułu p podstawienia grupy Γ_μ zredukują się do podstawień (a, b, c, d) grupy G, czyniących zadość kongruencji (11); innemi słowy, grupa Γ_μ zredukuje się do zbioru podstawień:

$$(a, b, c, (R + Sj)\, b),$$

który, zgodnie z twierdzeniem V, jest grupą rzędu $\frac{1}{2}p^2(p^2-1)$.

Wskaźnik μ wyniesie przeto $\frac{1}{2}p^2(p^4-1)$: $\frac{1}{2}p^2(p^2-1) = p^2 + 1$.

§ 11.

Ponieważ, jak to wpierw już było zaznaczone, stopień równania algebraicznego, któremu czyni zadość funkcja automorficzna przekształcona $\varphi(Tz)$, równać się musi wskaźnikowi najobszerniejszej wspólnej podgrupy grup $(0, 3;\ 2, 4, 5)$ i przekształconej $T^{-1}(0, 3;\ 2, 4, 5)\, T$, to zostało jednocześnie udowodnione twierdzenie:

Twierdzenie VII: Jeżeli liczba naturalna p spełnia 1^0, warunek:

$$\left(\frac{-5}{p}\right) = 1,$$

i 2^0, jest liczbą pierwszą w ciele $K(j)$, to przy rozważanem przez nas przekształceniu

$$T(z) = \frac{Mz + N}{-Nz + M}$$

p-go stopnia funkcji automorficznej $\varphi(z)$, należącej do grupy $(0, 3;\ 2, 4, 5)$, funkcja przekształcona $\varphi(Tz)$ jest pierwiastkiem równania algebraicznego stopnia $p^2 + 1$.

§ 12.

Liczby p, spełniające pierwszy warunek twierdzenia VII, tworzą szereg:

$$3, 7, 23, 29, 41, 43, 47, 61, \ldots\ldots$$

Po liczbie $p=3$, rozważanej przez Frickego, następuje[1]) liczba $p=7$, która jest pierwszą w ciele $K(j)$; zastosujemy ogólne nasze uwagi do tego przypadku.

Łatwo się najwpierw przekonamy, że liczba możliwych podstawień postaci

$$z' = \frac{Mz + N}{-Nz + M}$$

[1]) Przypadek liczby 5, która nie jest pierwszą w ciele $K(j)$, był przedmiotem cytowanej poprzednio pracy Frickego w Acta mathematica, 17; prowadzi on do grupy dwudziestościanu.

o wyznaczniku $M^2 + N^2 = 7$ wynosić będzie 4. W samej rzeczy, kładąc:

$$M = \alpha + \beta j, \quad N = \gamma + \delta j,$$

gdzie $\alpha, \beta, \gamma, \delta$ są liczbami całkowitemi wymiernemi, przekonamy się natychmiast, że liczby $\alpha, \beta, \gamma, \delta$, muszą spełniać warunek:

$$\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = 7;$$

rozkład zaś liczby 7 na sumę 4 kwadratów jest jeden:

$$2^2 + 1^2 + 1^2 + 1^2 = 7.$$

Uwzględniając jeszcze warunek

$$2(\alpha\beta + \gamma\delta) = \beta^2 + \delta^2,$$

który muszą spełniać liczby $\alpha, \beta, \gamma, \delta$, znajdziemy tylko następujące 4 możliwe układy wartości na liczby $\alpha, \beta, \gamma, \delta$:

$$\begin{matrix} 2, & 1, & -1, & 1 \\ 1, & -1, & 2, & 1 \\ 2, & 1, & 1, & -1 \\ -1, & 1, & 2, & 1. \end{matrix}$$

Do przekształcenia 7-go stopnia funkcji automorficznej $\varphi(z)$ możemy przeto użyć jednego z czterech następujących podstawień:

$$T_1 = \begin{pmatrix} 2+j, & -1+j \\ 1-j, & 2+j \end{pmatrix}, \quad T_2 = \begin{pmatrix} 1-j, & 2+j \\ -2-j, & 1-j \end{pmatrix},$$

$$T_3 = \begin{pmatrix} 2+j, & 1-j \\ -1+j, & 2+j \end{pmatrix}, \quad T_4 = \begin{pmatrix} 1-j, & -2-j \\ 2+j, & 1-j \end{pmatrix},$$

o wyznaczniku 7.

Liczbą $R + Sj$ będzie w rozważanym przypadku liczba $5 + 3j$; po nieważ sprawdzamy, że $(5 + 3j)^2 \equiv -1 \pmod 7$.

Przekonamy się dalej, że przy podstawieniach T_1 i T_2 wspólną podgrupę grupy $(0, 3; 2, 4, 5)$ i grupy przekształconej wyznacza kongruencja:

$$d \equiv (5 + 3j)\, b \pmod 7;$$

przy podstawieniach T_3 i T_4 odpowiednią podgrupę wyznaczy kongruencja:

$$d \equiv (2 + 4j)\, b \pmod 7.$$

Podstawienia $(1, b, 0, (5 + 3j)\, b)$, przekształcające podstawienie $(1, 1, 0, 5 + 3j)$ samo w siebie, tworzą grupę G_{49} rzędu 49. Grupa ta jest dzielnikiem normalnym grupy G_{1176} rzędu 1176. Funkcje przekształcone $\varphi(T_1 z)$, $\varphi(T_2 z)$, $\varphi(T_3 z)$, $\varphi(T_4 z)$ będą pierwiastkami równań algebraicznych stopnia 50.

ROMUALD WITWIŃSKI
lieutenant de cavalerie.

Recherches sur les réseaux isothermes des surfaces.

Badania nad sieciami izotermicznemi powierzchni [1]).

Les pages qui suivent ont pour principal objet d'étendre la notion de réseau isotherme, afin de faire rentrer dans une même théorie diverses classes de réseaux, notamment ceux qui caractérisent soit les surfaces isothermiques, soit les surfaces dont les lignes de courbure ont leur représentation sphérique isotherme, et ceux que Bianchi appelle isothermes-conjuguées.

Je commence par définir l'isothermie relative de deux réseaux et, après avoir montré qu'a deux réseaux qui présentent cette propriété on en peut toujours associer un troisième, qui est dans la même relation avec chacun d'eux, je donne sous forme invariante les conditions qui assurent l'isothermie relative de deux réseaux.

J'applique d'abord ces conditions aux surfaces à lignes de courbure isothermes, et je ramène l'un à l'autre les deux critères de S. Lie et de M. Weingarten relatifs à ces surfaces.

Une seconde application concerne les surfaces à lignes de courbure isothermes-conjuguées, dont l'étude a été commencée par Eisenhart (*American Journal of Mathematics*, t. XXV, p. 213—248). Par le fait même de son rattachement à une notion plus large, cette étude se trouve complétée sur divers points. Je calcule à nouveau, en la généralisant, l'équation aux dérivées partielles des surfaces de Eisenhart et j'en déduis leurs caractéristiques (lignes de courbure et lignes asymptotiques).

[1]) Praca, przedstawiona na posiedzeniu Warszawskiego Oddziału Polskiego Towarzystwa Matematycznego, listopad, 1923 r.