

Gdyby p było formy $12k+5$, to mielibyśmy

$$(-1)^{\frac{p-1}{2}} = (-1)^{6k+2} = +1 \quad \text{i} \quad \left(\frac{p}{5}\right) = \left(\frac{12k+5}{5}\right) = \left(\frac{2}{5}\right) = -1,$$

skąd $(-1)^{\frac{p-1}{2}} \left(\frac{p}{5}\right) = -1$ wbrew (30). Podobnie w razie $p=12k-5$ byłoby

$$(-1)^{\frac{p-1}{2}} = (-1)^{6k-3} = -1 \quad \text{i} \quad \left(\frac{p}{5}\right) = \left(\frac{12k-5}{5}\right) = \left(\frac{-5}{5}\right) = \left(\frac{1}{5}\right) = 1,$$

skąd $(-1)^{\frac{p-1}{2}} \left(\frac{p}{5}\right) = -1$ wbrew (30). Jest więc $p=12k+1$ albo $p=12k-1$. Lecz nie wszystkie czynniki pierwsze liczby N , która jest sama formy $12k-1$, mogą być formy $12k+1$; znajdzie się więc wśród nich co najmniej jeden formy $12k-1$. Stąd, jak wyżej, otrzymujemy wniosek sprzeczny z przypuszczeniem.

W postępie arytmetycznym

$$11, 23, 35, 47, 59, \dots$$

jest zatem nieskończenie wiele liczb pierwszych, c. b. d. o.

ROZDZIAŁ XV

ZARYS TEORII FORM KWADRATOWYCH

§ 1. Formy kwadratowe dwójkowe jednorodne i ich wyróżnik. Zagadnienie podstawowe teorii form kwadratowych. Formą kwadratową dwójkową jednorodną nazywamy wyrażenie

$$(1) \quad ax^2 + bxy + cy^2,$$

gdzie a, b i c są liczbami całkowitymi, a x i y — zmiennymi, przebiegającymi tylko wartości całkowite. Wyrażenie (1) oznaczamy przez

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

Liczbę

$$D = b^2 - 4ac$$

nazywamy *wyróżnikiem* (*dyskryminantą*) formy kwadratowej (1).

Będziemy zakładali, że D nie jest kwadratem liczby całkowitej, gdyż w przeciwnym razie forma (1) byłaby iloczynem dwu form liniowych. W razie bowiem $D = b^2 - 4ac = d^2$ i $a \neq 0$, byłoby $(b-d)(b+d) = 4ac$, skąd wnosimy z łatwością, że liczby $b-d$ i $b+d$ byłyby obie parzyste. Ale jeżeli $b-d = 2k$ i $b+d = 2l$, to $kl = ac$. Niech $(k, a) = \delta$. Wówczas byłoby $k = k_1\delta$ i $a = a_1\delta$, gdzie $(k_1, a_1) = 1$ i $k_1\delta l = a_1\delta c$, skąd $k_1 l = a_1 c$. Wobec $(k_1, a_1) = 1$ byłoby więc $a_1 | l$ czyli $l = l_1 a_1$, gdzie l_1 jest liczbą całkowitą, i mielibyśmy:

$$2ax + (b-d)y = 2\delta(a_1x + k_1y),$$

$$2ax + (b+d)y = 2a_1(\delta x + l_1y),$$

skąd wobec $d^2 = D$

$$4a(ax^2 + bxy + cy^2) = (2ax + b)^2 - D y^2 =$$

$$= [2ax + (b-d)y][2ax + (b+d)y] = 4a_1\delta(a_1x + k_1y)(\delta x + l_1y),$$

co daje wobec $a_1\delta = a$ po podzieleniu obu stron przez $4a$

$$ax^2 + bxy + cy^2 = (a_1x + k_1y)(\delta x + l_1y).$$

W razie zaś $a=0$ mielibyśmy wprost z (1)

$$ax^2 + bxy + cy^2 = (bx + cy)y.$$

Z założenia że liczba D nie jest kwadratowa, wynika, że $a \neq 0$ i $c \neq 0$.

Jeżeli dla liczby całkowitej m istnieją takie liczby całkowite x i y , że

$$m = ax^2 + bxy + cy^2,$$

to powiadamy, że liczba m daje się przedstawić przez formę (a, b, c) .

Zagadnienie podstawowe teorii form kwadratowych jest następujące:

Znaleźć kryterium przedstawialności liczby m przez daną formę kwadratorną i wyznaczyć wszystkie przedstawienia liczby m przez tę formę.

Bez ujemy dla ogólności możemy też założyć, że współczynniki a, b, c formy (1) nie mają wspólnego dzielnika większego od 1. Gdyby bowiem pewna liczba $d > 1$ była największym wspólnym dzielnikiem liczb a, b, c , to moglibyśmy przyjąć:

$$a = da', \quad b = db', \quad c = dc',$$

gdzie liczby a', b', c' już nie mają wspólnego dzielnika większego od 1, i badać przedstawienia liczby m/d przez formę (a', b', c') zamiast przedstawień liczby m przez formę (a, b, c) .

Podobnie, możemy założyć, że liczby x, y są względnie pierwsze, bo gdyby miały największy wspólny dzielnik $d > 1$, to przyjmując

$$x = dx', \quad y = dy',$$

moglibyśmy zastąpić

$$m = ax^2 + bxy + cy^2$$

przez

$$m, d^3 = ax'^2 + bx'y' + cy'^2,$$

gdzie liczby x' i y' są względnie pierwsze.

Przedstawienie liczby m przez formę (1), w którym x i y są względnie pierwsze, nazywamy *właściwym*.

Dla wyznaczenia wszystkich przedstawień liczby m przez daną formę, wystarczy więc wyznaczyć wszystkie przedstawienia właściwe liczby m/d^3 , podstawiając za d^3 wszystkie dzielniki kwadratowe liczby m .

§ 2. Równoważność właściwa i niewłaściwa dwu form kwadratowych. Klasy form kwadratowych. Niech a, β, γ i δ będą liczbami całkowitymi. Podstawmy do (1)

$$(2) \quad x = a\xi + \beta\eta, \quad y = \gamma\xi + \delta\eta.$$

Otrzymamy

$$ax^2 + bxy + cy^2 = a(a\xi + \beta\eta)^2 + b(a\xi + \beta\eta)(\gamma\xi + \delta\eta) + c(\gamma\xi + \delta\eta)^2 = \\ = (aa^2 + b\alpha\gamma + c\gamma^2)\xi^2 + (2a\alpha\beta + b(a\delta + \gamma\beta) + 2c\gamma\delta)\xi\eta + (a\beta^2 + b\beta\delta + c\delta^2)\eta^2,$$

co w oznaczeniach

$$(5) \quad \begin{cases} a_1 = aa^2 + b\alpha\gamma + c\gamma^2, \\ b_1 = 2a\alpha\beta + b(a\delta + \gamma\beta) + 2c\gamma\delta, \\ c_1 = a\beta^2 + b\beta\delta + c\delta^2 \end{cases}$$

przybiera postać

$$(4) \quad ax^2 + bxy + cy^2 = a_1\xi^2 + b_1\xi\eta + c_1\eta^2.$$

Możemy więc powiedzieć, że forma (a, b, c) przez podstawienie (2) przechodzi w formę (a_1, b_1, c_1) . Będziemy to pisali krótko

$$(5) \quad \begin{pmatrix} a, \beta \\ \gamma, \delta \end{pmatrix} (a, b, c) = (a_1, b_1, c_1).$$

Wzór (5) jest — jak łatwo widzieć — równoważny układowi równań (3).

Jeżeli dla dwu form (a, b, c) i (a_1, b_1, c_1) zachodzi wzór (5) przy pewnych całkowitych $\alpha, \beta, \gamma, \delta$, to każda liczba m , dająca się przedstawić przez formę (a, b, c) , daje się też przedstawić przez formę (a_1, b_1, c_1) .

Istotnie, niech liczba m daje się przedstawić przez formę (a_1, b_1, c_1) , czyli że przy pewnych całkowitych ξ, η

$$(6) \quad a_1\xi^2 + b_1\xi\eta + c_1\eta^2 = m.$$

Wyznaczając liczby całkowite x i y ze wzorów (2), otrzymamy w myśl (5) równość (4), a zatem wobec (6)

$$ax^2 + bxy + cy^2 = m,$$

co dowodzi, że liczba m daje się przedstawić przez formę (a, b, c) .

Niech w szczególności

$$(7) \quad \alpha\delta - \gamma\beta = \pm 1.$$

Na mocy (5) i (7) jest, jak łatwo sprawdzić,

$$\begin{aligned} a_1\delta^2 - b_1\delta\gamma + c_1\gamma^2 &= a, \\ -2a_1\delta\beta + b_1(\delta\alpha + \gamma\beta) - 2c_1\gamma\alpha &= b, \\ a_1\beta^2 - b_1\beta\alpha + c_1\alpha^2 &= c, \end{aligned}$$

co dowodzi, że

$$(8) \quad \begin{pmatrix} \delta, -\beta \\ -\gamma, \alpha \end{pmatrix} (a_1, b_1, c_1) = (a, b, c),$$

czyli że w przypadku (7) każda liczba, przedstawialna przez formę (a, b, c) , daje się też przedstawić przez formę (a_1, b_1, c_1) .

Jeżeli dla form (a, b, c) i (a_1, b_1, c_1) zachodzą wzory (5) i (7), to będziemy pisali krótko

$$(9) \quad (a, b, c) \sim (a_1, b_1, c_1).$$

Wówczas przyjmując oznaczenia

$$\alpha_1 = \delta, \quad \beta_1 = -\beta, \quad \gamma_1 = -\gamma, \quad \delta_1 = \alpha,$$

możemy napisać wzór (8) w postaci

$$(10) \quad \begin{pmatrix} \alpha_1, \beta_1 \\ \gamma_1, \delta_1 \end{pmatrix} (a_1, b_1, c_1) = (a, b, c),$$

przy czym na mocy (7) jest analogicznie

$$(11) \quad \alpha_1\delta_1 - \gamma_1\beta_1 = \delta\alpha - \gamma\beta = \pm 1,$$

skąd

$$(12) \quad (a_1, b_1, c_1) \sim (a, b, c).$$

Relacja $\sim$ jest więc symetryczna.

Dwie formy, dla których ta relacja zachodzi, nazywamy *równoważnymi*.

Każda liczba, dająca się przedstawić przez jedną z dwu form równoważnych, daje się więc też przedstawić przez drugą. Możemy zatem wypowiedzieć

Twierdzenie 1. *Na to, żeby dwie formy (a, b, c) i (a_1, b_1, c_1) były równoważne, potrzeba i wystarcza, by zachodził wzór (5) przy pewnych całkowitych $\alpha, \beta, \gamma, \delta$, spełniających warunek (7).*

Jeżeli przy tym $\alpha\delta - \gamma\beta = +1$, to mówimy, że forma (a, b, c) jest równoważna *właściwie* formie (a_1, b_1, c_1) , jeżeli zaś $\alpha\delta - \gamma\beta = -1$, to mówimy, że forma (a, b, c) jest równoważna *niewłaściwie* formie (a_1, b_1, c_1) .

Ponieważ wzór (5), przy warunku (7), pociąga za sobą — jak dowiedliśmy — wzór (10) i w myśl (11) jest $\alpha_1\delta_1 - \gamma_1\beta_1 = \delta\alpha - \gamma\beta$, więc jeżeli forma (a, b, c) jest równoważna formie (a_1, b_1, c_1) właściwie, to i forma (a_1, b_1, c_1) jest równoważna formie (a, b, c) właściwie. Ta sama wzajemność zachodzi dla równoważności niewłaściwej.

Oczywiście może się zdarzyć, że dana forma kwadratowa jest równoważna innej formie (lub sama sobie) zarówno właściwie jak niewłaściwie. Np. takimi są formy $(1, 0, -2)$ i $(-1, 0, 2)$, gdyż — jak łatwo sprawdzić:

$$\begin{pmatrix} 1, & 2 \\ -1, & -1 \end{pmatrix} (1, 0, -2) = (-1, 0, 2),$$

$$\begin{pmatrix} 1, & 2 \\ 1, & 1 \end{pmatrix} (1, 0, -2) = (-1, 0, 2).$$

Każda forma jest sama sobie zawsze równoważna właściwie, gdyż zawsze

$$\begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix} (a, b, c) = (a, b, c).$$

Jeżeli forma

$$(13) \quad ax^2 + bxy + cy^2$$

przez podstawienie

$$x = \alpha\xi + \beta\eta, \quad y = \gamma\xi + \delta\eta$$

przechodzi na formę

$$a_1\xi^2 + b_1\xi\eta + c_1\eta^2,$$

która przez podstawienie

$$\xi = \alpha_1t + \beta_1u, \quad \eta = \gamma_1t + \delta_1u$$

przechodzi na formę

$$(14) \quad a_2t^2 + b_2tu + c_2u^2,$$

to — jak łatwo widzieć — forma (13) przechodzi na formę (14) przez podstawienie

$$x = \alpha(\alpha_1 t + \beta_1 u) + \beta(\gamma_1 t + \delta_1 u), \quad y = \gamma(\alpha_1 t + \beta_1 u) + \delta(\gamma_1 t + \delta_1 u),$$

czyli przez podstawienie

$$x = (\alpha\alpha_1 + \beta\gamma_1)t + (\alpha\beta_1 + \beta\delta_1)u, \quad y = (\gamma\alpha_1 + \delta\gamma_1)t + (\gamma\beta_1 + \delta\delta_1)u.$$

Wzory

$$\begin{pmatrix} \alpha, \beta \\ \gamma, \delta \end{pmatrix} (a, b, c) = (a_1, b_1, c_1) \quad \text{i} \quad \begin{pmatrix} \alpha_1, \beta_1 \\ \gamma_1, \delta_1 \end{pmatrix} (a_1, b_1, c_1) = (a_2, b_2, c_2)$$

pociągają więc za sobą wzór

$$(15) \quad \begin{pmatrix} \alpha_2, \beta_2 \\ \gamma_2, \delta_2 \end{pmatrix} (a, b, c) = (a_2, b_2, c_2),$$

gdzie

$$\begin{aligned} \alpha_2 &= \alpha\alpha_1 + \beta\gamma_1, & \beta_2 &= \alpha\beta_1 + \beta\delta_1, \\ \gamma_2 &= \gamma\alpha_1 + \delta\gamma_1, & \delta_2 &= \gamma\beta_1 + \delta\delta_1, \end{aligned}$$

skąd — jak łatwo widzieć —

$$(16) \quad \alpha_2\delta_2 - \gamma_2\beta_2 = (\alpha\delta - \gamma\beta)(\alpha_1\delta_1 - \gamma_1\beta_1).$$

Wzory (15) i (16) dowodzą, że zachodzi następujące

Twierdzenie 2. Jeżeli formy (a, b, c) i (a_2, b_2, c_2) są obie właściwie lub obie niewłaściwie równoważne formie (a_1, b_1, c_1) , to forma (a, b, c) jest równoważna formie (a_2, b_2, c_2) właściwie; jeżeli zaś jedna z form (a, b, c) i (a_2, b_2, c_2) jest równoważna formie (a_1, b_1, c_1) właściwie, a druga niewłaściwie, to forma (a, b, c) jest równoważna formie (a_2, b_2, c_2) niewłaściwie.

Wynika stąd, że relacja $\sim$ jest przechodnia.

Ponadto zachodzi następujące

Twierdzenie 3. Formy równoważne mają ten sam wyróżnik.

Istotnie, wzory (5) dają, jak łatwo sprawdzić,

$$4a_1c_1 = b_1^2 + (4ac - b^2)(\alpha\delta - \gamma\beta)^2,$$

skąd wobec (7)

$$4a_1c_1 - b_1^2 = 4ac - b^2.$$

Ponieważ w myśl twierdzenia 2 dwie formy, równoważne jednej i tej samej trzeciej właściwie, są sobie równoważne właściwie, więc możemy wszystkie formy o danym wyróżniku D podzielić na klasy, zaliczając do jednej i tej samej klasy dwie formy o tym samym wyróżniku wtedy i tylko wtedy, gdy są równoważne właściwie.

§ 3. Grupy przedstawień liczby m przez formę (a, b, c) . Niech

$$(17) \quad m = ax^2 + bxy + cy^2$$

będzie przedstawieniem właściwym liczby $m \neq 0$ przez formę kwadratową (a, b, c) . Liczby x i y są więc względnie pierwsze. Wobec tego możemy wyznaczyć takie liczby całkowite p_0 i q_0 , że $q_0x - p_0y = 1$, przy czym — jak wiemy z Rozdziału II (§ 3, str. 37) — ogólne rozwiązanie równania

$$(18) \quad qx - py = 1$$

względem niewiadomych p i q dane jest przez wzory

$$(19) \quad p_k = p_0 + kx, \quad q_k = q_0 + ky,$$

gdzie k jest dowolną liczbą całkowitą. Niech

$$r_k = (2ax + by)p_k + (bx + 2cy)q_k.$$

Wobec (17) i (19) jest więc

$$r_k = r_0 + (2ax + by)kx + (bx + 2cy)ky = r_0 + 2km,$$

skąd widać, że wśród liczb r_k istnieje jedna i tylko jedna taka liczba

$$(20) \quad r = (2ax + by)p + (bx + 2cy)q,$$

że

$$(21) \quad 0 \leq r < 2|m|.$$

Za pomocą łatwego rachunku sprawdzamy, że

$$\begin{aligned} &4(ax^2 + bxy + cy^2)(ap^2 + bpq + cq^2) = \\ &= [(2ax + by)p + (bx + 2cy)q]^2 - D(qx - py)^2, \end{aligned}$$

skąd wobec (17), (18) i (20)

$$(22) \quad r^2 = D + 4m(ap^2 + bpq + cq^2),$$

a zatem

$$(23) \quad r^2 \equiv D \pmod{4m}.$$

Dowiedliśmy więc, że każdemu przedstawieniu właściwemu liczby m przez formę (a, b, c) odpowiada jeden i tylko jeden pierwiastek kongruencji (23), spełniający nierówności (21).

Wynika stąd

Twierdzenie 4. Na to, by liczba m dała się przedstawić przez formę (a, b, c) , potrzeba, żeby jej wyróżnik D był resztą kwadrata liczby $4m$.

Będziemy mówili, że dane przedstawienie (17) należy do pierwiastka r kongruencji (23). Wszystkie przedstawienia liczby m przez formę (a, b, c) , należące to tego samego pierwiastka kongruencji (23), zaliczać będziemy do jednej i tej samej grupy przedstawień tej liczby przez formę (a, b, c) .

Zachowując te same oznaczenia, weźmy pod uwagę liczbę

$$(24) \quad n = ap^2 + bpq + cq^2.$$

W myśl (17), (20) i (24) jest

$$\begin{aligned} ax^2 + bxy + cy^2 &= m, \\ 2axp + b(xq + yp) + 2cyq &= r, \\ ap^2 + bpq + cq^2 &= n, \end{aligned}$$

zatem

$$\begin{pmatrix} x, p \\ y, q \end{pmatrix} (a, b, c) = (m, r, n),$$

skąd wnosimy na mocy (18), że formy (a, b, c) i (m, r, n) są równoważne właściwie.

Według (22) i (24) jest $r^2 = D + 4mn$, skąd $n = \frac{r^2 - D}{4m}$. Możemy więc wypowiedzieć

Twierdzenie 5. *Na to, by wzór (17) dawał przedstawienie właściwe liczby m przez formę (a, b, c) należącą do pierwiastka r kongruencji (23), potrzeba, żeby formy*

$$(25) \quad (a, b, c) \quad \text{i} \quad \left(m, r, \frac{r^2 - D}{4m}\right)$$

były równoważne właściwie.

Okazemy, że warunek ten zarazem wystarcza na to, żeby istniało przynajmniej jedno przedstawienie liczby m przez formę (a, b, c) , należące do pierwiastka r kongruencji (23), spełniającego nierówność (21).

Dowód. Jeżeli r jest pierwiastkiem kongruencji (23), a więc jeżeli $r^2 - D$ jest liczbą podzielną przez $4m$, i jeżeli formy (25) są równoważne właściwie, to istnieją takie liczby całkowite $\alpha, \beta, \gamma, \delta$, że

$$(26) \quad \alpha\delta - \gamma\beta = 1 \quad \text{i} \quad \begin{pmatrix} \alpha, \beta \\ \gamma, \delta \end{pmatrix} (a, b, c) = \left(m, r, \frac{r^2 - D}{4m}\right).$$

Z ostatniego wzoru wynika — jak widzieliśmy — że

$$(27) \quad aa^2 + ba\gamma + c\gamma^2 = m,$$

$$(28) \quad 2aa\beta + b(a\delta + \gamma\beta) + 2c\gamma\delta = r.$$

Wzór (27) daje przedstawienie liczby m przez formę (a, b, c) ; istnieje więc jedno tylko rozwiązanie p, q równania

$$qa - p\gamma = 1,$$

dla którego

$$0 \leq (2aa + b\gamma)p + (ba + 2c\gamma)q < 2|m|,$$

a zatem w myśl (21), (26) i (28)

$$\beta = p \quad \text{i} \quad \delta = q,$$

co dowodzi, że przedstawienie (27) istotnie należy do pierwiastka r .

§ 4. Wyznaczanie wszystkich przedstawień należących do danej grupy. Zapytajmy obecnie, jak znając jedno przedstawienie liczby m należące do danej grupy, można wyznaczyć wszystkie inne przedstawienia, do niej należące.

Niech przedstawienia

$$(29) \quad ax^2 + bxy + cy^2 = m, \quad ax_1^2 + bx_1y_1 + cy_1^2 = m$$

należą do tego samego pierwiastka r kongruencji (23). Jest więc przy pewnych całkowitych p i q

$$qx - py = 1, \quad (2ax + by)p + (bx + 2cy)q = r;$$

ostatnie dwa wzory dają w jednej chwili

$$rx = (2ax + by)px + (bx + 2cy)(1 + py)$$

czyli

$$rx = 2pm + bx + 2cy$$

i podobnie

$$ry = (2ax + by)(qx - 1) + (bx + 2cy)qy$$

czyli

$$ry = 2qm - 2ax - by.$$

Otrzymane wzory dla rx i ry możemy napisać w postaci:

$$(30) \quad (r - b)x - 2cy = 2pm, \quad (r + b)y + 2ax = 2qm.$$

Podobnie dla drugiego z przedstawień (29):

$$(r - p)x_1 - 2cy_1 = 2p_1m, \quad (r + b)y_1 + 2ax_1 = 2q_1m.$$

Ostatnie cztery wzory dają:

$$\begin{aligned}(r-b)x-2cy &\equiv 0 \pmod{2m}, & (r+b)y+2ax &\equiv 0 \pmod{2m}, \\ (r-b)x_1-2cy_1 &\equiv 0 \pmod{2m}, & (r+b)y_1+2ax_1 &\equiv 0 \pmod{2m},\end{aligned}$$

skąd

$$\begin{aligned}2c(yx_1-xy_1) &\equiv 0 \pmod{2m}, & 2a(yx_1-xy_1) &\equiv 0 \pmod{2m}, \\ (r-b)(yx_1-xy_1) &\equiv 0 \pmod{2m}, & (r+b)(yx_1-xy_1) &\equiv 0 \pmod{2m}\end{aligned}$$

i na mocy ostatnich kongruencji

$$2b(yx_1-xy_1) \equiv 0 \pmod{2m}.$$

Gdyby yx_1-xy_1 nie było podzielne przez m , to wobec podzielności przez m każdego z iloczynów

$$a(yx_1-xy_1), \quad b(yx_1-xy_1), \quad c(yx_1-xy_1),$$

liczby a, b, c miałyby wspólny dzielnik, wbrew założeniu. Zatem

$$(31) \quad yx_1-xy_1 = mv,$$

gdzie v jest liczbą całkowitą. Lecz

$$\begin{aligned}(32) \quad 4(ax^2+bxy+cy^2)(ax_1^2+bx_1y_1+cy_1^2) &= \\ = [(2ax+by)x_1+(bx+2cy)y_1]^2 - D(x_1y_1-xy_1)^2,\end{aligned}$$

skąd wobec (29) i (30)

$$(33) \quad [(2ax+by)x_1+(bx+2cy)y_1]^2 = 4m^2 + Dm^2v^2,$$

a zatem

$$(34) \quad (2ax+by)x_1+(bx+2cy)y_1 = mu,$$

gdzie u jest liczbą całkowitą.

Z (33) i (34) dostajemy po podzieleniu przez m^2

$$(35) \quad u^2 - Dv^2 = 4,$$

rozwiązując zaś równania (30) i (32) względem x_1 i y_1 , otrzymujemy na mocy (29)

$$(36) \quad x_1 = \frac{u+bv}{2}x + cvy, \quad y_1 = \frac{u-bv}{2}y - avx.$$

Jeżeli więc przedstawienia (29) należą do tej samej grupy, to zachodzą wzory (36), gdzie u, v są liczbami całkowitymi, spełniającymi równanie (35).

Niech teraz para liczb całkowitych u, v będzie rozwiązaniem równania (35). Wyznamy x_1, y_1 ze wzorów (36) w założeniu, że $ax^2+bxy+cy^2$ jest przedstawieniem liczby m , należącym do pierwiastka r . Liczby $\frac{u+bv}{2}$ i $\frac{u-bv}{2}$ są całkowite, gdyż $D \equiv b^2 \pmod{4}$, skąd $u^2 - b^2v^2 \equiv 0 \pmod{4}$ na mocy (35).

Wobec założenia, że $ax^2+bxy+cy^2 = m$, wzory (34) dają

$$(37) \quad yx_1-xy_1 = mv$$

i $(2ax+by)x_1+(bx+2cy)y_1 = mu$, a zatem wobec tożsamości (31) $4m(ax_1^2+bx_1y_1+cy_1^2) = m^2u^2 - Dm^2v^2$, skąd w myśl (34)

$$(38) \quad ax_1^2+bx_1y_1+cy_1^2 = m.$$

Jeżeli przedstawienie x, y należy do pierwiastka r , to — jak widzieliśmy — zachodzą wzory (30), skąd:

$$(r-b)xx_1-2cyx_1 = 2pmx_1, \quad (r+b)yx_1+2axx_1 = 2qmx_1,$$

$$(r-b)xy_1-2cyy_1 = 2pmy_1, \quad (r+b)yy_1+2axy_1 = 2qmy_1,$$

a zatem wobec (37) oraz wobec parzystości liczb $r+b$ i $r-b$ (bo $r^2 = b^2 - 4ac + 4mn$):

$$(39) \quad x[(r-b)x_1-2cy_1] = 2m(px_1+cv),$$

$$(40) \quad x[(r+b)y_1+2ax_1] = m[2qx_1-(r+b)v] = 2ms,$$

$$(41) \quad y[(r-b)x_1-2cy_1] = m[2py_1+(r-b)v] = 2mt,$$

$$(42) \quad y[(r+b)y_1+2ax_1] = 2m(qy_1+av).$$

Gdyby $(r-b)x_1-2cy_1$ nie było podzielne przez $2m$, to wobec (39) i (41) liczby x i y miałyby wspólny dzielnik większy od jedności, wbrew założeniu. Podobnie wnosimy z (39) i (42), że $(r+b)y_1+2ax_1$ jest podzielne przez $2m$. Możemy więc napisać:

$$(43) \quad (r-b)x_1-2cy_1 = 2p_1m, \quad (r+b)y_1+2ax_1 = 2q_1m,$$

gdzie p_1 i q_1 są liczbami całkowitymi.

Mnożąc pierwszą z równości (43) przez $-y_1$, a drugą przez x_1 , dodając, otrzymujemy $2bx_1y_1+2cy_1^2+2ax_1^2 = 2m(q_1x_1-p_1y_1)$, skąd wobec (38)

$$(44) \quad q_1x_1-p_1y_1 = 1.$$

Liczby x_1, y_1 są na mocy (44) względnie pierwsze; wzór (58) daje więc przedstawienie właściwe liczby m przez formę (a, b, c) .

Mnożąc pierwszą z równości (43) przez q_1 , a drugą przez $-p_1$ i dodając otrzymujemy na mocy (44)

$$(45) \quad r = (bx_1 + 2cy_1)q_1 + (2ax_1 + by_1)p_1.$$

Wzory (44) i (45) dowodzą wobec warunku (21), że przedstawienie x_1, y_1 należy do pierwiastka r . Udowodniliśmy więc

Twierdzenie 6. *Warunkiem koniecznym i wystarczającym na to, by przedstawienie (29) należało do tego samego pierwiastka r , są wzory (36), w których u i v są liczbami całkowitymi, spełniającymi równanie (35).*

Łatwo też widzieć, że różnym układom u, v odpowiadają w myśl wzorów (36) różne układy x_1, y_1 . Istotnie, wzory (36) pociągają za sobą wzory (37) i (34), skąd wynika, że układ u, v jest przez układy x, y i x_1, y_1 określony jednoznacznie.

Doszliliśmy zatem do następującego wyniku: znając jedno przedstawienie liczby m przez formę (a, b, c) , należące do danej grupy, potrafimy za pomocą rozwiązań równania (35) wyznaczyć wszystkie przedstawienia, należące do tej grupy¹⁾.

Następnie — jak wynika z twierdzenia 5 — aby rozstrzygnąć, czy istnieje przedstawienie danej liczby przez daną formę, należące do danego pierwiastka, wystarczy rozstrzygnąć, czy pewne dwie formy kwadratowe są równoważne właściwie, czy nie, przy czym potrafimy wyznaczyć ewentualne przedstawienie, jeżeli znajdziemy podstawienie, przekształcające jedną z tych form w drugą.

Wreszcie, badanie pierwiastków, charakteryzujących grupy przedstawień, sprowadza się do badania kongruencji (23) czyli kongruencji drugiego stopnia, czemu poświęcony był Rozdział XIII.

W ten sposób zagadnienie podstawowe teorii form kwadratowych, sformułowane na początku tego Rozdziału (p. str. 352), sprowadza się ostatecznie do rozstrzygnięcia, czy dwie dane formy kwadratowe są czy nie są równoważne właściwie, i do ewentualnego wyznaczenia podstawienia, przekształcającego jedną z tych form w drugą.

¹⁾ Wszystkie rozwiązania równania (35) w liczbach parzystych otrzymamy oczywiście, podwajając rozwiązania równania Pella $x^2 - Dy^2 = 1$ w liczbach całkowitych (ob. Rozdział XI, poświęcony temu równaniu). Sposób zaś otrzymania wszystkich rozwiązań równania (35) w liczbach całkowitych wyłożony jest w drugim wydaniu tej książki (z 1925 r.), str. 215.

§ 5. Kryterium równoważności dwu form kwadratowych o wyróżniku dodatnim. Formy zredukowane dla $D > 0$. Zajmiemy się więc teraz pytaniem, jak rozstrzygnąć, czy dwie dane formy kwadratowe są, czy nie są równoważne właściwie. Rozróżnimy tu dwa przypadki: $D > 0$ i $D < 0$. Niech naprzód $D > 0$.

Liczbę niewymierną y nazywać będziemy *równoważną* liczbie x , pisząc $y \sim x$, jeżeli istnieją takie liczby całkowite a, β, γ, δ , że zachodzi wzór (7) oraz

$$y = \frac{ax + \beta}{\gamma x + \delta}.$$

Wtedy mówimy też, że liczba x przechodzi w liczbę y przez podstawienie $\begin{pmatrix} a, \beta \\ \gamma, \delta \end{pmatrix}$.

Jeżeli przy tym można dobrać liczby całkowite a, β, γ, δ tak, by we wzorze (7) zachodził znak $+$, to mówimy, że równoważność jest *właściwa*, jeżeli zaś można je dobrać tak, by we wzorze (7) zachodził znak $-$, to mówimy, że równoważność jest *niewłaściwa*.

Twierdzenie 7. *Na to, by formy (a, b, c) i (a_1, b_1, c_1) o wyróżniku $D > 0$ były równoważne właściwie, potrzeba i wystarcza, żeby liczby*

$$(46) \quad \omega = \frac{-b + \sqrt{D}}{2a} \quad \text{ i } \quad \omega_1 = \frac{-b_1 + \sqrt{D}}{2a_1}$$

były równoważne właściwie.

Dowód. Załóżmy naprzód, że formy (a, b, c) i (a_1, b_1, c_1) są równoważne właściwie. Zachodzą więc wzory (5) przy pewnych całkowitych a, β, γ, δ , spełniających warunek $a\delta - \gamma\beta = 1$. Mamy tedy

$$(47) \quad \omega_1 = \frac{-b_1 + \sqrt{D}}{2a_1} = \frac{-2a\alpha\beta - b(a\delta + \gamma\beta) - 2c\gamma\delta + \sqrt{D}}{2(a\alpha^2 + b\alpha\gamma + c\gamma^2)},$$

a że — jak łatwo sprawdzić —

$$(48) \quad \begin{aligned} & -2a\alpha\beta - b(a\delta + \gamma\beta) - 2c\gamma\delta + \sqrt{D} = \\ & = \frac{(2a\alpha + b\gamma + \gamma\sqrt{D})(2a\beta + b\delta - \delta\sqrt{D})}{2a}, \\ & 2(a\alpha^2 + b\alpha\gamma + c\gamma^2) = \\ & = \frac{(2a\alpha + b\gamma + \gamma\sqrt{D})(2a\alpha + b\gamma - \gamma\sqrt{D})}{2a}, \end{aligned}$$

więc

$$(49) \quad \omega_1 = -\frac{2a\beta + b\delta - \delta\sqrt{D}}{2a\alpha + b\gamma - \gamma\sqrt{D}} = \frac{-\beta + \frac{-b + \sqrt{D}}{2a}\delta}{\alpha - \frac{-b + \sqrt{D}}{2a}\gamma}$$

czyli $\omega_1 = \frac{\delta\omega - \beta}{-\gamma\omega + \alpha}$, co dowodzi wobec $\delta\alpha - (-\gamma)(-\beta) = 1$, że liczby ω i ω_1 są równoważne właściwie.

Załóżmy teraz, na odwrót, że liczby (46) są równoważne właściwie. Mamy więc przy pewnych całkowitych $\alpha, \beta, \gamma, \delta$

$$a\delta - \gamma\beta = 1 \quad \text{i} \quad \omega = \frac{a\omega_1 + \beta}{\gamma\omega_1 + \delta}$$

czyli $\omega_1 = \frac{\delta\omega - \beta}{-\gamma\omega + \alpha}$, skąd wynika wzór (49), który wobec (48) pociąga za sobą wzór (47). Zatem $b_1 = 2a\alpha\beta + b(\alpha\delta + \gamma\beta) + 2c\gamma\delta$ i $a_1 = a\alpha^2 + b\alpha\gamma + c\gamma^2$, skąd

$$c_1 = \frac{b_1^2 - D}{4a_1} = \frac{[2a\alpha\beta + b(\alpha\delta + \gamma\beta) + 2c\gamma\delta]^2 - D}{4(a\alpha^2 + b\alpha\gamma + c\gamma^2)},$$

a więc wobec (48)

$$c_1 = \frac{[(2a\alpha + b\gamma)^2 - \gamma^2 D] [2a\beta + b\delta]^2 - \delta^2 D}{4a[(2a\alpha + b\gamma)^2 - \gamma^2 D]} = \\ = \frac{(2a\beta + b\delta)^2 - \delta^2 D}{4a} = a\beta^2 + b\beta\delta + c\delta^2.$$

Dowiedliśmy w ten sposób, że jeżeli liczby ω i ω_1 są równoważne właściwie, to przy pewnych całkowitych $\alpha, \beta, \gamma, \delta$, spełniających warunek $a\delta - \gamma\beta = 1$, zachodzą wzory (5), skąd wynika, że formy (a, b, c) i (a_1, b_1, c_1) są równoważne właściwie. Twierdzenie 7 zostało więc udowodnione.

Zarazem dowiedliśmy, że jeżeli liczba ω_1 przechodzi w liczbę ω przez podstawienie $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, to forma (a, b, c) przechodzi przez to podstawienie w formę (a_1, b_1, c_1) i na odwrót. Dowiedliśmy jednocześnie, że każda liczba równoważna właściwie liczbie postaci $-\frac{b + \sqrt{D}}{2a}$ jest tejże postaci.

Jak łatwo widzieć, zachodzi to i dla równoważności niewłaściwej (co uzyskujemy, zmieniając w dowodzie znaki liczb α i γ).

Liczbę $x' = \frac{-b - \sqrt{D}}{2a}$ będziemy nazywali *sprzężoną* z liczbą x .

Liczby x i x' są więc pierwiastkami tego samego równania 2-go stopnia

$$(2at + b)^2 - D = 0.$$

Liczbę x nazywamy *zredukowaną*, jeżeli

$$0 < -x' < 1 < x.$$

Twierdzenie 8. Każda liczba postaci $x = \frac{-b + \sqrt{D}}{2a}$ (gdzie $D > 0$) jest równoważna właściwie pełnej liczbie zredukowanej.

Dowód. W myśl twierdzenia Lagrange'a (Rozdział XII, § 9, str. 293) liczba x rozwija się na ułamek łańcuchowy okresowy

$$x = q_0 + \frac{1}{q_1} + \frac{1}{q_2} + \dots$$

Niech P_n/Q_n będzie n -tym reduktom tego rozwinięcia i niech

$$x_n = q_n + \frac{1}{q_{n+1}} + \frac{1}{q_{n+2}} + \dots \quad \text{dla } n = 0, 1, 2, \dots$$

Wówczas

$$x = \frac{P_{n-1}x_n + P_{n-2}}{Q_{n-1}x_n + Q_{n-2}} \quad \text{dla } n = 1, 2, \dots$$

i, jak wiemy (ob. wzór (17), str. 269),

$$P_{n-1}Q_{n-2} - Q_{n-1}P_{n-2} = (-1)^{n-1}.$$

Dowodzi to, że

$$(50) \quad x \sim x_n \quad \text{dla } n = 1, 2, \dots$$

Przy tym, jeżeli n jest liczbą nieparzystą, to równoważność ta jest właściwa.

Wobec okresowości rozwinięcia liczby x na ułamek łańcuchowy istnieje oczywiście taka liczba nieparzysta k , że liczba

$$(51) \quad x_k = q_k + \frac{1}{q_{k+1}} + \frac{1}{q_{k+2}} + \dots$$

ma rozwinięcie o okresie czystym. Niech s będzie liczbą wyrazów tego okresu; możemy tu założyć, że $s > 1$, biorąc okres niekończennie najmniejszy.

Oznaczając przez $P_n^{(k)}/Q_n^{(k)}$ n -ty redukt ułamka łańcuchowego (51), mamy więc

$$x_k = \frac{P_{s-1}^{(k)}x_k + P_{s-2}^{(k)}}{Q_{s-1}^{(k)}x_k + Q_{s-2}^{(k)}},$$

skąd wnosimy, że x_k jest pierwiastkiem dodatnim równania

$$Q_{s-1}^{(k)}t^2 + (Q_{s-2}^{(k)} - P_{s-1}^{(k)})t - P_{s-2}^{(k)} = 0.$$

Liczba x'_k , sprzężona z x_k , jest zatem drugim pierwiastkiem tegoż równania i na mocy zależności między pierwiastkami równania 2-go stopnia a jego współczynnikami jest:

$$x_k x'_k = -\frac{P_{s-2}^{(k)}}{Q_{s-1}^{(k)}} < 0, \quad x_k + x'_k = \frac{P_{s-1}^{(k)} - Q_{s-2}^{(k)}}{Q_{s-1}^{(k)}},$$

skąd

$$(52) \quad (x_k + 1)(x'_k + 1) = x_k x'_k + x_k + x'_k + 1 = \\ = -\frac{P_{s-2}^{(k)}}{Q_{s-1}^{(k)}} + \frac{P_{s-1}^{(k)} - Q_{s-2}^{(k)}}{Q_{s-1}^{(k)}} + 1 = \frac{P_{s-1}^{(k)} + Q_{s-1}^{(k)} - P_{s-2}^{(k)} - Q_{s-2}^{(k)}}{Q_{s-1}^{(k)}} > 0,$$

gdyż oczywiście $P_{s-1}^{(k)} > P_{s-2}^{(k)}$ i $Q_{s-1}^{(k)} > Q_{s-2}^{(k)}$. Nierówność (52) wobec $x_k > 0$ i $x_k x'_k < 0$ daje $x'_k < 0$ i $x'_k + 1 > 0$, skąd $0 < -x'_k < 1$, a ponieważ $x_k > q_k \geq 1$, więc $0 < -x'_k < 1 < x_k$.

Liczba x_k jest zatem zredukowana. Lecz na mocy (50) jest $x \sim x_k$ i wobec nieparzystości liczby k , równoważność ta jest właściwa, c. b. d. d.

Nazywając formą zredukowaną każdą formę (a, b, c) o wyróżniku $D > 0$, dla której $\omega = \frac{-b + \sqrt{D}}{2a}$ jest liczbą zredukowaną, otrzymujemy z twierdzenia 7 następujący

Wniosek. Każda forma (a, b, c) o wyróżniku $D > 0$ jest równoważna właściwej pewnej formie zredukowanej.

Dla liczby zredukowanej $\omega = \frac{-b + \sqrt{D}}{2a}$ zachodzą, na mocy definicji, nierówności

$$0 < -\omega' < 1 < \omega,$$

gdzie $\omega' = \frac{-b - \sqrt{D}}{2a}$.

Gdyby było $a < 0$, to wobec $0 < -\omega'$ mielibyśmy $b + \sqrt{D} < 0$, skąd $b < 0$, wobec zaś $-\omega' < \omega$ mielibyśmy $b + \sqrt{D} > -b + \sqrt{D}$, skąd $b > 0$. Musi więc być $a > 0$, skąd — jak łatwo widzieć —

$$0 < b + \sqrt{D} < 2a \quad \text{ i } \quad 2a < -b + \sqrt{D},$$

a zatem

$$|b| < \sqrt{D} \quad \text{ i } \quad a < \sqrt{D},$$

co dowodzi, że przy danym $D > 0$ istnieje skończenie wiele liczb zredukowanych, a więc też skończenie wiele form zredukowanych (przy danym D forma (a, b, c) jest bowiem określona jednoznacznie przez a i b , gdyż $c = \frac{b^2 - D}{4a}$). Stąd

Twierdzenie 9. Liczba klas form kwadratowych o danym wyróżniku $D > 0$ jest zaroższona skończona.

§ 6. Formy dodatnie i formy zredukowane dla $D < 0$. Przykład $D = -4$. Niech teraz $D < 0$. Niech (a, b, c) będzie jakąkolwiek formą o wyróżniku $D < 0$, a $m \neq 0$ — jakąkolwiek liczbą, dającą się przedstawić przez tę formę. Jest więc przy pewnych x, y całkowitych $m = ax^2 + bxy + cy^2$, skąd

$$4am = (2ax + by)^2 - Dy^2,$$

a zatem wobec $D < 0$

$$4am > 0.$$

Wszystkie więc liczby m , dające się przedstawić przez formę (a, b, c) , mają ten sam znak co liczba a . Wynika stąd natychmiast, że jeżeli dwie formy (a, b, c) i (a_1, b_1, c_1) o wyróżniku $D < 0$ są równoważne, to liczby a i a_1 są tego samego znaku. Ponieważ zaś oczywiście równoważność właściwa form

$$(53) \quad (a, b, c) \quad \text{ i } \quad (a_1, b_1, c_1)$$

pociąga za sobą równoważność właściwą form

$$(54) \quad (-a, -b, -c) \quad \text{ i } \quad (-a_1, -b_1, -c_1)$$

i na odwrót oraz podstawienie $\begin{pmatrix} a, \beta \\ \gamma, \delta \end{pmatrix}$, które przekształca formy (53) jedną w drugą, przekształca również formy (54) jedną w drugą, więc badając równoważność właściwą dwu form o wyróżniku $D < 0$, możemy założyć, że pierwsze współczynniki tych form są dodatnie.

Formy takie nazywamy *dodatnimi*.

Formę (a, b, c) o wyróżniku $D < 0$ nazywamy *zredukowaną*, jeżeli $-a < b \leq a \leq c$.

Twierdzenie 10. Każda forma dodatnia (a, b, c) o wyróżniku $D < 0$ jest równoważna właściwie perowej formie zredukowanej.

Dowód. Wobec $b^2 - 4ac = D < 0$ i $a > 0$ jest $c > 0$. Niech

$$c = a_1.$$

Jest to liczba dodatnia. Wyznamy liczbę całkowitą δ tak, żeby

$$(55) \quad -\frac{1}{2} < -\frac{b}{2a_1} - \delta \leq \frac{1}{2}.$$

Jasne jest, że istnieje zawsze jedna i tylko jedna taka liczba całkowita δ .

Przez podstawienie $\begin{pmatrix} 0, 1 \\ -1, \delta \end{pmatrix}$ forma (a, b, a_1) przejdzie — jak łatwo widzieć — na równoważną jej właściwie formę (a_1, b_1, a_2) , gdzie $b_1 = -b - 2a_1\delta$; zatem wobec (55)

$$-a_1 < b_1 \leq a_1.$$

Jeżeli równocześnie $a_1 \leq a_2$, to forma (a_1, b_1, a_2) jest, w myśl określenia, zredukowana. Załóżmy więc, że

$$a_1 > a_2,$$

i postąpmy z formą (a_1, b_1, a_2) jak z formą (a, b, a_1) , co da nam nową formę (a_2, b_2, a_3) , równoważną poprzedniej właściwie i taką, że

$$-a_2 < b_2 \leq a_2.$$

Jeżeli znowu

$$a_2 > a_3,$$

to formę (a_2, b_2, a_3) przekształcimy jak wyżej na nową formę (a_3, b_3, a_4) itd. Ciąg nierówności

$$a_1 > a_2 > a_3 > \dots$$

nie może być nieskończony, gdyż wszystkie liczby a_i są naturalne. Dojdziemy więc do takiej formy (a_n, b_n, a_{n+1}) , że nie tylko $-a_n < b_n \leq a_{n+1}$, lecz jednocześnie $a_n \leq a_{n+1}$.

Forma (a_n, b_n, c_{n+1}) jest zatem zredukowana i — jak to wynika w jednej chwili ze sposobu jej otrzymania — równoważna formie (a, b, c) właściwie, c. b. d. d.

Nie tylko więc dowiedliśmy, że każda forma dodatnia (o wyznaczniku $D < 0$) jest równoważna właściwie pewnej formie zredukowanej, lecz nad to wskazaliśmy sposób przekształcenia formy danej w formę zredukowaną (za pomocą kolejnych podstawień).

Założmy teraz, że forma (a, b, c) o wyznaczniku $D < 0$ jest zredukowana. Jest więc

$$(56) \quad a \leq c \quad \text{ i } \quad |b| \leq a,$$

skąd $4a^2 \leq 4ac = b^2 - D \leq a^2 - D$ czyli $3a^2 \leq -D$ i przeto otrzymujemy $a \leq \sqrt{-D/3}$; zatem na mocy (56)

$$(57) \quad |b| \leq a \sqrt{-D/3},$$

co dowodzi, że dla danej wartości $D < 0$ istnieje skończona liczba form zredukowanych.

Liczba klas form kwadratowych jest więc dla każdego $D < 0$ skończona.

Niech w szczególności $D = -4$. W myśl nierówności (57) jest $a \leq \sqrt{4/3}$, skąd $a = 1$, oraz $|b| \leq 1$, skąd $b = 0$ lub $b = 1$.

Lecz $b \neq 1$, ponieważ wobec $b^2 \equiv D \pmod{4}$ i $D = -4$ liczba b musi być parzysta. Istnieje więc tylko jedna forma zredukowana o wyznaczniku $D = -4$, mianowicie $(1, 0, 1)$ czyli forma

$$x^2 + y^2.$$

Jako łatwy stąd wniosek otrzymujemy

Twierdzenie 11. Każda liczba pierwsza formy $4k+1$ jest sumą dwu kwadratów.

Dowód. Jeżeli p jest liczbą pierwszą formy $4k+1$, to — jak wiemy z Rozdziału IV (ob. str. 65) — istnieje taka liczba całkowita q , że $q^2 \equiv -1 \pmod{p}$. Liczba $r = \frac{q^2 + 1}{p}$ jest więc całkowita. Dla $x = 1$ i $y = 0$ liczba p daje się przedstawić przez formę dodatnią $(p, r, 2q)$ o wyznaczniku

$$D = (2q)^2 - 4pr = 4(q^2 - pr) = -4,$$

a więc też przez formę $(1, 0, 1)$, która — jak dowiedliśmy — jest formą zredukowaną dla każdej formy dodatniej o wyróżniku -4 . Liczba p daje się więc przedstawić przez formę $x^2 + y^2$, czyli jest sumą dwu kwadratów, c. b. d. o.

§ 7. Badanie równoważności właściwej dwu form zredukowanych o wyróżniku $D < 0$. Ponieważ każdą formę kwadratową dodatnią o wyróżniku $D < 0$ potrafimy przekształcić na równoważną jej właściwie formę zredukowaną, więc zagadnienie, kiedy dwie formy kwadratowe dodatnie o wyróżniku $D < 0$ są równoważne właściwie, sprowadza się do zagadnienia: jak rozstrzygnąć, czy dwie formy zredukowane o wyróżniku $D < 0$ są równoważne właściwie?

Założmy, że dwie różne formy zredukowane (53) o wyróżniku $D < 0$ są równoważne właściwie. Możemy oczywiście założyć, że

$$(58) \quad a_1 \leq a.$$

Wobec założenia równoważności właściwej form (53) istnieją takie liczby całkowite a, β, γ, δ , że zachodzi wzór

$$(59) \quad a\delta - \gamma\beta = 1$$

oraz wzory (3). Pierwszy ze wzorów (3) daje

$$(60) \quad 4aa_1 = (2a\alpha + b\gamma)^2 - D\gamma^2 \geq -D\gamma^2,$$

a ponieważ $a \leq \sqrt{-D/3}$ i $a_1 \leq \sqrt{-D/3}$ (bo założyliśmy, że formy są zredukowane), więc $4aa_1 \leq -4D/3$, a zatem w myśl (60) jest $-D\gamma^2 \leq -4D/3$, skąd $\gamma^2 \leq 4/3$ wobec $D < 0$, czyli albo $\gamma = 0$, albo $\gamma = \pm 1$.

Jednakże gdyby było $\gamma = 0$, mielibyśmy $a\delta = 1 + \gamma\beta = 1$, skąd $\alpha = \pm 1$ i $\delta = \pm 1$ oraz w myśl (60) $4aa_1 = (2a\alpha)^2 = 4a^2$, skąd $a_1 = a$; w myśl zaś drugiego z równań (3) byłoby $2\pm a\beta + b = b_1$ czyli

$$(61) \quad b_1 - b = \pm 2a\beta,$$

a że

$$(62) \quad -a < b \leq a, \quad -a_1 < b_1 \leq a_1 \quad \text{ i } \quad a_1 = a,$$

więc $|b_1 - b| < 2a$, skąd wobec (62) byłoby $\beta = 0$, a zatem $b_1 = b$. Formy (a, b, c) i (a_1, b_1, c_1) byłyby więc identyczne, wbrew założeniu. Musi przeto być $\gamma = \pm 1$.

Pierwsze z równań (3) daje dla $\gamma = \pm 1$

$$(63) \quad a_1 = aa^2 \pm ba + c,$$

skąd $aa^2 \pm ba = a_1 - c$, a że na mocy (58) i w myśl założenia, że forma (a, b, c) jest zredukowana, mamy

$$(64) \quad a_1 \leq a \leq c,$$

więc $aa^2 \pm ba \leq 0$. Z drugiej zaś strony, wobec całkowitości liczby a oraz nierówności $|b| < a$, mamy $|ba| \leq aa^2$, skąd $aa^2 \pm ba \geq 0$. Tak więc

$$(65) \quad aa^2 \pm ba = 0.$$

Wynika stąd na mocy (63), że $a_1 = c$, skąd na mocy (65)

$$a_1 = a = c.$$

Drugie zaś z równań (3) daje dla $\gamma = \pm 1$

$$b_1 = 2a\alpha\beta + b(a\delta \pm \beta) \pm 2c\delta,$$

a że na mocy (59) jest

$$b = b(a\delta \mp \beta),$$

więc dodając ostatnie dwie równości stronami, otrzymujemy

$$b_1 + b = 2a\alpha\beta + 2ba\delta \pm 2c\delta.$$

Wobec $c = a$ i (65) wnosimy stąd, że

$$(66) \quad b_1 + b = 2a(\alpha\beta \mp a^2\delta \pm \delta),$$

a ponieważ we wzorach (62) nie może być jednocześnie $b = a$ i $b_1 = a$, bo wówczas formy (a, b, c) i (a_1, b_1, c_1) byłyby identyczne wbrew założeniu, więc musi być $|b_1 + b| < 2a$.

Wzór (66) dowodzi przeto, że $b_1 + b = 0$ czyli $b_1 = -b$.

Jeżeli więc formy zredukowane (a, b, c) i (a_1, b_1, c_1) o wyróżniku $D < 0$, nie będąc identycznymi, są równoważne właściwie, to musi być $a_1 = a = c$ i $b_1 = -b$, skąd

$$c_1 = \frac{b_1^2 - D}{4a_1} = \frac{b^2 - D}{4a} = c.$$

Formy te muszą więc być postaci

$$(67) \quad (a, b, a) \quad \text{ i } \quad (a, -b, a).$$

Z drugiej zaś strony, z łatwością sprawdzamy, że formy (64) są zawsze równoważne właściwie, gdyż pierwsza przechodzi w drugą przez podstawienie

$$\begin{pmatrix} 0, & -1 \\ 1, & 0 \end{pmatrix}.$$

Tak więc udowodniliśmy

Twierdzenie 12. Dwie różne formy zredukowane o wyróżniku $D < 0$ są wtedy i tylko wtedy równoważne właściwie, gdy wszystkie cztery współczynniki skrajne mają wspólną wartość, a współczynniki środkowe w obu formach są równe co do bezwzględnej wartości, lecz różne co do znaku.

Okoliczność tę możemy oczywiście zawsze rozpoznać bezpośrednio z postaci samej formy kwadratowej.

Dlatego też rozpoznawanie równoważności właściwej dwu form zredukowanych o wyróżniku $D < 0$, a przez to (wobec twierdzeń 10 i 12) również zagadnienie rozpoznawania równoważności właściwej jakichkolwiek dwu form kwadratowych o wyróżniku $D < 0$ możemy uważać za rozstrzygnięte. Potrafimy też wyznaczyć podstawienie, za pomocą którego jedna z tych form przechodzi w drugą.

Ostatecznie więc badanie równoważności właściwej dwu form kwadratowych sprowadza się: dla $D > 0$ do badania równoważności właściwej dwu niewymierności 2-ego stopnia, a dla $D < 0$ — do badania równoważności właściwej dwu form zredukowanych, do czego wystarcza twierdzenie 12. Tym sposobem podstawowe zagadnienie teorii form kwadratowych (p. § 1, str. 352 i § 4, str. 362) będzie rozwiązane z chwilą, gdy potrafiemy rozstrzygnąć, czy dwie dane niewymierności 2-go stopnia są równoważne właściwie, czy nie. Zagadnieniem tym zajmiemy się w § 8, w którym damy odpowiedź na to pytanie.

§ 8. Badanie równoważności właściwej dwu niewymierności 2-go stopnia. Niech x i y będą dwiema niewymiernościami 2-go stopnia o rozwinięciach na ułamki łańcuchowe nieskończone:

$$(68) \quad x = a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \dots,$$

$$(69) \quad y = b_0 + \frac{1}{b_1} + \frac{1}{b_2} + \dots$$

i niech dla $n = 1, 2, \dots$:

$$(70) \quad x_n = a_n + \frac{1}{a_{n+1}} + \frac{1}{a_{n+2}} + \dots,$$

$$(71) \quad y_n = b_n + \frac{1}{b_{n+1}} + \frac{1}{b_{n+2}} + \dots$$

Twierdzenie 13. Dla równoważności dwu niewymierności 2-go stopnia x i y potrzeba i wystarcza, by istniały takie liczby naturalne k i l , że

$$(72) \quad x_k = y_l.$$

Dowód. Jak dowiedliśmy w § 5 (ob. (50), str. 365), dla n naturalnych zachodzą równoważności $x \sim x_n$ i $y \sim y_n$.

Jeżeli więc zachodzi równość (72), to $x \sim x_k$ i $y \sim y_l = x_k$ i dla dowodu równoważności

$$(73) \quad x \sim y$$

wystarczy okazać, że stosunek $\sim$ jest przechodni.

Można tego z łatwością dowieść bezpośrednio, a wynika to też z twierdzenia 7, uogólnionego na równoważność niewłaściwą (str. 364), oraz z przechodniości stosunku równoważności form (str. 356). Warunek jest więc konieczny.

Na odwrót, założmy teraz równoważność (73). Przy pewnych $\alpha, \beta, \gamma, \delta$ całkowitych zachodzi więc wzór (7) oraz wzór

$$(74) \quad y = \frac{\alpha x + \beta}{\gamma x + \delta},$$

jako też na mocy (68) i (69) wzór

$$(75) \quad x = \frac{P_{n-1}x_n + P_{n-2}}{Q_{n-1}x_n + Q_{n-2}}.$$

Wstawiając tę wartość do wzoru (74), dostajemy

$$(76) \quad y = \frac{(\alpha P_{n-1} + \beta Q_{n-1})x_n + \alpha P_{n-2} + \beta Q_{n-2}}{(\gamma P_{n-1} + \delta Q_{n-1})x_n + \gamma P_{n-2} + \delta Q_{n-2}}.$$

Okażemy, że zawsze można n dobrać tak, aby

$$(77) \quad \frac{\alpha P_{n-1} + \beta Q_{n-1}}{\alpha P_{n-2} + \beta Q_{n-2}} > 1.$$

Rozróżnimy następujące trzy przypadki:

1° $\alpha = 0$. Wówczas w myśl wzoru (7), musi być $\beta = \pm 1$;

liczba po lewej stronie wzoru (77) istnieje więc i wynosi $\frac{Q_{n-1}}{Q_{n-2}}$, jest zatem większa od 1 dla wszystkich $n > 2$.

2° $\alpha \neq 0$ i $x + \frac{\beta}{\alpha} > 0$,

3° $\alpha \neq 0$ i $x + \frac{\beta}{\alpha} < 0$.

Przypadek $x + \frac{\beta}{a} = 0$ jest oczywiście niemożliwy wobec założenia, że liczba x jest niewymierna.

W obu przypadkach 2° i 3° jest oczywiście dla dostatecznie wielkich n

$$(78) \quad \frac{aP_{n-1} + \beta Q_{n-1}}{aP_{n-2} + \beta Q_{n-2}} = \frac{Q_{n-1}}{Q_{n-2}} \cdot \frac{R_{n-1} + \frac{\beta}{a}}{R_{n-2} + \frac{\beta}{a}},$$

gdyż $R_{n-2} + \frac{\beta}{a}$ zmierza wraz z $n \rightarrow \infty$ do $x + \frac{\beta}{a}$, zatem do liczby różnej od zera i przeto dla dostatecznie wielkich n musi samo być różne od zera.

W przypadku 2° dobierzemy n parzyste i tak wielkie, żeby było

$$(79) \quad R_{n-2} + \frac{\beta}{a} > 0,$$

co jest możliwe, gdyż lewa strona tej nierówności zmierza do $x + \frac{\beta}{a} > 0$. Ponieważ dla n parzystego jest, jak wiemy (ob. (34), str. 272), $R_{n-1} > x > R_{n-2}$, więc

$$R_{n-1} + \frac{\beta}{a} > R_{n-2} + \frac{\beta}{a},$$

skąd wynika nierówność (77) na mocy (78) i (79), gdyż $Q_{n-1} \geq Q_{n-2}$.

W przypadku 3° dobierzemy n nieparzyste i tak wielkie żeby było

$$(80) \quad R_{n-2} + \frac{\beta}{a} < 0.$$

Ponieważ zaś dla n nieparzystego jest $R_{n-1} < x < R_{n-2}$, więc otrzymujemy teraz

$$R_{n-1} + \frac{\beta}{a} < R_{n-2} + \frac{\beta}{a},$$

skąd wobec (78) i (80) znowu wynika nierówność (77).

Dowiedliśmy więc istnienia wskaźników n , dla których zachodzi nierówność (77). Niech $n > 1$ będzie najmniejszym takim wskaźnikiem. Wobec wymierności lewej strony nierówności (77) możemy więc napisać

$$(81) \quad \frac{aP_{n-1} + \beta Q_{n-1}}{aP_{n-2} + \beta Q_{n-2}} = \frac{A}{B},$$

gdzie A i B są liczbami naturalnymi względnie pierwszymi i $A > B$.

Jak łatwo obliczyć, mamy na mocy (59)

$$(82) \quad \begin{aligned} & (aP_{n-1} + \beta Q_{n-1})(\gamma P_{n-2} + \delta Q_{n-2}) - \\ & - (\gamma P_{n-1} + \delta Q_{n-1})(aP_{n-2} + \beta Q_{n-2}) = \\ & = (a\delta - \gamma\beta)(P_{n-1}Q_{n-2} - Q_{n-1}P_{n-2}) = \pm (-1)^n. \end{aligned}$$

Gdyby było $\gamma P_{n-1} + \delta Q_{n-1} = 0$, mielibyśmy stąd

$$|(aP_{n-1} + \beta Q_{n-1})(\gamma P_{n-2} + \delta Q_{n-2})| = 1,$$

zatem $aP_{n-1} + \beta Q_{n-1} = \pm 1$, co niemożliwe wobec (77). Jest więc

$$(83) \quad \gamma P_{n-1} + \delta Q_{n-1} = \pm C,$$

gdzie C jest liczbą naturalną. Niech jeszcze

$$(84) \quad \gamma P_{n-2} + \delta Q_{n-2} = \pm D,$$

gdzie znak przy D bierzemy zgodny ze znakiem przy C . Liczba D jest więc w każdym razie całkowita.

Wzór (82) dowodzi, że lewa strona wzoru (81) jest ułamkiem nieprzywiedlnym, a że prawa strona wzoru (81) jest z założenia również ułamkiem nieprzywiedlnym, więc

$$(85) \quad aP_{n-1} + \beta Q_{n-1} = \pm A, \quad aP_{n-2} + \beta Q_{n-2} = \pm B,$$

przy czym znaki w obu wzorach są zgodne. Wobec (76), (85), (83) i (84) możemy napisać

$$(86) \quad \pm y = \frac{Ax_n + B}{Cx_n + D},$$

gdzie A, B, C, D są liczbami całkowitymi oraz

$$(87) \quad 0 < B < A \quad \text{ i } \quad C > 0,$$

a ponadto w myśl (82)

$$(88) \quad AD - CB = \pm 1.$$

Roźniamy liczbę wymierną A/C na ułamek łańcuchowy

$$(89) \quad \frac{A}{C} = q_0 + \frac{1}{q_1} + \dots + \frac{1}{q_m}$$

o liczbie ogniwi nieparzystej albo parzystej (p. str. 267), zależnie od tego, czy we wzorze (88) zachodzi znak górny, czy dolny.

Oznaczając przez A'/C' przedostatni redukt ułamka A/C (przypadek, kiedy redukt ten nie istnieje, pozostawiamy do zbadania czytelnikowi, jako nie następujący trudności), będziemy — jak łatwo widzieć — mieli

$$(90) \quad AC' - CA' = \pm 1,$$

gdzie znak będzie zgodny ze znakiem we wzorze (88). Wzory (88) i (90) dają w jednej chwili

$$(91) \quad A(D - C') = C(B - A'),$$

a że $(A, C) = 1$ na mocy (88), więc

$$(92) \quad B - A' = tA,$$

gdzie t jest liczbą całkowitą. Lecz oczywiście $0 \leq A' \leq A$. Wnosimy stąd wobec (87), że $|B - A'| < A$; we wzorze (92) musi więc być $t = 0$ czyli $B = A'$ i przeto wzór (91) daje $D = C'$. Wzór (86) możemy zatem napisać w postaci

$$\pm y = \frac{Ax_n + A'}{Cx_n + C'},$$

skąd na mocy (89)

$$(93) \quad \pm y = q_0 + \frac{1}{q_1} + \dots + \frac{1}{q_m} + \frac{1}{x_n}.$$

Jeżeli w tym wzorze zachodzi znak $+$, to oczywiście $y_{m+1} = x_n$.

Jeżeli zaś zachodzi w nim znak $-$, to rozróżnimy dwa przypadki: $q_1 = 1$ i $q_1 > 1$.

Niech $q_1 = 1$. Ponieważ z równości $-y = q_0 + \frac{1}{1} + \frac{1}{z}$ wynika równość $y = -q_0 - 1 + \frac{1}{z+1}$, więc w myśl (93) możemy napisać

$$y = -q_0 - 1 + \frac{1}{q_2 + 1} + \frac{1}{q_3} + \dots + \frac{1}{q_m} + \frac{1}{x_n},$$

skąd oczywiście $y_m = x_n$.

Niech wreszcie $q_1 > 1$. Ponieważ z równości $-y = q_0 + \frac{1}{z}$ wynika równość $y = -q_0 - 1 + \frac{1}{1 + \frac{1}{z-1}} = -q_0 - 1 + \frac{1}{1} + \frac{1}{z-1}$,

więc w myśl (93) możemy napisać

$$y = -q_0 - 1 + \frac{1}{1} + \frac{1}{q_1 - 1} + \frac{1}{q_2} + \dots + \frac{1}{q_m} + \frac{1}{x_n},$$

skąd w jednej chwili $y_{m+2} = x_n$.

Tak więc we wszystkich przypadkach dla pewnych liczb naturalnych k i l zachodzi równość (72), c. b. d. o.

Na mocy dowiedzonego twierdzenia 15, jeżeli dla danych liczb x i y znamy ich rozwinięcia na ułamki łańcuchowe, to potrafimy rozstrzygnąć, czy są one, czy nie są równoważne, i wyznaczyć współczynniki a, β, γ, δ wzoru (74).

Zapytamy obecnie, w jaki sposób można rozstrzygnąć, czy dane dwie niewymierności 2-go stopnia x i y są równoważne właściwie.

Otóż, stwierdzamy najpierw na mocy twierdzenia 15, czy są one w ogóle równoważne, a jeżeli są, to wyznaczamy współczynniki we wzorze (74). Jeżeli wzór ten ustala równoważność właściwą między x i y , to mamy odpowiedź twierdzącą na pytanie. W przeciwnym razie nie ma jeszcze odpowiedzi przeczącej, gdyż dwie liczby mogą być równoważne zarówno właściwie jak i niewłaściwie — takie są np. liczby $\sqrt{2} + 1$ i $\sqrt{2}$, gdyż $\sqrt{2} + 1 = (1 \cdot \sqrt{2} + 1) : (0 \cdot \sqrt{2} + 1)$ i $\sqrt{2} + 1 = (2 \cdot \sqrt{2} + 3) : (1 \cdot \sqrt{2} + 1)$ — lecz wówczas (wobec przechodniości stosunku równoważności) każda z tych liczb jest równoważna sama sobie zarówno właściwie jak i niewłaściwie. Ponieważ zaś każda liczba jest równoważna sama sobie właściwie, więc zagadnienie sprawdza się — jak widzimy — do tego, czy potrafimy dla każdej niewymierności 2-go stopnia rozstrzygnąć, czy jest ona sama sobie równoważna niewłaściwie.

Niech więc x będzie daną niewymiernością 2-go stopnia. Liczba x jest równoważna niewłaściwie liczbie $-x$, gdyż $-x = ((-1) \cdot x + 0) : (0 \cdot x + 1)$. Jeżeli więc liczba x jest sama sobie równoważna niewłaściwie, to z uwagi na to, że dwie liczby równoważne niewłaściwie trzeciej, są równoważne właściwie, liczba x jest równoważna liczbie $-x$ właściwie.

Na odwrót — jak łatwo widzieć — jeżeli liczby x i $-x$ są równoważne właściwie, to każda z nich jest sama sobie równoważna niewłaściwie.

Tak więc, aby stwierdzić, czy niewymierność 2-go stopnia x jest sama sobie równoważna niewłaściwie, wystarczy rozstrzygnąć, czy liczby x i $-x$ są równoważne właściwie, a to zagadnienie potrafimy już rozstrzygnąć za pomocą twierdzenia 13.

Zauważymy tu jeszcze, że — jak można dowieść — na to, żeby niewymierność 2-go stopnia była sama sobie równoważna niewłaściwie, potrzeba i wystarczy żeby okres jej rozwinięcia na ułamek łańcuchowy składał się z nieparzystej liczby ogniw¹⁾.

ROZDZIAŁ XVI

TEORIA LICZB CAŁKOWITYCH ZESPOLONYCH

§ 1. Liczby całkowite zespolone i ich norma. Liczby stowarzyszone. Przez *liczby całkowite zespolone* rozumiemy liczby zespolone $a+bi$, gdzie a i b są liczbami całkowitymi.

Wartość teorii liczb całkowitych zespolonych polega nie tyle na tym, że jest ona uogólnieniem teorii zwykłych liczb całkowitych, ile na tym, że jako jej proste zastosowanie otrzymujemy dowody różnych twierdzeń o zwykłych liczbach całkowitych, które na innej drodze są o wiele trudniejsze.

Z definicji działań arytmetycznych na liczbach zespolonych wynika natychmiast, że suma, różnica i iloczyn dwu lub więcej liczb zespolonych całkowitych jest liczbą zespoloną całkowitą.

ĆWICZENIA. 1. Znaleźć wszystkie rozkłady liczby 0 na sumę kwadratów dwu liczb całkowitych zespolonych.

Odpowiedź: $0 = (a+bi)^2 + (\pm b \mp ai)^2$, gdzie a i b są dowolnymi liczbami całkowitymi rzeczywistymi, a znaki należy użyć wszędzie górne lub wszędzie dolne.

2. Zbadać jakie liczby całkowite zespolone $x+yi$ są sumami dwu kwadratów liczb całkowitych zespolonych.

Rozwiązanie. Na to, by liczba całkowita zespolona $x+yi$ była sumą dwu kwadratów liczb całkowitych zespolonych, potrzeba i wystarczy, żeby y było liczbą parzystą oraz w przypadku, gdy x jest postaci $4t+2$, żeby y było podzielne przez 4.

Warunek jest konieczny, bo jeżeli

$$x+yi = (a+bi)^2 + (c+di)^2,$$

to

$$x = a^2 - b^2 + c^2 - d^2, \quad y = 2(ab + cd).$$

Jak łatwo stąd widzieć, x jest postaci $4t+2$ tylko wtedy, gdy co najmniej jedna z liczb a i b , a jednocześnie co najmniej jedna z liczb c i d jest parzysta. Lecz wówczas liczba $ab+cd$ jest parzysta, więc liczba y jest podzielna przez 4.

Warunek jest dostateczny, bo jeżeli $x = 2t+1$ i $y = 2u$, to

$$x+yi = (t+1+ui)^2 + (u-ti)^2,$$

¹⁾ Ob. 2-e wydanie tej książki, Warszawa 1925, str. 215.