§ 1. Statement of the result

Let $K$ be the classical quaternion field over the field $\mathbb{Q}$ of rational numbers with the quaternion units $1, i, j, k$, with relations $i^2 = j^2 = -1, k = ij = ji$. For a quaternion $x \in K$, we write its conjugate, trace and norm by $\bar{x}, Trx$ and $N_x$, respectively. Put

$$A = K \times K, \quad B = \mathbb{Q} \times K$$

and consider the map $h : A \to B$ defined by

$$h(z) = (N_x - N_y, 2xy), \quad z = (x, y) \in A.$$  

The map $h$ is the restriction on $\mathbb{Q}^8$ of the map $\mathbb{R}^8 \to \mathbb{R}^6$ which induces the classical Hopf fibration $S^7 \to S^4$ where each fibre is $S^3$.\(^1\) For a natural number $t$, put

$$S_{A}(t) = \{z = (x, y) \in A, N_x + N_y = t\},$$

$$S_{B}(t) = \{w = (u, v) \in B, u^2 + Nv = t\}.$$  

Then, $h$ induces a map

$$h_t : S_A(t) \to S_B(t^2).$$

Now, let $\mathfrak{o}$ be the unique maximal order of $K$ which contains the standard order $\mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k$. As is well-known, $\mathfrak{o}$ is given by

$$\mathfrak{o} = \mathbb{Z}\rho + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k, \quad \rho = \frac{1}{2}(1 + i + j + k).$$

The group $\mathfrak{o}^\times$ of units of $\mathfrak{o}$ is a finite group of order 24. The 24 units are: $\pm 1, \pm i, \pm j, \pm k, \frac{1}{2}(\pm 1 \pm i \pm j \pm k)$. We know that the number of quaternions in $\mathfrak{o}$ with norm $n$ is equal to $24s_\mathfrak{o}(n)$ where $s_\mathfrak{o}(n)$ denotes the sum of odd divisors of $n$.  

--Received November 6, 1974.--

Back to our geometrical situation, put

\[ A_Z = 0 \times 0, \quad B_Z = Z \times 0 \]

and define \( S_A(t)_Z, S_B(t)_Z \) by taking \( z, w \) in (1.2), (1.3) from \( A_Z, B_Z \), respectively. Then, the map \( h_t \) in (1.4) induces a map

\[(1.5) \quad h_{t,Z} : S_A(t)_Z \to S_B(t)_Z.\]

Because of the presence of 2 in (1.1), \( h_{t,Z} \) is actually a map \( S_A(t)_Z \to S_B(t^2)_Z \), where we have put

\[(1.6) \quad S_B(t^2)_Z = \{ w = (u, v) \in S_B(t)^2, \quad v \in 2o \}. \]

To each \( w \in S_B(t^2)_Z \), we shall associate two numbers as follows. First, we denote by \( a_w \) the number of \( z \in S_A(t)_Z \) such that \( h_{t,Z}(z) = w \). Next, we denote by \( n_w \) the greatest common divisor of the following six integers:

\[(1.7) \quad \frac{1}{2}(t + u), \frac{1}{2}(t - u), \frac{1}{2}T(\rho v), \frac{1}{2}T(i \beta), \frac{1}{2}T(j \beta), \frac{1}{2}T(k \beta). \]

The purpose of the present paper is to prove the relation:

\[(1.8) \quad a_w = 24s_o(n_w), \quad w \in S_B(t^2)_Z. \]

This is a type of formula which the author has in mind for the algebraic fibration over \( Z \) and has proved for Hopf fibrations of type \( S^3 \to S^2 \).\(^2\)

For proofs of facts concerning the arithmetic of quaternions the reader is referred to the report by Linnik.\(^3\)

\(\S\) 2. Change of the fibration.

Our problem is to determine the fibre of the map \( h_{t,Z} \) in (1.5). To do this, it is convenient to replace the map \( h \) by a map \( f \) in the following way. Namely, put

\[\Sigma = \{ \sigma = (a, \beta, c) \in Q \times K \times Q, \quad N\beta = ac \}, \]

\[f(z) = (Nx, zy, Ny), \quad z = (x, y) \in A = K \times K, \]

\[g(\sigma) = (a - c, 2\beta), \quad \sigma = (a, \beta, c) \in \Sigma, \]

\[\tau(\sigma) = (a, T(\rho \beta), T(i \beta), T(j \beta), T(k \beta), c) \quad \text{and} \quad \phi = \tau f. \]

---


\(^3\) Yu V. Linnik, Quaternions and Cayley numbers. Some applications of quaternion arithmetic. (Russian), Uspehi Mat. Nauk, IV, 5(33), (1949) 49–98.
Clearly, the diagram (2.1) is well-defined and commutative. If we restrict everything on the integral part, we obtain naturally the commutative diagram (2.2), where

\[ \Sigma_Z = \Sigma \cap (Z \times o \times Z) . \]

Next, consider the portion of (2.2) corresponding to a natural number \( t \) as follows. Put

\[ \Sigma(t)_Z = \{ \sigma = (a, \beta, c) \in \Sigma_Z, a + c = t \} , \]
\[ S(t)_Z = \{ s = (a, b_1, b_2, b_3, b_4, c) \in \mathbb{Z}^6, a + c = t \} . \]

Then, \( f_Z, \phi_Z \) induce the maps \( f_{t,Z}, \phi_{t,Z} \), respectively. It is almost trivial to check that the diagram (2.3) is well-defined and commutative. The only non-trivial map is \( g_{t,Z} \) and it is in fact a bijection: First of all, \( g_{t,Z} \) is well-defined, because we have

\[ g(\sigma) = (a - c, 2\beta) \quad \text{and} \quad N(g(\sigma)) = (a - c)^3 + 4N\beta = (a + c)^3 = t^3 \]

for \( \sigma = (a, \beta, c) \in \Sigma(t)_Z \). Next, suppose that \( g(\sigma) = g(\sigma') \) with \( \sigma = (a, \beta, c), \sigma' = (a', \beta', c') \in \Sigma(t)_Z \). Then we have \( \beta = \beta' \) and \( a - c = a' - c' \), but, since \( a + c = a' + c' = t \), we have \( \sigma = \sigma' \), i.e. \( g_{t,Z} \) is injective. Finally, take an element \( w = (u, v) \in S_B(t)^2 \), where \( u \in \mathbb{Z} \) and \( v \in 2o \) by (1.6). Put \( a = \frac{1}{2}(t + u), \beta = \frac{1}{2}v, c = \frac{1}{2}(t - u) \). Then \( \beta \in o \). Substituting \( v = 2\beta \) in the relation \( u^2 + Nv = t^2 \), we see that \( a, c \in \mathbb{Z}, a + c = t \) and \( N\beta = ac \), i.e. \( \sigma = (a, \beta, c) \in \Sigma(t)_Z \). Furthermore, we have \( g(\sigma) = (a - c, 2\beta) = (u, v) = w \), which proves that \( g_{t,Z} \) is surjective. Hence, the study of the map \( h_{t,Z} \) is reduced to the study of the map \( f_{t,Z} \). Now, we can make one more reduction in view of the equality

\[ f_{t,Z}^{-1}(\sigma) = f_Z^{-1}(\sigma) , \quad \sigma \in \Sigma(t)_Z , \]

which can be verified easily. Therefore, our problem is reduced to the determination of the structure of the fibre

\[ X(\sigma) = f_Z^{-1}(\sigma) \quad \text{for} \quad \sigma = (a, \beta, c) \in \Sigma_Z \quad \text{with} \quad a + c \geq 1 . \]
§ 3. Number of solutions

We shall denote by $I_K$ the set of all non-zero fractional right ideals of $K$ with respect to the maximal order $\mathfrak{o}$ and by $I_K^\mathfrak{o}$ the subset of $I_K$ consisting of right ideals in $\mathfrak{o}$. For an $n$-tuple $(a_1, \ldots, a_n) \neq (0, \ldots, 0)$, $a_i \in K$, we denote by $\text{id}_K (a_1, \ldots, a_n)$ the right ideal in $I_K$ generated by $a_1, \ldots, a_n$. As is well-known, every right ideal $\alpha$ in $I_K$ is principal: $\alpha = \alpha \mathfrak{o}$, $\alpha \in K^\times$. Hence, we may define the norm of $\alpha$ by $N\alpha = \mathcal{N}\alpha$.

**Lemma (3.1)** The following diagram is commutative:

$$
\begin{array}{ccc}
A_z & \xrightarrow{\text{id}_K} & I_K^\mathfrak{o} \\
\phi_x \downarrow & & \downarrow N \\
Z^\times & \xrightarrow{\text{id}_\mathfrak{o}} & \mathcal{N}.
\end{array}
$$

Here, the map $\phi_x$ is to take the greatest common divisor of six integers and $\phi_x (z) = \tau_z f_x (z) = (Nx, T(\rho \bar{x} y), T(i \bar{x} y), T(j \bar{x} y), T(k \bar{x} y), Ny)$.

**Proof.** Take an element $z = (x, y) \in A_z - \{0\}$. There is an $\alpha \in \mathfrak{o}$ such that $\text{id}_K (z) = x_0 + y_0 = \alpha_0$. We must prove that

\[(N\alpha)Z = (Nx)Z + T(\rho \bar{x} y)Z + T(i \bar{x} y)Z + T(j \bar{x} y)Z + T(k \bar{x} y)Z + (Ny)Z.
\]

Now, since $x_0 + y_0 = \alpha_0$, we can write $x = \alpha_0 \lambda$, $y = \alpha_0 \mu$ with $\lambda, \mu \in \mathfrak{o}$. Then, $Nx = (N\alpha)(N\lambda) \in (N\alpha)Z$, $Ny = (N\alpha)(N\mu) \in (N\alpha)Z$. Let $\epsilon$ be any one of the four quaternions $\rho, i, j, k$. Then we have

\[T(\epsilon \bar{x} y) = T(\epsilon \alpha_0 \lambda \mu) \in (N\alpha)Z.
\]

From these, we see that the right hand side of (3.2) is contained in the left hand side. To prove the other inclusion, write $\alpha = x_\xi + y_\eta$ with $\xi, \eta \in \mathfrak{o}$. Then, we have

\[N\alpha = (\xi x + \eta y)(x_\xi + y_\eta) = \xi \bar{x} x_\xi + \eta y_\eta + \xi x_\eta + \eta y_\xi = (Nx)(N\xi) + (Ny)(N\eta) + T(\xi \bar{x} y_\eta).
\]

Here, obviously, $(Nx)(N\xi) \in (Nx)Z$, $(Ny)(N\eta) \in (Ny)Z$. As for the term $T(\xi \bar{x} y_\eta)$, we have, first of all, $T(\xi \bar{x} y_\eta) = T(\eta \xi \bar{x} y)$. Next, write $\eta \xi$ as

\[\eta \xi = a_1 \rho + a_2 i + a_3 j + a_4 k \quad \text{with} \quad a_v \in \mathbb{Z}, \ 1 \leq v \leq 4.
\]

Then we have
which proves that the left hand side of (3.2) is contained in the right hand side, q.e.d.

For a natural number \( n \), put

\[
I^n_k(n) = \{ j \in I^n_k, N_j = n \}.
\]

This set is non-empty for any \( n \) (Lagrange) and contains \( s_q(n) \) elements.

Now, take an element \( \sigma = (\alpha, \beta, c) \in \Sigma_z \) with \( a + c \geq 1 \) and take a \( z = (x, y) \in X(\sigma) = f_z^{-1}(\sigma) \). Using the same \( \alpha, \beta \in \mathfrak{o} \) for \( z = (x, y) \) as in the proof of (3.1), we have, by (3.1),

\[
N(\text{id}_K (z)) = N\alpha = \text{id}_\mathfrak{q} (\phi_z(z)) = \text{id}_\mathfrak{q} (\tau_z f_z(z)) = \text{id}_\mathfrak{q} (\tau_z(\sigma)) .
\]

Hence, if we put

\[
n_\sigma = \text{id}_\mathfrak{q} (\tau_z(\sigma)) = \text{id}_\mathfrak{q} (a, T(\rho\beta), T(i\beta), T(j\beta), T(k\beta), c) ,
\]

we obtain a map

\[
d_\sigma : X(\sigma) \to I^n_k(n_\sigma) \text{ defined by } d_\sigma(z) = \text{id}_K(z) .
\]

Note that \( n_\sigma = n_w \) in (1.7) if \( w = g_{1,\mathfrak{S}}(\sigma) \) for \( \sigma \in \Sigma(t)_z \).

**Lemma (3.3)** The map \( d_\sigma \) is surjective.

**Proof.** Take any \( j \in I^n_k(n_\sigma) \) and write \( j = a\omega, \alpha \in \mathfrak{o} \). Since \( a + c \geq 1 \), either \( a \neq 0 \) or \( c \neq 0 \). Without loss of generality, we may assume that \( a \neq 0 \). Take \( \omega \in \mathfrak{o} \) such that \( \text{id}_K (a, \beta) = a\omega + \beta\omega = \omega\alpha \). Then, we have \( a = \omega\theta, \beta = \omega\psi \) with \( \theta, \psi \in \mathfrak{o} \). From (3.1), it follows that

\[
N\omega = N(\text{id}_K (a, \beta)) = \text{id}_\mathfrak{q} (\phi_z(a, \beta)) = \text{id}_\mathfrak{q} (Na, T(\rho\alpha\beta), T(i\alpha\beta), T(ja\beta), T(ka\beta), N\beta) = a \text{id}_\mathfrak{q} (a, T(\rho\beta), T(i\beta), T(j\beta), T(k\beta), c) = aN_\sigma = aN_j = aN\alpha .
\]

Hence we have \( a = N(\omega\alpha^{-1}) \). Put \( \gamma = \omega\alpha^{-1}, x = \eta^{-1}a \) and \( y = \eta^{-1}\beta \). Since we can also write \( x = \alpha\theta, y = \alpha\psi \), we see that \( z = (x, y) \in A_z - \{ 0 \} \). We claim that \( z \) is an element \( \in X(\sigma) \) such that \( d_\sigma(z) = j \). In fact, firstly, we have

\[
f(z) = (N\eta, \eta y, N\eta y) = (N(\eta^{-1}a), a\eta^{-1}\eta^{-1}\beta, N(\eta^{-1}\beta)) = (N(\eta^{-1})(a^2, a\beta, N\beta) = (N(\eta^{-1})a(a, \beta, c) = (a, \beta, c) = \sigma ,
\]
which shows that \( z \in X(\sigma) \). Next, we have

\[
d_\sigma (z) = \text{id}_\sigma (x, y) = \eta^{-1} \sigma_0 + \eta^{-1} \beta \sigma_0 = \eta^{-1} \omega_0 = \sigma_0 = j,
\]

which completes the proof of our assertion.

We shall now study the fibre \( d^{-1}_\sigma(j) \) for a fixed \( j \in I_\sigma(n_\sigma) \). Write \( j = \sigma_0 \) as before, and put \( \Gamma_1 = \sigma_0 \sigma_1^{-1} \), this being a finite group of order 24 depending only on \( j \) and not on the choice of the generator \( \sigma \).

**Lemma (3.4)** The group \( \Gamma_1 \) acts on the fibre \( d^{-1}_\sigma(j) \) simply and transitively by \( z = (x, y) \mapsto \lambda z = (\lambda x, \lambda y), \lambda \in \Gamma_1 \).

**Proof.** We shall first check that the action is well-defined. This follows from the relations

\[
f(\lambda z) = (N(\lambda x), x\lambda, N(\lambda y)) = N\lambda(Nx, xy, Ny)
\]

and

\[
d_\sigma (\lambda z) = \lambda \sigma_0 + \lambda y_0 = \lambda d_\sigma (z) = \lambda j = \lambda \sigma_0 = \sigma_0 = \sigma_0 = j,
\]

where \( \varepsilon \in \sigma^\times \). Next, clearly, the isotropy group is trivial everywhere. Finally, let \( z = (x, y), z' = (x', y') \) be any two points of \( d^{-1}_\sigma(j) \). Assume, for the moment, that both of \( x, y \) are \( \neq 0 \). Then, from the relation

\[
f(z) = (Nx, xy, Ny) = f(z') = (Nx', x'y', Ny'),
\]

we can find \( \lambda, \mu \in K \) with \( N\lambda = N\mu = 1 \) such that \( x' = \lambda x \) and \( y' = \mu y \). Substituting these in the relation \( x'y' = xy \), we get \( \lambda \mu = 1 \) and hence \( \lambda = \mu \). In case one of \( x \) or \( y \), say \( y = 0 \), then \( y' = 0 \) automatically, and we have \( x' = \lambda x, y' = \mu y, N\lambda = 1 \), again. In any case, we claim that this \( \lambda \) belongs to \( \Gamma_1 \). In fact, the assumption \( d_\sigma (z) = d_\sigma (z') = j \) implies that \( j = \sigma_0 = \sigma_0 + y_0 = x_0 + y_0 = \lambda \sigma_0 \) and so \( \lambda = \varepsilon \sigma \) for some \( \varepsilon \in \sigma \). However, since \( N\lambda = 1 \), we must have \( \varepsilon \in \sigma^\times \). Thus, \( \lambda = \varepsilon \sigma^{-1} \in \Gamma_1 \), q.e.d.

Combining (3.3) and (3.4), we obtain the following relation of cardinalities:

\[
\text{(3.5)} \quad \text{Card } (X(\sigma)) = \sum_1 \text{Card } (\Gamma_1) = 24 \text{ Card } (I_\sigma(n_\sigma)) = 24s_\sigma(n_\sigma).
\]

Our formula (1.8) is a translation of (3.5) through the bijection \( g_{i, z} \) in the diagram (2.3).

*The Johns Hopkins University*