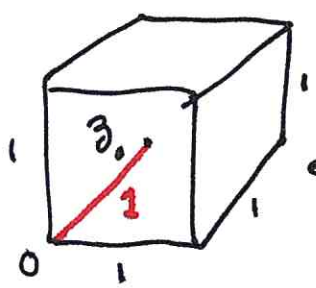
LECTURE 15: applications of quaternions, the four square theorem (§8.5, 8.6, 8.7, 8.8, 8.9)

§8.5: THE HURWITZ INTEGERS

The set $\mathbb{Z}[i,j,k] = \{a+bi+cj+dk \mid a,b,c,d \in \mathbb{Z}\}$ is a bit too sparse to support division. Consider $\alpha, \beta \in \mathbb{Z}[i,j,k]$ and note $\frac{\alpha}{\beta} \in \mathbb{Q}[i,j,k]$ and the grid of multiples of β fills $\mathbb{Z}[i,j,k]$ if $\mu\beta$ is closest β-multiple to $\frac{\alpha}{\beta}$ then $\alpha - \mu\beta$ = remainder term. As it stands, $|\alpha - \mu\beta| \not< |\beta|$ in all cases. In particular,

$$z_0 = \frac{1}{2} + \frac{i}{2} + \frac{j}{2} + \frac{k}{2}$$



$$|z_0| = \sqrt{\tfrac{1}{4}+\tfrac{1}{4}+\tfrac{1}{4}+\tfrac{1}{4}} = 1$$

← false picture, remember z_0 is at center of a 4-cube.

$\boxed{\text{Def}^{n}/\ \mathbb{Z}\left[\frac{1+i+j+k}{2}, i, j, k\right] \text{ are the Hurwitz integers (1896)}}$

Th^{m}/ the sum, difference and product of Hurwitz integers are Hurwitz integers. Also the norm of Hurwitz integer is an ordinary integer

Ex: $z = \frac{7+i+j+k}{2} = \frac{1+i+j+k}{2} + 3$ has $|z|^2 = \frac{49+1+1+1}{4} = \frac{52}{4} = 13.$

thus $z \neq \alpha\beta$ where $\text{norm}(\alpha), \text{norm}(\beta) < \text{norm}(z) = 13$. That is, $\frac{7+i+j+k}{2}$ is a Hurwitz prime.

Claim: $\text{Norm}\left(A\left(\frac{1+i+j+k}{2}\right) + Bi + Cj + Dk \right) \in \mathbb{Z}$

Proof: If $q = A\left(\frac{1+i+j+k}{2}\right) + Bi + Cj + Dk$ for $A, B, C, D \in \mathbb{Z}$, then

$$|q|^2 = \frac{A^2}{4} + \left(\frac{A}{2}+B\right)^2 + \left(\frac{A}{2}+C\right)^2 + \left(\frac{A}{2}+D\right)^2$$

$$= \frac{A^2}{4} + \frac{1}{4}(A+2B)^2 + \frac{1}{4}(A+2C)^2 + \frac{1}{4}(A+2D)^2$$

$$= \frac{1}{4}\left[A^2 + (A+2B)^2 + (A+2C)^2 + (A+2D)^2\right]$$

Consider, if $A \in 2\mathbb{Z}$ then $A^2, (A+2B)^2, (A+2C)^2, (A+2D)^2 \in 4\mathbb{Z}$ hence $|q|^2 \in \mathbb{Z}$. Likewise, if $A \in 2\mathbb{Z}+1$ then $A^2 \in 2\mathbb{Z}+1$ and likewise $A+2B, A+2C, A+2D$ are odd the sum of four odd squares has what form?

$$\left.\begin{aligned}
(2j_1+1)^2 &= 4j_1^2 + 4j_1 + 1 \\
(2j_2+1)^2 &= 4j_2^2 + 4j_2 + 1 \\
(2j_3+1)^2 &= 4j_3^2 + 4j_3 + 1 \\
(2j_4+1)^2 &= 4j_4^2 + 4j_4 + 1
\end{aligned}\right\} \text{ sum of these is in } 4\mathbb{Z} \quad \therefore |q|^2 \in \mathbb{Z}. //$$

Remark: this claim was crucial to reason that $q \in \mathbb{Z}\left[\frac{1+i+j+k}{2}, i, j, k\right]$ with $\text{norm}(q)$ an ordinary prime $\Rightarrow q$ a Hurwitz prime.

§8.6 CONJUGATES:

In LECTURE 14 we already discussed

$$q = a + ib + cj + dk \quad \text{has} \quad \bar{q} = a - bi - cj - dk$$

and $\overline{zw} = \bar{w}\bar{z}$, $\overline{z_1 \pm z_2} = \bar{z}_1 \pm \bar{z}_2$ and of course

$$\text{norm}(q) = |q|^2 \equiv q\bar{q} = a^2 + b^2 + c^2 + d^2$$

this beautiful algebra provides machinery to prove the following:

$\boxed{\text{Th}^{m}/ \text{ If } p \text{ is a prime in } \mathbb{Z} \text{ but not in Hurwitz-}\mathbb{Z} \text{ then } p = a^2+b^2+c^2+d^2 \text{ where } 2a, 2b, 2c, 2d \in \mathbb{Z}}$

<u>Proof</u>: Suppose $p = (a+bi+cj+dk)\gamma$ in $\mathbb{HZ}$ ← Hurwitz integers.

thus $\bar{p} = p = \bar{\gamma}(a-bi-cj-dk)$ hence,

$$\begin{aligned} p^2 &= (a+bi+cj+dk)\gamma\bar{\gamma}(a-bi-cj-dk) \\ &= (a+bi+cj+dk)(a-bi-cj-dk)\gamma\bar{\gamma} \\ &= (a^2+b^2+c^2+d^2)|\gamma|^2 \end{aligned}$$

But, as p is prime and $|\gamma| > 1 \Rightarrow \underline{a^2+b^2+c^2+d^2 = p}$.

Finally, $a, b, c, d \in \frac{1}{2}\mathbb{Z} \Rightarrow 2a, 2b, 2c, 2d \in \mathbb{Z}$. //

<u>Remark</u>: we showed in Lecture 14, $|zw| = |z||w|$

hence $|zw|^2 = |z|^2|w|^2$ so $\text{norm}(zw) = \text{norm}\, z \; \text{norm}\, w$

Thus, $p = (a+bi+cj+dk)\gamma \Rightarrow \text{norm}(p) = \text{norm}(a+bi+cj+dk)\,\text{norm}\,\gamma$

We derived this again here since I merely followed Stillwell pg. 150.

Claim: any ordinary prime $p \in \mathbb{Z}$ which is not a Hurwitz prime is the sum of four integer squares

Proof: Let $\alpha \in \mathbb{H}\mathbb{Z}$ and write,

$$\alpha = \omega + a' + b'i + c'j + d'k$$

where $a', b', c', d' \in 2\mathbb{Z}$ and $\omega = \frac{\pm 1 \pm i \pm j \pm k}{2}$ with some selection of signs. We can make such a decomposition for any $\alpha = A\left(\frac{1+i+j+k}{2}\right) + Bi + Cj + Dk$ where $A, B, C, D \in \mathbb{Z}$. Notice,

$$\omega\bar{\omega} = 1.$$

Consider $p = a^2 + b^2 + c^2 + d^2$ for $a, b, c, d \in \frac{1}{2}\mathbb{Z}$

$$\begin{aligned}
p &= (a + bi + cj + dk)(a - bi - cj - dk) \\
&= (\omega + a' + b'i + c'j + d'k)(\bar{\omega} + a' - b'i - c'j - d'k) \\
&= \Big[\underbrace{\omega\bar{\omega}}_{1} + \big(\underbrace{\underbrace{a' + b'i + c'j + d'k}_{a', b', c', d' \in 2\mathbb{Z}}}_{\text{integer comb. of } i, j, k, 1.}\big)\bar{\omega}\Big]\Big[\underbrace{\omega(\bar{\omega} - a' - b'i - c'j - d'k)}_{\text{conjugate}}\Big]
\end{aligned}$$

so for some, $A, B, C, D \in \mathbb{Z}$,

$$\begin{aligned}
&= [A + Bi + Cj + Dk][A - Bi - Cj - Dk] \\
&= \underline{A^2 + B^2 + C^2 + D^2}. \quad //
\end{aligned}$$

§8.7 A prime divisor property

S

Stillwell claims §8.5 contains proof of the division property for $\mathbb{Z}\left[\frac{1+i+j+k}{2}, i, j, k\right] = \mathbb{HZ}$. I don't see it there... let me attempt a proof. By now this argument should be familiar from our previous work in $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-2}]$ and the Eisenstein integers...

DIVISION PROP. FOR HURWITZ INTEGERS:
LET $\alpha, \beta \neq 0$ in $\mathbb{HZ}$ then $\exists\, \mu, \rho \in \mathbb{HZ}$ for which $\alpha = \mu\beta + \rho$ where $\text{norm}(\rho) < \text{norm}(\beta)$

Almost a proof:

Notice quaternion, well $\mathbb{HZ}$ multiples of β fill the space of quaternions in some 4-dim'l lattice. Consider

$\frac{\alpha}{\beta}$ is some quaterion and hence $\exists$ some closest

point in ~~β~~$(\mathbb{HZ})$ that is say ~~...~~ $z \in \mathbb{HZ}$

Hence, $\left|\frac{\alpha}{\beta} - z\right| < 1 \leftarrow$ ☆(JUMP!)☆

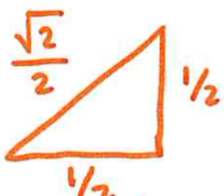
$$\frac{\alpha}{\beta} = q_1 + q_2 i + q_3 j + q_4 k, \quad z = a + bi + cj + dk \quad \text{for } a,b,c,d \in \tfrac{1}{2}\mathbb{Z}$$

$$|q_1 - a| \leq \tfrac{1}{2}, \quad |q_2 - b| \leq \tfrac{1}{2}, \quad |q_3 - c| \leq \tfrac{1}{2}, \quad |q_4 - d| \leq \tfrac{1}{2}$$

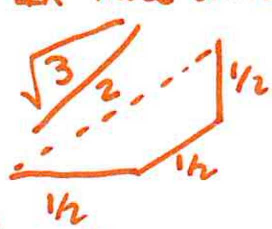
Then once I've justified the JUMP! we set $\rho = \alpha - z\beta$. Hence $\mu = z$ and $\alpha = \mu\beta + \rho$. Calculate,

$$\left|\frac{\alpha}{\beta} - z\right|^2 < 1 \iff |\alpha - \mu\beta|^2 < |\beta|^2 \iff |\rho|^2 < |\beta|^2$$
$$\iff \text{norm}(\rho) < \text{norm}(\beta). \quad //$$

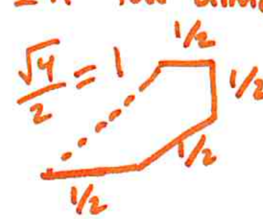
In two dimensions,



In three dimensions,



In four dimensions,



I guess they can't all be 1/2.

§ 8.7 continued

Def$^{\underline{n}}$/ δ is *right-divisor* of α if $\alpha = \gamma\delta$ for some γ

If α and β have a common right divisor δ then $\exists\, \gamma, \varepsilon$ such that $\alpha = \gamma\delta$ and $\beta = \varepsilon\delta$ hence

$$\rho = \alpha - \mu\beta = \gamma\delta - \mu\varepsilon\delta = (\gamma - \mu\varepsilon)\delta$$

It follows:

Prop: If the division of α by β produces quotient μ and remainder $\rho = \alpha - \mu\beta$ then δ a right-divisor of α & β is also a right-divisor of the remainder ρ.

If we begin with α, β then follow the Euclidean algorithm using right divisors we'll get

$$(\alpha, \beta) \longrightarrow (\beta, \rho) \longrightarrow \cdots \text{ right gcd}(\alpha, \beta)$$

By proposition above a common R-divisor of α & β is also a common right divisor of β and ρ etc. The usual arguments transfer to our context in $\mathbb{H}$ provided we are careful not to commute terms. We get a Bezout-type identity,

~~Prop: ∃ μ, ν Hurwitz integers s.t. for α, β ∈~~

Th$^{\underline{m}}$/ If $\alpha, \beta \in \mathbb{H}\mathbb{Z}$ then $\exists\, \mu, \nu \in \mathbb{H}\mathbb{Z}$ s.t.

$$\text{right gcd}(\alpha, \beta) = \mu\alpha + \nu\beta$$

7

Prime divisor Property of $\mathbb{Z}\left[\frac{1+i+j+k}{2}, i, j, k\right] = \mathbb{HZ}$,

If p is a real prime and if $p \mid \alpha\beta$ for some $\alpha, \beta \in \mathbb{HZ}$ then $p \mid \alpha$ or $p \mid \beta$ (weakened P.D.P. vs. one we gave previously ~~for $\mathbb{Z}[i]$~~ etc..)

Proof: Suppose $p \nmid \alpha$ then $1 = \text{right gcd}(p, \alpha)$ hence $\exists\, \mu, \nu \in \mathbb{HZ}$ s.t. $1 = \text{rightgcd}(p, \alpha) = \mu p + \nu\alpha$.
Multiply by β to obtain:

$$\beta = \mu p \beta + \nu\alpha\beta$$

Observe $p \mid \mu p \beta$ and $p \mid \alpha\beta$ hence $p \mid \nu\alpha\beta$ $\therefore$ $p \mid \mu p \beta + \nu\alpha\beta$
Hence $p \mid \beta$ and we're done. //

Remark: I'm not sure if $\mathbb{HZ}$ has the full prime divisor property: If a Hurwitz prime $\bar{\omega} \mid \alpha\beta$ then $\bar{\omega} \mid \alpha$ or $\bar{\omega} \mid \beta$.
In any event, the prime divisor property for ordinary primes alone apparently suffices for what follows next

§8.8 PROOF OF THE FOUR SQUARE THEOREM:

Observe $1 = 0^2 + 0^2 + 0^2 + 1^2$
$2 = 0^2 + 0^2 + 1^2 + 1^2$

Then $n = ab$ for a, b odd primes if we have a, b sums of four integer squares then the 4-square identity gives n as sum of 4 squares. Likewise for $n = abc$ apply 4-sq. identity to bc then to a with bc. It follows that we just need to show all odd primes are sums of 4 squared integers.

Prop: If $p = 2n+1$ then $\exists\, l, m \in \mathbb{Z}$ such that p divides $1 + l^2 + m^2$

~ Lagrange's Lemma for $\mathbb{H}\mathbb{Z}$

Proof: let x^2, y^2 be calculated for $x, y \in \{0, 1, 2, \dots, n\}$ with $x \neq y$ then $x^2 \not\equiv y^2 \bmod p$ since:

$$x^2 \equiv y^2 \bmod p \Rightarrow x^2 - y^2 \equiv 0 \pmod{p}$$
$$\Rightarrow (x-y)(x+y) \equiv 0 \pmod{p}$$
$$\Rightarrow x \equiv y \text{ or } x + y \equiv 0 \bmod p$$

However $p = 2n+1$ and $0 \leq x + y \leq 2n < 2n+1$ hence $x + y \not\equiv 0 \pmod{p}$ and $x \equiv y \bmod p \Rightarrow x - y \equiv 0 \bmod p$ and again $1 < |x-y| < n-1 \therefore x - y \not\equiv 0 \bmod p$.
$\therefore l = 0, 1, 2, \dots, n$ give $(n+1)$ incongruent values of l^2 modulo p.
Likewise
$m = 0, 1, 2, \dots, n$ give $(n+1)$ incongruent values of m^2 mod p and so $-m^2$ and $-1-m^2$ also takes $(n+1)$-incongruent values modulo p. If $p = 2n+1$ then $\exists\, 2n+1$ incongruent values mod p and $(n+1) + (n+1) = 2n+2 \Rightarrow l^2$ and $-1-m^2$ must share some value, at least one
$\therefore \exists\, l, m \in \mathbb{Z}$ s.t. $-1-m^2 \equiv l^2 \bmod p \therefore \underline{p \mid m^2 + l^2 + 1}$ //

FOUR SQUARE THEOREM:
every $n \in \mathbb{N}$ is sum of $a^2+b^2+c^2+d^2 = n$ for some $a, b, c, d \in \mathbb{N} \cup \{0\}$.

Proof: $1 = 1^2+0^2+0^2+0^2$, $2 = 1^2+1^2+0^2+0^2$ and for $n = ab$ if $a = \sum_{i=1}^{4} a_i^2$ and $b = \sum_{j=1}^{4} b_j^2$ then the four square identity shows $n = \sum_{k=1}^{4} c_k^2$ where c_k is constructed from a_i & b_j according to the identity. (See Lecture 14 for the f-la)

Hence $n = abc = a(bc)$ also expressed as sum of 4-squares if a, b, c are. Likewise for k-factors by repeated application of this argument. Thus it suffices to show p an odd prime is written as sum of 4 squares.

Prop. on 8 showed $p \mid m^2+l^2+1$ for some $m, l \in \mathbb{Z}$. Consider the factorization in $\mathbb{H}\mathbb{Z}$,

$$m^2+l^2+1 = (1-li-mj)(1+li+mj)$$

thus $p \mid m^2+l^2+1 \Rightarrow p \mid (1-li-mj)$ OR $p \mid (1+li+mj)$

[if p was in fact not just a prime, but also a Hurwitz prime]

But, $p \mid 1 \pm li \pm mj \Rightarrow 1 \pm li \pm mj = \gamma p$ for some $\gamma \in \mathbb{H}\mathbb{Z}$

$$\Rightarrow \frac{1 \pm li \pm mj}{p} = \gamma \text{ for some } \gamma \in \mathbb{H}\mathbb{Z}$$

and $\nexists$ such $\gamma \in \mathbb{H}\mathbb{Z}$ as $p \neq 2$. Therefore p is a prime, but not a Hurwitz prime thus, $\exists A, B, C, D \in \mathbb{Z}$ such that $p = A^2+B^2+C^2+D^2$. // (by page 4)

§8.9 DISCUSSION:

two-square identity

Diophantus ≈ 200 AD knew it

Viète Discovered Geometric meaning 1593

next see next page

Cotes de Moivre Gauss, Euler etc... $e^{i\theta} = \cos\theta + i\sin\theta$ and associated identities

Dedekind clearly & elegantly used $\mathbb{Z}[i]$ to derive identity & related Th^m's.

4-square identity

Euler stated it 1748

Rodrigues 1840 product of rotations (details not in Stillwell so far as I see)

Computer graphics sometimes based on quaternionic calculation as it makes for better rotation computationally (so I've been told, I don't know the details.)

Hamilton discovered $\mathbb{H}$ in 1843 after searching for multiplication in $\mathbb{R}^3$ with multiplicative norm property (would ⇒ 3 square identity which was already known to not exist by ~~Lagrange's~~ Legendre's older work)

Hurwitz integers applied to give natural derivation of 4-square th^m (1896)

Def^n/ A normed division algebra is a vector space over $\mathbb{R}$ paired with multiplication which satisfies norm$(z * w)$ = norm(z) norm(w) for some norm (usually take norm$(z) = \|z\|$, but in # theory we square it as to remove squareroots and allow direct arguments from norm$(z) \in \mathbb{Z}$...)

- Th^m/ Only normed division algebras are $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ and Octonians
- Th^m/ Hurwitz: only for $n = 1, 2, 4, 8$ does $\exists$ an n-square identity.

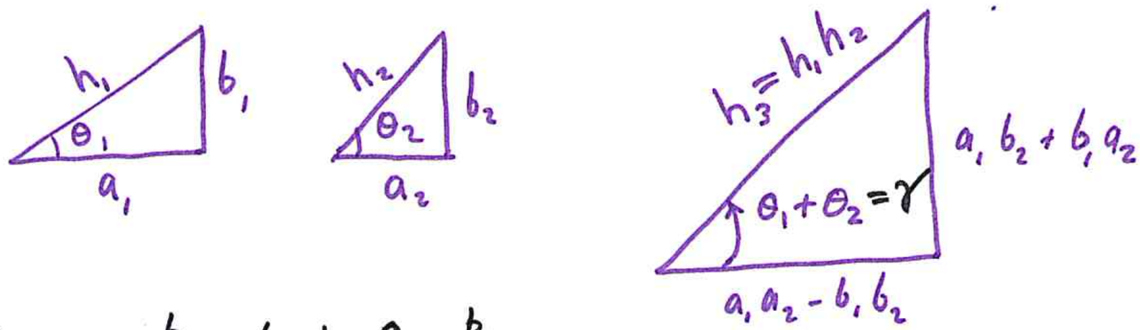
2-square identity

$$(a_1 + ib_1)(a_2 + ib_2) = a_1a_2 - b_1b_2 + i(a_1b_2 + b_1a_2)$$

Hence, by $|zw|^2 = |z|^2|w|^2$,

$$(a_1^2 + b_1^2)(a_2^2 + b_2^2) = (a_1a_2 - b_1b_2)^2 + (a_1b_2 + b_1a_2)^2$$

Geometrically, not to scale,



$$\tan\theta_1 = \frac{b_1}{a_1} \quad \& \quad \tan\theta_2 = \frac{b_2}{a_2} \qquad\qquad \tan(\gamma) = \frac{a_1b_2 + b_1a_2}{a_1a_2 - b_1b_2}$$

Consider,

$$\tan\gamma = \frac{a_1b_2 + b_1a_2}{a_1a_2 - b_1b_2} = \frac{a_1a_2\tan\theta_2 + a_1a_2\tan\theta_1}{a_1a_2 - a_1a_2\tan\theta_1\tan\theta_2}$$

$$= \frac{\tan\theta_2 + \tan\theta_1}{1 - \tan\theta_1\tan\theta_2}$$

$$= \frac{\cos\theta_1\sin\theta_2 + \cos\theta_2\sin\theta_1}{\cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2}$$

$$= \frac{\sin(\theta_1+\theta_2)}{\cos(\theta_1+\theta_2)}$$

$$= \tan(\theta_1+\theta_2) \quad \therefore \quad \underline{\gamma = \theta_1 + \theta_2}.$$

Complex exp. notation slicker here,

or, $\left.\begin{array}{l} a_1 + ib_1 = h_1e^{i\theta_1} \\ a_2 + ib_2 = h_2e^{i\theta_2} \end{array}\right\}$ $(a_1+ib_1)(a_2+ib_2) = h_1h_2e^{i\theta_1}e^{i\theta_2}$

$$= \underline{h_1h_2e^{i(\theta_1+\theta_2)}}.$$

Quaternions and Rotations?

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} \text{ or } \begin{pmatrix} \bar{x} \\ \bar{y} \\ \bar{z} \end{pmatrix} = \begin{bmatrix} \cos\theta & -\sin\theta & 0 \\ +\sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} x\cos\theta - y\sin\theta \\ +x\sin\theta + y\cos\theta \\ z \end{bmatrix}$$

Hope for $\vec{\alpha}' = R\vec{\alpha}$ where $\alpha = xi + yj + zk$

might have extra stuff so $R\vec{\alpha} = \vec{\alpha}'$

notational stupidity aside,

$$x'i + y'j + z'k = (ai + bj + ck)(xi + yj + zk) = \cancel{R(xi+yj+zk)}$$

$$= (\cos\theta x + \sin\theta y)i + (-x\sin\theta + y\cos\theta)j + zk$$

$$= (bz - cy)i + (cx - az)j + (ay - bx)k$$

Actually, not how it works!

Following Wikipedia (there is MUCH more there, I just explore briefly here)

$$\bar{p} = q p q^{-1} \quad \text{where } q = e^{\frac{\theta}{2}(u_x i + u_y j + u_z k)}$$

$$q = \cos\left(\frac{\theta}{2}\right) + (u_x i + u_y j + u_z k)\sin\left(\frac{\theta}{2}\right).$$

& $\vec{u} = u_x i + u_y j + u_z k$ is along the axis for the rotation.

Let's try

$\vec{u} = k$ since z-axis is rotation we're studying

$$q = \cos\left(\frac{\theta}{2}\right) + k\sin\left(\frac{\theta}{2}\right) \quad \& \quad q^{-1} = q^* = \cos\left(\frac{\theta}{2}\right) - k\sin\left(\frac{\theta}{2}\right)$$

$$\bar{p} = q p q^{-1}$$

$$= \left(\cos\frac{\theta}{2} + k\sin\frac{\theta}{2}\right)(xi + yj + zk)\left(\cos\frac{\theta}{2} - k\sin\frac{\theta}{2}\right)$$

$$= \left(\cos\frac{\theta}{2} + k\sin\frac{\theta}{2}\right)\left(x\cos\frac{\theta}{2}\, i + y\cos\frac{\theta}{2}\, j + z\cos\frac{\theta}{2}\, k + x\sin\frac{\theta}{2}\, j - y\sin\frac{\theta}{2}\, i + z\sin\frac{\theta}{2}\right)$$

$$= x\cos^2\frac{\theta}{2}\, i - y\sin\frac{\theta}{2}\cos\frac{\theta}{2}\, i - y\sin\frac{\theta}{2}\cos\frac{\theta}{2}\, i - x\sin^2\frac{\theta}{2}\, i + \cdots$$

$$= \left[x\left(\cos^2\frac{\theta}{2} - \sin^2\frac{\theta}{2}\right) - y\left(2\sin\frac{\theta}{2}\cos\frac{\theta}{2}\right)\right] i + \cdots = [x\cos\theta - y\sin\theta]\, i + \cdots$$