Michal Szabados

Integral Quaternions

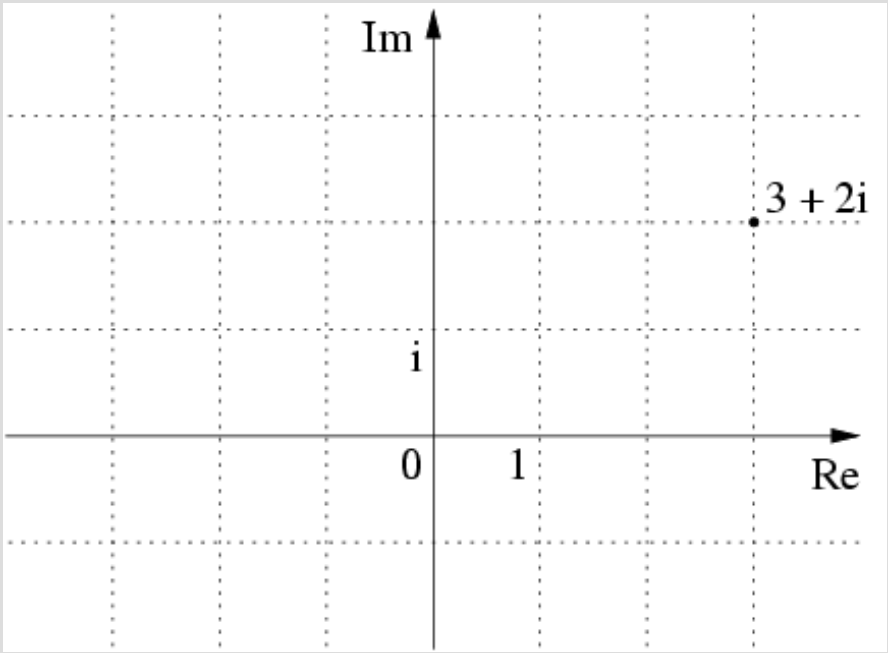
Fall school of Department of the Algebra (2010)

What I´m about to say

- How to define integral quaternions
- Basic properties
- Primes
- Lagrange's four-square theorem

Motivation

- Gaussian integers
  $\mathbf{Z}[i] = \{a+bi \mid a,b \in \mathbf{Z}\}$
- Euclidean domain
  $\Rightarrow$ UFD
- Prime $p = 4k+1$
  $\Rightarrow p = a^2+b^2$
  (Fermat)



First approach

- Lipschitz integers:

$$\mathbf{L} = \{a+bi+cj+dk \mid a,b,c,d \in \mathbf{Z}\}$$

- Problem: not Euclidean!

$$1+i+j+k = Q.2 + R$$

Impossible to choose Q and R such that

$$|R| < 2$$

- „Reason“: (½+½i+½j+½k) has distance 1 to the vertices of unit hypercube

„The Right Integers“

- Hurwitz integers:

$$\mathbf{H} = \{a+bi+cj+dk \mid \text{all } a,b,c,d \in \mathbf{Z} \text{ or all } a,b,c,d \in \mathbf{Z}+\tfrac{1}{2}\}$$

- We do not allow mixed coefficients!

- Proof of being Euclidean:

$$Z/D = a+bi+cj+dk \in \mathbf{Q}$$

take nearest $Q = A+Bi+Cj+Dk \in \mathbf{H}$, then

$$Z = Q.D + (a+bi+cj+dk-Q).D$$

Finally $|a+bi+cj+dk-Q| < \sqrt{\tfrac{1}{4}+\tfrac{1}{4}+\tfrac{1}{4}+\tfrac{1}{4}} = 1$.

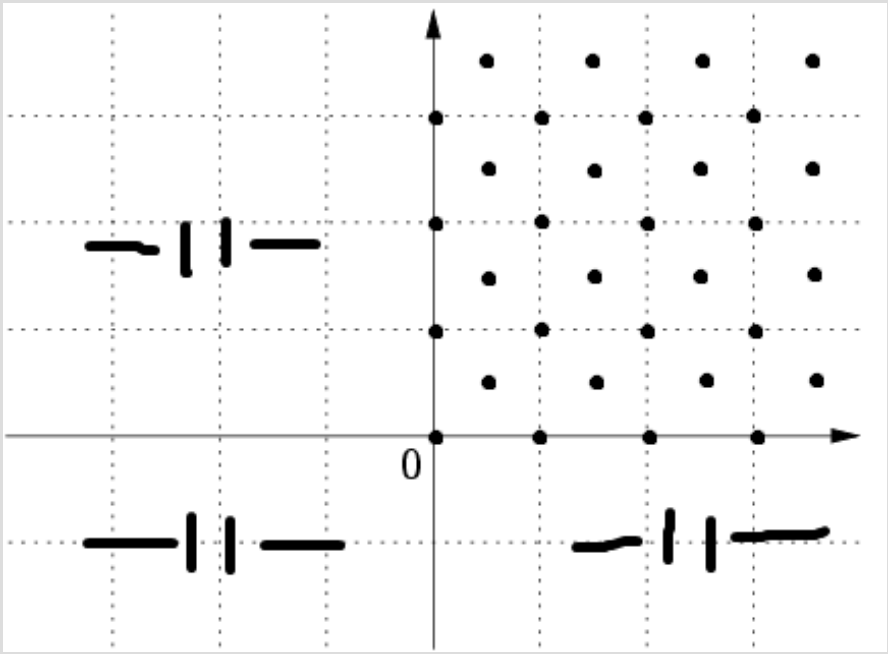
Properties

- $N(h) \in \mathbf{Z}$
- Closed under + and ·
- 24 units
- Euclidean $\Rightarrow$ PID
  $\Rightarrow$ UFD:

  Prime factorization

  $$Q = P_0 P_1 \cdots P_n$$

  is unique up to „unit migration“



A bit of number theory

- Euler's four-square identity

$$
\begin{aligned}
(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) = \\
(a_1 b_1 - a_2 b_2 - a_3 b_3 - a_4 b_4)^2 + \\
(a_1 b_2 + a_2 b_1 + a_3 b_4 - a_4 b_3)^2 + \\
(a_1 b_3 - a_2 b_4 + a_3 b_1 + a_4 b_2)^2 + \\
(a_1 b_4 + a_2 b_3 - a_3 b_2 + a_4 b_1)^2 .
\end{aligned}
$$

- |A||B| = |AB|

A bit of number theory

- Lagrange proved:

> Every natural number can be written as sum of (at most) four squares.

- With Euler's identity it is sufficient to prove this property for primes
- If for every prime p there exists Lipschitz integer with norm p, we are done

A picture: Adolf Hurwitz

Hurwitz primes

Strategy of the proof:
Let P be Hurwitz prime, p ordinary prime.

- $N(P) = p$ or $N(P) = p^2$ for some p
- p is not Hurwitz prime
- P is Hurwitz prime iff $N(P) = p$ for some p
- $N(P) \in \mathbf{Z}$

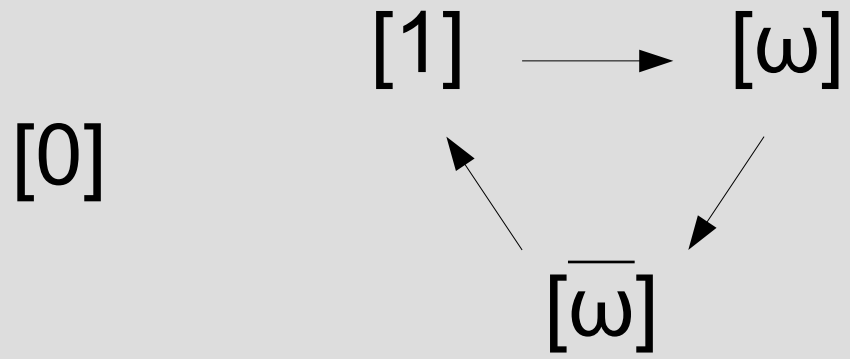
Lattices inside Hurwitzians

- Denote $\omega = \frac{1}{2}(-1+i+j+k)$. Then $\omega^2 = \overline{\omega}$.

$$\mathbf{H} = \mathbf{L} \cup \omega\mathbf{L} \cup \overline{\omega}\mathbf{L}$$

$$D_4 = \mathbf{L} \cap \omega\mathbf{L} \cap \overline{\omega}\mathbf{L}$$

  i.e. **H** contains 3 (not disjunct) copies of **L**!



- WOW: This shows that N(q) is sum of four squares for any Hurwitz integer q!

What I've already said

- Hurwitz integers with half-integer coefficients are better than Lipschitz integers
- Easy proof of Euler's four-square identity
- Some properties of Hurwitz primes
- Proof of Lagrange's four-square theorem
- The „WOW“ property

… if I had enough time.

Thank you for your attention!

Michal Szabados

Integral Quaternions

based on:

Conway, Smith: On Quaternions and Octonions

mail me:

misko.sz@gmail.com

Fall school of Department of the Algebra (2010)

Cheat Sheet I

- P has norm p or p^2:

$$N(P) = P\overline{P} = p_1 p_2 \cdots p_n \Rightarrow$$

$$P\overline{P} = p_1$$

$$\text{or } P\overline{P} = p_1 p_2 \Rightarrow P\overline{P} = p^2$$

- $2 = (1+i)(1-i)$
- Odd p is not Hurwitz prime:

$$\exists\ a,b: \quad p \mid 1+a^2+b^2$$

$$\Rightarrow p \mid (1+ai+bj)(1-ai-bj)$$

$$\Rightarrow (1/p \pm a/p.i \pm b/p.j) \in \mathbf{H} \ldots \text{ contradiction.}$$

Cheat Sheet II

$$\omega = \frac{-1+i+j+k}{2} \qquad \omega^2 = \overline{\omega} = \frac{-1-i-j-k}{2}$$

$$\begin{aligned}(a+bi+cj+dk+\omega)\cdot\omega &= \frac{-a-b-c-d-1}{2} + \frac{a-b+c-d-1}{2}i \\ &\quad + \frac{a-b-c+d-1}{2}j + \frac{a+b-c-d-1}{2}k\end{aligned}$$

$$\begin{aligned}(a+bi+cj+dk+\omega)\cdot\overline{\omega} &= \frac{-a-b-c-d}{2} + \frac{a-b+c-d}{2}i \\ &\quad + \frac{a-b-c+d}{2}j + \frac{a+b-c-d}{2}k + 1\end{aligned}$$