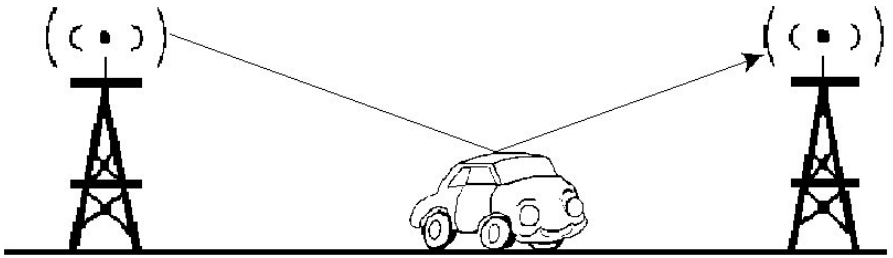
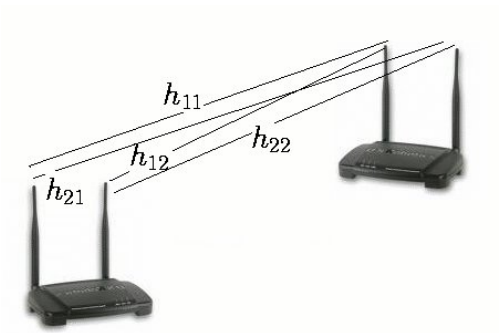
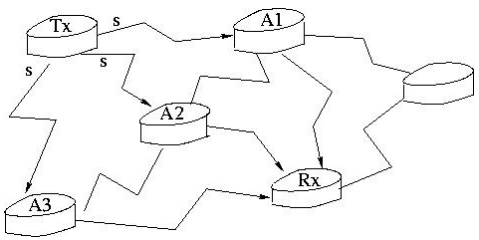
Lecture 4: Wireless Communications and Quaternion Algebras

F. Oggier

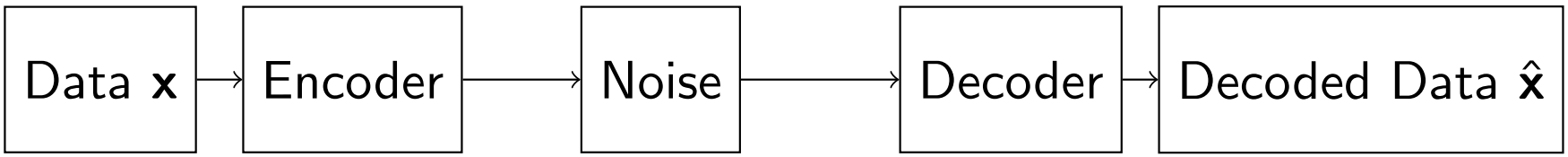
Journées Algébriques du Gabon, Libreville, Mars 2025




h_{11}
h_{12}
h_{21}
h_{22}


Tx
s
s
s
A1
A2
A3
Rx

Transmitter Channel Receiver

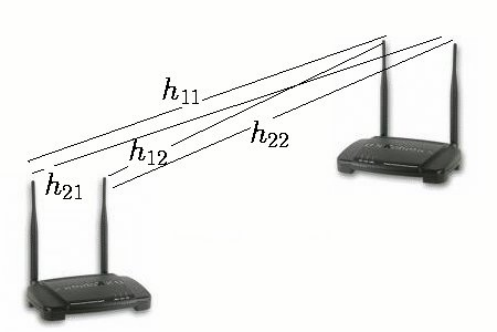


$$\mathbf{x} = (x_1, \ldots, x_k) \mapsto \underbrace{\mathbf{c} = (c_1, \ldots, c_n)}_{\text{codeword, } n \geq k} \longrightarrow \mathbf{y} \to \hat{\mathbf{x}} = (\hat{x}_1, \ldots, \hat{x}_k)$$

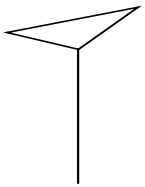
where $\mathbf{y}$ is the noisy channel output.

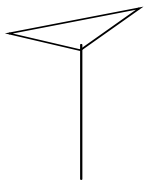
$$\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{C}^n \qquad \underbrace{\mathbf{H}}_{\textit{fading}}, \underbrace{\mathbf{w}}_{\textit{noise}} \qquad \mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{C}^n$$

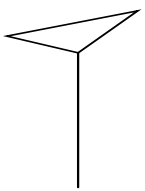
where $\mathbf{H}, \mathbf{w}$ have Gaussian random coefficients.

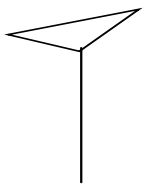


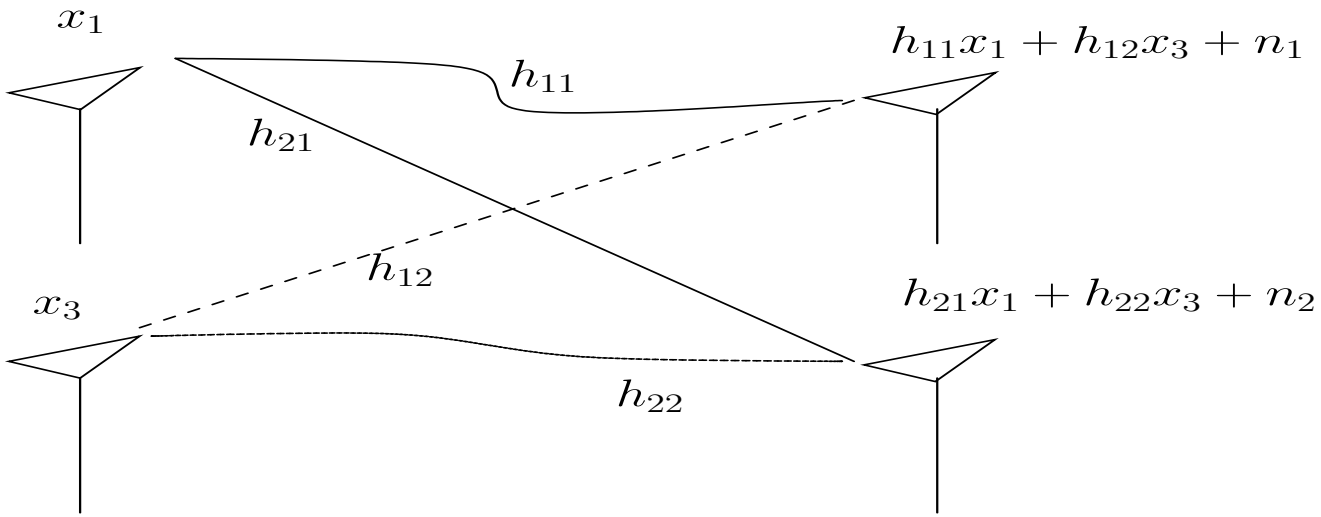
- Multiple Input Multiple Output

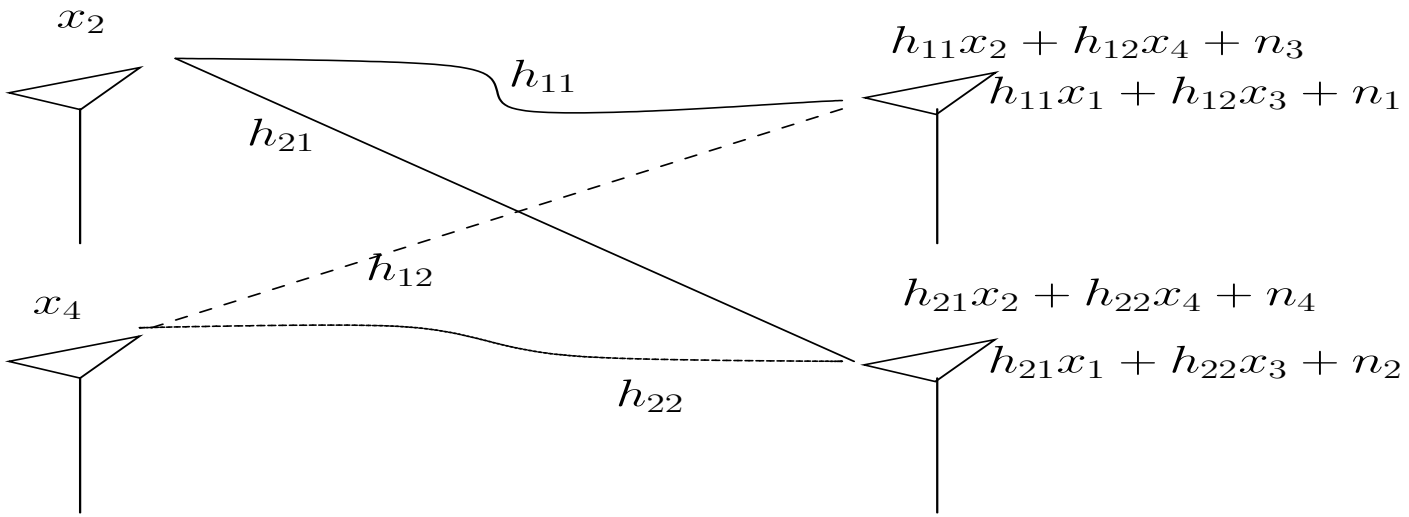


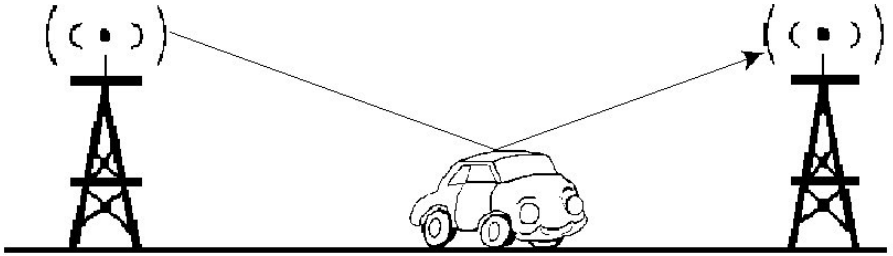




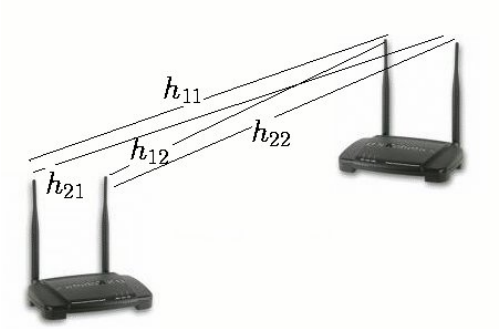


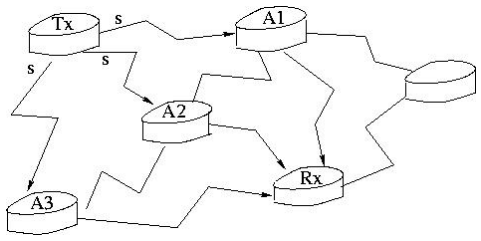

x_1
$h_{11}x_1 + h_{12}x_3 + n_1$
h_{11}
h_{21}
h_{12}
x_3
$h_{21}x_1 + h_{22}x_3 + n_2$
h_{22}


x_2
h_{11}
$h_{11}x_2 + h_{12}x_4 + n_3$
$h_{11}x_1 + h_{12}x_3 + n_1$
h_{21}
h_{12}
x_4
$h_{21}x_2 + h_{22}x_4 + n_4$
$h_{21}x_1 + h_{22}x_3 + n_2$
h_{22}



$$\mathbf{y} = H\mathbf{x} + \mathbf{w}, \;\; H = \mathrm{diag}(\alpha_1, \ldots, \alpha_n).$$





$$\mathbf{Y} = \begin{pmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{pmatrix} \underbrace{\begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}}_{space-time \;\; codeword \;\; \mathbf{X}} + \mathbf{W}$$

How do we design a code to achieve reliability? It depends on the channel.

- Hamming distance in the presence of erasures.
- Product "distance" for a single antenna channel:

$$P(\mathbf{x} \to \mathbf{y}) \leq \frac{const, SNR}{d_p^{(l)}(\mathbf{x}, \mathbf{y})^2}, \; d_p^{(l)}(\mathbf{x}, \mathbf{y}) = \prod_{x_i \neq y_i} |x_i - y_i|$$

  for the design of a finite constellation carved from a lattice $L \subset \mathbb{R}^n$.

- Determinant criterion for a multiple antennna channel:

$$P(\mathbf{X} \to \mathbf{Y}) \leq \frac{const, SNR}{|\det(\mathbf{X} - \mathbf{Y})|^4}.$$

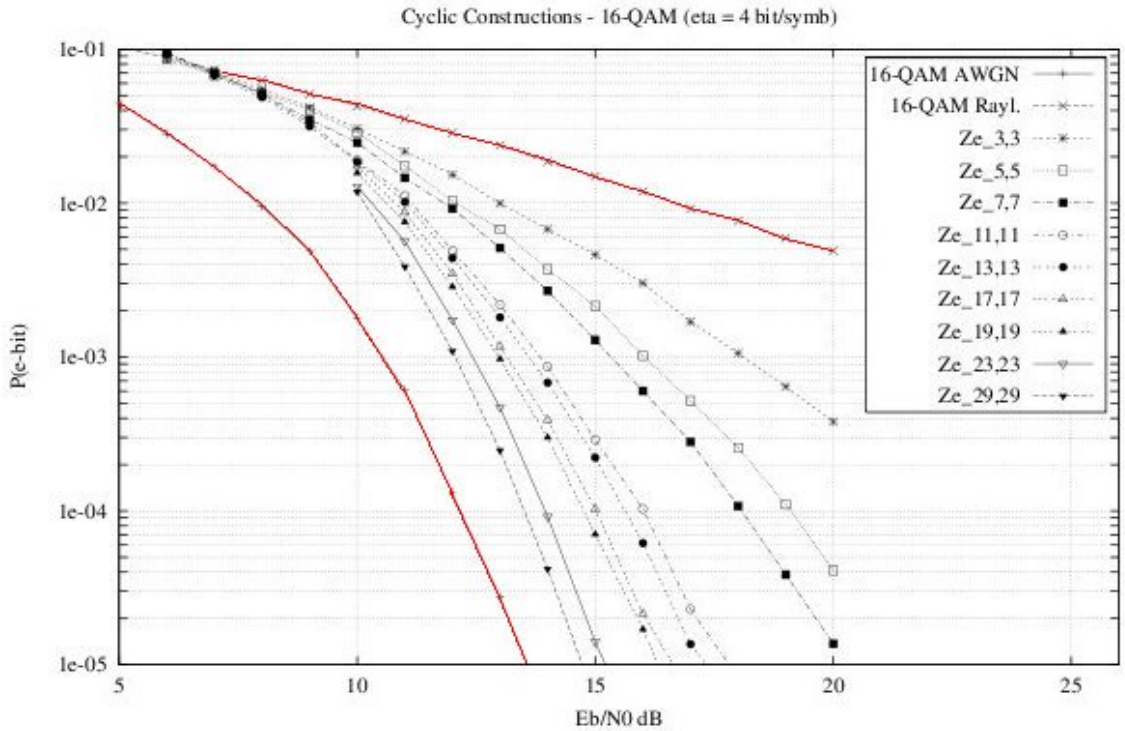
  for the design of the codebook $\mathcal{C}$:

$$\mathcal{C} = \left\{ \mathbf{X} = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} | x_1, x_2, x_3, x_4 \in \mathbb{C} \right\}$$

Fading and Diversity

- Design a *fully-diverse* lattice L such that $\min(l) = n$.
- Design a *fully-diverse* codebook $\mathcal{C}$ such that

$$\det(\mathbf{X} - \mathbf{X}') \neq 0, \ \mathbf{X} \neq \mathbf{X}' \in \mathcal{C}.$$



We need:

- a lattice such that $\min(I) = n$ is the minimum number of distinct components between any two constellation points.
  - Use a lattice built from a totally real number field.
- a family of matrices $\mathcal{C}$ such that

$$\det(\mathbf{X} - \mathbf{X}') \neq 0.$$

  - Use a division algebra.

The idea behind division algebras:

- The difficulty: the non-linearity of the determinant

$$\det(\mathbf{X} - \mathbf{X}') \neq 0, \ \mathbf{X} \neq \mathbf{X}' \in \mathcal{C}.$$

- If $\mathcal{C}$ is taken inside an algebra of matrices, the problem simplifies to

$$\det(\mathbf{X}) \neq 0, \ \mathbf{0} \neq \mathbf{X} \in \mathcal{C}.$$

- A *division algebra* is a non-commutative field.

- Recall: $\mathbb{C}$?
- $\mathbb{C}$=vector space of dimension 2 over $\mathbb{R}$, with basis

$$\{1, i\},\ i^2 = -1.$$

- Now: $\mathbb{H}$?
- $\mathbb{H}$=vector space of dimension 4 over $\mathbb{R}$, with basis

$$\{1, i, j, k\}.$$

- Rules: $i^2 = -1$, $j^2 = -1$, $k = ij = -ji$.

Complex Numbers	*Hamiltonian Quaternions*
$\mathbb{C} = \{x + yi \mid x, y \in \mathbb{R}\}$	$\mathbb{H} = \{x + yi + zj + wk \mid x, y, z, w \in \mathbb{R}\}$

Hamiltonian Quaternions form a division algebra.

- To see: $q = x + yi + wk \neq 0$ is invertible.

Hamiltonian Quaternions form a division algebra.

- To see: $q = x + yi + wk \neq 0$ is invertible.
- Define the conjugate of q:

$$\bar{q} = x - yi - zj - wk.$$

- Compute that

$$q\bar{q} = x^2 + y^2 + z^2 + w^2, \ x, y, z, w \in \mathbb{R}.$$

- The inverse of the quaternion q is given by

$$q^{-1} = \frac{\bar{q}}{q\bar{q}}.$$

How to get matrices:

- Any quaternion $q = x + yi + zj + wk$ can be written as

$$(x + yi) + j(z - wi) = \alpha + j\beta,\ \alpha,\ \beta \in \mathbb{C}.$$

- Now compute the multiplication by q:

$$\begin{aligned} \underbrace{(\alpha + j\beta)}_{q}(\gamma + j\delta) &= \alpha\gamma + j\bar{\alpha}\delta + j\beta\gamma + j^2\bar{\beta}\delta \\ &= (\alpha\gamma - \bar{\beta}\delta) + j(\bar{\alpha}\delta + \beta\gamma) \end{aligned}$$

- Write this equality in the basis $\{1, j\}$:

$$\begin{pmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{pmatrix} \begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} \alpha\gamma - \bar{\beta}\delta \\ \bar{\alpha}\delta + \beta\gamma \end{pmatrix}$$

Check list for the design of the codebook $\mathcal{C}$:

$$\mathcal{C} = \left\{ \mathbf{X} = \begin{pmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{pmatrix} | \alpha, \beta \in \mathbb{C} \right\}$$

- Linearity ✓
- Diversity ✓

$$\det(\mathbf{X} - \mathbf{X}') = \det \begin{pmatrix} \alpha - \alpha' & -\overline{(\beta - \beta')} \\ \beta - \beta' & \overline{\alpha - \alpha'} \end{pmatrix} = 0$$
$$\iff |\alpha - \alpha'|^2 + |\beta - \beta|^2 = 0$$

A quaternion algebra is a particular case of a cyclic algebra.

- Let $L = \mathbb{Q}(i, \sqrt{d}) = \{u + \sqrt{d}v,\ u, v\ \in \mathbb{Q}(i)\}$. A *cyclic algebra* $\mathcal{A}$ is defined as follows

$$\mathcal{A} = L \oplus eL$$

with $e^2 = \gamma$ and

$$\lambda e = e\sigma(\lambda) \text{ where } \sigma(u + \sqrt{d}v) = u - \sqrt{d}v.$$

- Recall that $(\mathbb{C} = \mathbb{R} \oplus i\mathbb{R})$

$$\mathbb{H} = \mathbb{C} \oplus j\mathbb{C}$$

with

$$j^2 = -1 \text{ and } ij = -ji$$

- We associate to an element its multiplication matrix

$$x = x_0 + ex_1 \in \mathcal{A} \leftrightarrow \begin{pmatrix} x_0 & \gamma\sigma(x_1) \\ x_1 & \sigma(x_0) \end{pmatrix}$$

- as we did for the Hamiltonian Quaternions.

$$q = \alpha + j\beta \in \mathbb{H} \leftrightarrow \begin{pmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{pmatrix}$$

Note, two information symbols (α, β) versus four (x_0, x_1, x_2, x_3).

- The Golden code is related to the Golden number $\theta = \frac{1+\sqrt{5}}{2}$, a root of $X^2 - X - 1 = 0$ ($\sigma(\theta) = \bar{\theta} = \frac{1-\sqrt{5}}{2}$ is the other).
- We define the code $\mathcal{C}$ as

$$\mathcal{C} = \left\{ \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} = \begin{bmatrix} a + b\theta & c + d\theta \\ i(c + d\bar{\theta}) & a + b\bar{\theta} \end{bmatrix} : a, b, c, d \in \mathbb{Z}[i] \right\}$$

- This code has been built from the cyclic algebra $\mathcal{A}$, given by

$$\mathcal{A} = \{y = (u + v\theta) + e(w + z\theta) \mid e^2 = i,\ u, v, w, z \in \mathbb{Q}(i)\}.$$

- We have the code $\mathcal{C}$ as

$$\mathcal{C} = \left\{ \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} = \begin{bmatrix} a+b\theta & c+d\theta \\ i(c+d\bar{\theta}) & a+b\bar{\theta} \end{bmatrix} : a,b,c,d \in \mathbb{Z}[i] \right\}$$

- $\mathcal{C}$ is a linear code, i.e., $\mathbf{X}_1 + \mathbf{X}_2 \in \mathcal{C}$ for all $\mathbf{X}_1, \mathbf{X}_2 \in \mathcal{C}$.
- The minimum determinant of $\mathcal{C}$ is given by

$$\delta_{\min}(\mathcal{C}) = \min_{\mathbf{X}_1 \neq \mathbf{X}_2 \in \mathcal{C}} |\det(\mathbf{X}_1 - \mathbf{X}_2)|^2 = \min_{\mathbf{0} \neq \mathbf{X} \in \mathcal{C}} |\det(\mathbf{X})|^2.$$

We need to show that $\mathcal{A}$ is a division algebra.

We need to prove that the algebra $\mathcal{A} = (L/\mathbb{Q}(i), \sigma, i)$ is a division algebra.

- We have

$$\det \begin{bmatrix} a + b\theta & c + d\theta \\ i(c + d\bar{\theta}) & a + b\bar{\theta} \end{bmatrix} = N_{L/\mathbb{Q}(i)}(a + b\theta) - iN(c + d\theta).$$

- Since

$$N_{L/\mathbb{Q}(i)}(a + b\theta) - iN(c + d\theta) = 0 \iff \frac{N_{L/\mathbb{Q}(i)}(a + b\theta)}{N(c + d\theta)} = i$$

it is enough to show that i is not a norm in $L/\mathbb{Q}(i)$.

- We are looking at $L = \mathbb{Q}(i, \sqrt{5})$, we will give a proof that works for $p \equiv 5 \pmod 8$.
- Let $L = \mathbb{Q}(i, \sqrt{p})$ be a relative extension of $\mathbb{Q}(i)$. Let $x \in L$, $x = a + b\sqrt{p}$, $a, b \in \mathbb{Q}(i)$. Its relative norm is

$$N_{L/\mathbb{Q}(i)}(x) = (a + b\sqrt{p})(a - b\sqrt{p}) = a^2 - pb^2.$$

- We thus need to show that $a^2 - pb^2 = i$ has no solution in L.

- To prove that $a^2 - pb^2 = i$ has no solution in L, we prove it has not solution in the field of p-adic numbers $\mathbb{Q}_p$.
- Let $\mathbb{Z}_p = \{x \in \mathbb{Q}_p | \nu_p(x) \geq 0\}$ be the valuation ring of $\mathbb{Q}_p$, where $\nu_p(x)$ denotes the valuation of x in p.
- There are embeddings of $\mathbb{Q}(i)$ into $\mathbb{Q}_p$ if $X^2 + 1$, the minimal polynomial of i, has roots in $\mathbb{Z}_p$. Using Hensel's Lemma, it is enough to check that -1 is a square in $\mathbb{F}_p$.
- By assumption, $p \equiv 5 \pmod 8$, thus $p \equiv 1 \pmod 4$.
- Recall that $x \in \mathbb{F}_p^*$ is a square if and only if $x^{(p-1)/2} = 1$ and that consequently, if $p \equiv 1 \pmod 4$, -1 is a square in $\mathbb{F}_p$.

- We want to prove that

$$a^2 - pb^2 = i, \ a, b \in \mathbb{Q}(i)$$

has no solution in L.

- Using the embedding of $\mathbb{Q}(i)$ into $\mathbb{Q}_p$, this equation can be seen in $\mathbb{Q}_p$ as

$$a^2 - pb^2 = y + px, \ a, b \in \mathbb{Q}_p, \ x, y \in \mathbb{Z}_p,$$

where $y^2 = -1$.

- If there is a solution to the original equation, then this solution still holds in $\mathbb{Q}_p$. Thus proving that no solution exists in $\mathbb{Q}_p$ would conclude the proof.

We first show that a and b are in fact in $\mathbb{Z}_p$.

- In terms of valuation, we have

$$\nu_p(a^2 - pb^2) = \nu_p(y + px).$$

- Since $x \in \mathbb{Z}_p$, the right term yields $\nu_p(y + px) \geq \inf\{\nu_p(y), \nu_p(x) + 1\} = 0$, and we have equality since the valuations are distinct.
- Now the left term becomes $0 = \nu_p(a^2 - pb^2) = \inf\{2\nu_p(a), 2\nu_p(b) + 1\}$. The only possible case is $\nu_p(a) = 0$, implying $a \in \mathbb{Z}_p$ and consequently $b \in \mathbb{Z}_p$.

We conclude showing that

$$a^2 - pb^2 = y + px, \;\; a, b, x, y \in \mathbb{Z}_p$$

has no solution.

- Reducing (mod $p\mathbb{Z}_p$), we see that y has to be a square in $\mathbb{F}_p$.
- Since $y^2 = -1$, $y^{(p-1)/2} = (-1)^{(p-1)/4} = -1$ by choice of $p \equiv 5 \pmod 8$.
- Then by the above characterization of squares, y is not a square, which is a contradiction. $\square$

This result does not hold for $p \equiv 1 \pmod 8$. Consider $L = \mathbb{Q}\left(\sqrt{17}, i\right)$, and $x = \frac{3(i-1)}{4} - \frac{(i-1)\sqrt{17}}{4}$. We check that $N_{L/\mathbb{Q}(i)}(x) = i$.

- Let $\mathbf{X} \in \mathcal{C}$, then

$$\begin{aligned}
\det(\mathbf{X}) &= \det \begin{pmatrix} a+b\theta & c+d\theta \\ i(c+d\bar{\theta}) & a+b\bar{\theta} \end{pmatrix} \\
&= (a+b\theta)(a+b\bar{\theta}) - i(c+d\theta)(c+d\bar{\theta}) \\
&= a^2 + ab(\bar{\theta}+\theta) - b^2 - i[c^2 + cd(\theta+\bar{\theta}) - d^2] \\
&= a^2 + ab - b^2 + i(c^2 + cd - d^2),
\end{aligned}$$

  $a, b, c, d \in \mathbb{Z}[i]$.

- Thus

$$\det(\mathbf{X}) \in \mathbb{Z}[i] \Rightarrow \delta_{min}(\mathcal{C}) = |\det(\mathbf{X})|^2 \geq 1.$$

- Does *not* depend on the cardinality of $\mathcal{C}$.

In fact, we have

$$\det \begin{bmatrix} a+b\theta & c+d\theta \\ i(c+d\bar{\theta}) & a+b\bar{\theta} \end{bmatrix} = N_{L/\mathbb{Q}(i)}(a+b\theta) - iN(c+d\theta)$$

so the property that $\det(\mathbf{X}) \in \mathbb{Z}[i]$ follows from a property of the norm.

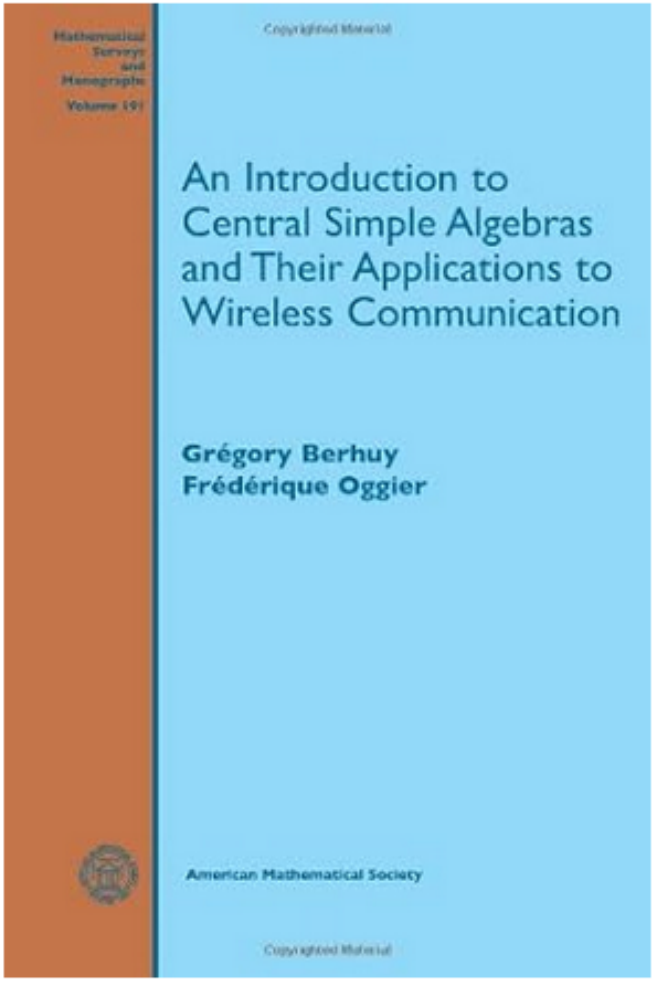
More:

- cyclic algebras,
- crossed product algebras,
- lattice structure
- Construction A

Quaternion algebras are of interest:

- to mathematicians working on quadratic forms and non-commutative algebras,
- to cryptographers ('ideal' lattices),
- to coding theorists (MIMO channels).

A variation of such a code was impletemented in a standard.


Mathematical Surveys and Monographs
Volume 191
An Introduction to Central Simple Algebras and Their Applications to Wireless Communication
Grégory Berhuy
Frédérique Oggier
American Mathematical Society