Math 210B. Quaternions

1. Introduction

Inside the $\mathbf{C}$-algebra $\mathrm{Mat}_n(\mathbf{C})$ there is the $\mathbf{R}$-subalgebra $\mathrm{Mat}_n(\mathbf{R})$ with the property that the natural map of $\mathbf{C}$-algebras

$$\mathbf{C} \otimes_{\mathbf{R}} \mathrm{Mat}_n(\mathbf{R}) \to \mathrm{Mat}_n(\mathbf{C})$$

(satisfying $c \otimes M \mapsto cM$) is an isomorphism. (Proof: compare $\mathbf{C}$-bases on both sides, using the standard $\mathbf{R}$-basis of $\mathrm{Mat}_n(\mathbf{R})$ and the analogous $\mathbf{C}$-basis for $\mathrm{Mat}_n(\mathbf{C})$.) There are many other $\mathbf{R}$-subalgebras $A \subset \mathrm{Mat}_n(\mathbf{C})$ with the property that the natural map of $\mathbf{C}$-algebras $\mathbf{C} \otimes_{\mathbf{R}} A \to \mathrm{Mat}_n(\mathbf{C})$ is an isomorphism: $A = g\mathrm{Mat}_n(\mathbf{R})g^{-1}$ for any $g \in \mathrm{GL}_n(\mathbf{C})$. This is a bit "fake" since such an $\mathbf{R}$-subalgebra A is just $\mathrm{Mat}_n(\mathbf{R})$ embedded into $\mathrm{Mat}_n(\mathbf{C})$ via applying an automorphism of $\mathrm{Mat}_n(\mathbf{C})$ (namely, g-conjugation) to the usual copy of $\mathrm{Mat}_n(\mathbf{R})$ inside $\mathrm{Mat}_n(\mathbf{C})$.

But are there any fundamentally different A, such as one that is *not isomorphic* to $\mathrm{Mat}_n(\mathbf{R})$ as an $\mathbf{R}$-algebra? Any such A would have to have $\mathbf{R}$-dimension equal to n^2. In the mid-19th century, Hamilton made the important discovery that for $n = 2$ there *is* a very different choice for A. This exotic 4-dimensional $\mathbf{R}$-algebra is denoted $\mathbf{H}$ in his honor, called the *quaternions*.

2. Basic construction

Define $\mathbf{H} \subset \mathrm{Mat}_2(\mathbf{C})$ to be the $\mathbf{R}$-span of the elements

$$\mathbf{1} := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \mathbf{i} := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \mathbf{j} := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \mathbf{k} := \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Explicitly, for $a, b, c, d \in \mathbf{R}$ we have

$$a \cdot \mathbf{1} + b \cdot \mathbf{i} + c \cdot \mathbf{j} + d \cdot \mathbf{k} = \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix}$$

for $\alpha = a + bi, \beta = c + di \in \mathbf{C}$. It follows that such an $\mathbf{R}$-linear combination vanishes if and only if $\alpha, \beta = 0$, which is to say $a, b, c, d = 0$, so $\{\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ is $\mathbf{R}$-linearly independent; we call it the *standard basis* for $\mathbf{H}$. These calculations also show that $\mathbf{H}$ can be alternatively described as the set of elements of $\mathrm{Mat}_2(\mathbf{C})$ admitting the form

$$M = \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix}$$

for $\alpha, \beta \in \mathbf{C}$.

It is easy to verify by direct calculation (do it!) that the following relations are satisfied:

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{1}, \;\; \mathbf{ij} = \mathbf{k} = -\mathbf{ji}$$

and likewise

$$\mathbf{jk} = -\mathbf{kj} = \mathbf{i}, \;\; \mathbf{ki} = -\mathbf{ik} = \mathbf{j}.$$

For any two quaternions

$$h = a \cdot \mathbf{1} + b \cdot \mathbf{i} + c \cdot \mathbf{j} + d \cdot \mathbf{k}, \;\; h' = a' \cdot \mathbf{1} + b' \cdot \mathbf{i} + c' \cdot \mathbf{j} + d' \cdot \mathbf{k}$$

with $a, b, c, d, a', b', c', d' \in \mathbf{R}$, the product $hh' \in \mathrm{Mat}_2(\mathbf{C})$ expands out as an $\mathbf{R}$-linear combination in the products $\mathbf{e}\mathbf{e}'$ for $\mathbf{e}, \mathbf{e}'$ in the standard basis $\{\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$. But we just saw that all products among pairs from this standard basis are in $\mathbf{H}$, establishing the first assertion in:

Proposition 2.1. *The $\mathbf{R}$-subspace $\mathbf{H} \subset \mathrm{Mat}_2(\mathbf{C})$ is an $\mathbf{R}$-subalgebra and the natural map of $\mathbf{C}$-algebras $\mu : \mathbf{C} \otimes_{\mathbf{R}} \mathbf{H} \to \mathrm{Mat}_2(\mathbf{C})$ is an isomorphism.*

The stability of $\mathbf{H}$ under multiplication could also be checked using the description as matrices of the form $\left(\begin{smallmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{smallmatrix} \right)$ with $\alpha, \beta \in \mathbf{C}$.

Proof. It remains to prove that the $\mathbf{C}$-linear map μ is an isomorphism. The source and target of μ are 4-dimensional over $\mathbf{C}$, so it suffices to check injectivity. More specifically, this is the assertion that the standard $\mathbf{R}$-basis of $\mathbf{H}$ (viewed inside $\mathrm{Mat}_2(\mathbf{C})$) is even linearly independent over $\mathbf{C}$ (not just over $\mathbf{R}$).

Taking a, b, c, d from $\mathbf{C}$ (not just $\mathbf{R}$), we have

$$a \cdot \mathbf{1} + b \cdot \mathbf{i} + c \cdot \mathbf{j} + d \cdot \mathbf{k} = \begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix},$$

so if this vanishes then we have $a \pm bi = 0 = \pm c + di$ with $a, b, c, d \in \mathbf{C}$ (not necessarily in $\mathbf{R}$!) and *both* signs. It is then clear that $a = 0$, so $b = 0$, and likewise that $di = 0$, so d and c vanish too. ■

The *center* of an associative ring with identity is the subset of elements commuting with everything under multiplication. This is a commutative subring (with the same identity).

Corollary 2.2. *The center of $\mathbf{H}$ coincides with $\mathbf{R} = \mathbf{R} \cdot \mathbf{1}$.*

Proof. Let $Z \subset \mathbf{H}$ be the center, so $\mathbf{R} \subset Z$. To prove equality it suffices to show $\dim_{\mathbf{R}} Z \le 1$. But $\mathbf{C} \otimes_{\mathbf{R}} Z$ is certainly contained in the center of $\mathbf{C} \otimes_{\mathbf{R}} \mathbf{H} \simeq \mathrm{Mat}_2(\mathbf{C})$, and the center of the latter is just the evident copy of $\mathbf{C}$. This shows that $\dim_{\mathbf{R}} Z = \dim_{\mathbf{C}}(\mathbf{C} \otimes_{\mathbf{R}} Z) \le 1$. ■

3. Conjugation and norm

For $h = a \cdot \mathbf{1} + b \cdot \mathbf{i} + c \cdot \mathbf{j} + d \cdot \mathbf{k}$, define its *conjugate* to be

$$\overline{h} = a \cdot \mathbf{1} - b \cdot \mathbf{i} - c \cdot \mathbf{j} - d \cdot \mathbf{k},$$

so clearly $\overline{\overline{h}} = h$. We call h a *pure quaternion* if $a = 0$, or equivalently $\overline{h} = -h$. Although multiplication in $\mathbf{H}$ is not commutative, in a special case commutativity holds:

Proposition 3.1. *The products $h\overline{h}$ and $\overline{h}h$ coincide and are equal to $a^2 + b^2 + c^2 + d^2$. This is also equal to $\det(h)$ viewing h inside $\mathrm{Mat}_2(\mathbf{C})$.*

There is also a much easier identity: $h + \overline{h} = 2a = \mathrm{Tr}(h)$, using the trace of h viewed as an element of $\mathrm{Mat}_2(\mathbf{C})$.

Proof. The expression $a^2 + b^2 + c^2 + d^2$ is unaffected by replacing h with $\overline{h}$, so if we can prove $h\overline{h}$ is equal to this expression in general then applying that to $\overline{h}$ gives the same for $\overline{h} \cdot \overline{\overline{h}} = \overline{h}h$. Hence, we focus on $h\overline{h}$. Writing h as a 2×2 matrix, we have

$$h = \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix}$$

for $\alpha = a + bi$ and $\beta = c + di$. Since $a - bi = \overline{\alpha}$ and $-c - di = -\beta$, $\overline{h}$ corresponds to the analogous matrix using $\overline{\alpha}$ in place of α and $-\beta$ in place of β. Hence,

$$h\overline{h} = \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \begin{pmatrix} \overline{\alpha} & -\beta \\ \overline{\beta} & \alpha \end{pmatrix} = \begin{pmatrix} \alpha\overline{\alpha} + \beta\overline{\beta} & 0 \\ 0 & \overline{\beta}\beta + \alpha\overline{\alpha} \end{pmatrix}.$$

This is $\mathbf{1}$ multiplied against the real scalar $|\alpha|^2 + |\beta|^2 = a^2 + b^2 + c^2 + d^2$. ■

We call $a^2 + b^2 + c^2 + d^2$ the *norm* of h, and denote it as $\mathrm{N}(h)$; in other words,

$$\mathrm{N}(h) = h\overline{h} = \overline{h}h$$

by viewing $\mathbf{R}$ as a subring of $\mathbf{H}$ via $c \mapsto c\mathbf{1}$. The equality $\mathrm{N}(h) = \det(h)$ gives that $\mathrm{N}(hh') = \mathrm{N}(h)\mathrm{N}(h')$, so $\mathrm{N}(hh') = \mathrm{N}(h'h)$ even though typically $hh' \neq h'h$.

It is clear by inspection of the formula that if $h \neq 0$ then $\mathrm{N}(h) \in \mathbf{R}^\times$, so in such cases $\overline{h}/\mathrm{N}(h)$ is a 2-sided (!) multiplicative inverse to h. Hence,

$$\mathbf{H}^\times = \mathbf{H} - \{0\};$$

we say $\mathbf{H}$ is a *division algebra* (akin to a field, but without assuming multiplication is commutative; multiplicative inverses are required to work on both sides). The $\mathbf{R}$-algebra $\mathbf{H}$ is very different from $\mathrm{Mat}_2(\mathbf{R})$ since the former is a division algebra whereas the latter has lots of zero-divisors!

Remark 3.2. The $\mathbf{R}$-linear operation $h \mapsto \overline{h}$ is an "anti-automorphism" of $\mathbf{H}$: it satisfies $\overline{hh'} = \overline{h'} \cdot \overline{h}$ for any $h, h' \in \mathbf{H}$. One way to see this quickly is to note that the cases $h = 0$ or $h' = 0$ are easy, and otherwise it suffices to check equality after multiplying on the left against $hh' \in \mathbf{H}^\times$. But

$$(hh')\overline{hh'} = \mathrm{N}(hh') = \mathrm{N}(h)\mathrm{N}(h') = h\overline{h}\mathrm{N}(h') = h\mathrm{N}(h')\overline{h} = hh'\overline{h'} \cdot \overline{h}$$

(the second to last equality using that $\mathbf{R}$ is central in $\mathbf{H}$, and the final equality using associativity).

For any associative ring A we define A^{opp} to be the same underlying additive group but with multiplication defined in the opposite order (i.e., we use the new multiplication law $a_1 * a_2 = a_2 a_1$). The anti-automorphism $h \mapsto \overline{h}$ defines an $\mathbf{R}$-algebra isomorphism $\mathbf{H}^{\mathrm{opp}} \simeq \mathbf{H}$. (Group algebras $A = k[G]$ also satisfy $A^{\mathrm{opp}} \simeq A$, via inversion on G.) In general A^{opp} is not isomorphic to A, though it turns out that 4-dimensional division algebras over a field *always* satisfy $A^{\mathrm{opp}} \simeq A$, due to the existence of an analogue of the conjugation operation on $\mathbf{H}$.

For more general finite-dimensional division algebras over fields (examples of which can be constructed in abundance in very large dimension over many interesting fields, such as over any finite extension of $\mathbf{Q}$ or over $\mathbf{C}(x, y)$), an isomorphism $A^{\mathrm{opp}} \simeq A$ rarely exists; this is best understood in terms of the structure theory of finite-dimensional central simple algebras over fields, and in particular involves Brauer groups of fields. That involves a systematic study of Galois cohomology and so lies beyond the scope of this course. Brauer groups of fields are an essential tool in many topics: the study of group representations over general fields (not assumed algebraically closed), the structure of abelian varieties over any field (even algebraically closed), the classification of linear algebraic groups and quadratic forms over general fields, class field theory, ...