Algebra and Geometry

lecture 2: algebras over a field

Misha Verbitsky

Université Libre de Bruxelles

October 13, 2016

Algebra over a field

Fix a ground field k. Recall that a map $(V_1 \times V_2) \xrightarrow{\mu} V_3$ of vector spaces is called **bilinear** of for any $v_1 \in V_1$, $v_2 \in V_2$, the maps $\mu(v_1, \cdot) : V_2 \longrightarrow V_3$, $\mu(\cdot, v_2) : V_1 \longrightarrow V_3$ (one element is fixed) is k-linear.

To express this, we use the tensor product sign, and write $mu : V_1 \otimes V_2 \longrightarrow V_3$.

DEFINITION: Let A be a vector space over k, and $\mu : A \otimes A \longrightarrow A$ a bilinear map (called **"multiplication"**). The pair (A, μ) is called **algebra over a field k** if μ is **associative**: $\mu(a_1, \mu(a_2, a_3)) = \mu(\mu(a_1, a_2), a_3))$. The product in algebra is written as $a \cdot b$ or ab. If, in addition, there is an element $1 \in A$ such that $\mu(1, a) = \mu(a, 1) = a$ for all $a \in A$, this element is called **unity**, a and A **an algebra with unity**.

DEFINITION: A **homomorphism** of algebras $r : A \longrightarrow A'$ is a linear map which is compatible with a product. **Isomorphism** of algebras is an invertible homomorphism. **Subalgebra** of an algebra A is a vector subspace which is closed under multiplication.

Matrix algebra

EXAMPLE: Let V be a vector space, and End(V) the space of endomorphisms, with $\mu(a,b) = a \cdot b$ the composition. Then End(V) is an algebra.

DEFINITION: In this situation End(V) is called **matrix algebra**, and denoted Mat(V).

EXERCISE: Prove that End(V) **is non-commutative.**

EXERCISE: Let A be an algebra with unity. Prove that A **can be realized as a subalgebra in** Mat(V) for some vector space V.

Division algebras

DEFINITION: An algebra A with unity is called **division algebra** if $A\backslash 0$ with its multiplicative structure is a group. In other words, **A is a division algebra if all non-zero elements of A are invertible.**

EXAMPLE: Let $\mathbb{H}$ be a 4-dimensional space over $\mathbb{R}$ with basis $1, I, J, K$. Consider multiplication defined on the basis by $I^2 = J^2 = K^2 = -1$ and $I \cdot J = -J \cdot I = K$. Then $\mathbb{H}$ is called **the quaternion algebra**.

DEFINITION: Define **the conjugation map** on $\mathbb{H}$ by $a+bI+cJ+dK \longrightarrow a-bI-cJ-dK$, denoted by $z \longrightarrow \overline{z}$.

CLAIM: (properties of quaternionic conjugation)
1. $\overline{x \cdot y} = \overline{y} \cdot \overline{x}$.
2. $z\overline{z} = a^2 + b^2 + c^2 + d^2$, for any $z = a + bI + cJ + dK$. **Prove this!**.

COROLLARY: Non-zero quaternions are a group with respect to multiplication.

Proof: Since multiplication of quaternions is already associative, **it remains only to check that any quaternion is invertible.** However, $z \cdot \frac{\overline{z}}{z\overline{z}} = 1$, and the quaternion $z\overline{z}$ is invertible, because it is real. ■

Group of unitary quaternions

DEFINITION: A quaternion z is called **unitary** if $|z|^2 := z\overline{z} = 1$. The group of unitary quaternions is denoted by $U(1,\mathbb{H})$. **This is a group of all quaternions satisfying $z^{-1} = \overline{z}$.**

CLAIM: Let $\operatorname{im}\mathbb{H} := \mathbb{R}^3$ be the space $aI+bJ+cK$ of all imaginary quaternions. The map $x, y \longrightarrow -\operatorname{Re}(xy)$ defines scalar product on $\operatorname{im}\mathbb{H}$.

CLAIM: This scalar product is positive definite.

Proof: Indeed, if $z = aI + bJ + cK$, $\operatorname{Re}(z^2) = -a^2 - b^2 - c^2$. ■

COROLLARY: Consider the action of $U(1,\mathbb{H})$ on $\operatorname{Im} H$ with $h \in U(1,\mathbb{H})$ mapping $z \in \operatorname{Im}\mathbb{H}$ to $hz\overline{h}$. Since $\overline{hz\overline{h}} = h\overline{z}\overline{h}$, this quaternion also imaginary. Also, $|hz\overline{h}|^2 = hz\overline{h}h\overline{z}\overline{h} = h|z|^2\overline{h} = |z|^2$. **This implies that $U(1,\mathbb{H})$ acts on the space $\operatorname{im}\mathbb{H}$ by isometries.**

DEFINITION: Denote the group of all oriented linear isometries of $\mathbb{R}^3$ by $SO(3)$. This group is called **the group of rotations of $\mathbb{R}^3$.**

REMARK: We have just defined a group homomorphism $U(1,\mathbb{H}) \longrightarrow SO(3)$ mapping h, z to $hz\overline{h}$.

Group of rotations of $\mathbb{R}^3$

Similar to complex numbers which can be used to describe rotations of $\mathbb{R}^2$, quaternions can be used to describe rotations of $\mathbb{R}^3$.

THEOREM: Let $U(1,\mathbb{H})$ be the group of unitary quaternions acting on $\mathbb{R}^3 = \operatorname{Im} H$ as above: $h(x) := hx\bar{h}$. Then **the corresponding group homomorphism defines an isomorphism $\Psi: U(1,\mathbb{H})/\{\pm 1\} \xrightarrow{\sim} SO(3)$.**

COROLLARY: The group $SO(3)$ is identified with the real projective space $\mathbb{R}P^3$.
Proof: Indeed, $U(1,\mathbb{H})$ is identified with a 3-sphere, and $\mathbb{R}P^3 := S^3/\{\pm 1\}$.■

Proof. Step 1: First, any quaternion h which lies in the kernel of the homomorpism $U(1,\mathbb{H}) \longrightarrow SO(3)$ commmutes with all imaginary quaternions, Such a quaternion must be real **(check this).** Since $|h| = 1$, we have $h = \pm 1$. **This implies that Ψ is injective.**

It remains only to prove that Ψ is surjective.

Group of rotations of $\mathbb{R}^3$ (2)

THEOREM: Let $U(1,\mathbb{H})$ be the group of unitary quaternions acting on $\mathbb{R}^3 = \operatorname{Im} H$ as above: $h(x) := hx\bar{h}$. Then **the corresponding group homomorphism defines an isomorphism $\Psi : U(1,\mathbb{H})/\{\pm 1\} \tilde{\longrightarrow} SO(3)$.**

(It remains only to prove that Ψ is surjective)

Step 2: Suppose that $\tau \in SO(3)$ is a rotation around axis l on $2\pi\alpha$ degrees. Denote by $L \in S^2 \subset \operatorname{Im} \mathbb{H}$ a unit vector in the line l. We are going to prove that **that $\Psi(\exp(\alpha L)) = \pm\tau$ (sign is determined by the choice of one of two unit vectors in l).**

Step 3: Indeed, $\Psi(\exp(\alpha L))$ preserves l, and any isometry of $\mathbb{R}^3$ which fixes a line is a rotation around this line as an axis. It remains to determine the degree of rotation. What is clear that $t \xrightarrow{\psi} \Psi(\exp(tL))$ is a homomorphism from $\mathbb{R}$ to the group U_l of rotations around the axis l. However, $L^2 = -1$, because $\bar{L} = -L$, hence the algebra generated by L is isomorphic to complex numbers, which gives $\exp(2\pi L) = 1$, and we obtain that ψ defines a map from $\mathbb{R}/2\pi\mathbb{Z}$ to U_l. **Then $\psi(t)$ is necessarily a rotation around l on angle t, which gives $\Psi(\exp(\alpha L))$.** ■

The group $SO(4)$

Consider the following scalar product on $\mathbb{H} = \mathbb{R}^4$: $g(x,y) = \operatorname{Re}(x\overline{y})$. Clearly, it is positive definite. Let $U(1,\mathbb{H})\times U(1,\mathbb{H})$ act on $\mathbb{H}$ as follows: $h_1, h_2, z \longrightarrow h_1 z \overline{h}_2$, with $z \in \mathbb{H}$ and $h_1, h_2 \in U(1,\mathbb{H})$. Clearly, $|h_1 z \overline{h}_2|^2 = h_1 z \overline{h}_2 h_2 \overline{z} \overline{h}_1 = h_1 z \overline{z} \overline{h}_1 = z\overline{z}$, hence **the group $U(1,\mathbb{H}) \times U(1,\mathbb{H})$ acts on $\mathbb{H} = \mathbb{R}^4$ by isometries.** Clearly, $\ker\Psi$ contains a pair $(-1,-1) \subset U(1,\mathbb{H}) \times U(1,\mathbb{H})$. We denote the group generated by $(-1,-1)$ as $\{\pm 1\} \subset U(1,\mathbb{H}) \times U(1,\mathbb{H})$.

THEOREM: Denote by $SO(4)$ the group of linear orthogonal automorphisms of $\mathbb{R}^4$, and let $\Psi: U(1,\mathbb{H}) \times U(1,\mathbb{H})/\{\pm 1\} \longrightarrow SO(4)$ be the group homomorphism constructed above, $h_1, h_2(x) = h_1 x \overline{h}_2$. **Then Ψ is an isomorphism**.

Proof. Step 1: Again, let $(h_1, h_2) \in \ker\Psi$. Since $\Psi(h_1,h_2)(1) = 1$, tjis gives $h_2 = \overline{h}_1 = h_1^{-1}$. However, $h_1 z h_1^{-1} = z$ means that h_1 commutes with z, which implies that h_1 commutes with all quaternions, hence it is real. Then $h_1 = \pm 1$. **This proves injectivity of Ψ.**

The group $SO(4)$ (2)

THEOREM: Denote by $SO(4)$ the group of linear orthogonal automorphisms of $\mathbb{R}^4$, and let $\Psi : U(1,\mathbb{H}) \times U(1,\mathbb{H})/\{\pm 1\} \longrightarrow SO(4)$ be the group homomorphism constructed above, $h_1, h_2(x) = h_1 x \overline{h}_2$. **Then Ψ is an isomorphism**.

It remains only to prove injectivity of Ψ.

Step 2: The classification of elements of $SO(4)$ similar to that of $SO(3)$ is possible: **Any orthogonal endomorphism of $\mathbb{R}^4$ is a rotation along two orthogonal 2-dimensional planes; prove it**. However, unlike in dim = 3 case, the explicit form of inverse map Ψ^{-1} is complicated. I give a "heuristic" (not very rigorous, because I omit the proof of the key lemma) argument using dimension count.

The group $SO(4)$ (3): dimension of $SO(4)$.

DEFINITION: An **matrix Lie group** is a subgroup $G \subset GL(V)$ of the group $GL(V)$ of all invertible linear automorphisms of $GL(V)$ which is locally homeomorphic to $\mathbb{R}^k$, and k is its **dimension**.

LEMMA: Let $G_0 \subset G$ matrix Lie groups of the same dimension. Assume that G is connected. Then $G_0 = G$.

Step 3: The dimension of the space $\mathrm{Gr}_2(R^4)$ of 2-planes in $\mathbb{R}^4$ is counted as follows. Firstly we chose a line l in this plane. It is given by a point in $\mathbb{R}P^3$, this is 3 dimensions. Secondly, we chose another line orthogonal to the first: 2 more dimensions. To cancel the ambiguity of the choice of the first line, we identify all pairs of directions in $\mathbb{R}^2$, acting by rotations of $\mathbb{R}^2$; minus 1 dimension. **This gives** $\dim \mathrm{Gr}_2(R^4) = 3 + 2 - 1 = 4$**.**

An element of $SO(4)$ is determined by a plane and a pair of rotation angles, which gives $\dim SO(4) = 4 + 2 = 6$. We obtain $\dim(U(1,\mathbb{H}) \times U(1,\mathbb{H})) = \dim SO(4) = 6$**, and by the lemma above,** $\Psi: U(1,\mathbb{H}) \times U(1,\mathbb{H}) \longrightarrow SO(4)$ **has to be surjective.** ■

More algebras: hypercomplex numbers

DEFINITION: Center of a group G is the set of all $s \in G$ such that $sg = gs$ for all $g \in G$. **Central subgroup** is a subgroup of a center.

DEFINITION: Central extension of a group G_0 is a group G_1 with central subgroup Z, such that $G_1/Z = G_0$.

DEFINITION: Let G be a finite group containing a central element denoted by -1 and with all elements of order at most 4. Denote elements of this group by $\pm 1, \pm I_1, \pm I_2, ..., \pm I_n$. Let $\mathbb{H}_G$ be the vector space over $\mathbb{R}$ with basis $1, I_1, ..., I_n$ and multiplication determined by the table of multiplication in G: $I_k I_l = \pm I_{\mu(i,j)}$. Then $\mathbb{H}_G$ is called **algebra of hypercomplex numbers**.

EXAMPLE: Let $G = \mathbb{Z}/4 = \{\pm 1, \pm I\}$. Then $\mathbb{H}_G = \mathbb{C}$.

EXAMPLE: Let $G = \{\pm 1, \pm I, \pm J, \pm K\} \subset \mathbb{H}$. (this group is called **quaternion group**). Then $\mathbb{H}_G = \mathbb{H}$ (by definition).

REMARK: Since all elements of $G/\pm 1$ have order 2, this group is abelian and its order is 2^n. **Then G has order 2^{n+1}.**

Split quaternions

EXAMPLE: Let $G = \{\pm 1, \pm R, \pm T, \pm S\}$, with relations $R^2 = T^2 = 1, S^2 = -1$, $RT = -TR = S$. Then $\mathbb{H}_G$ is called **algebra of split quaternions**.

CLAIM: Algebra of split quaternions is isomorphic to $\operatorname{Mat}(\mathbb{R}^2)$.

Proof: Let $R = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $T = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Then $\pm 1, \pm R, \pm T, \pm S$ is a basis in $\operatorname{Mat}(\mathbb{R}^2)$ which satisfies $R^2 = T^2 = 1, S^2 = -1$, $RT = -TR = S$. ■