Algebras and Arithmetic Groups

Stefan Kühnlein, Karlsruhe, December 2022

A. Generalities on Algebras

Let F be a field, A a finite dimensional algebra over F, associative with unit element.

For every $a \in A$ there is the map $L_a : A \to A, x \mapsto ax$, which is an endomorphism of the vector space A over F. As a can be reovered from L_a via $a = L_a(1)$ the map $L : A \to \mathrm{End}_{F-vsp}(A)$ is injective. It is a homomorphism between F-algebras. Choosing a basis of A over F we can identify A with a subalgebra of the matrix algebra $M_d(F)$, $d = \dim_F(A)$. The units in A are just elements in A having non-zero determinant: $A^\times = A \cap \mathrm{GL}(d, F)$. The determinant of an element in $a \in A$ is called its norm $N(a)$. It does not depend on the chosen basis.

B. Some skew fields

An algebra over F is called *central simple* if its center is F and if there are no non-trivial twosided ideals in A. A four-dimensional central simple F-algebra is called a quaternion algebra.

Lemma. If A is a quaternion algebra which is not a division algebra, then it is isomorphic to $M_2(F)$ ("it splits").

Proof. Assume $A \setminus \{0\}$ to contain a non-unit a. Then L_a is not bijective and hence $\exists b \in A \setminus \{0\} : ab = 0$. The left ideal Ab has dimension at least 1 and at most 3. If it had dimension 1 then the action of A on Ab would give an algebra homomorphism from A to $F = \mathrm{End}_F(Ab)$ which would possess a nontrivial ideal of A as its kernel, contradicting the simpleness of A. If it had dimension 3 then the same argument for A/Ab gives a contradition. Therefore, $\dim(Ab) = 2$ and – after a choice of a basis – the action of A on this vectorspace gives an isomorphism between A and $M_2(F)$. ◯

We now restrict to $\mathrm{char}\,(F) \neq 2$.

If A is a non-split quaternion algebra and $q \in A \setminus F$, then $F[q]$ is a field and A is a (left) $F[q]$-vectorspace. We necessarily have $\dim_F F[q] = \dim_{F[q]} A = 2$, and hence have an $I \in F[q] \setminus F$ such that $a := I^2 \in F^\times$. Conjugation with I on A is an automorphism κ of order 2 on A, because I is not in the center of A but I^2 is. Let $J \in A$ be an eigenvector for κ with eigenvalue -1. Then $A = F[I] \oplus F[I]J$ is the decomposition of A in eigenspaces for κ. As $\kappa(J^2) = (\kappa(J))^2 = (-1)^2 J^2 = J^2$, we have $J^2 \in F[I]$. If J^2 would generate $F[I]$, then $\kappa(J) = J$, because I were a polynomial in J. This is false, and hence $b := J^2 \in F^\times$. This almost shows:

Lemma. Every quaternion algebra admits a basis $1, I, J, K$ *such that* $IJ = -JI = K$ *and* $I^2, J^2 \in F^\times$.

For $M_2(F)$ *one can take* $a = b = 1$. ◯

In fact, for every choice of $a, b \in F^\times$, there is such a quaternion algebra with $I^2 = a, J^2 = b, IJ = -JI$, denoted by $\left(\frac{a,b}{F}\right)$.

For $q := w + xI + yJ + zK \in \left(\frac{a,b}{F}\right)$ we have

$$N_{red}(q) := (w + xI + yJ + zK)(w - xI - yJ - zK) = w^2 - ax^2 - by^2 + abz^2 \in F,$$

which is called the reduced norm of q. One checks that $N_{red}(q)^2 = N(q)$, the honest norm. Therefore, $\left(\frac{a,b}{F}\right)$ is a skew-field iff the quadratic form $w^2 - ax^2 - by^2 + abz^2$ on F^4 is anisotropic (i.e. there is no nonzero q with $N_{red}(q) = 0$).

Example: For $F = \mathbb{R}$ there are up to isomorphism the two quaternion algebras

$$\mathbb{H} := \left(\frac{-1,-1}{\mathbb{R}}\right), M_2(\mathbb{R}) \cong \left(\frac{1,-1}{\mathbb{R}}\right).$$

Example: For $F = \mathbb{Q}$ and a prime number p congruent to 3 modulo 4, $p \in \{3, 7, 11, 19, 23, 31, 43, 47, 59, \dots\}$ the algebra

$$\left(\frac{-1,p}{\mathbb{Q}}\right)$$

is a skew field.

Because: If $w^2 + x^2 - p(y^2 + z^2) = 0$, we may assume wlog $w, x, y, z \in \mathbb{Z}$ and find

$$(w + x\mathrm{i})(w - x\mathrm{i}) = p(y + z\mathrm{i})(y - z\mathrm{i}),$$

an equation in $\mathbb{Z}[\mathrm{i}]$. As p is a prime element in $\mathbb{Z}[\mathrm{i}]$ it has to divide $w + x\mathrm{i}$ or $w - x\mathrm{i}$, but then it divides the other one as well: p^2 divides the left hand side. After dividing the equation by p one may apply the argument to the factors on the right and inductively sees that every power of p divides $w + x\mathrm{i}$ and $y + z\mathrm{i}$, which hence have to be zero.

Note, however, that

$$\mathbb{R} \otimes_{\mathbb{Q}} \left(\frac{-1,p}{\mathbb{Q}}\right) = \left(\frac{-1,p}{\mathbb{R}}\right) \cong M_2(\mathbb{R}),$$

showing that our skew field is contained as a subring in $M_2(\mathbb{R})$.

Every quaternion algebra A over $\mathbb{Q}$ satisfies

$$A \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} \cong M_2(\overline{\mathbb{Q}}).$$

One hence says that A is a $\mathbb{Q}$-form of M_2 and $A^\times$ is a $\mathbb{Q}$-form of GL_2.

C. Orders

Let $F = \mathbb{Q}$ and A a be finite dimensional algebra over $\mathbb{Q}$. Then an *order* in A is a subring $\mathcal{O}$ such that its additive group is finitely generated and contains a basis of A as a $\mathbb{Q}$-vector space.

Orders always exist: Take $\mathcal{O} := A \cap M_d(\mathbb{Z})$, where A again is tacitely embedded into $M_d(\mathbb{Q})$. $(\mathcal{O}, +)$ always is a free abelian group of rank $d = \dim_{\mathbb{Q}}(A)$.

If $A = \left(\frac{k,l}{\mathbb{Q}}\right)$ with $k, l \in \mathbb{Z} \smallsetminus \{0\}$, then a possible choice of order is

$$\mathcal{O} = \{w + xI + yJ + zK \mid w, x, y, z \in \mathbb{Z}\}.$$

The normform takes integer values on your favourite order, and the units in $\mathcal{O}$ are

$$\mathcal{O}^\times = \{a \in \mathcal{O} \mid N(a) = \pm 1\}.$$

More generally, if $a \in \mathcal{O}$ has norm $N(a) \neq 0$, then the index of the left ideal $\mathcal{O}a \subseteq \mathcal{O}$ is $|N(a)|$. As there are only finitely many subgroups in $\mathcal{O}$ of given finite index, we find that for any given $B > 0$ there is a finite subset $R = R_B \subset \mathcal{O}$ of elements with $0 < |N(r)| \leq B$ such that for every element $a \in \mathcal{O}$ with $0 < |N(a)| \leq B$ there is an $r \in R$ with $\mathcal{O}a = \mathcal{O}r$, and this implies that

$$\exists \gamma \in \mathcal{O}^\times : a = \gamma r.$$

D. Reality

Let A be a d-dimensional $\mathbb{Q}$-algebra, $\mathcal{O}$ an order in A. Then $A_{\mathbb{R}} := \mathbb{R} \otimes_{\mathbb{Q}} A$ is a real algebra of dimension d and $\mathcal{O}$ is a lattice in $A_{\mathbb{R}}$.

The norm, defined on the $\mathbb{Q}$-algebra A extends to the norm on $A_{\mathbb{R}} \subseteq M_d(\mathbb{R})$, and therefore $\mathcal{O}^\times$ is a discrete subgroup of $G = \{x \in A_{\mathbb{R}} \mid N(x) = \pm 1\}$. The group G is a smooth hypersurface in $A_{\mathbb{R}}$, defined by a polynomial equation. It sometimes is convenient to restrict to the finite index subgroup of units with norm 1 or – in the quaternion case – to the units with reduced norm 1. We may see this group as the group of real-valued points of an algebraic subgroup of GL_d defined over $\mathbb{Q}$.

Choose a euclidean structure on $A_{\mathbb{R}}$ and take some compact, convex, centrally symmetric subset of $A_{\mathbb{R}}$ with volume $\mathrm{vol}(S) \geq 2^d \mathrm{cov}(\mathcal{O})$. For every $g \in G$, gS also is compact, convex, centrally symmetric with the same volume as S, because the multiplication with g on $A_{\mathbb{R}}$ has determinant ± 1.

Therefore Minkowski's lattice point theorem asserts that for every $g \in G$ there exists a nonzero $a_g \in \mathcal{O} \cap Sg$. As S is compact, the absolute value of the norm is

bounded on S by some constant B. As $|N|$ does not change under multiplication by $g \in G$ we find the same bound on Sg :

$$\forall g \in G : |N(a_g)| \leq B.$$

Taking the set R from C. we find:

$$\forall g \in G : [N(a_g) \neq 0 \Rightarrow \exists r_g \in R, \gamma_g \in \mathcal{O}^\times : a_g = r_g \cdot \gamma_g].$$

If now A is a division algebra, then $N(a_g)$ always is nonzero, as $a_g \neq 0$. Therefore,

$$\forall g \in G : g^{-1} \in \gamma_g^{-1} r_g^{-1} (S \cap G) \subseteq \mathcal{O}^\times \left(\bigcup_{r \in R} (r^{-1} S \cap G) \right).$$

As R is finite, $C := \bigcup_{r \in R} (r^{-1} S \cap G)$ is compact.

We hence have shown:

Theorem: If A is a finite dimensional division algebra over $\mathbb{Q}$, then for every order $\mathcal{O}$ in A the unit group acts cocompactly on the group of units in $A_\mathbb{R}$ with norm ± 1.

E. Special cases

If A is a quaternion algebra over $\mathbb{Q}$ which is a skew field with indefinite reduced norm form, then for every order $\mathcal{O}$ in A the group $\Gamma = \{a \in \mathcal{O} \mid N_{red}(a) = 1\}$ is discrete and cocompact in $G = \{a \in A_\mathbb{R} \mid N_{red}(a) = 1\} \cong \mathrm{SL}(2, \mathbb{R})$.

If A is a number field, $A = \mathbb{Q}(\alpha) \cong \mathbb{Q}[X]/(f)$ for some irreducible polynomial in $\mathbb{Q}[X]$, then

$$A_\mathbb{R} \cong \mathbb{R}[X]/(f) \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2},$$

corresponding to the real and non real roots of f in $\mathbb{C}$, using the Chinese remainder theorem. The norm then ist

$$N(x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2}) = x_1 \cdot \ldots \cdot x_{r_1} \cdot |z_1|^2 \cdot \ldots \cdot |z_{r_2}|^2.$$

The group G_1 of norm one units in $A_\mathbb{R}$ contains the compact subgroup

$$T := \{(x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2}) \mid \forall i, j : |x_i| = |z_j| = 1\} = \{\pm 1\}^{r_1} \times (S^1)^{r_2}.$$

This is the kernel of the map

$$\begin{aligned} \mathcal{L} : G_1 \to \mathbb{R}^{r_1 + r_2}, \quad & \mathcal{L}(x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2}) \\ & = (\log |x_1|, \ldots, \log |x_n|, \log |z_1|^2, \ldots, \log |z_{r_2}|^2). \end{aligned}$$

Due to the norm condition, the image of $\mathcal{L}$ is $\{(u_1, \ldots, u_{r_1+r_2}) \mid \sum u_i = 0\}$. If $\mathcal{O}$ is an order in A, then $\mathcal{O}_1 := \mathcal{O} \cap G_1$ is a finite index subgroup in $\mathcal{O}^\times$, acting cocompactly on G_1. Hence $\mathcal{L}(\mathcal{O}_1)$ is a lattice in a real vector space of dimension $r_1 + r_2 - 1$, as $\mathcal{O}_1 \cap T$ is finite. This proves Dirichlet's unit theorem:

Theorem. If A is an algebraic number field with r_1 real embeddings and r_2 pairs of complex embeddings (pairs come from complex conjugation) and $\mathcal{O}$ is any order in A, then $\mathcal{O}^\times$ is a finitely generated abelian group of rank $r_1 + r_2 - 1$.