1. Quaternion algebras

1.1. Definition and general properties. Let F be a field of characteristic $\neq 2$. Let $a, b \in F^\times$. As it is easily checked, there is a unique unital associative F-algebra of dimension 4 with F-basis $1, i, j, k$ such that $i^2 = a$, $j^2 = b$ and $ij = -ji = k$ (so $k^2 = -ab$). We denote this F-algebra by

$$\left(\frac{a,b}{F}\right).$$

Its presentation as an F-algebra is thus given by $F\{i,j\}/(i^2 - a, j^2 - b, ij = -ji)$.

A *quaternion algebra* over F is an F-algebra isomorphic to such an algebra for some $a, b \in F^\times$. If $\mu \in F^\times$, there are F-algebra isomorphisms

$$\left(\frac{a,b}{F}\right) \simeq \left(\frac{b,a}{F}\right), \quad \left(\frac{a\mu^2,b}{F}\right) \simeq \left(\frac{a,b}{F}\right), \quad \left(\frac{1,b}{F}\right) \simeq M_2(F),$$

induced respectively by $(i,j) \mapsto (j,i)$, $(i,j) \mapsto (i\mu^{-1}, j)$ and $i \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $j \mapsto \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}$. It follows that $M_2(F)$ is a quaternion algebra, called the *trivial* or *split* quaternion algebra. If F is algebraically closed, or even if any element of F is a square, the formulae above show that $M_2(F)$ is the unique quaternion algebra over F. If F'/F is a field extension, we have

$$\left(\frac{a,b}{F}\right) \otimes_F F' \simeq \left(\frac{a,b}{F'}\right)$$

so $D \otimes_F \overline{F} \simeq M_2(\overline{F})$ for any quaternion F-algebra D.

Proposition 1.2. *If D is an F-algebra of rank 4, then the following properties are equivalent : (a) D is a quaternion F-algebra, (b) D has center F and is simple (i.e. it has no non-trivial two-sided ideal), (c) $D \otimes_F \overline{F} \simeq M_2(\overline{F})$.*

If these properties hold, either $D \simeq M_2(F)$ or D is a division algebra.[1]

Proof — We have seen (a) $\Rightarrow$ (c), and (c) $\Rightarrow$ (b) follows at once from the fact that $M_2(\overline{F})$ is simple with center $\overline{F}$.

Assume now that (b) holds and let us check first the last assertion (and then (a)).

Assume that for some $x \neq 0 \in D$, $Dx \subsetneq D$. Then the set of proper left-ideals of D is nonempty, hence has an element I of minimal F-dimension. The action by left-translations of D on I induces an F-linear injection $D \to \mathrm{End}_F(I)$ as D is simple, so I has F-dimension 2 or 3. In the first case $D \simeq M_2(F)$. In the second, each proper left-ideal of D has dimension 3, hence there is a unique such ideal (consider intersection of such ideals), which is I. It follows that I is a right-ideal as well, which is absurd. As a consequence, either $D \simeq M_2(F)$ or D is a division algebra.

To check (a) we may thus assume that D is a division algebra. In this case, for any $x \in D \backslash F$ then $F[x]$ is a field of degree 2 over F as D is not commutative, and it coincides with its centralizer in D for the same reason. Fix such an x. As the characteristic of F is not 2, there is some $i \in F[x] \backslash F$ such that $i^2 = a$ and $a \in F^\times$ is not a square in F. The conjugation by i on D has order 2, and its 1-eigenspace is $F(i)$ (by the remark above),

[1]This means that for any $x \in D \backslash \{0\}$, there is a $y \in D$ such that $xy = yx = 1$.

and its -1-eigenspace is thus non-zero : there exists $j \in D$ such that $ij = -ji$ (again use $2 \in F^\times$). But then j^2 commutes with i, hence belongs to $F(i)$, so $j^2 = ci + b$, for $c, b \in F$. If $c \neq 0$ then $F(j) \supsetneq F(i)$ and $F(j) = D$: absurd, so $c = 0$ and $b \in F^\times$. It follows that there is a natural F-algebra morphism $\left(\frac{a,b}{F}\right) \to D$, necessarily injective as the source is simple, hence bijective. □

1.3. Quaternion algebras and quadratic forms. The F-linear automorphism $x = (1, i, j, k) \mapsto x^* = (1, -i, -j, -k)$ defines an anti-involution of $D = \left(\frac{a,b}{F}\right)$: $(xy)^* = y^*x^*$ and $(x^*)^* = x$. We define the *trace* and the *norm* of a quaternion x as the elements $T(x) = x + x^* \in F$ and $N(x) = xx^* \in F$.[2] The trace is an F-linear map $D \to F$, the F-bilinear map $(x, y) \mapsto T(xy)$ is easily checked to be symmetric and non-degenerated. The norm defines a 4-variables quadratic form over F

$$N(\alpha + \beta i + \gamma j + \delta k) = \alpha^2 - a\,\beta^2 - b\,\gamma^2 + ab\,\delta^2,$$

which is non-degenerated and has discriminant $1 \in F^\times/(F^\times)^2$. We have $N(x+y) = N(x) + N(y) + T(xy^*)$ for all $x, y \in D$.

Via the isomorphisms $D \otimes_F \overline{F} \simeq M_2(\overline{F})$, one easily checks that $T \otimes_F \overline{F}$ is the usual trace and $N \otimes_F \overline{F}$ is the determinant. As each $\overline{F}$-automorphism of $M_2(\overline{F})$ is the conjugation by some element in $\mathrm{GL}_2(\overline{F})$, it follows that T and N only depends on the F-algebra structure on D (and not on the choice of a, b defining D), as well as $x \mapsto x^* = T(x) - x$. Moreover[3], $N(xy) = N(x)N(y)$ for all $x, y \in D$. By definition, the fixed points of $*$ coincide with $F \subset D$ and the subspace $D^0 \subset D$ where $x^* = -x$ (or $T(x) = 0$) is the orthogonal complement of F in D for the norm. It is called the space of pure quaternions. We have $D = F \oplus D^0$ and $D^0 = Fi + Fj + Fk$.

Proposition 1.4. *The map $D \mapsto N_{|D^0}$ defines a bijection between the set of isomorphism classes of quaternion F-algebras and the equivalence classes of non-degenerate quadratic forms on F^3 with discriminant 1. In this bijection, $M_2(F)$ corresponds to the unique isotropic such form $x^2 - y^2 - z^2$.*

Proof — By the remarks above, if D is a quaternion algebra then the 3-dim quadratic space $Q(D) := (D^0, N_{|D^0})$ is well defined, non-degenerated, with discriminant 1. As any such quadratic space has the form $-ax^2 - by^2 + abz^2$ for some $a, b \in F^\times$, the map of the statement is surjective. Note that for $x \in D^0$ we have $N(x) = xx^* = -x^2$, and if furthermore $y \in D^0$, then x is orthogonal to y iff $0 = xy^* + x^*y = -(xy + yx)$, i.e. iff $xy = -yx$. It follows that if $Q(D) \simeq Q(\left(\frac{a,b}{F}\right))$, then D^0 contains elements x, y such that $x^2 = a$, $y^2 = b$ and $xy = -yx$, thus $D \simeq \left(\frac{a,b}{F}\right)$ by the presentation of this latter algebra. To check the last assertion, remark that by the multiplicativity of the norm and the relation $xx^* = N(x) \in F$, D is a division algebra if and only if N is anisotropic. As the quadratic form N has 4 variables and discriminant 1, it turns out that its index is either 0 or 2 (but not 1), thus N is anisotropic iff $N_{|D^0}$ is anisotropic. □

[2] Note that the Cayley-Hamilton identity $x^2 - T(x)x + N(x) = 0 = (x - x)(x - x^*)$ holds in D.

[3] The reader can check as an exercise that N is the unique nonzero multiplicative quadratic form on a quaternion algebra F.

1.5. The case of local and global fields. If $F^\times/(F^\times)^2$ is finite, there are finitely many quaternion algebras over F by the simple isomorphisms above. This applies to local fields, in which case we even have:

PROPOSITION 1.6. *If F is a local field and $F \neq \mathbb{C}$, then there is exactly one non-split quaternion algebra over F up to isomorphism. If F is a finite extension of $\mathbb{Q}_p$ this algebra is $\left(\frac{a,\pi}{F}\right)$ where π is a uniformizer of F and $a \in \mathcal{O}_F^\times$ is an element such that $F(\sqrt{a})$ is the quadratic unramified extension of F.*

Proof — Indeed, over $\mathbb{R}$, it is clear that Hamilton's quaternions $\left(\frac{-1,-1}{\mathbb{R}}\right)$ is the unique non-trivial quaternion algebra. If F is a finite extension of $\mathbb{Q}_p$, it is a good exercise that we leave to the reader to check that there is a unique anisotropic quadratic form over F^3 with discriminant 1, which is isomorphic to

$$q(x,y,z) = -ax^2 - \pi y^2 + a\pi z^2$$

where $\pi \in F$ and $a \in \mathcal{O}_F^\times$ are as in the statement (use e.g. similar arguments as in the proof of the examples below). Let us simply check here that for $p > 2$ this form is indeed anisotropic. In this case the second assertion means that a is not a square mod π. If (x,y,z) is a non-trivial zero in F^3, then we may assume that $x,y,z \in \mathcal{O}_F$ and that one of them is in $\mathcal{O}_F^\times$. From $q(x,y,z) = 0$ we get that $\pi | x$, and dividing everything by π and reducing mod π it follows that $y^2 \equiv az^2 \bmod \pi$. As a is not a square mod π it follows that π divides y and z : absurd. When $p = 2$ one does the same by arguing mod 4π, after the change of variables $y = 2y'$ and $z = 2z'$. □

The following classical theorem is the main theorem on the classification of quaternion algebras over number fields, it follows from the Hasse-Minkowski theorem on quadratic form and of the study of the Hilbert symbol (see e.g. Serre's *cours d'arithmétique* for a complete study in the case $F = \mathbb{Q}$, in that case the study of the Hilbert symbol reduces to the quadratic reciprocity law : see the examples below for some flavor).

THEOREM 1.7. *Let F be a number field. If D is a quaternion algebra over F, the set* $\mathrm{Ram}(D) \subset S(F)$ *of places v such that D is ramified at v, i.e. such that $D_v := D \otimes_F F_v$ is not split, is a finite set with an even number of elements.*

For any finite set $S \subset S(F)$ such that $|S|$ is even, there is a unique quaternion algebra over F such that $\mathrm{Ram}(D) = S$.

DEFINITION 1.8. *A quaternion algebra over $\mathbb{Q}$ is called definite if D_∞ is not split, indefinite otherwise. Of course $\left(\frac{a,b}{\mathbb{Q}}\right)$ is definite iff a and b are < 0.*

EXAMPLE 1.9. *For each prime p, there is a unique (definite) quaternion algebra D over $\mathbb{Q}$ ramified exactly at p and ∞. Concretely, we may take:*

(i) $D = \left(\frac{-1,-1}{\mathbb{Q}}\right)$ *if* $p = 2$,

(ii) $D = \left(\frac{-1,-p}{\mathbb{Q}}\right)$ *if* $p \equiv 3 \bmod 4$,

(iii) $D = \left(\frac{-2,-p}{\mathbb{Q}}\right)$ *if* $p \equiv 5 \bmod 8$,

(iv) $D = \left(\frac{-\ell,-p}{\mathbb{Q}}\right)$ *if* $p \equiv 1 \bmod 8$ *whenever ℓ is a prime* $\equiv 3 \bmod 4$ *which is a square mod p (there always exist such primes!).*

Let us check that those D have the required properties using only Prop. 1.4. First, they are obviously definite.

— Let q be an odd prime. If $a_i \in \mathbb{Z}_q^\times$, observe that the form $\sum_{i=1}^n a_i X_i^2$ represents 0 in $\mathbb{Q}_q^n$ if $n \geq 3$. Indeed, by successive approximation mod q^m, $m \geq 1$, one easily reduces to show that its reduction mod q represents 0, but it is well known that any non-degenerate quadratic form in ≥ 3 variables over a finite field of odd characteristic represents 0. It follows from this that for any D as in the statement above, and for each prime $q \neq 2, p$, with furthermore $q \neq \ell$ case (iv), then D is split at q.

— Remark that for $a \in \mathbb{Z}_p^\times$ and p odd, the form $aX^2 + pY^2 + apZ^2$ represents 0 if and only if $-a$ is a square mod p. It follows that the D in (ii) to (iv) is ramified at p, as respectively -1, -2 and $-\ell$ are not squares mod p in those cases. It also shows that in case (iv) the algebra D is split at ℓ as $-p$ is a square mod ℓ.

— This shows in all cases that $\{\infty\} \subset \mathrm{Ram}(D) \subset \{\infty, p\}$. If we allow ourselves to use that $|\mathrm{Ram}(D)|$ is even, this concludes the proof.

— The behaviors at the prime 2 can of course be checked directly, for instance as follows. To conclude in case (i), note that indeed $X^2+Y^2+Z^2$ does not represent 0 over $\mathbb{Q}_2$: we may assume that $(x,y,z) \in \mathbb{Z}_2^3 \backslash (2\mathbb{Z}_2)^3$ and argue mod 4. In the other cases, use the following observation that one checks by successive approximation : if $q = \sum_{i=1}^n a_i X_i^2$ with $a_i \in \mathbb{Z}_2 \backslash \{0\}$ for all i, and if $q(x_i) \equiv 0 \bmod 8$ for some $(x_i) \in \mathbb{Z}_2^n$ with the property that $x_j \in \mathbb{Z}_2^\times$ for some j such that $a_j \in \mathbb{Z}_2^\times$, then q represents 0 in $\mathbb{Z}_2^n$. We leave as an exercise to the reader to show that $2 \notin \mathrm{Ram}(D)$ in cases (ii) to (iv) using this criterion (multiply first the form by 2 in case (iii)).

Exercises: (i) Let F be a number field and $D = \left(\frac{a,b}{F}\right)$. Show that for each finite prime v of odd residual characteristic and such that $a_v, b_v \in O_{F_v}^\times$, D_v is split. In particular, D_v is split for all but finitely many $v \in S(F)$ (that is the easy part of the theorem above).

(ii) Let q be a quadratic form on $\mathbb{Q}_p^3$ with discriminant 1. Show that q represents 0 in any quadratic extension of $\mathbb{Q}_p$. For any real quadratic field $F/\mathbb{Q}$, give an explicit quaternion algebra D over F such that $\mathrm{Ram}(D) = S(F)_\mathbb{R}$.

(iii) (Image of the norm) Let D be a quaternion algebra over F and consider the group homomorphism $N : D^\times \to F^\times$. Show that N is surjective if F is a finite extension of $\mathbb{Q}_p$. If F is a number field, show that the image of N is the subgroup of elements $x \in F^\times$ such that $x_v > 0$ for each $v \in S(F)_\mathbb{R}$ such that D_v is not split (use Hasse-Minkowski's theorem).

2. Arithmetic of quaternion algebras over $\mathbb{Q}$

As in the case of number fields, we shall use a local-global method to study the arithmetic of quaternion algebras over $\mathbb{Q}$.

2.1. Orders and fractional ideals of quaternion algebras over $\mathbb{Q}_p$. Let D be a quaternion algebra over $\mathbb{Q}_p$. An *order* of D is a $\mathbb{Z}_p$-subalgebra $\mathcal{O} \subset D$ which is a $\mathbb{Z}_p$-lattice of the underlying $\mathbb{Q}_p$-vector space of D. A *fractional (right-)ideal* of $\mathcal{O}$ is a $\mathbb{Z}_p$-lattice $I \subset D$ such that $I\mathcal{O} \subset I$.

An order $\mathcal{O}$ necessarily has rank 4 over $\mathbb{Z}_p$ and is made of elements x which are integral over $\mathbb{Z}_p$. In particular, the bilinear form T of D is $\mathbb{Z}_p$-valued on $\mathcal{O}$ and $\mathcal{O}$ has a discriminant $\delta(\mathcal{O})$: it is the ideal of $\mathbb{Z}_p$ generated by the determinant of the matrix $T(x_i x_j)$ for any $\mathbb{Z}_p$-basis x_i of $\mathcal{O}$. It is non-zero as T is non-degenerated on D. It follows that *any $\mathcal{O}$ is contained in a* maximal order *(for the inclusion).*

PROPOSITION 2.2. - *When $D = M_2(\mathbb{Q}_p)$, the maximal orders are the $\mathrm{GL}_2(\mathbb{Q}_p)$-conjugate of $M_2(\mathbb{Z}_p)$, they have discriminant* 1.

- *If D is the non-split quaternion algebra, there is a unique maximal order, it has discriminant p^2.*
- *In both cases, each fractional ideal I of a maximal order $\mathcal{O}$ of D has the form $x\mathcal{O}$ for some $x \in D^\times$ which is unique up to multiplication by $\mathcal{O}^\times$ on the right.*

Proof — Assume first $D = M_2(\mathbb{Q}_p)$. The order $M_2(\mathbb{Z}_p)$ is a maximal order as it has discriminant (1). As any order $\mathcal{O} \subset D$ preserves a lattice in $\mathbb{Q}_p^2$, it follows that the maximal orders are exactly of the stabilizers of lattices in $\mathbb{Q}_p^2$, i.e. the $xM_2(\mathbb{Z}_p)x^{-1}$ for some $x \in \mathrm{GL}_2(\mathbb{Q}_p)$ (note that maximal orders are not unique !). The map $I \mapsto I(\mathbb{Z}_p^2)$ induces a bijection between the set of fractional ideals of $M_2(\mathbb{Z}_p)$ and the set of $\mathbb{Z}_p$-lattices in $\mathbb{Q}_p^2$: this may be seen directly (exercise) or as a special case of Morita equivalence. In particular, any fractional ideal of $M_2(\mathbb{Z}_p)$ is principal, i.e. of the form $xM_2(\mathbb{Z}_p)$ for some $x \in \mathrm{GL}_2(\mathbb{Q}_p)$. If $xM_2(\mathbb{Z}_p) = M_2(\mathbb{Z}_p)$ then clearly $x \in \mathrm{GL}_2(\mathbb{Z}_p)^\times$.

Assume now that D is a field. As for finite extensions of $\mathbb{Q}_p$, the norm of $\mathbb{Q}_p$ extends uniquely to a multiplicative non-archimedean discretely valued norm $|.|$ on D. It follows that $\mathcal{O}_D = \{x \in D, |x| \leq 1\}$ is an order of D, containing all the elements of D which are integral over $\mathbb{Z}_p$, hence all the orders of D : it is the unique maximal order (note the difference with the split case). It follows that any fractional ideal of $\mathcal{O}_D$ is principal (and two-sided). The subset $\{x \in \mathcal{O}_D, |x| < 1\}$ is the maximal ideal of $\mathcal{O}_D$, fix π a generator. We have $up = \pi^e$ for some unique $e \geq 1$ and $u \in \mathcal{O}_D^\times$ (i.e. $|u| = 1$). If p^f is the cardinal of the finite field $k_D := \mathcal{O}_D/(\pi)$ (necessariliy commutative) it follows that $ef = [D : \mathbb{Q}_p] = 4$. As any element of $\mathcal{O}_D$ has degree 2 over $\mathbb{Z}_p$, we see that $f \leq 2$ and that $e \leq 2$ so $e = f = 2$.

If we write

$$D = \left(\frac{a, p}{\mathbb{Q}_p}\right)$$

where $a \in \mathbb{Z}_p^\times$ is such that $K = \mathbb{Q}_p(\sqrt{a})$ is the unramified quadratic extension of $\mathbb{Q}_p$, then $\mathcal{O}_K + j\mathcal{O}_K$ is an order of D, thus

$$\mathcal{O}_K + j\mathcal{O}_K \subset \mathcal{O}_D. \tag{2.1}$$

But $\mathcal{O}_D$ has discriminant $\neq 1$ as $j \notin p\mathcal{O}_D$ (apply N) and $T(j\mathcal{O}_D) \subset p\mathbb{Z}_p$. A direct computation shows that the left-hand side has discriminant (p^2), thus the only possibility is that the inclusion (2.1) is an equality. □

Exercises: (i) Assume $D = M_2(\mathbb{Q}_p)$ and $\mathcal{O} = \mathrm{M}_2(\mathbb{Z}_p)$. Show that under the bijection above, the right ideals of $\mathcal{O}$ containing p correspond to the lines in $\mathbb{F}_p^2$. In particular, there are $p + 1$ such ideals and each of them has index p^2 in $\mathcal{O}$.

(ii) Let D be a quaternion algebra over $\mathbb{Q}_p$ and $\mathcal{O}$ a maximal order. Show that for any fractional ideal $I \subset \mathcal{O}$, $[\mathcal{O} : I]$ is a square.

(iii) Let D be the non trivial quaternion algebra over $\mathbb{Q}_p$ and π a uniformizer of D. Show that $\{1 + \pi^n \mathcal{O}_D, n \geq 1\}$ is a basis of neighborhoods of 1 in $D^\times$ consisting of normal open subgroups of $D^\times$. Show that $D^\times/\mathbb{Q}_p^\times$ is a compact group. Deduce that the smooth irreducible complex representations of $D^\times$ are finite dimensional. (Compare with the case $D = M_2(\mathbb{Q}_p)$).

2.3. The ideal class set of a quaternion algebra over $\mathbb{Q}$. Let D be a quaternion algebra over $\mathbb{Q}$. An order of D is a subring $\mathcal{O} \subset D$ which is a $\mathbb{Z}$-lattice in D, and a fractional ideal of $\mathcal{O}$ is a $\mathbb{Z}$-lattice $I \subset D$ such that $I\mathcal{O} \subset I$. For the same reasons as in the local case (non degeneracy of T on D), orders have a non-zero discriminant in $\mathbb{Z}$ (this is even a well-defined number here) and each order is included in a maximal order. We fix such a maximal order $\mathcal{O}$. We assume from now on that D is a division algebra.

Orders and fractional ideals can be studied by the local-global method. If $\Lambda \subset D$ is a $\mathbb{Z}$-lattice, and if p is a prime, write Λ_p for the lattice $\mathbb{Z}_p\Lambda \subset D_p = D \otimes_{\mathbb{Q}} \mathbb{Q}_p$.

Lemma 2.4. *(localization lemma) The map $\Lambda \mapsto (\Lambda_p)$ is a bijection between $\mathbb{Z}$-lattices in D and the set of collections of local lattices (L_p) for all primes p such that $L_p = \mathcal{O}_p$ for all but finitely many p. Furthermore, Λ is an order (resp. a maximal order, resp. a fractional ideal of $\mathcal{O}$) iff Λ_p has this property for each p (resp. Λ_p is a fractional ideal of $\mathcal{O}_p$ for each p).*

Proof — The first statement would hold for any finite dimensional vector space over $\mathbb{Q}$ replacing D with a given $\mathbb{Z}$-lattice $\mathcal{O}$. It follows from the fact that the functor $\Lambda \mapsto \Lambda \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}} = (\Lambda_p)$ is exact on finitely generated abelian groups and preserves the indices of sublattices : $\widehat{\mathbb{Z}}$ is flat over $\mathbb{Z}$ and $X = X \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$ for any finite abelian group X. For the second statement, note that a lattice $\mathcal{O} \subset D$ is an order iff the lattice $\mathcal{O}.\mathcal{O}$ is included in $\mathcal{O}$. By the first statement this holds iff it holds at each prime p, but clearly $(\mathcal{O}.\mathcal{O})_p = \mathcal{O}_p.\mathcal{O}_p$ for each prime p. Thus $\mathcal{O}$ is an order iff each $\mathcal{O}_p$ is, and $\mathcal{O}$ is maximal iff each $\mathcal{O}_p$ is. The statement about ideals is similar. □

It follows from this and the previous local computation (plus a simple archimedean one) that

Corollary 2.5. *The maximal orders of D are the orders with discriminant d^2 where d is the (squarefree) product of the finite primes at which D is ramified. We often call this number d the discriminant of D.*

It follows from the classification theorem that for each squarefree positive d there is a unique quaternion algebra with discriminant d. It is definite iff d has an odd number of prime divisors.

We denote by $\mathrm{Cl}(\mathcal{O})$ the set of equivalence classes[4] of fractional ideals of $\mathcal{O}$ for the relation $I \sim J \Leftrightarrow I = xJ$ for some $x \in D^\times$. We denote by $D_f^\times$ the subgroup of

[4]As any order $\mathcal{O}$ is necessarily stable by $x \mapsto x^*$, we obtain a natural bijection between left and right fractional ideals of $\mathcal{O}$, and between the "left" and "right" ideal class sets.

$\prod_p D_p^\times$ whose elements (x_p) are such that $x_p \in \mathcal{O}_p^\times$ for all but finitely many primes p. The definition of $D_f^\times$ is independent of $\mathcal{O}$ and the diagonal inclusion $D^\times \to \prod_p D_p^\times$ falls inside $D_f^\times$.

THEOREM 2.6. *The class set* $\mathrm{Cl}(\mathcal{O})$ *is finite and there is a canonical bijection*

$$\mathrm{Cl}(\mathcal{O}) \xrightarrow{\sim} D^\times \backslash D_f^\times / \prod_p \mathcal{O}_p^\times.$$

Its cardinal h *does not depend on the choice of* $\mathcal{O}$*. Moreover, there are at most* h $D^\times$*-conjugacy classes of maximal orders in* D*.*

Proof — By Prop. 2.2, the fractional ideals of $\mathcal{O}_p$ are the $x_p\mathcal{O}_p$ where $x_p \in D_p^\times$, the element x_p being unique up to multiplication by $\mathcal{O}_p^\times$ on the right. By this and the localization lemma, the map $I \mapsto (x_p) \in D_f^\times$ where $I_p = x_p\mathcal{O}_p$ for each p, induces a bijection between $\mathrm{Cl}(\mathcal{O})$ and the double cosets of the statement. If $\mathcal{O}'$ is another maximal order of D, then we may find $(z_p) \in D_f^\times$ such that $\mathcal{O}'_p = z_p^{-1}\mathcal{O}_p z_p$ for all p, by Prop. 2.2, thus the multiplication by (z_p) on the right on the double coset space induces a bijection

$$\mathrm{Cl}(\mathcal{O}) \simeq \mathrm{Cl}(\mathcal{O}').$$

The last assertion follows as any two maximal orders are locally conjugate at each prime p.

Let us check the finiteness statement now. Let I be a fractional ideal of $\mathcal{O}$. Up to equivalence we may assume that $I \subset \mathcal{O}$. Choose $x \in I$ such that the integer $|N(x)|$ is non-zero and minimal. Equip D_∞ with the sup norm $|.|$ with respect to a $\mathbb{Z}$-basis of its lattice $\mathcal{O}$, view N as a function $D_\infty \to \mathbb{R}$, and pick $\delta > 0$ such that $|N(z)| < 1$ for $|z| < \delta$ in D_∞. By the *almost euclidean algorithm* applied to δ, D_∞ and the lattice $\mathcal{O}$, there is an integer $M > 0$ such that for each $v \in D_\infty$ there is a $z \in \mathcal{O}$ and $1 \leq k \leq M$ such that $|N(kv - z)| < 1$. Apply this to $v = x^{-1}y$ where $y \in I$. We get $|N(kx^{-1}y - z)| < 1$, thus $|N(ky - xz)| < |N(x)|$ and $ky \in x\mathcal{O}$ by minimality of x. It follows that

$$M!\, x\, \mathcal{O} \subset M!\, I \subset x\, \mathcal{O}$$

thus I is equivalent to the fractional ideal $x^{-1}M!I$ which sits inside $M!\mathcal{O}$ and $\mathcal{O}$: there are only finitely many such ideals. □

LEMMA 2.7. *(Almost euclidean algorithm) Fix* $n \geq 1$ *an integer, as well as* $\delta > 0$*. There exists an integer* M *such that for all* $v \in \mathbb{R}^n$ *there is a integer* $1 \leq k \leq M$ *and a* $z \in \mathbb{Z}^n$ *such that* $|kv - z|_{\mathrm{sup}} < \delta$*.*

Proof — This follows form the pigeon-hole principle : choose $r \in \mathbb{N}$ and write $v = (v_i)$, the fractional parts vectors $(\langle kv_i \rangle)_{i=1}^n$ for $k = 0, \dots, r^n$ all belong to $[0,1[^n$, thus at least two of them are in the same box of size $1/r$. To conclude pick $r \geq 1/\delta$ and $M \geq r^n$. □

In the following statement, we endow $D_f^\times$ with its natural product topology. It is a locally compact topological space. We set for short $\widehat{\mathcal{O}}^\times := \prod_p \mathcal{O}_p^\times$, it is a compact open subgroup and a neighborhood of 1 in $D_f^\times$.

PROPOSITION 2.8. *If D is definite then :*

(a) *$D^\times$ is a discrete subgroup of $D_f^\times$,*

(b) *For any $x \in D_f^\times$ then $xD^\times x^{-1} \cap \widehat{\mathcal{O}}^\times$ is a finite group. In particular, $\mathcal{O}^\times$ is a finite group,*

Proof — To check that $D^\times$ is discrete it is enough to show that $D^\times \cap \widehat{\mathcal{O}}^\times$ is finite as $\widehat{\mathcal{O}}^\times$ is an open neighborhood of 1 in $D_f^\times$. But $D^\times \cap \widehat{\mathcal{O}}^\times = \mathcal{O}^\times$ is the set of element of norm 1 in $\mathcal{O}$ (-1 is not a possible norm as N is positive). As N is definite there are only finitely many such elements. Part (b) follows from (a) as the given intersection is at the same time discrete and compact. □

REFERENCES: The arithmetic of quaternion algebras have been mostly discovered by Deuring, and then studied by Eichler. See the book of Vigneras on quaternion algebras for a modern treatment as well as many results.

2.9. Some examples. Using the strong approximation theorem, one can actually show that $h = 1$ if D is indefinite. The situation is very different for definite D, what we assume now. Perhaps surprisingly compared to the case of number fields, there is however a simple close formula for $h = h(d)$ in terms of the discriminant d of D. For instance if d is prime then h is the genus of $X_0(d)$ plus 1. In particular, in this prime case we have $h(d) = 1$ iff $d = 2, 3, 5, 7, 13$, and $h(d) = 2$ iff $d = 11, 17, 19$.

EXAMPLE A: (Hurwitz quaternions and Lagrange theorem) Let $D = \left(\frac{-1,-1}{\mathbb{Q}}\right)$ be the quaternion algebra of discriminant 2. It is well-known that in this case

$$\mathcal{O} := \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k + \mathbb{Z}(1 + i + j + k)/2$$

is a maximal order, and the approach below shows that it has class number 1 ("Hurwitz quaternions"). It follows that this is the unique maximal order of D up to conjugacy. The finite group $\mathcal{O}^\times$ has order[5] 24, it contains as a normal subgroup the usual quaternion group of order 8, as well as the elements $\frac{\pm 1 \pm i \pm j \pm k}{2}$. A standard application of $\mathrm{Cl}(\mathcal{O}) = 1$ is that any odd prime p is the sum of 4 squares of integers in exactly $8(p + 1)$ ways (Lagrange, Jacobi). Indeed, considering congruences modulo the two-sided ideal $(1 + i)\mathcal{O}$, whose quotient is $\mathbb{F}_4 = \mathbb{F}_2[\overline{\tau}]$ where $\tau = \frac{1+i+j+k}{2}$ ($\tau^3 = -1$), one easily sees[6] that it is equivalent to show that for any odd prime p, the equation $p = N(x)$ has $24(p + 1)$ solutions $x \in \mathcal{O}$. But for $x \in \mathcal{O}$, $p = N(x)$ if and only if $x\mathcal{O}$ is an ideal of index p^2 in $\mathcal{O}$. As $\mathcal{O}_p \simeq M_2(\mathbb{Z}_p)$ for $p > 2$, $\mathcal{O}_p$ has exactly $p + 1$ distinct ideals of index p^2, so $\mathcal{O}$ has exactly $p + 1$ ideal of index p^2 by the localization lemma. All of them are principal as $\mathrm{Cl}(\mathcal{O}) = 1$. We conclude the proof as $x\mathcal{O} = x'\mathcal{O}$ iff $x = ux'$ for $u \in \mathcal{O}^\times$, and $|\mathcal{O}^\times| = 24$.

In general, $\mathrm{Cl}(\mathcal{O})$ is closely related to the set of equivalence classes of 4-variables integral quadratic forms in the same genus as $(\mathcal{O}, N)$.

[5]The natural map $\mathcal{O}^\times \to \mathcal{O}_3^\times = \mathrm{GL}_2(\mathbb{Z}_3)$ induces thus an isomorphism $\mathcal{O}^\times \xrightarrow{\sim} \mathrm{SL}_2(\mathbb{F}_3)$.

[6]Remark that for $x \in \mathcal{O}_2^\times$, $x \equiv 1 \bmod (1 + i)$ iff $x \in \mathbb{Z}_2 + i\mathbb{Z}_2 + j\mathbb{Z}_2 + k\mathbb{Z}_2$.

EXAMPLE B: Let $D = \left(\frac{-1,-11}{\mathbb{Q}}\right)$ be the quaternion algebra with discrimimant 11. A discriminant computation shows that a maximal order $\mathcal{O}$ is given by $\mathbb{Z}[z] + i\mathbb{Z}[z]$ where $z = \frac{1+j}{2}$. If $Q(u,v,w,t) = N(u + vz + wi + tiz)$ then

$$Q(u,v,w,t) = u^2 + uv + 3v^2 + w^2 + tw + 3t^2.$$

(the discriminant of the associated bilinear form, namely $(x,y) \mapsto T(xy^*)$, is 11^2.) We see that $\mathcal{O}^\times = \langle i \rangle$ has order 4. Note that this form represents 2 in exactly $4 = |\mathcal{O}^\times|$ ways.[7] It follows that only one of the 3 ideals of $\mathcal{O}$ of index 4 is principal, namely $(1+i)\mathcal{O}$. In particular, $|\mathrm{Cl}(\mathcal{O})| > 1$. Consider the index 4 ideal $I = 2\mathcal{O} + (z-i)\mathcal{O}$. One easily checks that I is the subset of $a + bz + ci + dzi \in \mathcal{O}$ with $b - c$ and $a - d$ even. In particular $1 + i \notin I$ and I is not principal. One can actually show that

$$\mathrm{Cl}(\mathcal{O}) = \{[\mathcal{O}], [I]\}.$$

As a $\mathbb{Z}$-module, $I = \mathbb{Z}e + \mathbb{Z}f + \mathbb{Z}g + \mathbb{Z}h$ where $e = z - i$, $f = z + i$, $g = 1 + zi$ and $h = 1 - zi$. A computation shows that the quadratic form $Q'(u,v,w,t) := \frac{1}{2}N(ue + vf + wg + th)$ is

$$Q'(u,v,w,t) = 2(u^2 + v^2 + w^2 + t^2) + 2uv + ut + vw - 2wt,$$

which is another positive definite integral 4-variables quadratic form of discriminant 11^2, non equivalent[8] to Q. Although we shall not use this, one could check that the forms $\{Q, Q'\}$ are the only two such forms up to $\mathbb{Z}$-equivalence ! Note that there are 12 elements $x \in I$ such that $N(x) = 4$, namely $\pm e, \pm f, \pm g, \pm h, \pm 2i \pm 2$. Using these elements one easily sees that the subgroup of $u \in D^\times$ such that $uI = I$ is the group generated by $\frac{g}{2} = \frac{1+zi}{2}$, which has order 6 and satisfies $\frac{g}{2}e = f$.

Lagrange-Jacobi's theorem admits the following variant in this setting. If $p \neq 11$ is a prime, and if $J_1 \dots J_{p+1}$ are the $p+1$ ideals of $\mathcal{O}$ of index p^2 containing p, then some of the J_i (say A) will belong to the class of $[\mathcal{O}]$ and some others (say B) to the class $[I]$. We have $A + B = p + 1$ and a bit of quaternion arithmetic (see below) shows that $4A$ (resp.[9] $6B$) is also the number Q_p (resp. Q'_p) of ways to represent p by the integral form Q (resp. Q'). In particular,

$$\frac{Q_p}{4} + \frac{Q'_p}{6} = p + 1$$

but as we shall see below, to compute the individual Q_p and Q'_p is more complicated involves modular forms !

Exercise: (i) Let $D = \left(\frac{-1,-11}{\mathbb{Q}}\right)$ and $\tau = \frac{-1+\frac{i+k}{2}}{2}$. Show that $\tau^3 = 1$ and that $\mathbb{Z}[\tau] + j\mathbb{Z}[\tau]$ is an order of D. If $\mathcal{O}'$ is a maximal order containing that latter order, show that $\mathcal{O}'$ is not conjugate to the $\mathcal{O}$ chosen in the example above.

(ii) Let D be a definite quaternion algebra, $\mathcal{O}$ a maximal order, and $I \subset \mathcal{O}$ a right ideal of index[10] M^2. Show that $q_I(x) := N(x)/M$ is an integral quadratic form on I, which is in the same genus as $(\mathcal{O}, N(-))$ (in particular, positive definite of

[7]Indeed, $a^2 + ab + 3b^2 = (a + b/2)^2 + 11b^2/4$.

[8]Check that Q' does not represent 1.

[9]The explanation of the 6 here is that the subgroup of $u \in D^\times$ such that $uI = I$ has order 6.

[10]It may be convenient to observe the following facts. If I is a fractional ideal of $\mathcal{O}$, the index $[\mathcal{O} : I] \in \mathbb{Q}^\times$ is actually the square of a rational that we sometimes denote by $N(I)$ "the Norm of I". Indeed, this can be checked locally, in which case it is a previous exercise. For $x \in D^\times$ we see that $N(xI) = N(x)N(I)$, so $N(x\mathcal{O}) = N(x)$ is consistant with previous use.

discriminant $\mathrm{disc}(\mathcal{O})$), and whose equivalence class only depends on the ideal class of I.

(iii) (continuation) Let p be a prime. Show that an ideal $J \subset \mathcal{O}$ of index p^2 is in the same class as I iff there exists $x \in I$ such that $pJ = x^{-1}I$. In this case, show that x is unique up to multiplication by an element of the finite subgroup $G_I \subset D^\times$ of elements u such that $uI = I$, and that q_I represents p. If D is split at p, deduce the formula

$$p + 1 = \sum_{[I] \in \mathrm{Cl}(\mathcal{O})} \frac{n_I(p)}{|G_I|}$$

where $n_I(p)$ is the number of ways to represent p by q_I.

(iv) (continuation) Fix I as above. Show that the number of principal ideals $J \subset I$ of index p^2 is $\frac{n_I(p)}{|\mathcal{O}^\times|}$.

3. Modular forms on definite quaternion algebras

3.1. Definition. Let D be the definite quaternion algebra over $\mathbb{Q}$ with discriminant d and fix $\mathcal{O}$ a maximal order of D. Recall that $\widehat{\mathcal{O}}^\times = \prod_\ell \mathcal{O}_\ell^\times$.

We shall typically denote by K a compact open subgroup of $\widehat{\mathcal{O}}^\times$ of the form $\prod_\ell K_\ell$. If $(\ell, d) = 1$, then[11] $K_\ell = \mathrm{GL}_2(\mathbb{Z}_l)$, so for any integer N prime to D it makes sense to define $K_1(N) \subset \widehat{\mathcal{O}}^\times$ as the compact open subgroup of elements (x_ℓ) such that for any $\ell | N$ we have

$$x_\ell \equiv \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \mod N\mathbb{Z}_\ell.$$

If $k \geq 2$ is an integer, we denote by W_k the algebraic representation $\mathrm{Symm}^{k-2}(\mathbb{C}^2)$ of $D_\mathbb{C}^\times = \mathrm{GL}_2(\mathbb{C})$. Each such W_k can be viewed by restriction as a representation of $D^\times$.

DEFINITION 3.2. *The space of modular forms of level K and weight $k \geq 2$ for D is the complex vector space $S_k(K)$ of functions $D_f^\times \to W_k$ such that $f(\gamma x y) = \gamma f(x)$ for all $\gamma \in D^\times$, $x \in D_f^\times$, and $y \in K$. For $(N, d) = 1$ we set $S_k^D(N) = S_k(K_1(N))$.*

As for modular forms there is an obvious definition for $S_k(N, \varepsilon)$ such that $S_k(N) = \oplus_\varepsilon S_k(N, \varepsilon)$ where ε runs over all the Dirichlet characters $(\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$, but we shall not really need this.

By the finiteness of the class number of $\mathcal{O}$ and prop 2.8, there is a finite number $s = s(K)$ of elements $x_i \in D_f^\times$ such that $D_f^\times = \coprod_{i=1}^s D^\times x_i K$, and the groups $\Gamma_i := D^\times \cap x_i K x_i^{-1}$ are finite. We even have $s \leq h|\widehat{\mathcal{O}}^\times / K|$. We immediately get :

THEOREM 3.3. *The evaluation map $f \mapsto (f(x_i))$ induces an isomorphism*

$$S_k(K) \to \prod_i^s W_k^{\Gamma_i}.$$

[11] This identification is well defined up to inner automorphisms of $\mathrm{GL}_2(\mathbb{Z}_\ell)$, so the indeterminacy is harmless and we shall never mention this problem again and even write $K_\ell = \mathrm{GL}_2(\mathbb{Z}_l)$ for such an ℓ.

In particular, $S_k(K)$ is finite dimensional of "explicit dimension".

Exercise: If $K = K_1(N)$ with $N \geq 5$, show that $\Gamma_i = \{1\}$ for each $1 \leq i \leq s(K)$. In particular, for such a K we have $\dim S_k(N) = (k-1)s(K)$.

We now deal with Hecke operators. The group $D_f^\times$ acts by right translations on the vector-space S_k of all the functions $D_f^\times \to W_k$ such that $f(\gamma x) = \gamma f(x)$ for all $(\gamma, x) \in D^\times \times D_f^\times$. By definition, the K-invariants are $S_k^K = S_k(K)$ and the subspace of smooth vectors of this space is thus exactly $\bigcup_K S_k(K)$. It follows that each $S_k(K)$ inherits of an action of the Hecke-algebra of $(D_f^\times, K)$, i.e. of the restricted tensor product of the Hecke-algebra of the $(D_\ell^\times, K_\ell)$ for each ℓ. Recall that if $g_\ell \in D_\ell^\times$, the double coset $K_\ell g_\ell K_\ell$ is compact open hence admits a finite decomposition

$$K_\ell g_\ell K_\ell = \bigcup_i g_{i,\ell} K_\ell,$$

and the Hecke operator $T(g_\ell) : S_W(K) \to S_W(K)$ is (well-)defined by the mean formula

$$T(g_\ell)(f)(x) = \sum_i f(xg_i).$$

Here we view g_i as an adèle whose component is 1 at each prime different from ℓ, and is g_i at ℓ. Of course, two such $T(g_\ell)$ for two different ℓ commute. When ℓ splits D and $\mathcal{O}_\ell^\times = K_\ell \simeq \mathrm{GL}_2(\mathbb{Z}_\ell)$, the Hecke algebra of $(D_\ell^\times, K_\ell)$ is generated by the double cosets of $(1, \ell)$ and (ℓ, ℓ), the first class giving rise to the so-called T_ℓ operator. In this case we have already encountered the explicit formula

$$\mathrm{GL}_2(\mathbb{Z}_\ell) \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix} \mathrm{GL}_2(\mathbb{Z}_l) = \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix} \mathrm{GL}_2(\mathbb{Z}_\ell) \cup \coprod_{i=0}^{\ell-1} \begin{pmatrix} 1 & 0 \\ i & \ell \end{pmatrix} \mathrm{GL}_2(\mathbb{Z}_\ell).$$

Again, T_ℓ and T'_ℓ obviously commute whenever they are defined and $\ell \neq \ell'$. As for modular forms, the most interesting modular forms will be the common eigenforms for all the Hecke operators.

DEFINITION 3.4. *A quaternionic eigenform for D of level N and weight $k \geq 2$ is a common eigenvector $f \neq 0 \in S_k^D(N)$ for all the T_ℓ operators with $(\ell, Nd) = 1$.*

LEMMA 3.5. *If f is such a modular form, say such that $T_\ell(f) = a_\ell f$ for each ℓ, the subfield $\mathbb{Q}(\{a_\ell, \ell\}) \subset \mathbb{C}$ is a number field called the coefficient field of f.*

Indeed, remark that there exists a number field $F \subset \mathbb{C}$ such that $D \otimes_{\mathbb{Q}} F = M_2(F)$, and $W_{k|D^\times}$ is naturally defined over such an F, an F-structure being $\mathrm{Sym}^{k-2}(F^2)$. An F-structure of $S_k(K)$ is given by the sub-F-vector space of functions with value in $\mathrm{Sym}^{k-2}(F^2)$. That it is indeed an F-structure follows at once from the theorem above, as each $\mathrm{Sym}^{k-2}(F^2)^{\Gamma_i}$ is an F-structure of $W_k^{\Gamma_i}$ (justify!). The formula above show that Hecke operators preserves this F-structure, and the lemma follows. (As we may choose two linearly disjoint (quadratic) F in the argument above, we even also see that the characteristic polynomial of the Hecke operators have rational coefficients.)

3.6. A non-trivial example. $S_2(1)$ is simply the space of functions $\mathrm{Cl}(\mathcal{O}) \to \mathbb{C}$. If $(\ell, \mathrm{disc}(\mathcal{O})) = 1$ is a prime, and f such a function, then $T_\ell(f)([I]) = \sum_{i=0}^{\ell} f([I_i])$ where $I_i \subset I$ runs over the $\ell+1$ fractional ideals of index ℓ^2. In particular, the 1-dim subspace of constant functions $\mathbb{C}e$ is stable under each T_ℓ, with eigenvalue $\ell+1$.

Assume now that $D = \left(\frac{-1,-11}{\mathbb{Q}}\right)$ is the quaternion algebra of discriminant 11, so that $\mathrm{Cl}(\mathcal{O})$ has 2 elements as we already said. Applying the definition we see that the action of T_ℓ on the 1-dimensional quotient $S_2(1,1)/\mathbb{C}e$ is the multiplication by the element λ_ℓ which is the number of principal ideals inside $\mathcal{O}$ of index ℓ^2 minus the number of principal ideals inside a non-trivial class I of index ℓ^2. Quaternion arithmetic, i.e. the exercices related to Example B above, also expresses this number as

$$\lambda_\ell = \frac{Q_\ell}{4} - \frac{Q'_\ell}{4}$$

where Q_ℓ and Q'_ℓ are the number of ways to represent ℓ by Q and Q' respectively. This is a certainly very interesting collection of integers $(\lambda_\ell)_{\ell \neq 11}$ but that is not quite the end of the story (by the way, had we defined T_n for each n prime to 11, we would have obtained the same formula for λ_n and obtained the rather non-trivial fact that $\lambda_{nm} = \lambda_n \lambda_m$ whenever $(n,m) = 1$!).

Consider, for the two quadratic forms $F = Q$ and Q', the associated θ-series

$$\Theta_F = \sum_{n \geq 0} q^{F(n)} = \sum_{n \geq 0} F_n q^n.$$

(so F_n is the number of ways F represents the integer n). As Q, Q' are 4-variables integral quadratic forms which are positive definite and with discriminant 11^2, it can be shown that the two theta series above are modular forms of weight 2 for the subgroup $\Gamma_0(11)$ (see for instance the book of A. Ogg on modular forms). We have $\Theta_Q = 1 + 4q + 4q^2 + \cdots$ and $\Theta_{Q'} = 1 + 12q^2 + 12q^3 + \cdots$ so $\frac{\Theta_Q - \Theta_{Q'}}{4} = q - 2q^2 + \cdots$. But the space of modular forms of weight 2 and level $\Gamma_0(11)$ is well-known to have dimension 2 : it is generated by an Eisenstein series not vanishing at ∞, namely $E_2(q) - 11E_2(q^{11})$, and by the cusp form $q \prod_{n \geq 1}(1-q^n)^2(1-q^{11n})^2 = \sum_{n \geq 1} a_n q^n$. Thus the only possibility is that

$$\frac{\Theta_Q(q) - \Theta_{Q'}(q)}{4} = q \prod_{n \geq 1} (1-q^n)^2 (1-q^{11n})^2$$

so $\lambda_\ell = a_\ell$ for each $\ell \neq 11$. This is a particular instance of the Jacquet-Langlands correspondence. Remembering that those $\ell+1-a_\ell$ are also the number of points mod $\ell \neq 11$ of the elliptic curve $y^2 + y = x^3 - x^2$ over $\mathbb{Q}$, we see that the collection of λ_ℓ is indeed really interesting from an arthmetic point of view. From a computational way, it even looks easier to compute λ_ℓ by counting first $|E(\mathbb{F}_\ell)|$.

A very similar story holds for instance for the quaternion algebra of discriminant 17^2 and for the elliptic curve $y^2 + xy + y = x^3 - x^2 - x$ of discriminant ... 17.

3.7. The Jacquet-Langlands correspondence. Recall the space $S_k(N) = \oplus_\varepsilon S_k(N, \varepsilon)$ of cuspidal modular forms of weight k and level N. The following theorem is a special case of the Jacquet-Langlands correspondence.

THEOREM 3.8. *(Jacquet-Langlands) Assume* $(N, d) = 1$. *If* $k > 2$ *there is a* $\mathbb{C}$*-linear embedding*

$$S_k^D(N) \to S_k(Nd)$$

commuting with all the T_ℓ *for* $(\ell, Nd) = 1$. *If* $k = 2$, *the same statement holds if we replace* $S_2^D(N)$ *by its quotient by the* 1*-dimensional subspace of constant functions.*

In both cases, the image of this embedding is exactly the subspace $S_k(Nd)^{d-new}$ *of d-new forms as defined by Atkin-Lehner.*

This correspondence, and its natural generality, is best understood in terms of automorphic representations, and results from the comparison of the Arthur-Selberg trace formula for the algebraic groups GL_2 and $D^\times$. Of course we don't have time to explore this point of view here and we refer to the book of Jacquet and Langlands. We have not defined what a d-new form is. Let us simply say that it has the following properties, which characterize it :

– (NEW1) if $f \in S_k(Nd)^{d-new}$, then $f_{|k}\gamma = f$ for all $\gamma \in \Gamma_0(d) \cap \Gamma_1(N)$,

– (NEW2) an eigenform $f \in S_k(Nd)$ is in $S_k(Nd)^{d-new}$ iff there is no eigenform $g \in S_k(Nd')$ for $d'|d$ and $d' \neq d$ with the same eigenvalues of T_ℓ as f for each ℓ prime to Nd,

– (NEW3) $S_k(Nd)^{d-new} \subset S_k(Nd)$ is a direct summand as $\mathbb{C}[\{T_\ell, (\ell, Nd) = 1\}]$-module.

Example : Assume d prime. As there is no modular form of weight 2 and level 1, it follows that

$$\mathrm{Cl}(\mathcal{O}) = \dim S_2^D(1) = 1 + \dim S_2(d, 1) = 1 + \mathrm{genus}(X_0(d)),$$

as mentionned earlier.

From the existence of Galois representations attached to modular forms we deduce the following important fact.

COROLLARY 3.9. *Let* $f \in S_k^D(N)$ *is an eigenform,* E *its coefficient field and* λ *a finite place of* E *above the prime* p. *There exists a unique continuous semisimple* p*-adic representation*

$$\rho_{f,\lambda} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(E_\lambda)$$

which is unramified outside Ndp, *and such that* $\mathrm{trace}(\rho_{f,\lambda}(\mathrm{Frob}_\ell)) = a_\ell$ *for each prime* ℓ *prime to* Ndp.

If $k = 2$ and f is a constant function, we have seen that $T_\ell(f) = (\ell + 1)f$ for each $(\ell, Np) = 1$. In particular $E = \mathbb{Q}$ and we may define $\rho_{f,p}$ as $\mathbb{Q}_p \oplus \mathbb{Q}_p(-1)$.