Arithmetic of Quaternion Algebras: Orders and Ideals

Marios Magioladitis

Forschungsseminar SS2008

Institute for Experimental Mathematics (IEM)
University of Duisburg-Essen
May 2008

Forschungsseminar Sommersemester 2008.
Organisers: Gebhard Böckle, Juan Marcos Cerviño, Lassina Dembélé, Gerhard Frey, Gabor Wiese.

Lecture **Arithmetic of Quaternion Algebras: Orders and Ideals** was given on the 8th of May 2008 in the University of Duisburg-Essen, Campus Essen.

Marios Magioladitis
Homepage: http://www.iem.uni-due.de/~magiolad
E-mail: magiolad@iem.uni-due.de

References

[1] M.-F. Vignéras, *Arithmétique des Algbèbres de Quaternions*
[2] M. Kirschmer *Konstruktive Idealtheorie in Quaternionalgebren*

Chapter 1

Orders and Ideals

Definition 1.1. *A commutative integral domain R is said to be a Dedekind domain if it is Noetherian, integrally closed in its fraction field and every nonzero prime ideal in R is a maximal ideal.*

Example 1.2. *Examples of Dedekind domains are: $\mathbb{Z}, \mathbb{Z}[1/p]$, where p is prime and $\mathbb{Z}[i]$. In addition, every integer ring of a local or global field is a Dedekind domain.*

In the following R will always be a Dedekind domain, K will be its quotient field and H/K a quaternion algebra over K.

Definition 1.3. *Let $h \in H$. The reduced trace of h is $t(h) = h + \bar{h}$. The reduced norm of h is $n(h) = h\bar{h}$.*

Definition 1.4. *An R-**lattice** L of K-vector space V is a finitely generated R-submodule of V.*

We say that L has **full dimension** *if $KL = V$ with*

$$KL = \{\sum_i{}' x_i \ell_i \mid x_i \in K, \ell_i \in L\}.$$

Definition 1.5. *An element $x \in H$ is said to be an* **integral** *(with respect to R) if $R[x]$ is an R-lattice of H.*

We state without proof the following

Lemma 1.6. (Bourbaki) *An element $x \in H$ is integral if and only if its reduced trace and reduced norm are elements of R.*

The above lemma gives us a criterion to determine if an element is an integral.

Remark 1.7. *The integral elements of H don't form a ring in the general case. Take for example $H = M_2(\mathbb{Q})$ and consider the matrices*

$$X = \begin{bmatrix} \frac{1}{2} & -3 \\ \frac{1}{4} & \frac{1}{2} \end{bmatrix}, Y = \begin{bmatrix} 0 & \frac{1}{5} \\ 5 & 0 \end{bmatrix}.$$

X, Y are integrals of H but neither

$$X + Y = \begin{bmatrix} \frac{1}{2} & \frac{-14}{5} \\ \frac{21}{4} & \frac{1}{2} \end{bmatrix}$$

nor

$$XY = \begin{bmatrix} -15 & \frac{1}{10} \\ \frac{5}{2} & \frac{1}{20} \end{bmatrix}$$

is an integral.

Definition 1.8. *An ideal of H is a full dimension R-lattice. An order $\mathcal{O}$ of H is*

(1) an ideal of H that is a ring or (equivalently, see proposition 1.13)

(2) a ring of integers that contains R, and s.t. $K\mathcal{O} = H$.

Definition 1.9. *A order is called* **maximal** *if is not contained in any other order. An* **Eichler order** *is the intersection of two maximal orders.*

Remark 1.10. *Example of ideals are the free R-modules $L = R(a_i)$ generated by a basis $\{a_1, a_2, a_3, a_4\}$ of H/K.*

Let I be an ideal. We can canonically associate two orders,

$$\mathcal{O}_l = \mathcal{O}_l(I) = \{h \in H, hI \subset I\}$$

$$\mathcal{O}_r = \mathcal{O}_r(I) = \{h \in H, Ih \subset I\}$$

They are called **left order** and **right order** respectively.

Remark 1.11. *The left and the right order are orders indeed.*

Proof. Obviously they are rings and R-modules. It remains to prove that they are full dimension R-lattices.

Let $a \in R \cap I$ non-zero, then $\mathcal{O}_l \subset a^{-1}I$ since the following holds:

$$x \in \mathcal{O}_l \Rightarrow xI = I \Rightarrow xa \in I \Rightarrow xaa^{-1} = x \in Ia^{-1} = a^{-1}I.$$

If $h \in H$ then $\exists b \in R$ s.t.

$$bhI \subset I.$$

It follows that $H = K\mathcal{O}_l$. □

We are stating now a lemma usefull for many proofs that follow.

Lemma 1.12. *Let $I \subset H$ be a R-module. If there exist ideals J_1, J_2 s.t.*

$$J_1 \subset I \subset J_2,$$

then I is an ideal.

Proof. $J_1 \subset I \subset J_2 \Rightarrow KJ_1 \subset KI \subset KJ_2 \Rightarrow H \subset I \subset H \Rightarrow KI = H.$ □

Proposition 1.13. *The definitions (1) and (2) of an order are equivalent.*

Proof. (1) $\Rightarrow$ (2) is clear.

We show that (2) $\Rightarrow$ (1).

Let $\{a_1, a_2, a_3, a_4\}$ be a basis of H/K contained in $\mathcal{O}$. An element $h \in \mathcal{O}$ can be written

$$h = \sum_{i=1}^{4} x_i a_i, \ x_i \in K.$$

Since $\mathcal{O}$ is a ring of integers, $ha_i \in \mathcal{O}$ and

$$t(ha_i) = t\left(\left(\sum_{j=1}^{4} x_j a_j\right) a_i\right) = \sum_{j=1}^{4} x_j t(a_j a_i) \in R.$$

We have that,

$$(t(a_j a_i)) \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \in R^4$$

The Cramer rule implies that

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \in d^{-1}R^4,$$

where $d = \det(t(a_j a_i)) \neq 0$.

Let $L = \sum_1^4 O_K a_i$. L is an ideal. We have that $h \in d^{-1}L$. Thus,

$$L \subset \mathcal{O} \subset d^{-1}L.$$

From the last lemma we deduce that $\mathcal{O}$ is an ideal. □

Remark 1.14. *Orders exist and every order is contained in a maximal order.*

Proof. Let $\mathcal{O}$ be an order in H, and let C be the collection of orders in H containing $\mathcal{O}$. Let $\{\mathcal{O}_i\}$ be a chain of orders containing $\mathcal{O}$. $U = \sum_i \mathcal{O}_i = \cup_i \mathcal{O}_i$ is a subring of H containing R and

$$KU = H.$$

Each $x \in U$ lies in some $\mathcal{O}_i$, hence is integral over R.

It can be shown that U is an order in H.

We have now shown that any increasing chain of elements of C has an upper bound in C. By Zorn's lemma, C has a maximal element, which is then obviously a maximal order H. □

Definition 1.15. *Let I be an ideal with left order $\mathcal{O}_l$ and right order $\mathcal{O}_r$. We say that I is*
two-sided *if $\mathcal{O}_l = \mathcal{O}_r$,*
normal *if $\mathcal{O}_l, \mathcal{O}_r$ are maximal,*
integral *if $I \subset \mathcal{O}_l, \mathcal{O}_r$,*
principal *if $I = \mathcal{O}_l h = h\mathcal{O}_r$.*

It's **inverse** *is $I^{-1} = \{h \in H, IhI \subset I\}$.*

Definition 1.16. *Let I, J be two ideals in H. The product IJ is defined as*

$$IJ = \left\{ \sum\nolimits' hk,\ h \in I, k \in J \right\}$$

Remark 1.17. *The product of two ideals is an ideal.*

Lemma 1.18. *Let I be an ideal.*

1. *The product of ideals is associative.*
2. *I is integral $\Leftrightarrow$ $I \subset \mathcal{O}_l$ or $I \subset \mathcal{O}_r$*
3. *I^{-1} is an ideal.*
4. *I^{-1} satisfies the following properties:*

$$\mathcal{O}_l(I^{-1}) \supset \mathcal{O}_r(I),$$
$$\mathcal{O}_r(I^{-1}) \supset \mathcal{O}_l(I),$$
$$II^{-1} \subset \mathcal{O}_l(I),$$
$$I^{-1}I \subset \mathcal{O}_r(I)$$

Proof.

1. Clear, since the product in H is associative.
2. $I \subset \mathcal{O}_l \Leftrightarrow II \subset I \Leftrightarrow I \subset \mathcal{O}_r$.
3. Let $m \in R^*$ s.t. $mI \subset \mathcal{O}_l \subset m^{-1}I$.

   We have on the one hand that: $Im\mathcal{O}_l I = mI\mathcal{O}_l I \subset \mathcal{O}_l\mathcal{O}_l I = \mathcal{O}_l I = I$. Hence, $m\mathcal{O}_l \subset I^{-1}$.

   On the other hand, $m^{-1}II^{-1}m^{-1}I = m^{-2}II^{-1}I \subset m^{-2}I$. This implies that $I^{-1} \subset m^{-2}I$.

   We deduce that I^{-1} is an ideal.

4. $I\mathcal{O}_r I^{-1}\mathcal{O}_l I \subset I$. We have that

$$x \in \mathcal{O}_r \Rightarrow Ix \subset I \Rightarrow IxhI \subset IhI,\ \forall h:\ IhI \subset I \Rightarrow$$
$$xh \in I^{-1},\ \forall h \in I^{-1} \Rightarrow x \in \mathcal{O}_l(I^{-1}).$$

Hence, $\mathcal{O}_l(I^{-1}) \supset \mathcal{O}_r$ and $\mathcal{O}_r(I^{-1}) \supset \mathcal{O}_l$.

Since $II^{-1}I \subset I$ (by definition of I^{-1}) we have that $II^{-1} \subset \mathcal{O}_l$ (by definition of $\mathcal{O}_l$) and $I^{-1}I \subset \mathcal{O}_r$ (by definition of $\mathcal{O}_r$).

□

1.1 Properties of principal ideals

Let $\mathcal{O}$ be an order and $I = \mathcal{O}h$ be a principal ideal. The left order of I is equal to $\mathcal{O}$ and its right order is $\mathcal{O}' = h^{-1}\mathcal{O}h$. Obviously, $I = h\mathcal{O}'$.

Now, we consider the principal ideal $I' = \mathcal{O}h'$ whose left order is $\mathcal{O}'$. We have:

$$I^{-1} = h^{-1}\mathcal{O} = \mathcal{O}'h^{-1}$$

$$II^{-1} = \mathcal{O}$$

$$I^{-1}I = \mathcal{O}'$$

$$I' = \mathcal{O}hh' = hh'\mathcal{O}'',$$

where $\mathcal{O}'' = h'^{-1}\mathcal{O}'h'$ is a right order of I'.

We consider the following multiplication rules:

$$\mathcal{O}_l(I) = \mathcal{O}_r(I^{-1}) = II^{-1},$$
$$\mathcal{O}_r(I) = \mathcal{O}_l(I^{-1}) = I^{-1}I,$$
$$\mathcal{O}_l(IJ) = \mathcal{O}_l(I),$$
$$\mathcal{O}_r(IJ) = \mathcal{O}_r(J),$$

$$(IJ)^{-1} = J^{-1}I^{-1}.$$

We already showed that the above nupliplication rules hold for principal ideals. Moreover, they hold if $\mathcal{O}_l, \mathcal{O}_r$ are maximal. More specific

Proposition 1.19. *Let I be an ideal.*

$$\mathcal{O}_l(I) \text{ is maximal } \Rightarrow II^{-1} = \mathcal{O}_l(I)$$
$$\mathcal{O}_r(I) \text{ is maximal } \Rightarrow I^{-1}I = \mathcal{O}_r(I)$$

Proof. [2], Korollar 2.5.24 (page 38) □

The proof is using the following lemma:

Lemma 1.20. *Let $\mathcal{O}$ be a maximal order and I be a two-sided ideal of $\mathcal{O}$.*

$$I \subsetneqq \mathcal{O} \Rightarrow \mathcal{O} \subsetneqq I^{-1}$$

Proof. Obviously, $\mathcal{O} \subset I^{-1}$. We assume that $\mathcal{O} = I^{-1}$. It exists a prime ideal P of $\mathcal{O}$ s.t.

$$I \subset P \subsetneqq \mathcal{O}$$

We fix an $r \in R \cap P$. We take prime ideals P_i s.t.

$$P_1 ... P_k \subset r\mathcal{O} \subset P.$$

We assume that k is the minimum that this incusions hold.

Since P is prime, $P = P_i$ for some i. Let

$$B := P_1 ... P_{i-1} \text{ and}$$
$$C := P_{i+1} ... P_k$$

Then, it holds:

$$r^{-1}BPC \subset \mathcal{O} \Rightarrow Br^{-1}PCB \subset B \Rightarrow r^{-1}PCB = \mathcal{O}_r(B) = \mathcal{O} = \mathcal{O}_l(P) \Rightarrow$$

$$r^{-1}CB \subset P^{-1} = \mathcal{O} \Rightarrow CB \subset r\mathcal{O}.$$

This implies that it k was not minimum and this is a contraction. Thus, $\mathcal{O} \neq I^{-1}$. □

The multiplication rules hold in the case of normal ideals as well.

Proposition 1.21. *Let $\mathcal{O}$ be an order. Let I, J be two normal ideals of $\mathcal{O}$. The following hold:*

$$\mathcal{O}_l(IJ) = \mathcal{O}_l(I),$$
$$\mathcal{O}_r(IJ) = \mathcal{O}_r(J),$$
$$\mathcal{O}_l(I) = \mathcal{O}_r(I^{-1}) = II^{-1},$$
$$\mathcal{O}_r(I) = \mathcal{O}_l(I^{-1}) = I^{-1}I,$$
$$(I^{-1})^{-1} = I.$$

Proof. [2], Korollar 2.5.28 (page 40) □

For the following, we suppose that these multiplication rules hold for all the orders and the ideals that we consider.

1.2 Two-sided ideals

Definition 1.22. *Let $\mathcal{O}$ be an order. We say that a two-sided, integral ideal $P(\neq 0, \mathcal{O})$ is* **prime** *if*

$$IJ \subset P \Rightarrow I \subset P \vee J \subset P, \forall I, J \subset \mathcal{O}.$$

Theorem 1.23. *The two-sided ideals of $\mathcal{O}$ form a free Abelian group under ideal multiplication generated by the prime ideals.*

In order to prove this theorem we 'll need some lemmas and we 'll assume that the multiplication rules we stated previously hold.

Lemma 1.24. *Let $\mathcal{O}$ be an order. The maximal integral two-sided ideals of $\mathcal{O}$ are exactly its prime ideals.*

Proof. Let I be a maximal integral two-sided ideal of $\mathcal{O}$. We show that I is prime.

Let J, J' two-sided integral ideals with $JJ' \subset I$.

If $J \not\subset I$, then $I \subsetneq I + J = \mathcal{O}$ by maximality of I.

We multiply $I + J = \mathcal{O}$ by J' and get

$$J' = IJ' + JJ' \subset IJ' + I \subset I$$

($IJ' \subset I$ since $J' \subset \mathcal{O}$).

Similarly, if $J' \not\subset I$ we get that $J \subset I$.

Now, we show that any prime ideal is maximal.

Let P be a prime ideal s.t. $P \subsetneq I \subsetneq \mathcal{O}$, for some I.

By the multiplication rules we have that $P = I(I^{-1}P)$. Since P is prime, we have that $I^{-1}P \subset P$.

This is a contradiction, since $I^{-1} \not\subset \mathcal{O}$ but $\mathcal{O}$ is the biggest ring s.t. $\mathcal{O}P \subset P$. □

Lemma 1.25. *Let $\mathcal{O}$ be an order. Let $I \subset J$ be two two-sided ideals of $\mathcal{O}$. Then,*

$$IJ^{-1} =: C \text{ and}$$

$$J^{-1}I =: D$$

are integral two-sided ideals.

In particular, $I = CJ$ and $I = JD$.

Proof.

$$I \subset J \Leftrightarrow I^{-1} \supset J^{-1}$$

So we have that

$$J^{-1}I \subset I^{-1}I \subset \mathcal{O}$$
$$IJ^{-1} \subset II^{-1} \subset \mathcal{O}$$

Thus, C, D are integral two-sided ideals and the equalities follow from the multiplication rules. □

Lemma 1.26. *Let $P, Q,\ P \neq Q$, be two two-sided prime ideals. Then, $PQ = QP$.*

Proof. We have that $QP \subset P$, since $Q \subsetneq \mathcal{O}$. By lemma 1.25, $\exists Q'$ s.t. $QP = PQ'$ with $QP \subset Q'$.

$PQ' = QP \subset Q$.

Since Q is prime, we get that $Q' \subset Q$.

Lemma 1.25 gives $Q' = QD$ for some ideal D. Hence, $QP \subset QD$. Thus, $P \subset D$.

Hence, $P = D$ or $P = \mathcal{O}$.

Assume $P = D$. Then, $Q' = QP = PQ'$, which is a contradiction. □

Proof. of Theorem 1.23. Suppose we want to factor the integral ideal $I = I_0$. We do the following process:

1. Choose a prime ideal P_0 s.t. $I_0 \subsetneqq P_0$. By lemma 1.25
$$I_0 = P_0 I_1,$$
for some integral $I_1 \supsetneqq I_0$.
2. Choose a prime ideal P_1 s.t. $I_1 \subsetneqq P_0$. By lemma 1.25
$$I_0 = P_0 P1 I_2,$$
for some integral $I_2 \supsetneqq I_1$.
3. Continue this process to get
$$I_0 \subsetneqq I_1 \subsetneqq I_2 \subsetneqq ...$$

Since $\mathcal{O}$ is Noetherian, at some point I_n will be maximal $= P_n$ for some n.

We get that
$$I_0 = P_0 P_1 ... P_n$$

Let now a two-sided ideal J. $\exists n \in R \setminus \{0\}$ s.t. $nJ = (n)J \subset \mathcal{O}$. This means that nJ is integral.

With the above process exist prime ideals $P_1, ..., P_s$ s.t.
$$nJ = P_1 ... P_s$$

and prime ideals $Q_1, ..., Q_t$ s.t.
$$(n) = Q_1 ... Q_t.$$

Hence, I can be written as:
$$I = (n)^{-1} P_1 ... P_s = Q_1^{-1} ... Q_t^{-1} P_1 ... P_s.$$

We immediately see that the factorisation is unique. (Use the fact that if a product of prime ideals is contained in a prime ideal P, then at least one of the factors of the product is equal to P). The theorem is proved. □

1.3 Properties of non two-sided ideals

Let $\mathcal{O}$ be an order. We say that an integral ideal P of a left order $\mathcal{O}$ is **irreducible**, if $P(\neq 0, \mathcal{O})$ is maximal by inclusion in the set of integral ideals of the left order $\mathcal{O}$ which are different from $\mathcal{O}$.

1. P is a maximal ideal in the set of integral right ideals of $\mathcal{O}_r(P)$.
2. If $\mathcal{O}$ is a maximal order, P contains only one two-sided ideal of $\mathcal{O}$.
3. If $M = \mathcal{O}/P$, the ideal $I = \{x \in \mathcal{O}, xM = 0\}$ is called the **annihilator** of M in $\mathcal{O}$.
4. An integral ideal is the product of irreducible ideals.

Definition 1.27. *The* **reduced norm** $n(I)$ *of an ideal I is the fractional ideal of R generated by the reduced norms of its elements i.e.*

$$n(I) =< n(h) \mid h \in I >\subset R$$

If $I = \mathcal{O}h$ is a principal ideal, $n(I) = Rn(h)$.

If $J = \mathcal{O}'h'$ is a principal ideal of a left order $\mathcal{O}' = h^{-1}\mathcal{O}h$, we have $IJ = \mathcal{O}hh'$ and $n(IJ) = n(I)n(J)$.

The last relation is true for non-principal ideals as well.

We use the fact that an ideal is finitely generated in R.

For the ideals we consider later, the multipliticativity of the norm of the ideals follow from the multipliticativity of the norms of the principal ideals.

1.4 Differents and Discriminants

Definition 1.28. *The* **different** $\mathcal{O}^{*-1}$ *of an order $\mathcal{O}$ is the inverse of the dual of $\mathcal{O}$ for a bilinear form induced by the reduced trace:*

$$\mathcal{O}^{\#} = \{x \in H, t(x\mathcal{O}) \subset R\}.$$

Remark 1.29. $\mathcal{O}^{\#-1}$ *is an integral two-sided ideal of $\mathcal{O}$.*

Definition 1.30. *The* **reduced discriminant** *of $\mathcal{O}$ is defined as*

$$d(\mathcal{O}) := n(\mathcal{O}^{\#-1})$$

We are going to prove the following:

Lemma 1.31.

1. *Let I an ideal. The set $I^{\#} = \{x \in H, t(xy) \subset R, \forall y \in I\}$ is a two-sided ideal.*
2. *Let $\mathcal{O}$ be an order. The ideal $O^{\#-1}$ is an integral two-sided ideal.*
3. *Let $\mathcal{O}$ be a free R-module with basis $\{u_i\}$. Then,*

$$d(\mathcal{O})^2 = R(\det(t(u_i u_j)).$$

Proof.

1. It is clear that $I^{\#}$ is an R-module. The same trick we used to prove the equivalence of the two definitions of the orders (see 1.13) shows that there exists $d \in R$ s.t. $d\mathcal{O} \subset I^{\#} \subset d^{-1}\mathcal{O}$, where $I^{\#}$ is an ideal. Since $t(xy) = t(yx)$, it is clear that the left order $\{x \in H : t(xI^{\#}I) \subset R\}$ is equal to $\{x \in H : t(I^{\#}xI) \subset R\}$.
2. Since $1 \in \mathcal{O}^{\#}$ we have that $\mathcal{O}^{\#}\mathcal{O}^{\#-1} \supset \mathcal{O}^{\#-1}$.
3. Let $\mathcal{O}$ be a principal ring. $\mathcal{O}^{\#}$ is the ideal generated by the dual basis $(u_i^{\#})$ defined by

$$t(u_i u_j^{\#}) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

   If $u_i^{\#} = \sum_j a_{ij} u_j$ we have that $t(u_i u_j^{\#}) = \sum_k a_{jk} t(u_i u_k)$.

   We conclude that $\det(t(u_i u_j^{\#})) = \det(a_{ij} \det(t(u_i u_j))$.

   On the other hand, $\mathcal{O}^{\#} = \mathcal{O}x, x \in H^*$. Because $\mathcal{O}^{\#}$ is principal, we have that $\{u_i x\}$ is another basis of the R-module $\mathcal{O}$.

   Since $n(x)^2$ is the determinant of the endomorphism $x \to hx$, we have that $\det(a_i j) = n(x)^2 u,\ u \in R^*$. We deduce that

$$R\left(\det(t(u_i u_j))\right) = n(\mathcal{O}^*)^{-2} = n(\mathcal{O}^{*-1})^{-2} = d(\mathcal{O})^2.$$

   The property (3) is true even if $\mathcal{O}$ is not principal.

□

Remark 1.32. *Let $\mathcal{O}, \mathcal{O}'$ be two orders.*

$$\mathcal{O}' \subset \mathcal{O} \Rightarrow d(\mathcal{O}') \subset d(\mathcal{O}).$$

$$d(\mathcal{O}) = d(\mathcal{O}') \Rightarrow \mathcal{O} = \mathcal{O}'.$$

Proof. Let $\{u_i\}$ be a basis of $\mathcal{O}$ and $\{v_i\}$ a basis of $\mathcal{O}'$. Let (a_{ij}) be the base change matrix between these basis.

So, $v_i = \sum_{j=1}^{4} a_{ij} u_j$. We have that

$$\det(t(v_i v_j)) = \det^2(a_{ij}) \det(t(u_i u_j)).$$

□

This remark gives us a criterion to determine if an order is maximal.

Example 1.33.

1. *The order $M_2(R)$ over $M_2(K)$ is maximal because it reduced discriminant is equal to R.*
2. *In the quaternion algebra $H = \{-1, -1\}$ defined over $\mathbb{Q}$ (the Hamiltonians), the order $\mathbb{Z}(1, i, j, ij)$ has reduced discriminant $4\mathbb{Z}$ and it's not maximal since it is contained in the order $\mathbb{Z}(1, i, j, \frac{1+i+j+ij}{2})$ which has reduced discriminant $2\mathbb{Z}$. The latter is a maximal order of H.*

1.5 Ideal classes

Definition 1.34. *Two ideals I, J are* **equivalent from the right** $\Leftrightarrow I = Jh$, *for some $h \in H^*$.*

We define the equivalency class $\sim_r$ as follows:

$$I \sim_r I \Leftrightarrow I = Jh, \text{ for some } h \in H^*$$

The classes of left ideals of an order $\mathcal{O}$ are called the **left classes** *of $\mathcal{O}$.*

We define the **left class number** *of an order $\mathcal{O}$ as*

$$\#\{I \mid \mathcal{O}_l(I) = \mathcal{O}\}/\sim_r$$

We define the right classes and the right class number of $\mathcal{O}$ in the same way.

It is easy to verify the following:

Lemma 1.35.

1. *The map $I \to I^{-1}$ induces a bijection between the left and the right classes of $\mathcal{O}$.*
2. *Let J be an ideal. The map $I \to JI$ induces a bijection between the left classes of $\mathcal{O}_l(I) = \mathcal{O}_r(J)$ and the left classes of $\mathcal{O}_l(J)$.*

The above lemma shows us that the right class number and the left class number of an order are equal.

Definition 1.36. *The* **class number** $h(\mathcal{O})$ *of a given order $\mathcal{O}$ is defined as the class number (finite or infinite) of left (or right) ideals of that order.*

The class number of H is the class number of its maximal orders.

Definition 1.37. *Two conjugate orders by an inner homomorphism of H are said to be of the* **same type**, *i.e.*

$$\mathcal{O}, \mathcal{O}' \text{ are of the same type } \Leftrightarrow \exists h \in H^* \ : \ \mathcal{O}' = h^{-1}\mathcal{O}h$$

Definition 1.38. *An order $\mathcal{O}'$ is* **linked to** *$\mathcal{O}$, if it is a right order of a left ideal of $\mathcal{O}$.*

Lemma 1.39. *Let $\mathcal{O}, \mathcal{O}'$ be two orders. The following properties are equivalent.*

1. *$\mathcal{O}, \mathcal{O}'$ are of the same type.*
2. *$\mathcal{O}, \mathcal{O}'$ are linked by a principal ideal.*

Proof. If $\mathcal{O}' = h^{-1}\mathcal{O}h$, the principal ideal $\mathcal{O}h$ links $\mathcal{O}$ to $\mathcal{O}'$ and conversely. □

Definition 1.40. *Let $\mathcal{O}$ be an order. The* **type number** *$t(\mathcal{O})$ of $\mathcal{O}$ is*

$$t(\mathcal{O}) := \#\{\mathcal{O}' \text{ order } \mid \mathcal{O}' \text{ is linked to } \mathcal{O}\}/\sim,$$

where $\sim$ is the equivalence class defined as:

$$\mathcal{O} \sim \mathcal{O}' \Leftrightarrow \mathcal{O}, \mathcal{O}' \text{ are of the same type}$$

Lemma 1.41. *Any two maximal orders of H are linked.*

Proof. Let $\mathcal{O}, \mathcal{O}'$ be two maximal orders. We have that

$$\mathcal{O}, \mathcal{O}' \subset \mathcal{O}\mathcal{O}'$$

Due to maximality we have that

$$\mathcal{O}_l(\mathcal{O}\mathcal{O}') = \mathcal{O}$$
$$\mathcal{O}_r(\mathcal{O}\mathcal{O}') = \mathcal{O}'$$

□

Theorem 1.42. *Let $\mathcal{O}$ be an order and $h(\mathcal{O})$ be finite.*

$$t(\mathcal{O}) \leq h(\mathcal{O}).$$

Proof. The following maps induces a surjection.

$$\{I \mid \mathcal{O}_l(I) = \mathcal{O}\}/\sim_r \overset{I \to \mathcal{O}_r(I)}{\longrightarrow} \{\mathcal{O}' \mid \mathcal{O}' \text{ linked to } \mathcal{O}\}/\sim$$

□

Definition 1.43. *The type number of H is the type number of any of its maximal orders.*

1.6 Groups of units of an order

The **units** of an order are the invertible elements which are contained in this order as well with their inverses. They naturally form a group, that we denote $\mathcal{O}^*$.

$$\mathcal{O}^* = \{x \in \mathcal{O} \mid x^{-1} \in \mathcal{O}\}$$

The units with reduced norm 1 form a group denoted $\mathcal{O}^1$.

$$\mathcal{O}^1 = \{x \in \mathcal{O}^* \mid n(x) = 1\}$$

Lemma 1.44.

$$x \in \mathcal{O}^* \Leftrightarrow n(x) \in R^*.$$

Proof.
($\Rightarrow$) $x, x^{-1} \in \mathcal{O} \Rightarrow n(x), n(x^{-1}) = n(x)^{-1} \in R \Rightarrow n(x) \in R^*$.
($\Leftarrow$) $x \in \mathcal{O}, n(x) \in R^* \Rightarrow \bar{x} \in \mathcal{O}, n(x)^{-1} \in R \Rightarrow x^{-1} = n(x)^{-1}\bar{x} \in \mathcal{O}$. □