Dr. Marques Sophie
Office 519

Number theory

Spring Semester 2014

marques@cims.nyu.edu

# Problem Set #7

**Exercise 1:**
Let $D > 1$ be a square free integer and $d$ the discriminant of the real quadratic number field $K = \mathbb{Q}(\sqrt{D})$. Let $x_1$, $y_1$ be the uniquely determined rational integer solution of the equation

$$x^2 - Dy^2 = -4$$

or $-$ in case this equation has no rational integers solutions of the equation

$$x^2 - Dy^2 = 4$$

for which $x_1$, $y_1 > 0$ are as small as possible. Then

$$\epsilon_1 = \frac{x_1 + y_1\sqrt{D}}{2}$$

is a fundamental unit of $K$. (The pair of equations $x^2 - dy^2 = \pm 4$ is called **Pell's equation**.)

***Solution:***
*First, since $K = \mathbb{Q}(\sqrt{D})$ with $D > 0$ real implies $r = 2$, $s = 0$ and then by Dirichlet's unit theorem, there is exactly $r + s - 1 = 2 - 1 = 1$ fundamental units $\epsilon \in \mathcal{O}_K$. We have proven that*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\frac{1+\sqrt{D}}{2}] & if\ D \equiv 1 \ mod\ 4 \\ \mathbb{Z}[\sqrt{D}] & if\ D \equiv 2, 3\ mod\ 4 \end{cases}$$

*and units are $\pm 1\epsilon^n$, since $\pm 1$ are the only 2-roots of unity in $\mathbb{Q}(\sqrt{D})$).*
*Now, we recall that $\epsilon \in \mathcal{O}_K*$ if and only if $N_{K/\mathbb{Q}}(\epsilon) = \pm 1$. Now,*

1. *if $D \equiv\ 1\ mod\ 4$, $\epsilon = 1/2x + 1/2\sqrt{D}y \in \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ with $x, y \in \mathbb{Z}$ so that $x^2 - Dy^2 = \pm 4$ and*

2. *if $D \equiv 2, 3\ mod\ 4$, $\epsilon = x + \sqrt{D}y \in \mathbb{Z}[\sqrt{D}]$ with $x, y \in \mathbb{Z}$ so that $x^2 - Dy^2 = \pm 1$ so that $\epsilon = x + \sqrt{D}y$ with $x$, $y \in \mathbb{Z}$. But now this is equivalent to $x^2 - Dy^2 = \pm 4$. Indeed, if $D \equiv 2\ mod\ 4$, $x^2 \equiv 0 mod 2$ then $x$ is even implying $y$ to be even. Now if $D \equiv 3\ mod\ 4$, $x^2 \equiv 3y^2\ mod\ 4$ but since square mod 4 are either congruent to 1 or 0, the only possibility is that $x$ and $y$ are even.*

*Notice that if $u$, $v \in \mathbb{Z}$ satisfy $(u/2)^2 - N(v/2)^2 = \pm 1$ and $u/2 + v/2\sqrt{D} > 1$, then $u/2 - v/2\sqrt{D}$, being equal to $(u/2 + v/2\sqrt{D})^{-1}$ lies between $-1$ and 1. Addition of the inequalities $u/2 + v/2\sqrt{D} \geq 1$ and $-1 \leq u/2 - v/2\sqrt{D} \leq 1$ implies $u > 0$. Substraction of these inequalities yields $v > 0$. So, requiring that $u$ and $v$ are minimal is equivalent* *to asking that $u/2 + v/2\sqrt{D}$ is minimal greater than 1. Clearly if $x^2 - Dy^2 = -4$ as a solution the minimal one will be smaller than the minimal one for $x^2 - Dy^2 = 4$.*

*Finally by Dirichlet theorem we know that there is a fundamental unit $e$ such that for any other unit $u \in \mathcal{O}_K*$ there is a $n$ such that $e^n = u$ and up to passing to the inverse, we can suppose that $e > 1$. But then if $\epsilon_1$ is not a fundamental, then $\epsilon_1 = e^n$ with $n \geq 0$ since $e$ and $\epsilon_1 > 1$ but then $\epsilon_1 > e > 1$ since $e > 1$ which is in contradiction with the minimality of $\epsilon_1$. As a consequence, $\epsilon_1$ is a fundamental unit.*

**Exercise 2:**
Check the following table of fundamental units $\epsilon_1$ for $\mathbb{Q}(\sqrt{D})$:

| $D$ | 2 | 3 | 5 | 6 | 7 | 10 |
|---|---|---|---|---|---|---|
| $\epsilon_1$ | $1+\sqrt{2}$ | $2+\sqrt{3}$ | $(1+\sqrt{5})/2$ | $5+2\sqrt{6}$ | $8+3\sqrt{7}$ | $3+\sqrt{10}$ |

***Solution:***
*Noting that $2, 3, 6, 7, 10 \equiv 2, 3 \ mod 4$ and $5 \equiv 1 \ mod \ 4$.*
*To solve this exercise, thank to the previous exercise it is enough to show that all the $\epsilon_1$ satisfies $N_{K/\mathbb{Q}}(\epsilon_1) = \pm$ and are minimal $> 1$ as described before.*

**Exercise 3:**
Let $\zeta$ be a primitive $m$-root of unity, $p$ an odd prime. Show that

$$\mathbb{Z}[\zeta]^* = (\zeta)\mathbb{Z}[\zeta + \zeta^{-1}]^*$$

Show that

$$\mathbb{Z}[\zeta]* = \{\pm\zeta^k(1+\zeta)^n | 0 \leq k < 5, n \in \mathbb{Z}\}$$

if $p = 5$.

***Solution:***
*If we do assume, that we know that $\mathcal{O}_K = \mathbb{Z}[\zeta]$ (Proposition 10.2 up to proving it). Note that, $K_{\mathbb{R}} = \mathbb{Q}(\zeta + \zeta^{-1})$ , since clearly $\zeta + \zeta^{-1}$ is real and it has index 2 over $K$ because it satisfies the irreducible polynomial*

$$x^2 - (\zeta^{-1} + \zeta)x + 2 = 0$$

*And*

$$\mathcal{O}_{K_{\mathbb{R}}} = \mathcal{O}_K \cap K_{\mathbb{R}} = \mathbb{Z}[\zeta^{-1} + \zeta]$$

*So that*

$$\mathbb{Z}[\zeta^{-1} + \zeta]^* \subseteq \mathbb{Z}[\zeta]^*$$

*Now, the group of the roots of unity $\mu(K)$ of $K$ is clearly $(\zeta)$. So that $(\zeta)\mathbb{Z}[\zeta^{-1} + \zeta]^* \subseteq \mathbb{Z}[\zeta]^*$.*
*As a consequence, it is enough to prove that any $\epsilon \in \mathbb{Z}[\zeta]^*$, there exists a unit $\epsilon_1 \in \mathcal{O}_{K+}^*$ and an integer $r$ such that $\epsilon = \zeta^r \cdot \epsilon_1$.*

*Choose then $\epsilon$ as above and set $\alpha = \epsilon/\bar{\epsilon}$. Clearly, $\alpha$ is an algebraic integer with absolute value 1; also, all of its conjugates have absolute value 1, since they commute with conjugation.*
Claim: *An algebraic integer $\alpha$ whose Galois conjugates all have absolute value 1 must be a root of unity.*
Proof of the claim: *Say that the degree of $\alpha$ is $d$. Then each of its powers have degree no more than $d$. Let $f(x)$ be the minimal polynomial for a power of $\alpha$. Then the $i^{th}$ coefficient of $f$ is bounded by the binomial coefficient $\left(\begin{array}{c} i \\ d \end{array}\right)$ since all conjugates of $\alpha$ are bounded by 1. Therefore there are only finitely many such polynomials, ergo finitely many powers of $\alpha$.*
*The only roots of unity in $K$ are $\pm\zeta^a$, so $\epsilon/\bar{\epsilon} = \pm\zeta^a$ for some $a$. We will now show that $\pm = +$.*
*Assume that $\pm = -$. Since $\epsilon$ is an integer,*

$$\epsilon = b_0 + b_1\zeta + ... + b_{p-2}\zeta^{p-2} \equiv b_0 + b_1 + ... + b_{p-2} \ mod \ \zeta - 1$$

*Since $\bar{\epsilon} = b_0 + b_1\zeta^i + ..$, the same congruence is true for $\bar{\epsilon}$. therefore,*

$$\epsilon = -\zeta^a\bar{\epsilon} \equiv -\epsilon \ mod \ \zeta - 1$$

*and $2\epsilon \equiv 0 \ mod \ \zeta - 1$. But this is impossible because $\zeta - 1$ is relatively prime to 2 and $\epsilon$ is a unit.*
*Thus, we conclude that $\epsilon/\bar{\epsilon} = \zeta^a$. Letting $2r \equiv a \ mod \ p$ and $\epsilon_1 = \zeta^{-r}\epsilon$, we get $\epsilon = \zeta^r\epsilon_1$ and $\bar{\epsilon_1} = \epsilon_1$ so that $\epsilon_1 \in K_{\mathbb{R}}$.*

*For the case when $p = 5$; Recall that the Galois group $K/\mathbb{Q}$ is*

$$Gal(K/\mathbb{Q}) = \{\sigma : \zeta \mapsto \zeta^a, a \in (\mathbb{Z}/n\mathbb{Z})^\times\}$$

*Note that $K$ is a totally complex field, there is $r_1 = 0$ real embeddings of $K$ into $\mathbb{C}$ and $r_2 = (p-1)/2$ conjugate pairs of complex embeddings. Note that every $p^{th}$ root of unity not equal to 1 is primitive, so the embeddings $K \to \mathbb{C}$ are given by $\zeta \mapsto \zeta^a$ for $a = 1, .., p-1$. Clearly each of these is not a real embedding. Thus they are complex embedding and the result follows, since $deg(K/\mathbb{Q}) = r_1 + 2r_2$.*
*As $p | 2^{p-1} - 1$, so that $z^{2^{p-1}} = z$, $1 + \zeta \in \mathbb{Z}[\zeta]$ and*

$$N_{K/\mathbb{Q}}(1+\zeta) = \prod_{\sigma} \sigma(1+\zeta) = (1+z)...(1+z^{p-1}) = \frac{z^2-1}{z-1}...\frac{z^{2^{p-1}}-1}{z^{2^{p-2}}-1} = 1$$

*So that $1 + \zeta \in \mathcal{O}_K^*$.*
*Now, observe that $\zeta + \zeta^{-1}$, for $p = 5$, satisfies $\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$; and this can be rearranged to*

$$(\zeta + \zeta^{-1})^2 + (\zeta + \zeta^{-1}) - 1 = 0$$

*so that letting $\theta = \zeta + \zeta^{-1}$ we get:*

$$\theta^2 + \theta - 1 = 0$$

*As a consequence* $\theta = \frac{-1\pm\sqrt{5}}{2}$.
*But since* $\theta = e^{2i\pi/5} + e^{-2i\pi/5} = 2cos(2\pi/5) > 0$*, then* $\theta = \frac{-1+\sqrt{5}}{2}$.
*So that* $\mathbb{Q}(\sqrt{5}) = \mathbb{Q}(\zeta + \zeta^{-1})$ *is a subfield of* $K$ *and "the" fundamental unit for* $\mathbb{Q}(\sqrt{5})$ *is as shown earlier* $\eta = (1+\sqrt{5})/2$.
*Let* $u$ *a unit in* $\mathbb{Q}(\zeta)$ *then* $u\bar{u}$ *is a unit in* $\mathbb{Q}(\sqrt{5})$ *(where* $\bar{u}$ *is the complex conjugate of* $u$*). In fact* $u\bar{u}$ *is in* $K_{\mathbb{R}} = \mathbb{Q}(\sqrt{5})$*, since* $\overline{u\bar{u}} = u\bar{u}$ *and it is a unit. Note that* $(1+\zeta)(1+\zeta^{-1}) = 2 + \zeta + \zeta^{-1} = 2 + \frac{-1+\sqrt{5}}{2} = \frac{3+\sqrt{5}}{2} = \eta^2$.
*But now, if* $1+\zeta$ *is not a fundamental unit in* $K$ *then there is a fundamental unit in* $K$ *and an integer* $n$ *such that such that* $1+\zeta = u^n$*, and* $(u\bar{u})^n = \frac{3+\sqrt{5}}{2}$*. But, for* $n > 1$*, the* $\sqrt[n]{\frac{3+\sqrt{5}}{2}}$ *is not in* $\mathbb{Z}[(1+\sqrt{5})/2]$.

**Exercise 4:**
Let $\zeta$ be a primitive $m^{th}$ root of unity, $m \geq 3$. Show that the numbers $\frac{1-\zeta^k}{1-\zeta}$ for $(k,m) = 1$ are units in the ring of integers of the field $\mathbb{Q}(\zeta)$. The subgroup of the group of units they generate is called the group of **cyclotomic units**.

***Solution:***
*Since* $\frac{1-\zeta^k}{1-\zeta} = 1 + \zeta + \zeta^2 + ... + \zeta^{k-1} \in \mathbb{Z}[\zeta] = \mathcal{O}_K$*. Now, since* $(k,m) = 1$ *then there is a* $r \in \mathbb{Z}$ *such that* $kr \equiv 1 \bmod p$ *and then* $p|kr-1$ *so that* $\zeta^{kr} = \zeta$*. Then, the inverse*

$$\frac{1-\zeta}{1-\zeta^k} = \frac{1-\zeta^{kr}}{1-\zeta^k} = \frac{1-(\zeta^k)r}{1-\zeta^k} = 1 + \zeta^k + ... + (\zeta^k)^{r-1} \in \mathbb{Z}[\zeta] = \mathcal{O}_K$$

**Exercise 5:**
$\mathfrak{a}$ and  are ideals of $A$, then one has $\mathfrak{a} = \mathfrak{a}B \cap A$ and $\mathfrak{a}|\mathfrak{b} \Leftrightarrow \mathfrak{a}B|\mathfrak{b}B$.

***Solution:***
*We start by proving that* $\mathfrak{a}|\mathfrak{b} \Leftrightarrow \mathfrak{a}B|\mathfrak{b}B$.
*If* $\mathfrak{a}|\mathfrak{b}$ *then* $\mathfrak{b} \subseteq \mathfrak{a}B$*, so that* $\mathfrak{b}B \subseteq \mathfrak{a}B$.
*For the converse, first notice the following.*
*Let* $\mathfrak{a}$ *and* $\mathfrak{b}$ *be ideals of* $A$.
*We can write them uniquely as a product of coprime prime:*

$$\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$$

$$\mathfrak{b} = \prod_{i=1}^{l} \mathfrak{q}_i^{f_i}$$

*As a consequence, the unique factorization in prime for* $\mathfrak{a}B$ *and* $\mathfrak{b}B$*,*

$$\mathfrak{a}B = \prod_{i=1}^{r}(\prod_{j=1}^{r_i} \mathfrak{P}_{ij}^{e_{ij}})^{e_i}$$

$$\mathfrak{b}B = \prod_{i=1}^{l}(\prod_{j=1}^{l_i}\mathfrak{Q}_{ij}^{f_{ij}})^{f_i}$$

*Where the* $\mathfrak{P}_{ij}$ *of* $B$ *are the prime over* $\mathfrak{p}_i$ *and* $\mathfrak{Q}_{ij}$ *of* $B$ *are the prime over* $\mathfrak{q}_i$.
*So, that the only prime appearing in the factorization of* $\mathfrak{a}B$ *are the prime above the* $\mathfrak{p}_i$ *and of* $\mathfrak{b}B$ *are the prime above the* $\mathfrak{q}_i$.
*Now, suppose that* $\mathfrak{a}B|\mathfrak{b}B$. *So that all the* $\mathfrak{P}_{ij}$ *appear in the decomposition of* $\mathfrak{b}B$. *We first prove that the prime appearing in the decomposition of* $\mathfrak{a}$ *divide also* $\mathfrak{b}$. *Indeed, take one of the* $\mathfrak{p}_i$, *if* $\mathfrak{p}_i \nmid \mathfrak{b}$, *then* $\mathfrak{p}_i$ *is not one of the* $\mathfrak{q}_i$, *so that the* $\mathfrak{P}_{ij}$*'s over* $\mathfrak{p}_I$ *cannot appear in the decomposition of* $\mathfrak{b}B$, *and this contradict what we have just said above.*
*Now, we just have that* $e_i = v_{\mathfrak{a}}(\mathfrak{p}_i) \leq v_{\mathfrak{b}}(\mathfrak{p}_i)$. *For that we write*

$$\mathfrak{b} = \prod_{i=1}^{r}\mathfrak{p}_i^{f_i}\mathfrak{c}$$

*with* $(\mathfrak{c}, \mathfrak{p}_i) = 1$ *for any* $i$. *Then, we get:*

$$\mathfrak{b}B = \prod_{i=1}^{l}(\prod_{j=1}^{l_i}\mathfrak{P}_{ij}^{e_{ij}})^{f_i}(\mathfrak{c}B)$$

*And since* $\mathfrak{a}B|\mathfrak{b}B$, *and we are in Dedekind domain then*

$$e_{ij}e_i = v_{\mathfrak{a}B}(\mathfrak{P}_{ij}) \leq e_{ij}f_i = v_{\mathfrak{b}B}(\mathfrak{P}_{ij})$$

*So that,*

$$v_{\mathfrak{a}}(\mathfrak{p}_i) \leq v_{\mathfrak{b}}(\mathfrak{p}_i)$$

*as wanted.*
*And, we have just proved that,* $\mathfrak{a}|\mathfrak{b}$.
*Notice that then we have that* $\mathfrak{a} = \mathfrak{b}$ *if and only if* $\mathfrak{a}B = \mathfrak{b}B$. $(*)$
*Now, we prove that* $\mathfrak{a}B \cap A = \mathfrak{a}$. *Clearly,* $\mathfrak{a} \subseteq \mathfrak{a}B \cap A$, *for* $a \in \mathfrak{a}$ *then since* $1 \in B$, $a = a \cdot 1 \in \mathfrak{a}B$ *and* $a \in A$ *as in an ideal of* $A$, *so that* $a \in \mathfrak{a}B \cap A$.
*Noticing that* $(\mathfrak{a}B \cap A)B = \mathfrak{a}B$. *In fact,* $\mathfrak{a} \subseteq \mathfrak{a}B$ *and* $\mathfrak{a} \subseteq A$ *then* $\mathfrak{a}B \subseteq (\mathfrak{a}B \cap A)B$ *but now* $\mathfrak{a}B \cap A \subseteq \mathfrak{a}B$ *so we get the other inclusion. But using the previous remark* $(*)$, *we get exactly what we wanted.*

**Preliminary about flatness and Dedekind domain.**
An $A$-module $M$ is called flat (over $A$) if for every injective homomorphism of $A$-modules $N \to N'$, $N \otimes_A M \to N' \otimes_A M$ is injective.
Let $A$ be an integral domain and $M$ and $M$ an $A$-module. An element $x \in M$ is called torsion element if there is a non-zero $a \in A$ such that $ax = 0$. We call $M$ torsion free over $A$ if there is no nonzero torsion element in $M$. Here theorems about flatness easily found in the literature, good to know.
Let $A$ be a principal ideal domain. An $A$-module $M$ is flat if and only if it is torsion-free over $A$.
Let $M$ be an $A$-module. The following properties are equivalent:

1. $M$ is flat over $A$;
2. $M_\mathfrak{p}$ is flat over $A_\mathfrak{p}$ for every prime ideal $\mathfrak{p}$ of $A$;
3. $M_\mathfrak{m}$ is flat over $A_\mathfrak{m}$ for every maximal ideal $\mathfrak{m}$ of $A$;

Moreover, a Dedekind domain is a Noetherian integral domain $A$ whose localizations $A_\mathfrak{p}$ at the prime ideals $\mathfrak{p}$ are principal ideal domains.
Let $A$ be a Dedekind domain An $A$-module is flat if and only if it is torsion-free over $A$. In particular, every injective ring homomorphism $A \to B$ with $B$ an integral domain is flat.

**Exercise 5:**
$\mathfrak{a}$ and  are ideals of $A$, then one has $\mathfrak{a} = \mathfrak{a}B \cap A$ and $\mathfrak{a}|\mathfrak{b} \Leftrightarrow \mathfrak{a}B|\mathfrak{b}B$.

***Solution:***
*Recall that if $M$ is a $A$-module. Then $M = 0$ if and only if $M_\mathfrak{m} = 0$ for every maximal ideal $\mathfrak{m}$ of $A$.*
***Proof:*** *Let $x \in M$. Let us consider the ideal $I = \{a \in A | ax = 0\}$. If $I \neq A$, there exists a maximal ideal $\mathfrak{m}$ of $A$ such that $I \subseteq \mathfrak{m}$. As $M_\mathfrak{m} = 0$, there exists an $s \in A \backslash \mathfrak{m}$ such that $sx = 0$. Hence $s \in I$, which contradicts the assumption that $I \subseteq \mathfrak{m}$. Consequently, $I = A$ and $1 \in I$ and hence $x = 0$.*
*Recall also a very important lemma in commutative algebra: (Nakayama's lemma). Let $A$ be a local ring with maximal ideal $\mathfrak{m}$ and a finitely generated $A$-module such that $M = \mathfrak{m}$. Then $M = 0$.*
***Proof:*** *Let $\{x_1, ..., x_n\}$ be a system of generators of $M$. We may suppose $n$ minimal. There exist $\alpha_i \in \mathfrak{m}$ such that $x_n = \sum \alpha_i x_i$. Hence $(1 - \alpha_n)x_n = \sum_{i<n} \alpha_i x_i$. As $1 - \alpha_n$ is invertible, and $n$ is assumed to be minimal, it follows that $n = 1$ and $x_n = 0$.*

*Note that since $B$ is Dedekind, then for any $\mathfrak{p}$ (prime) maximal, we have proven that $\mathfrak{p}B \neq B$.*
*Claim: If $N$ is a finitely generated as $A$-module. we have that $B \otimes_A N = 0$ implies $N = 0$.*
*Indeed, from the first remark, we may assume that $A$ is local with maximal ideal $\mathfrak{m}$. By tonsuring with $k = A/\mathfrak{m}$, we obtain $M/\mathfrak{m}M \otimes_k N/\mathfrak{m}N = 0$. It follows that $N/\mathfrak{m}N = 0$. (Since now we have a tensor product of vector space, if we have a basis $\{e_i\}$ a base*

*of $M/\mathfrak{m}M$ and $\{f_i\}$ a base of $N/\mathfrak{m}N$ then $\{e_i \otimes f_j\}$ is a base on the tensor product). Hence $N = 0$, by Nakayama's Lemma.*
*Notice that $\mathfrak{a} \subseteq \mathfrak{a}B \cap A$, for $a \in \mathfrak{a}$ then since $1 \in B$, $a = a \cdot 1 \in \mathfrak{a}B$ and $a \in A$ as in an ideal of $A$, so that $a \in \mathfrak{a}B \cap A$. so that, the map $A/\mathfrak{a} \to B/\mathfrak{a}B$. Notice that $B/\mathfrak{a}B = B \otimes_A A/\mathfrak{a}$ is well define. Let $N$ to be the kernel of this map, then we get the exact sequence $1 \to N \to A/\mathfrak{a} \to B/\mathfrak{a}B$. Tensoring by $B$ over $A$, by flatness of $B$ over $A$ (since $A \to B$ is an injective ring homomorphism with $A$ Dedekind and $B$ an integral domain), we get the exact sequence $1 \to N \otimes_A B \to B/\mathfrak{a}B \to B/\mathfrak{a}B \otimes_A B$.*
*But, now $B/\mathfrak{a}B \to B/\mathfrak{a}B \otimes_A B$ is injective. (since now, $B/\mathfrak{a}B$ and $B$ are both $B$ module, if $y \otimes 1 = 0$ then $(y) \otimes (1) = 0$ and we can apply the claim since $(y)$ and $(1)$ are finitely generated, and find that $y = 0$).*
*So that $N \otimes_A B = 0$ and then $N$ equals $0$, which means that the first map is injective. As a consequence $\mathfrak{a}B \cap A = \mathfrak{a}$.*

*If $\mathfrak{a}|\mathfrak{b}$ then $\mathfrak{b} \subseteq \mathfrak{a}B$, so that $\mathfrak{b}B \subseteq \mathfrak{a}B$. Now, if $\mathfrak{b}B \subseteq \mathfrak{a}B$. Now, if $\mathfrak{b}B \subseteq \mathfrak{a}B$, then $\mathfrak{b}B \cap A \subseteq \mathfrak{a}B \cap A$, then $\mathfrak{b} \subseteq \mathfrak{a}$.*