[5] J. Milnor and D. Husemoller, *Symmetric Bilinear Forms*, Springer, Berlin–Heidelberg–New York 1974.
[6] O. T. O'Meara, *Introduction to Quadratic Forms*, Berlin–Göttingen–Heidelberg 1963.
[7] R. Perlis and K. Szymiczek, *Matching Witts with number fields*, Preprint, 1988.
[8] K. Szymiczek, *Matching Witts locally and globally*, Math. Slovaca (to appear).

INSTITUTE OF MATHEMATICS
SILESIAN UNIVERSITY
Bankowa 14, PL-40-007 Katowice, Poland

Received on 30.3.1989
and in revised form on 29.12.1989 (1920)

ACTA ARITHMETICA
LVIII.1 (1991)

Generalization of a theorem of Siegel

by

JONATHAN W. SANDS (Burlington, Vt.)

I. Introduction. The arithmetic of non-maximal orders in number fields has gained importance with the rise of computational number theory. Indeed it is a subtle problem to determine an integral basis for the maximal order and at times one would prefer to compute in a non-maximal order for which an integral basis is available. Yet references on the arithmetic of non-maximal orders in number fields are few. Dedekind's work [5] is still perhaps the most complete. We will present a modern formulation of some basic results as background, and then focus our interest on regulators. Our main result may then be viewed as an appendix (after Siegel) to Dedekind's monograph.

If $\mathcal{O}$ is an order contained in the maximal order $\mathcal{O}_K$ of a number field K, the regulator $R_{\mathcal{O}}$ is defined for $\mathcal{O}$ just as it is for $\mathcal{O}_K$, after replacing the unit group $\mathcal{O}_K^*$ by the smaller group $\mathcal{O}^*$. The primary goal of this paper is to obtain an effective upper bound on $R_{\mathcal{O}}$. Siegel [12] did this in the case of $\mathcal{O} = \mathcal{O}_K$ by proving an effective version of a result of Landau [7]. Our result builds on Siegel's by using a formula of Dedekind [5] to relate $R_{\mathcal{O}}$ to $R_K = R_{\mathcal{O}_K}$ and then applying a result of Robin [10] based on the method of Rosser–Schoenfeld [11].

The results of Siegel and Dedekind involve class numbers as well. Define the class group $Cl_{\mathcal{O}}$ of $\mathcal{O}$ to be the group of invertible fractional ideals of $\mathcal{O}$ modulo the group of nonzero principal fractional ideals of $\mathcal{O}$: $Cl_{\mathcal{O}} = I_{\mathcal{O}}/P_{\mathcal{O}}$. This group is finite [2], [5] of order $h_{\mathcal{O}}$, the class number of $\mathcal{O}$. Siegel [12] defines $g_K = 2^{r_1}h_K R_K/w_K$, where r_1 is the number of real embeddings of K and w_K is the order of the torsion subgroup of $\mathcal{O}_K^*$. Put $w_{\mathcal{O}}$ equal to the order of the torsion subgroup of $\mathcal{O}^*$, and furthermore put $t_{\mathcal{O}}$ equal to the order of the torsion subgroup of $I_{\mathcal{O}}$. Of course $t_{\mathcal{O}_K}$ equals 1, but in general we will see that $t_{\mathcal{O}}$ must only be finite. We generalize Siegel's definition by setting $g_{\mathcal{O}} = 2^{r_1}h_{\mathcal{O}}R_{\mathcal{O}}/w_{\mathcal{O}}t_{\mathcal{O}}$. This allows us to devise a new statement of Dedekind's formula.

THEOREM (Dedekind). $g_{\mathcal{O}} = g_{\mathcal{O}_K}$.

Research supported by NSF EPSCoR Grant R11-810679.

The definition of $t_{\mathcal{O}}$ is new, and we will present an updated proof of this result. It is worth noting the

COROLLARY (Dedekind). *h_K divides $h_{\mathcal{O}}$.*

Our main result is (see 5.4)

THEOREM. *Let M denote the index $(\mathcal{O}_K:\mathcal{O})$, $n>1$ the degree $[K:Q]$, and $d_{\mathcal{O}}$ the discriminant of $\mathcal{O}$. Then*

$$2^{r_1}h_{\mathcal{O}}R_{\mathcal{O}}/w_{\mathcal{O}} < 4\left(\frac{4}{n-1}\right)^{n-1}\sqrt{|d_{\mathcal{O}}|}(\log|d_{\mathcal{O}}|)^{n-1}(\log\log|d_{\mathcal{O}}|)^{n/2}.$$

Remark. Siegel's effective version of Landau's theorem implies that the inequality above holds without the factor $(\log\log|d_{\mathcal{O}}|)^{n/2}$ when $\mathcal{O}=\mathcal{O}_K$.

A related result of independent interest which we will prove (5.3) is the following.

PROPOSITION. *If $(\mathcal{O}_K:\mathcal{O})=M>1$ then $(\mathcal{O}_K^*:\mathcal{O}^*)<2M\log\log(3M^2)$.*

Thanks go to Johannes Buchmann for his question which led us to the latter theorem and ultimately to this work. I am also indebted to J. L. Nicolas and G. Robin for showing me how to apply their results, and to H. Zassenhaus who referred me to the work of Dedekind.

The remainder to the paper is organized as follows. Section II provides background on orders and introduces the group $\mathrm{Tor}(I_{\mathcal{O}})$. The conductor and its role are described in Section III. As Dedekind observed, ideals relatively prime to the conductor are well-behaved in passing between $\mathcal{O}$ and $\mathcal{O}_K$. Section IV concerns our adaptation of Dedekind's formula and related results. The bounds on regulators are obtained in Section V.

II. Orders. This section introduces the study of orders in algebraic number fields for our purposes. References [2] and [4] provide a deeper understanding through different points of view. For a more general approach emphasizing non-commutative orders, see [9].

We begin with some standard definitions which carefully extend those commonly used in the case of maximal orders. As in the introduction, fix an algebraic number field K, let $\mathcal{O}$ be an order of K (subring of rank $[K:Q]$ as a Z-module) and let $\mathcal{O}_K$ be the maximal order of K. Thus $\mathcal{O}$ may be described as a subring of $\mathcal{O}_K$ of finite index M. Hence the field of fractions of $\mathcal{O}$ is K. A fractional ideal of $\mathcal{O}$ is a finitely generated $\mathcal{O}$-submodule of K. An integral ideal (or just an ideal) of $\mathcal{O}$ is a fractional ideal contained in $\mathcal{O}$. The product $\mathfrak{ab}$ of two fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ of $\mathcal{O}$ is the smallest $\mathcal{O}$-submodule of K containing $\{\alpha\beta:\ \alpha\in\mathfrak{a},\beta\in\mathfrak{b}\}$. The quotient is $\mathfrak{a}\div\mathfrak{b}=\{\gamma\in K:\ \gamma\mathfrak{b}\in\mathfrak{a}\}$. A fractional ideal $\mathfrak{c}$ is called a *proper* fractional ideal of $\mathcal{O}$ if $\mathfrak{c}\div\mathfrak{c}=\mathcal{O}$. It is called *principal* if $\mathfrak{c}=\gamma\mathcal{O}$ for some γ in $\mathcal{O}$. The inverse of $\mathfrak{c}$ is $\mathfrak{c}^{-1}=\mathcal{O}\div\mathfrak{c}$. Then $\mathfrak{c}$ is called *invertible* in $\mathcal{O}$ if $\mathfrak{c}\mathfrak{c}^{-1}=\mathcal{O}$. It is immediate that a principal fractional

ideal of $\mathcal{O}$ is inverlible. One also finds that if $\mathfrak{a}$ and $\mathfrak{b}$ are fractional ideals of $\mathcal{O}$ such that $\mathfrak{ab}=\mathcal{O}$, then $\mathfrak{a}$ is invertible and $\mathfrak{a}^{-1}=\mathfrak{b}$.

LEMMA 2.1. *If $\mathfrak{a}$ and $\mathfrak{b}$ are nonzero fractional ideals of $\mathcal{O}$ with $\mathfrak{b}$ invertible, then $\mathfrak{a}\div\mathfrak{b}=\mathfrak{ab}^{-1}$.*

Proof. Let $\gamma\in\mathfrak{a}\div\mathfrak{b}$; then $\gamma\mathfrak{b}\subset\mathfrak{a}$. Multiplying by $\mathfrak{b}^{-1}$ gives $\gamma\mathcal{O}=\gamma\mathfrak{b}\mathfrak{b}^{-1}\subset\mathfrak{ab}^{-1}$. So $\gamma\in\mathfrak{ab}^{-1}$ and $\mathfrak{a}\div\mathfrak{b}\subset\mathfrak{ab}^{-1}$. The reverse inclusion is clear.

COROLLARY 2.2. *An invertible fractional ideal of $\mathcal{O}$ is proper.*

Proof. Suppose $\mathfrak{c}$ is invertible. By the lemma and the definition of invertible, $\mathfrak{c}\div\mathfrak{c}=\mathfrak{c}\mathfrak{c}^{-1}=\mathcal{O}$. Thus $\mathfrak{c}$ is proper.

Fundamental to our study are the following objects. The fact that they are *groups* is easily checked.

$I_{\mathcal{O}}$ is the group of all invertible fractional ideals of $\mathcal{O}$ under multiplication.

$P_{\mathcal{O}}$ is the subgroup of all principal fractional ideals.

$Cl_{\mathcal{O}}=I_{\mathcal{O}}/P_{\mathcal{O}}$ is what we will call the *ideal class group* of $\mathcal{O}$. It is isomorphic to what has been called the "locally free class group" of $\mathcal{O}$ [9]. This is a finite group [2, p. 128] of order $h_{\mathcal{O}}$, which we will call the *class number* of $\mathcal{O}$.

$\mathcal{O}^*$ is the group of units of $\mathcal{O}$.

Whenever a subscript of $\mathcal{O}_K$ arises, we will simply use the subscript K. For example, Cl_K denotes the ideal class group of K, rather than $Cl_{\mathcal{O}_K}$.

Although it is true whenever K is an imaginary quadratic field [8, p. 90] the converse of the previous corollary does not hold in general: a proper ideal need not be invertible.

EXAMPLE 2.3 [4, p. 45]. Let θ be an algebraic integer of degree $n>2$, $K=Q(\theta)$, $\mathcal{O}=Z+2Z[\theta]$, and $\mathfrak{a}=Z+Z\theta+2Z[\theta]$. Then $\mathfrak{a}$ is a proper fractional ideal of $\mathcal{O}$ and $\mathfrak{a}^{n-1}=Z[\theta]$. Hence $\mathfrak{a}$ is not an invertible fractional ideal of $\mathcal{O}$, because $Z[\theta]$ clearly is not. The fact that $\mathfrak{a}^{n-1}$ is not even a proper fractional ideal of $\mathcal{O}$ shows that the proper fractional ideals of $\mathcal{O}$ do not form a group. This is a major reason for our restricting attention to invertible ideals.

Concerning the structure of $\mathcal{O}$, it is noetherian by virtue of the fact that it is a finitely generated Z-module. It is not integrally closed unless $\mathcal{O}=\mathcal{O}_K$, so is not a Dedekind domain, but is still of Krull dimension one.

PROPOSITION 2.4. *Every nonzero ideal in $\mathcal{O}$ is of finite index, and every nonzero prime ideal is maximal.*

Proof. A nonzero ideal contains a nonzero principal ideal, which necessarily has the same Z-rank as $\mathcal{O}$ itself. Hence the index of both ideals is finite. A prime ideal of finite index is maximal because a finite integral is a field.

Of central interest to us is the order of the group $\mathcal{O}_K^*/\mathcal{O}^*$. This will be considered extensively in Section V. We begin here with the following simple observation.

LEMMA 2.5. *$\mathcal{O}_K^*/\mathcal{O}^*$ is a finite group.*

Proof. $\mathcal{O}_K^*/\mathcal{O}^*$ is a quotient of $\mathcal{O}_K^*/(\mathcal{O}_K^* \cap (1+M\mathcal{O}_K))$, which injects into the finite group $(\mathcal{O}_K/M\mathcal{O}_K)^*$. (Recall that M is the index of $\mathcal{O}$ in $\mathcal{O}_K$.)

Now we can provide an alternative description of the group $\mathrm{Tor}(I_\mathcal{O})$. Further analysis of its order will be found in Section III.

Let $\sim: I_\mathcal{O} \to I_K$ be the homomorphism obtained by extension of fractional ideals: $\sim(\mathfrak{a}) = \tilde{\mathfrak{a}} = \mathfrak{a}\mathcal{O}_K$. Let $\ker(\sim)$ be its kernel.

PROPOSITION 2.6. *$\mathrm{Tor}(I_\mathcal{O}) = \ker(\sim)$, and is a finite group.*

Proof. $\sim(\mathrm{Tor}(I_\mathcal{O})) \subset \mathrm{Tor}(I_K) = \{\mathcal{O}_K\}$. Hence $\mathrm{Tor}(I_\mathcal{O}) \subset \ker(\sim)$. Conversely, suppose $\mathfrak{a} \in \ker(\sim)$, so $\mathfrak{a}\mathcal{O}_K = \mathcal{O}_K$. Then $\mathfrak{a}^h = \gamma\mathcal{O}$ is principal and $\gamma\mathcal{O}_K = \mathcal{O}_K$, so $\gamma \in \mathcal{O}_K^*$. By the preceeding lemma, we can choose r such that $\gamma^r \in \mathcal{O}^*$. Finally $\mathfrak{a}^{hr} = \gamma^r\mathcal{O} = \mathcal{O}$, demonstrating that $\mathfrak{a} \in \mathrm{Tor}(I_\mathcal{O})$.

To see that $\ker(\sim)$ is finite, observe that if $\mathfrak{a} \in \ker(\sim)$ then $\mathcal{O}_K = \mathfrak{a}\mathcal{O}_K \supset \mathfrak{a} = \mathfrak{a}\mathcal{O} \supset \mathfrak{a}M\mathcal{O}_K = M\mathfrak{a}\mathcal{O}_K = M\mathcal{O}_K$. Then $\mathfrak{a}$ is one of the finitely many subgroups of $\mathcal{O}_K$ which contain the subgroup $M\mathcal{O}_K$.

III. The conductor

DEFINITION. The *conductor* of $\mathcal{O}$ in $\mathcal{O}_K$ is $\mathfrak{f} = \mathcal{O} \div \mathcal{O}_K$.

Observe that $\mathfrak{f}$ is the largest ideal of $\mathcal{O}$ which is also an ideal of $\mathcal{O}_K$, and $\mathfrak{f} \supset M\mathcal{O}_K$.

Two ideals $\mathfrak{a}$ and $\mathfrak{m}$ of $\mathcal{O}$ are called *relatively prime* if $\mathfrak{a}+\mathfrak{m} = \mathcal{O}$, where $\mathfrak{a}+\mathfrak{m}$ is the smallest ideal of $\mathcal{O}$ containing $\mathfrak{a}$ and $\mathfrak{m}$. In this situation, one has the Chinese Remainder Theorem: $\mathcal{O}/\mathfrak{a}\mathfrak{m} \cong \mathcal{O}/\mathfrak{a} \oplus \mathcal{O}/\mathfrak{m}$. We say that an invertible fractional ideal $\mathfrak{c}$ of $\mathcal{O}$ is *prime* to $\mathfrak{m}$ if $\mathfrak{c} = \mathfrak{a}\mathfrak{b}^{-1}$ with $\mathfrak{a}$ and $\mathfrak{b}$ invertible integral ideals of $\mathcal{O}$ which are relatively prime to $\mathfrak{m}$.

Note that the integral ideals of $\mathcal{O}$ prime to $\mathfrak{f}$ form a monoid (set closed under associative binary operation with identity). The next theorem also appears in [8, pp. 92, 94].

THEOREM 3.1 (Dedekind). *There is a multiplicative bijection given by extension and contraction of ideals between the monoid of ideals of $\mathcal{O}$ which are relatively prime to $\mathfrak{f}$ and the monoid of ideals of $\mathcal{O}_K$ which are relatively prime to $\mathfrak{f}$.*

Proof. Multiplicativity of the extension map is clear. First, assume that $\mathfrak{a}$ is an ideal of $\mathcal{O}$ and prime to $\mathfrak{f}$. Then $\mathfrak{a}\mathcal{O}_K$ is prime to $\mathfrak{f}$ in $\mathcal{O}_K$. We show that $(\mathfrak{a}\mathcal{O}_K) \cap \mathcal{O} = \mathfrak{a}$.

$$(\mathfrak{a}\mathcal{O}_K) \cap \mathcal{O} = [(\mathfrak{a}\mathcal{O}_K) \cap \mathcal{O}]\mathcal{O} = [(\mathfrak{a}\mathcal{O}_K) \cap \mathcal{O}](\mathfrak{a}+\mathfrak{f}) \subset \mathcal{O}\mathfrak{a} + \mathfrak{a}\mathcal{O}_K\mathfrak{f}$$
$$= \mathfrak{a} + \mathfrak{a}\mathfrak{f} \subset \mathfrak{a} + \mathfrak{a}\mathcal{O} = \mathfrak{a} + \mathfrak{a} = \mathfrak{a}.$$

This completes one inclusion, and the reverse inclusion is clear.

Second, assume that $\mathfrak{A}$ is an ideal of $\mathcal{O}_K$ and prime to $\mathfrak{f}$. Then $\mathcal{O} = \mathcal{O}_K \cap \mathcal{O} = (\mathfrak{A}+\mathfrak{f}) \cap \mathcal{O} \subset (\mathfrak{A} \cap \mathcal{O}) + \mathfrak{f} \subset \mathcal{O}$, so $\mathfrak{A} \cap \mathcal{O}$ is indeed prime to $\mathfrak{f}$ in $\mathcal{O}$.

We now show that $(\mathfrak{A} \cap \mathcal{O})\mathcal{O}_K = \mathfrak{A}$.

$$\mathfrak{A} = \mathfrak{A}[(\mathfrak{A} \cap \mathcal{O}) + \mathfrak{f}] \subset \mathcal{O}_K(\mathfrak{A} \cap \mathcal{O}) + \mathfrak{A}\mathfrak{f} \subset \mathcal{O}_K(\mathfrak{A} \cap \mathcal{O}) + (\mathfrak{A} \cap \mathfrak{f})$$
$$\subset \mathcal{O}_K(\mathfrak{A} \cap \mathcal{O}) + (\mathfrak{A} \cap \mathcal{O}) \subset \mathcal{O}_K(\mathfrak{A} \cap \mathcal{O}).$$

Again this proves one inclusion, and the reverse is easy.

COROLLARY 3.2. *Suppose $\gamma \in \mathcal{O}$ and $\gamma\mathcal{O}$ is prime to $\mathfrak{f}$. Then $(\gamma\mathcal{O}_K) \cap \mathcal{O} = \gamma\mathcal{O}$.*

Proof. Apply 3.1 to the ideal $\gamma\mathcal{O}$.

COROLLARY 3.3. *An integral ideal $\mathfrak{a}$ of $\mathcal{O}$ which is prime to $\mathfrak{f}$ is invertible.*

Proof. Let $\mathfrak{A} = \mathfrak{a}\mathcal{O}_K$, so $\mathfrak{A}$ is prime to $\mathfrak{f}$ in $\mathcal{O}_K$ by the theorem. $\mathfrak{A}^{hK}$ is principal in $\mathcal{O}_K$ and since $(\mathcal{O}_K/\mathfrak{f})^*$ is finite, we can choose a positive integer r so that $\mathfrak{A}^{hKr} = \gamma\mathcal{O}_K$ with $\gamma \in 1+\mathfrak{f} \subset \mathcal{O}$. Evidently $\gamma\mathcal{O}+\mathfrak{f} = \mathcal{O}$, so by the lemma, $\gamma\mathcal{O}_K \cap \mathcal{O} = \gamma\mathcal{O}$. Then by the theorem, $\mathfrak{A}^{hKr} \cap \mathcal{O} = \mathfrak{a}^{hKr}$. Hence $\mathfrak{a}^{hKr} = \gamma\mathcal{O}$ and $\mathfrak{a}^{hKr}\gamma^{-1} = \mathcal{O}$. It is now clear that the fractional $\mathcal{O}$-ideal $\mathfrak{a}^{hKr-1}\gamma^{-1}$ is the inverse of $\mathfrak{a}$.

In the other extreme, we will need to consider ideals which contain $\mathfrak{f}$ as we begin to study $\mathrm{Tor}(I_\mathcal{O})$.

LEMMA 3.4. *If $\mathfrak{b}$ is a fractional ideal of $\mathcal{O}$ and $\mathfrak{b} \subset \mathcal{O}_K$ then $\mathfrak{b}^{-1} \supset \mathfrak{f}$.*

Proof. $\mathfrak{b}\mathfrak{f} \subset \mathcal{O}_K\mathfrak{f} = \mathfrak{f} \subset \mathcal{O}$.

LEMMA 3.5. *If $\mathfrak{a} \in \mathrm{Tor}(I_\mathcal{O})$ then $\mathfrak{f} \subset \mathfrak{a} \subset \mathcal{O}_K$.*

Proof. Since $\mathrm{Tor}(I_\mathcal{O}) = \ker(\sim)$ by 2.6, $\mathfrak{a}\mathcal{O}_K = \mathcal{O}_K$ and $\mathfrak{a} \subset \mathcal{O}_K$. Likewise $\mathfrak{b} = \mathfrak{a}^{-1} \subset \mathcal{O}_K$, and we apply the lemma.

The following proof is based on [4, p. 49].

PROPOSITION 3.6. *If $\mathfrak{a} \in \mathrm{Tor}(I_\mathcal{O})$ then $\mathfrak{a} = \alpha\mathcal{O}+\mathfrak{f}$ for some $\alpha \in \mathcal{O}_K$ such that $\alpha\mathcal{O}_K+\mathfrak{f} = \mathcal{O}_K$.*

Proof. Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ be the maximal ideals of $\mathcal{O}$ containing $\mathfrak{f}$, and let $\mathfrak{b} = \mathfrak{a}^{-1}$. By 3.5, both $\mathfrak{a}$ and $\mathfrak{b}$ lie between $\mathfrak{f}$ and $\mathcal{O}_K$. For each i, $1 \leqslant i \leqslant n$, choose $\alpha_i \in \mathfrak{a}$ and $\beta_i \in \mathfrak{b}$ so that $\alpha_i\beta_i \notin \mathfrak{m}_i$. Since the $\mathfrak{m}_i$ are relatively prime, we can also apply the Chinese Remainder Theorem to choose an element $\varepsilon_i \in \mathcal{O}$ for each i such that $\varepsilon_i \equiv 1\ (\mathfrak{m}_i)$, and $\varepsilon_i \equiv 0\ (\mathfrak{m}_j)$ for $j \neq i$. Put $\alpha = \sum_1^n \alpha_i\varepsilon_i \in \mathfrak{a}$ and $\beta = \sum_1^n \beta_i\varepsilon_i \in \mathfrak{b}$. Then since $\alpha_i\beta_j \in \mathcal{O}$ for each i and j, we have $\alpha\beta = \sum_{i,j} \alpha_i\beta_j\varepsilon_i\varepsilon_j \equiv \alpha_k\beta_k \not\equiv 0\ (\mathfrak{m}_k)$, for each k. Hence $\alpha\beta \in \mathcal{O}$ and $\mathfrak{f}$ are relatively prime. This implies that $\alpha\beta$ and $\mathfrak{f}^2$ are relatively prime. So $\mathcal{O} = \mathfrak{a}\mathfrak{b} \supset (\alpha\mathcal{O}+\mathfrak{f})(\beta\mathcal{O}+\mathfrak{f}) \supset \alpha\beta\mathcal{O}+\mathfrak{f}^2 = \mathcal{O}$. Finally, $(\alpha\mathcal{O}+\mathfrak{f})(\beta\mathcal{O}+\mathfrak{f}) = \mathcal{O}$ implies that $\mathfrak{a} \supset \alpha\mathcal{O}+\mathfrak{f} = (\beta\mathcal{O}+\mathfrak{f})^{-1} \supset \mathfrak{b}^{-1} = \mathfrak{a}$. The remaining assertions of the theorem are clear.

Now we can compute the order of $\mathrm{Tor}(I_\mathcal{O})$. Let $\Phi_K(\mathfrak{f})$ denote the order of the multiplicative group $(\mathcal{O}_K/\mathfrak{f})^*$ and $\Phi_\mathcal{O}(\mathfrak{f})$ denote the order of $(\mathcal{O}/\mathfrak{f})^*$.

THEOREM 3.7. *The order of* $\mathrm{Tor}(I_\mathfrak{o})$ *is* $t_\mathfrak{o} = |\mathrm{Tor}(I_\mathfrak{o})| = \Phi_K(\mathfrak{f})/\Phi_\mathfrak{o}(\mathfrak{f})$.

Proof. If $\alpha \in \mathcal{O}_K$ represents an element of $(\mathcal{O}_K/\mathfrak{f})^*$, then there exists $\beta \in \mathcal{O}_K$ representing its inverse, so $\alpha\beta \equiv 1 \bmod \mathfrak{f}$ and $\alpha\beta$ is relatively prime to $\mathfrak{f}$ *in* $\mathcal{O}$. As above, we then have $(\alpha\mathcal{O}+\mathfrak{f})(\beta\mathcal{O}+\mathfrak{f}) = \mathcal{O}$, which shows that $(\alpha\mathcal{O}+\mathfrak{f})$ is invertible. Furthermore, it is clearly an element of $\ker(\sim) = \mathrm{Tor}(I_\mathfrak{o})$. Hence we can define a map $(\mathcal{O}_K/\mathfrak{f})^* \to \mathrm{Tor}(I_\mathfrak{o})$ by $\alpha \bmod \mathfrak{f} \mapsto \alpha\mathcal{O}+\mathfrak{f}$. To see that it is multiplicative, we must check that $(\alpha\mathcal{O}+\mathfrak{f})(\gamma\mathcal{O}+\mathfrak{f}) = \alpha\gamma\mathcal{O}+\mathfrak{f}$ when $\gamma\mathcal{O}_K+\mathfrak{f} = \mathcal{O}_K$. Note that $(\alpha\mathcal{O}+\mathfrak{f})(\gamma\mathcal{O}+\mathfrak{f})$ is in $\mathrm{Tor}(I_\mathfrak{o})$, being the product of two elements in this group. Hence it must contain $\mathfrak{f}$, by 3.6, and the equality is clear. Proposition 3.6 shows that this map is onto, and its kernel is clearly $(\mathcal{O}/\mathfrak{f})^* \subset (\mathcal{O}_K/\mathfrak{f})^*$. In other words, we have an exact sequence

$$1 \to (\mathcal{O}/\mathfrak{f})^* \to (\mathcal{O}_K/\mathfrak{f})^* \to \mathrm{Tor}(I_\mathfrak{o}) \to 1.$$

As a consequence, we have a bound on the unit index $(\mathcal{O}_K^*:\mathcal{O}^*)$.

COROLLARY 3.8. $(\mathcal{O}_K^*:\mathcal{O}^*)$ *is the order of* $P_\mathfrak{o} \cap \mathrm{Tor}(I_\mathfrak{o})$ *and hence divides the integer* $\Phi_K(\mathfrak{f})/\Phi_\mathfrak{o}(\mathfrak{f})$.

Proof. The group $\mathcal{O}_K^*$ clearly maps onto the subgroup $P_\mathfrak{o} \cap \ker(\sim) = P_\mathfrak{o} \cap \mathrm{Tor}(I_\mathfrak{o})$ of $\mathrm{Tor}(I_\mathfrak{o})$ with kernel $\mathcal{O}^*$, by $\varepsilon \mapsto \varepsilon\mathcal{O}$.

Further development of this bound will be taken up in Section V.

IV. Ideal class groups. To compute the order of $Cl_\mathfrak{o}$ we will pass to modified class groups, working with fractional ideals which are relatively prime to the conductor. Then we can make use of the one-to-one correspondence of 3.1. Hence we consider the following groups.

$I_\mathfrak{o}(\mathfrak{f}) \subset I_\mathfrak{o}$ is the group of invertible fractional ideals of $\mathcal{O}$ which are relatively prime to $\mathfrak{f}$.

$P_\mathfrak{o}(\mathfrak{f}) = P \cap I_\mathfrak{o}(\mathfrak{f})$ is the subgroup of nonzero principal ideals of $\mathcal{O}$ which are relatively prime to $\mathfrak{f}$.

Our task is to compare $I_\mathfrak{o}(\mathfrak{f})/P_\mathfrak{o}(\mathfrak{f})$ with $Cl_\mathfrak{o}$.

LEMMA 4.1. $I_\mathfrak{o} = I_\mathfrak{o}(\mathfrak{f}) \cdot P_\mathfrak{o} \cdot \mathrm{Tor}(I_\mathfrak{o})$.

Proof. Suppose $\mathfrak{a} \in I_\mathfrak{o}$; $\tilde{\mathfrak{a}} = \mathfrak{a}\mathcal{O}_K$ is its extension to $\mathcal{O}_K$. Choose an integral ideal $\tilde{\mathfrak{b}}$ which is relatively prime to $\mathfrak{f}$ and represents the same class as $\tilde{\mathfrak{a}}$ in Cl_K. Then $\tilde{\mathfrak{b}}$ is indeed the extension of $\mathfrak{b} = \tilde{\mathfrak{b}} \cap \mathcal{O}$, by 3.1. We have $\tilde{\mathfrak{a}} = \tilde{\mathfrak{b}}\gamma$, for some γ in K. Also, $\mathfrak{b}$ is relatively prime to $\mathfrak{f}$, and therefore invertible by 3.3. Putting $\mathfrak{c} = (1/\gamma)\mathfrak{a}\mathfrak{b}^{-1}$, we have $\tilde{\mathfrak{c}} = \mathcal{O}_K$, so that $\mathfrak{c} \in \ker(\sim) = \mathrm{Tor}(I_\mathfrak{o})$. Finally, $\mathfrak{a} = \mathfrak{b}\gamma\mathfrak{c}$, which shows that $\mathfrak{a} \in I_\mathfrak{o}(\mathfrak{f}) \cdot P_\mathfrak{o} \cdot \mathrm{Tor}(I_\mathfrak{o})$.

Our study of $\mathrm{Tor}(I_\mathfrak{o})$ in Section III allows us to simplify the result of 4.1 in the following key lemma.

LEMMA 4.2. $\mathrm{Tor}(I_\mathfrak{o}) \subset I_\mathfrak{o}(\mathfrak{f}) \cdot P_\mathfrak{o}$.

Proof. If $\mathfrak{a} \in \mathrm{Tor}(I_\mathfrak{o})$ then by 3.6, $\mathfrak{a} = \alpha\mathcal{O}+\mathfrak{f}$ and $\mathfrak{a}^{-1} = \beta\mathcal{O}+\mathfrak{f}$ with α and β in $\mathcal{O}_K$, and $\alpha\beta$ relatively prime to $\mathfrak{f}$ *in* $\mathcal{O}$. Writing $\mathfrak{a} = \alpha(\alpha\beta\mathcal{O}+\alpha\mathfrak{f})^{-1}$, we see that it suffices to show that $\alpha\beta\mathcal{O}+\alpha\mathfrak{f}$ is relatively prime to $\mathfrak{f}$. First of all, it is *integral* because $\alpha\beta \in \mathcal{O}$ and $\alpha\mathfrak{f} \subset \mathcal{O}_K\mathfrak{f} = \mathfrak{f} \subset \mathcal{O}$. Second, it is relatively prime to $\mathfrak{f}$ because $\alpha\beta\mathcal{O}$ is. This completes the proof.

A version of the following proposition has been proved more generally for non-commutative orders by Jacobinski [6].

PROPOSITION 4.3. $I_\mathfrak{o}(\mathfrak{f})/P_\mathfrak{o}(\mathfrak{f}) \cong Cl_\mathfrak{o}$.

Proof. Combining the two lemmas of this section, we have $I_\mathfrak{o} = I_\mathfrak{o}(\mathfrak{f}) \cdot P_\mathfrak{o}$. Hence

$$Cl_\mathfrak{o} = I_\mathfrak{o}/P_\mathfrak{o} = I_\mathfrak{o}(\mathfrak{f}) \cdot P_\mathfrak{o}/P_\mathfrak{o} \cong I_\mathfrak{o}(\mathfrak{f})/(I_\mathfrak{o}(\mathfrak{f}) \cap P_\mathfrak{o}) = I_\mathfrak{o}(\mathfrak{f})/P_\mathfrak{o}(\mathfrak{f}).$$

Now we come to the formula which was actually obtained by Dedekind. (See also [1, Section 13].)

THEOREM 4.4 (Dedekind). $h_\mathfrak{o} = h_K(\Phi_K(\mathfrak{f})/\Phi_\mathfrak{o}(\mathfrak{f}))/(\mathcal{O}_K^*:\mathcal{O}^*)$.

Proof. The proof consists in checking the exactness of the sequence

$$1 \to \mathrm{Tor}(I_\mathfrak{o}) \cdot P_\mathfrak{o}/P_\mathfrak{o} \xrightarrow{\iota} I_\mathfrak{o}(\mathfrak{f}) \cdot P_\mathfrak{o}/P_\mathfrak{o} \xrightarrow{\varepsilon} I_K(\mathfrak{f}) \cdot P_K/P_K \to 1,$$

where ε is induced by extension of fractional ideals. The first nontrivial group in the sequence is isomorphic to $\mathrm{Tor}(I_\mathfrak{o})/(\mathrm{Tor}(I_\mathfrak{o}) \cap P_\mathfrak{o})$, whose order is $(\Phi_K(\mathfrak{f})/\Phi_\mathfrak{o}(\mathfrak{f}))/(\mathcal{O}_K^*:\mathcal{O}^*)$, by 3.6 and 3.7. The second nontrivial group is isomorphic to $I_\mathfrak{o}(\mathfrak{f})/(I_\mathfrak{o}(\mathfrak{f}) \cap P_\mathfrak{o}) = I_\mathfrak{o}(\mathfrak{f})/P_\mathfrak{o}(\mathfrak{f})$, whose order is $h_\mathfrak{o}$, by 4.3. Likewise, the final nontrivial group in the sequence has order h_K. Therefore the result will follow once exactness is established.

Exactness on the left: The homomorphism ι is simply an inclusion. Notice that this is possible by 4.2.

Exactness in the middle: That $\mathrm{im}(\iota) \subset \ker(\varepsilon)$ is obvious. Suppose then that $\mathfrak{a} \in I_\mathfrak{o}(\mathfrak{f}) \cdot P_\mathfrak{o}$ represents an element of $\ker(\varepsilon)$. Then $\mathfrak{a}\mathcal{O}_K = \gamma\mathcal{O}_K$ for some γ in K, and $\mathfrak{a}\gamma^{-1}\mathcal{O}_K = \mathcal{O}_K$. Putting $\mathfrak{c} = \mathfrak{a}\gamma^{-1}\mathcal{O}$, we have $\mathfrak{c} \in \mathrm{Tor}(I_\mathfrak{o})$ and $\mathfrak{a} = \mathfrak{c}\gamma\mathcal{O} \in \mathrm{Tor}(I_\mathfrak{o}) \cdot P_\mathfrak{o}$. This show that $\mathfrak{a} \in \mathrm{im}(\iota)$.

Exactness on the right: Suppose $\mathfrak{C}\gamma\mathcal{O}_K$ represents an element of $I_K(\mathfrak{f}) \cdot P_K/P_K$. By definition, $\mathfrak{C} = \mathfrak{A}\mathfrak{B}^{-1}$ with $\mathfrak{A}$ and $\mathfrak{B}$ integral and relatively prime to $\mathfrak{f}$. Hence $\mathfrak{A} = \mathfrak{a}\mathcal{O}_K$ and $\mathfrak{B} = \mathfrak{b}\mathcal{O}_K$ for some $\mathfrak{a}$ and $\mathfrak{b}$ integral and relatively prime to $\mathfrak{f}$ in $\mathcal{O}$, according to 3.1. $\mathfrak{a}$ and $\mathfrak{b}$ are invertible by 3.3, so $\mathfrak{a}\mathfrak{b}^{-1} \in I_\mathfrak{o}(\mathfrak{f})$. Clearly $\mathfrak{C}\gamma\mathcal{O}_K$ is the image under ε of the element represented by $\mathfrak{a}\mathfrak{b}^{-1}\gamma\mathcal{O}$. Hence ε is surjective and the proof is complete.

COROLLARY 4.5. h_K *divides* $h_\mathfrak{o}$.

Proof. 4.4 and 3.8.

Before formally stating the theorem of the introduction, we note that the regulator $R_{\mathcal{O}}$ of the order $\mathcal{O}$ is defined as

$$R_{\mathcal{O}} = \det_{1 \leqslant i,j \leqslant r} (\log \|\varepsilon_i^{(j)}\|),$$

where ε_i for $1 \leqslant i \leqslant r$ form a maximal system of independent units of $\mathcal{O}$, the $\varepsilon_i^{(j)}$ are their images under nonconjugate embeddings of K in $\boldsymbol{C}$, and $\| \ \|$ denotes the absolute value or its square, depending on whether the embedding is real or complex. Again, $w_{\mathcal{O}} = |\mathrm{Tor}(\mathcal{O}^*)|$ and $g_{\mathcal{O}} = 2^{r_1} h_{\mathcal{O}} R_{\mathcal{O}} / w_{\mathcal{O}} t_{\mathcal{O}}$, r_1 being the number of real embeddings of K.

COROLLARY 4.6. $g_{\mathcal{O}} = g_K$.

Proof. Since $R_{\mathcal{O}}/R_K = (\mathcal{O}_K^* : \mathcal{O}^*)/(w_K/w_{\mathcal{O}})$ and $t_K = 1$, this follows immediately from 4.4.

V. Regulator bounds. Since $2^{r_1} h_{\mathcal{O}} R_{\mathcal{O}} / w_{\mathcal{O}} = t_{\mathcal{O}} g_{\mathcal{O}} = t_{\mathcal{O}} g_K$, we will combine Siegel's bound on g_K with a bound on $t_{\mathcal{O}}$. It is also possible to define the zeta-function of $\mathcal{O}$ and determine its analytic continuation, functional equation and residue at $s = 1$ by Hecke's second method. Then one can rederive Siegel's bound and a generalization. However, the same factor $t_{\mathcal{O}}$ intervenes and the result is the same.

For positive integers N, define the Dedekind function $\psi(N)$ by

$$\psi(N)/N = \prod_{p|N} (1 + 1/p).$$

The product is taken over all primes p dividing N. Recall that $M = (\mathcal{O}_K : \mathcal{O}) \in \mathfrak{f}$ and $n = [K : \boldsymbol{Q}]$.

PROPOSITION 5.1. $t_{\mathcal{O}} \leqslant M (\psi(M)/M)^{n/2}$.

Proof. For $\mathfrak{a}$ a nonzero integral ideal of $\mathcal{O}$, let $N_{\mathcal{O}}(\mathfrak{a}) = (\mathcal{O} : \mathfrak{a})$, and let $N_K = N_{\mathcal{O}_K}$. Let $\mathfrak{P}^{r(\mathfrak{P})}$ be the prime powers in the factorization of $\mathfrak{f}$ in $\mathcal{O}_K$ and let $N_K(\mathfrak{P}) = p^{f(\mathfrak{P})}$. Then the $\mathfrak{P} \cap \mathcal{O}$ are prime ideals in $\mathcal{O}$, so are coprime in pairs by 2.4, when they are distinct. Thus the ideals $(\mathfrak{P} \cap \mathcal{O})^{r(\mathfrak{P})}$ are coprime in pairs, and the same goes for the larger ideals $\mathfrak{P}^{r(\mathfrak{P})} \cap \mathcal{O}$. The intersection of these latter ideals in $\mathcal{O}$ is $\mathfrak{f}$, so that $\mathcal{O}/\mathfrak{f}$ is isomorphic to the product of the $\mathcal{O}/(\mathfrak{P}^{r(\mathfrak{P})} \cap \mathcal{O})$, by the Chinese Remainder Theorem, and $(\mathcal{O}/\mathfrak{f})^*$ is isomorphic to the product of the $\mathcal{O}/(\mathfrak{P}^{r(\mathfrak{P})} \cap \mathcal{O})^*$. Now $\mathcal{O}/(\mathfrak{P}^{r(\mathfrak{P})} \cap \mathcal{O})$ is a local ring with maximal ideal $\mathfrak{P} \cap \mathcal{O}$ so that $\mathcal{O}/(\mathfrak{P}^{r(\mathfrak{P})} \cap \mathcal{O})^*$ has order

$$(\mathcal{O} : (\mathfrak{P}^{r(\mathfrak{P})} \cap \mathcal{O}))(1 - 1/N_{\mathcal{O}}(\mathfrak{P} \cap \mathcal{O})).$$

We conclude that

$$\Phi_{\mathcal{O}}(\mathfrak{f}) = (\mathcal{O} : \mathfrak{f}) \prod_{\mathfrak{P} \cap \mathcal{O}} (1 - 1/N_{\mathcal{O}}(\mathfrak{P} \cap \mathcal{O})) \geqslant (\mathcal{O} : \mathfrak{f}) \prod_{\mathfrak{P}} (1 - 1/N_{\mathcal{O}}(\mathfrak{P} \cap \mathcal{O})).$$

The difference between the last two expressions is that the latter has extra factors when the $\mathfrak{P} \cap \mathcal{O}$ are not all distinct.

Using 3.7, we have that

$$t_{\mathcal{O}} = \frac{\Phi_K(\mathfrak{f})}{\Phi_{\mathcal{O}}(\mathfrak{f})} \leqslant \frac{(\mathcal{O}_K : \mathfrak{f}) \prod_{\mathfrak{P}|\mathfrak{f}} (1 - 1/N_K(\mathfrak{P}))}{(\mathcal{O} : \mathfrak{f}) \prod_{\mathfrak{P}|\mathfrak{f}} (1 - 1/N_{\mathcal{O}}(\mathfrak{P} \cap \mathcal{O}))}$$

$$= (\mathcal{O}_K : \mathcal{O}) \prod_{\mathfrak{P}|\mathfrak{f}} \frac{1 - 1/N_K(\mathfrak{P})}{1 - 1/N_{\mathcal{O}}(\mathfrak{P} \cap \mathcal{O})} \leqslant M \prod_{\mathfrak{P}|\mathfrak{f}} \frac{1 - 1/p^{f(\mathfrak{P})}}{1 - 1/p}$$

$$\leqslant M \prod_{\mathfrak{P}|M} \frac{1 - 1/p^{f(\mathfrak{P})}}{1 - 1/p} = M \prod_{p|M} \prod_{\mathfrak{P}|p} \frac{1 - 1/p^{f(\mathfrak{P})}}{1 - 1/p}.$$

We now consider $\prod_{\mathfrak{P}|p} \frac{1 - 1/p^{f(\mathfrak{P})}}{1 - 1/p}$. First,

$$\frac{1 - 1/p^{f(\mathfrak{P})}}{1 - 1/p} = 1 + 1/p + \ldots + 1/p^{f(\mathfrak{P}) - 1},$$

and one easily sees by comparing terms with like power of $1/p$ in the expansion of both sides that

$$(1 + 1/p + \ldots + 1/p^{f(\mathfrak{P}) - 1})^2 \leqslant (1 + 1/p)^{f(\mathfrak{P})}.$$

Thus

$$\frac{1 - 1/p^{f(\mathfrak{P})}}{1 - 1/p} \leqslant (1 + 1/p)^{f(\mathfrak{P})/2},$$

and since $\sum_{\mathfrak{P}|p} f(\mathfrak{P}) \leqslant n$, we conclude that

$$\prod_{\mathfrak{P}|p} \frac{1 - 1/p^{f(\mathfrak{P})}}{1 - 1/p} \leqslant (1 + 1/p)^{n/2}.$$

Combining our inequalities results in

$$t_{\mathcal{O}} \leqslant M \prod_{p|M} (1 + 1/p)^{n/2} = M (\psi(M)/M)^{n/2}.$$

For effective results, we refer now to the work of Robin.

PROPOSITION 5.2. $\psi(N)/N < 2 \log\log(3N^2)$ *for all* $N > 1$.

Proof. In [10, Theorem 2], Robin proves that $\sigma(N)/N < 1.8 \log\log(N) + 0.7/\log\log(N)$ for $N \geqslant 3$, where $\sigma(N)$ is the sum of the divisors of N. This implies that $\sigma(N)/N < 2 \log\log(N)$ for $N \geqslant 48$. Now it is easy to see that $\psi(N) \leqslant \sigma(N)$, so

$$\psi(N)/N \leqslant \psi(3N^2)/3N^2 < 2 \log\log(3N^2) \qquad (N \geqslant 4).$$

The cases $N = 2, 3$ are left to the reader.

COROLLARY 5.3. *If* $(\mathcal{O}_K : \mathcal{O}) = M > 1$ *then* $(\mathcal{O}_K^* : \mathcal{O}^*) < 2M \log\log(3M^2)$.

Proof. 3.7, 3.8, 5.1, 5.2.

THEOREM 5.4.

$$2^{r_1}h_{\mathcal{O}}R_{\mathcal{O}}/w_{\mathcal{O}} < 4\left(\frac{2}{n-1}\right)^{n-1}\sqrt{|d_{\mathcal{O}}|}\,(\log|d_{\mathcal{O}}|)^{n-1}(2\log\log|d_{\mathcal{O}}|)^{n/2}.$$

Proof. Our assumption that $n > 1$ implies that $|d_{\mathcal{O}}| = |d_K|M^2 \geqslant 3M^2$. Then by 5.2,

$$\psi(M)/M < 2\log\log(3M^2) \leqslant 2\log\log(|d_{\mathcal{O}}|) \quad \text{if } M > 1.$$

It follows that $\psi(M)/M < 2\log\log|d_{\mathcal{O}}|$, except when $M = 1$, $|d_K| < 6$. Combining this inequality with 5.1 leads to

$$t_{\mathcal{O}} < M(2\log\log|d_{\mathcal{O}}|)^{n/2}.$$

Siegel's bound [12] is

$$g_K < 4\left(\frac{2}{n-1}\right)^{n-1}\sqrt{|d_K|}\,(\log|d_K|)^{n-1}.$$

Hence using 4.6 we obtain our result:

$$\begin{aligned}2^{r_1}h_{\mathcal{O}}R_{\mathcal{O}}/w_{\mathcal{O}} &= g_{\mathcal{O}}t_{\mathcal{O}} = g_K t_{\mathcal{O}}\\ &< 4\left(\frac{2}{n-1}\right)^{n-1}\sqrt{|d_K|}\,(\log|d_K|)^{n-1}M(2\log\log|d_{\mathcal{O}}|)^{n/2}\\ &= 4\left(\frac{2}{n-1}\right)^{n-1}\sqrt{|d_K|M^2}\,(\log|d_K|)^{n-1}(2\log\log|d_{\mathcal{O}}|)^{n/2}\\ &\leqslant 4\left(\frac{2}{n-1}\right)^{n-1}\sqrt{|d_{\mathcal{O}}|}\,(\log|d_{\mathcal{O}}|)^{n-1}(2\log\log|d_{\mathcal{O}}|)^{n/2}.\end{aligned}$$

When $M = 1$ and $|d_K| < 6$, the only possibilities are $K = Q(\sqrt{-3})$ and $K = Q(\sqrt{5})$, due to the fact that the Minkowski bound must exceed 1. It is easy to verify the desired inequality directly in these two cases.

References

[1] L. M. Adleman and M. A. Huang, *Recognizing primes in random polynomial time*, preprint.

[2] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York 1966.

[3] J. Buchmann, *Zur Komplexität der Berechnung von Einheiten und Klassenzahlen algebraischer Zahlkörper*, Habilitationsschrift, Düsseldorf.

[4] E. C. Dade, O. Taussky and H. Zassenhaus, *On the theory of orders, in particular on the semigroup of ideal classes and genera of an order in an algebraic number field*, Math. Ann. 148 (1962), 31–64.

[5] R. Dedekind, *Über die Anzahl der Ideal-Klassen in den verschiedenen Ordnungen eines endlichen Körpers*, in *Festschrift der Technischen Hochschule in Braunschweig zur Säkularfeier des Geburtstages von C. F. Gauss*, Braunschweig 1877, pp. 1–55.

[6] H. Jacobinski, *Genera and decompositions of lattices over orders*, Acta Math. 121 (1968), 1–29.

[7] E. Landau, *Verallgemeinerung eines Pólyaschen Satzes auf algebraische Zahlkörper*, Nachr. Göttingen (1918), 478–488.

[8] S. Lang, *Elliptic Functions*, Addison-Wesley, Reading, Mass., 1973.

[9] I. Reiner, *Maximal Orders*, Academic Press, New York 1975.

[10] G. Robin, *Grandes valeurs de la fonction somme des diviseurs et hypothèse de Riemann*, J. Math. Pures Appl. 63 (1984), 187–213.

[11] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. 6 (1962), 64–94.

[12] C. L. Siegel, *Abschätzung von Einheiten*, Nachr. Göttingen 9 (1969), 71–86.

DEPARTMENT OF MATHEMATICS AND STATISTICS
UNIVERSITY OF VERMONT
Burlington, Vermont 05405-3357 USA

Received on 14.4.1989 (1925)