FINITENESS OF THE CLASS GROUP OF BASIC ARITHMETIC RINGS

ALEXANDER STASINSKI

Abstract. We give a purely algebraic definition of a class of Dedekind domains which includes the rings of integers of global fields, and give a uniform proof that all rings in this class have finite ideal class group.

1. Introduction

In [2], P. L. Clark asked whether there exists a “purely algebraic” proof of the finiteness of the class group of global fields and whether there exist any “structural” conditions on a Dedekind domain that imply the finiteness of its class group.

In this note we answer these questions in the affirmative. More precisely, we introduce a class of Dedekind domains, called basic arithmetic rings (Definition 2.2), which is defined purely algebraically (i.e., without using any topology or metric) and which contains the rings of integers of global fields. Our main result is a uniform proof that any basic arithmetic ring has finite ideal class group. This shows that the finiteness of the class groups of global fields can be proved uniformly without the Artin–Whaples axioms, without adeles and without methods from the geometry of numbers.

We note that the main result of this paper seems to have been unexpected, at least among certain specialists. For example, [2] says “[...] it is generally held that the finiteness of the class number is one of the first results of algebraic number theory which is truly number-theoretic in nature and not part of the general study of commutative rings” and in [10, B.1, p. 334] the authors write “Note well that for a general Dedekind domain, $Cl_K$ need not be finite. This shows that one essentially needs some analysis to supplement the abstract algebra in Chapter 5”.

A key idea of the proof is to estimate the norm of an element from above algebraically using that a determinant is a homogeneous polynomial in the entries of a matrix (see the proof of Lemma 3.2). A somewhat similar idea for estimating the norm appeared in [7, Thm. 96] (although only in the number field case), and an explicit use of the idea appears in [3, (20.10)] and [8, p. 300] (again only in the number field case). By contrast, the standard non-adelic and non-geometric proof of the finiteness of the class group in the number field case (see, e.g., [9, Ch.V, Sec. 4]) expresses the field norm in terms of the complex absolute values of Galois conjugates, and in the function field case this needs a modification involving absolute values.

In the final section, we give a known argument showing how to deduce the finiteness of the class group of a ring of $S$-integers in a global field, or more generally, any overring of a basic arithmetic ring. We also show that the ring of $S$-integers $\mathbb{Z}_p[1/p]$ is not a basic arithmetic ring and pose some open questions.
2. Basic PIDs and basic arithmetic rings

All rings are commutative with identity. Let \( \mathbb{N} \) denote the set of positive integers. We use the fairly standard acronym PID for “Principal Ideal Domain”. A ring \( R \) is called a \textit{finite quotient domain} or is said to have \textit{finite quotients} if for every non-zero ideal \( I \) of \( R \), the quotient \( R/I \) is a finite ring. If \( R \) is a finite quotient domain, \( I \subseteq R \) a non-zero ideal and \( x \in R \) is non-zero, we write \( N_R(I) = |R/I| \) and \( N_R(x) = |R/\langle x \rangle R| \). We also define \( N_R(0) = 0 \). The function \( N_R: R \to \mathbb{N} \cup \{0\} \) is called the \textit{ideal norm} on \( R \). It is well-known that if \( R \) is a finite quotient Dedekind domain, then \( N_R \) is multiplicative.

**Definition 2.1.** We call a PID \( A \) a \textit{basic PID} if the following conditions are satisfied:

1. \( A \) is a finite quotient domain,
2. for each \( m \in \mathbb{N} \),
   \[ \# \{ x \in A \mid N_A(x) \leq m \} > m \]
   (i.e., \( A \) has “enough elements of small norm”),
3. there exists a constant \( C \in \mathbb{N} \) such that for all \( x, y \in A \),
   \[ N_A(x + y) \leq C \cdot (N_A(x) + N_A(y)) \]
   (i.e., \( N_A \) satisfies the “quasi-triangle inequality”).

We remark that in a PID which is a finite quotient domain, neither the second nor the third condition in Definition 2.1 is necessary. Take, for instance, the PID \( A = \mathbb{Z}[\sqrt{-163}] \), so that \( N_A(a + b\sqrt{-163}) = a^2 + 163b^2 \), for \( a, b \in \mathbb{Z} \) not both zero. Then \( a^2 + 163b^2 \leq 17 \) has only 17 solutions. On the other hand, take the PID \( A = \mathbb{Z}[\sqrt{2}] \), whose fundamental unit is \( u = 1 + \sqrt{2} \). Let \( \overline{u} = 1 - \sqrt{2} \), and for any \( r \in \mathbb{N} \), write \( u^r = a_r + b_r \sqrt{2} \), for \( a_r, b_r \in \mathbb{Z} \). Then \( a_r \) grows with \( r \) and

\[ N_A(u^r + \overline{u}^r) = N(2a_r) = |N_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(2a_r)| = 4a_r^2, \]

while \( N_A(u^r) + N_A(\overline{u}^r) = 2 \cdot |N_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(1 + \sqrt{2})|^r = 2 \).

**Definition 2.2.** Let \( A \) be a basic PID. We call a ring \( B \) a \textit{basic arithmetic ring} (over \( A \)) if the following conditions are satisfied:

1. \( B \) is a Dedekind domain.
2. \( B \) is a finitely generated free module over \( A \).

Our goal in the next section is to prove that any basic arithmetic ring has finite ideal class group. The most important examples of basic arithmetic rings are the rings of integers in global fields:

**Proposition 2.3.** Let \( K \) be a global field (i.e., a finite extension of \( \mathbb{Q} \) or of \( \mathbb{F}_q(t) \)), and let \( \mathcal{O} \) be its ring of integers. Then \( \mathcal{O} \) is a basic arithmetic ring over \( \mathbb{Z} \) or \( \mathbb{F}_q[t] \), respectively.

**Proof.** First, it is straightforward to check that \( \mathbb{Z} \) is a basic PID. Next, let \( R = \mathbb{F}_q[t] \). For any \( f(t) \in R \) we have

\[ N_R(f(t)) = q^{\deg(f)}, \]
so $R$ is a finite quotient domain and

$$\# \{ x \in R \mid N_R(x) \leq m \} = \# \{ x \in R \mid \deg(x) \leq \lfloor \log_q(m) \rfloor \} \leq q^{\lfloor \log_q(m) \rfloor + 1} > q^{\log_q(m)} = m,$$

so the second property in Definition 2.1 is satisfied. Furthermore, for $f(t), g(t) \in R$ we have

$$N_R(f(t)+g(t)) = q^{\deg(f+g)} = q^{\max\{\deg f, \deg g\}} \leq q^{\deg f} + q^{\deg g} = N_R(f(t)) + N_R(g(t)),$$

so $F_q[t]$ is a basic PID.

It is well-known that the ring of integers in any global field is a Dedekind domain and is free of finite rank over $\mathbb{Z}$ or $F_q[t]$, respectively (see, e.g. [9, I.4.7] for the number field case and [9, X.1.7] for the function field case). Thus $R$ is a basic arithmetic ring.

Let $B$ be a basic arithmetic ring over the basic PID $A$, let $K$ be the fraction field of $A$ and let $L$ be the fraction field of $B$. Since $B$ is free over $A$, and hence torsion-free, we may consider $A$ as a subring of $B$ via the embedding $a \mapsto a \cdot 1$ and $K$ as a subfield of $L$ via the induced embedding. With this notation, we have the following result:

**Proposition 2.4.** The field extension $L/K$ is of finite degree and $B$ is the integral closure of $A$ in $L$. Conversely, let $L'/K$ be a finite separable extension and let $B'$ be the integral closure of $A$ in $L'$. Then $B'$ is a basic arithmetic ring over $A$.

**Proof.** Let $S = A \setminus \{0\}$. Then (by a simple argument) $S^{-1}B$ is finitely generated over $S^{-1}A = K$. But $S^{-1}B$ is an integral domain which is finitely generated over a field, so $S^{-1}B$ is a field, that is, $S^{-1}B = L$. Hence $L/K$ is finite. Furthermore, since $B$ is finitely generated over $A$, $B$ is integral over $A$ (see, e.g. [9, I.2.10]). Thus $B$ lies inside the integral closure $C$ of $A$ in $L$. Since $B \subseteq C \subseteq L$, the fraction field of $C$ is $L$. Any $x \in C$ is integral over $A$, hence integral over $B$. Since $B$ is a Dedekind domain it is integrally closed, so $x \in B$. Thus $C = B$, that is, $B$ is the integral closure of $A$ in $L$.

For the converse, it is well-known that $B'$ is a Dedekind domain which is finitely generated over $A$ (see, e.g. [9, I.4.7 and I.6.2]). Since $B'$ is torsion-free, it is free over $A$. Finally, by [9, V.3.6] $B'$ has finite quotients and thus $B'$ is a basic arithmetic ring over $A$. \qed

### 3. Norm estimates

Throughout this section, let $B$ be a basic arithmetic ring over the basic PID $A$ and let $K$ and $L$ be the field of fractions of $A$ and $B$, respectively.

For $\alpha \in L$ we let $T_\alpha$ denote the endomorphism $L \to L$, $x \mapsto \alpha x$, and define the norm $N_{L/K}(\alpha) = \det(T_\alpha)$. As is well-known, the fact that $B$ is the integral closure of $A$ in $L$ implies that $N_{L/K}(B) \subseteq A$.

The following lemma is a consequence of [9, IV.6.9 and V.3.6] (which is valid when $A$ is a Dedekind domain, not necessarily a PID). We give a simple proof in our setting (where $A$ is a PID), exploiting the Smith normal form.

**Lemma 3.1.** For any non-zero $\alpha \in B$, we have $N_B(\alpha) = N_A(N_{L/K}(\alpha))$. 

Proof. We have \( N_B(\alpha) = |B/\alpha B| \) and \( B/\alpha B \) is the cokernel of the map \( T_\alpha : B \to B \). By the Smith normal form, we have

\[
B/\alpha B \cong A/p_1A \oplus \cdots \oplus A/p_nA,
\]

where \( n \) is the rank of \( B \) over \( A \), and \( p_i \in A \) are some non-units such that \( \det(T_\alpha) = u^{-1}p_1 \cdots p_n \), for some unit \( u \in A \) (\( u = \det(PQ) \) where \( PT_\alpha Q \) is the Smith normal form, with \( T_\alpha \) identified with its matrix with respect to some chosen basis).

Now observe that for any \( m_1, \ldots, m_k \in A \), we have

\[
|A/m_1 \cdots m_k A| = \prod_{i=1}^k |A/m_i A|,
\]

which follows from the Chinese remainder theorem, combined with the fact that for any irreducible element \( m \in A \) and \( i \in \mathbb{N} \), we have \( |m^i A/m^{i+1} A| = |A/m A| \).

Thus

\[
N_A(N_{L/K}(\alpha)) = |A/N_{L/K}(\alpha) A| = |A/\det(T_\alpha) A| = |A/p_1A| \cdots |A/p_nA| = |B/\alpha B| = N_B(\alpha).
\]

\[\square\]

Lemma 3.2. Let \( x_1, \ldots, x_n \) be a basis for \( B \) over \( A \). Let \( \alpha \in B \) and write \( \alpha = c_1x_1 + \cdots + c_nx_n \), with \( c_i \in A \). Then there exists a homogeneous polynomial \( f(T_1, \ldots, T_n) \) over \( A \) of degree \( n \) such that

\[
N_{L/K}(\alpha) = f(c_1, \ldots, c_n).
\]

Moreover, there exists a constant \( C \in \mathbb{N} \) such that

\[
N_B(\alpha) \leq C \cdot \max_i \{N_A(c_i)\}^n.
\]

Proof. For \( 1 \leq i, j, k \leq n \), let \( r_{ij}^{(k)} \in A \) be such that

\[
x_i x_j = \sum_{k=1}^n r_{ij}^{(k)} x_k.
\]

Then

\[
\alpha x_i = c_1 x_i x_1 + \cdots + c_n x_i x_n = c_1 \sum_{k=1}^n r_{i1}^{(k)} x_k + \cdots + c_n \sum_{k=1}^n r_{in}^{(k)} x_k
\]

\[= \sum_{k=1}^n \left( \sum_{j=1}^n c_j r_{ij}^{(k)} \right) x_k,
\]

so the matrix of \( T_\alpha \) with respect to the basis \( x_1, \ldots, x_n \) has \( (i, k) \)-entry equal to \( \sum_{i=1}^n c_j r_{ij}^{(k)} \), for \( 1 \leq i, k \leq n \). Hence each entry of the matrix of \( T_\alpha \) is a linear form in \( c_1, \ldots, c_n \), and therefore \( \det(T_\alpha) = f(c_1, \ldots, c_n) \) for some homogenous polynomial \( f \) of degree \( n \).

Moreover, write \( f(c_1, \ldots, c_n) = a_1 c_1^{n_1} \cdots c_n^{n_1} + \cdots + a_k^{n_k} \cdots c_n^{n_k} = n, \) for every \( i \). By Lemma 3.1 and the fact that
A is a basic PID (the third property), there exists a constant $C_0 \in \mathbb{N}$ such that
\begin{align*}
N_B(\alpha) &= N_A(N_{L/K}(\alpha)) = N_A(f(c_1, \ldots, c_n)) \\
&\leq C_0(N_A(a_1)N_A(c_1)^{n_1} \cdots N_A(c_n)^{n_1} + \cdots \\
&+ N_A(a_k)N_A(c_1)^{n_k} \cdots N_A(c_n)^{n_k}) \\
&\leq C_0 \cdot \max_i \{N_A(a_i)\}(\max_i \{N_A(c_i)\})^n.
\end{align*}

Hence the result follows by letting $C = C_0 k \cdot \max_i \{N_A(a_i)\}$.
\[ \square \]

**Theorem 3.3.** Suppose that $B$ is a basic arithmetic ring over $A$. There exists a constant $C \in \mathbb{N}$ such that for any ideal $I$ in $B$, there exists a non-zero element $\alpha \in I$ such that
\[ N_B(\alpha) \leq C \cdot N_B(I). \]
Hence the ideal class group of $B$ is finite.

**Proof.** Let $n$ be the rank of $B$ over $A$ and let $x_1, \ldots, x_n$ be a basis for $B$ over $A$. Let $m$ be the unique positive integer such that $m^n \leq N_B(I) < (m + 1)^n$. The fact that $A$ is a basic PID (the second property) says that the set $S := \{ x \in A \mid N_A(x) \leq m \}$ has at least $m + 1$ elements. Hence the set $Sx_1 + \cdots + Sx_n$ has at least $(m + 1)^n$ distinct elements. Since $(m + 1)^n > \left| B/I \right|$, there exist two distinct elements $s$ and $t$ in the set $Sx_1 + \cdots + Sx_n$ which are congruent mod $I$. Write $s = \sum_{i=1}^n a_i x_i$ and $t = \sum_{i=1}^n b_i x_i$, with $a_i, b_i \in S$. Then
\[ s - t = \sum_{i=1}^n (a_i - b_i)x_i \]
is a non-zero element of $I$ and by the third property of Definition 2.1 there is a $C_0 \in \mathbb{N}$ such that
\[ N_A(a_i - b_i) \leq C_0(N_A(a_i) + N_A(b_i)) \leq C_0 2m. \]

Thus Lemma 3.2 implies that there is a $C_1 \in \mathbb{N}$ such that
\[ N_B(s - t) \leq C_1 \cdot \max_i \{N_A(a_i - b_i)\}^n \leq C_1(C_0 2m)^n, \]
and setting $C = C_1(2C_0)^n$, we get
\[ N_B(s - t) \leq C \cdot N_B(I). \]

We have established the first assertion of the theorem and a well-known argument now implies the finiteness of the class group of $B$ (see, e.g., [10 Ch. 4, Lem. 3.8-3.9]).
\[ \square \]

The above theorem, together with Proposition 2.3 imply that rings of integers of global fields have finite ideal class group.
4. Overrings

Let \( D \) be an integral domain with field of fractions \( K \). A ring \( R \) such that \( D \subseteq R \subseteq K \) is called an overring of \( D \). The following is a known result:

**Lemma 4.1.** Let \( D \) be a Dedekind domain with finite class group. Then any overring \( R \) of \( D \) is a Dedekind domain with finite class group.

**Proof.** It is well known that \( R \) is a Dedekind domain (see, e.g. [1] Lem. 1-1]). Since the class group of \( D \) is finite, hence torsion, a result independently due to Davis [1] Thm. 2], Gilmer and Ohm [5] Cor. 2.6] and Goldman [6] §1, Cor. (1)], implies that \( R \) is the localisation of \( D \) at a multiplicative subset of \( D \). Then, by a straightforward argument (see [1] Prop. 1-2, Cor. 1-3]), the class group of \( R \) is a quotient of the class group of \( D \), hence is finite. \(\square\)

The above result shows that it is possible to give a purely algebraic definition of a class of Dedekind domains with finite class groups, namely the class of overrings of basic arithmetic rings, which is more general than the class of basic arithmetic rings.

The class of overrings of basic arithmetic rings includes all \( S \)-integer rings, for any finite set \( S \) of places containing the archimedeans ones. On the other hand, the following result implies that rings of \( S \)-integers will in general not be basic arithmetic rings.

**Proposition 4.2.** Let \( p \in \mathbb{Z} \) be a prime. The ring \( \mathbb{Z}[\frac{1}{p}] \) is a PID which is not finitely generated and free over any basic PID.

**Proof.** It is well-known that \( \mathbb{Z}[\frac{1}{p}] \) is a Euclidean domain (with Euclidean norm \( N(p^nx) = |x| \), where \( x \in \mathbb{Z} \) is prime to \( p \)). Assume that \( \mathbb{Z}[\frac{1}{p}] \) is finitely generated and free over a basic PID \( A \), that is, that \( \mathbb{Z}[\frac{1}{p}] \) is a basic arithmetic ring. Then, by Proposition [2,4], \( \mathbb{Z}[\frac{1}{p}] \) is the integral closure of \( A \) in the fraction field \( \mathbb{Q} \) of \( \mathbb{Z}[\frac{1}{p}] \). Since \( \mathbb{Q} \) is the characteristic zero prime field, the fraction field of \( A \) must also be \( \mathbb{Q} \). We have \( A \subseteq \mathbb{Z}[\frac{1}{p}] \subseteq \mathbb{Q} \), and since \( A \) is integrally closed, we must have \( A = \mathbb{Z}[\frac{1}{p}] \).

To get a contradiction, we now show that \( \mathbb{Z}[\frac{1}{p}] \) is not a basic PID. First note that since \( p \) is a unit in \( \mathbb{Z}[\frac{1}{p}] \), the ideal norm in \( \mathbb{Z}[\frac{1}{p}] \) satisfies

\[
N_{\mathbb{Z}[\frac{1}{p}]}(p^n x) = N_{\mathbb{Z}[\frac{1}{p}]}(x),
\]

for any \( x, n \in \mathbb{Z} \). Moreover, when \( x \) is prime to \( p \), the \( \mathbb{Z} \to \mathbb{Z}[\frac{1}{p}] \) induces an inclusion \( \mathbb{Z}/x\mathbb{Z} \to \mathbb{Z}[\frac{1}{p}]/x\mathbb{Z}[\frac{1}{p}] \), so we always have \( N_{\mathbb{Z}[\frac{1}{p}]}(x) \geq N_{\mathbb{Z}}(x) \). Thus, for \( n \in \mathbb{N} \),

\[
N_{\mathbb{Z}[\frac{1}{p}]}(1 + p^n) \geq 1 + p^n,
\]

which grows with \( n \), while \( N_{\mathbb{Z}[\frac{1}{p}]}(1) + N_{\mathbb{Z}[\frac{1}{p}]}(p^n) = 2 \) is bounded. Thus the third condition in Definition [2,1] fails for the ring \( \mathbb{Z}[\frac{1}{p}] \). \(\square\)

The examples \( \mathbb{Z}[\frac{1+\sqrt{-5}}{2}] \) and \( \mathbb{Z}[\sqrt{2}] \), following Definition [2,1] of PIDs which are not basic PIDs have the property that they are finitely generated and free over \( \mathbb{Z} \), which is a basic PID. Therefore any Dedekind domain which is finitely generated and free over one of these PIDs will be a basic arithmetic ring over \( \mathbb{Z} \). Proposition [4,2] shows that this is not a general phenomenon.
We do not know whether there exists a Dedekind domain $B$ which is finitely generated and free over a PID $A$ with finite quotients and such that $B$ has finite class group. Theorem 3.3 shows that if such an example exists, then the second or third condition in the definition of basic PID must fail for $A$. If we take $A = \mathbb{Z}[\frac{1}{p}]$ and let $B$ be the integral closure of $A$ in a finite extension of $\mathbb{Q}$, then $B$ is finitely generated and free over $A$. However, since integral closure is compatible with localisations, $B$ will be the $S$-integers in an algebraic number field, which we know has finite class group.

It is a trivial fact that there exist Dedekind domains (even PIDs) with finite class groups which are not overrings of any basic arithmetic ring. Indeed, the polynomial ring $\mathbb{C}[X]$ is a PID but is not a finite quotient domain, so cannot be an overring of a basic arithmetic ring (finite quotient domains are stable under localisation). However, we do not know whether there exists a finite quotient Dedekind domain which is not the overring of any basic arithmetic ring. It would also be interesting to know whether there exists a basic arithmetic ring which is not the ring of integers of a global number field.

References

[1] L. Claborn, Dedekind domains and rings of quotients, Pacific J. Math. 15 (1965), 59–64.
[2] P. L. Clark, Is there a “purely algebraic” proof of the finiteness of the class number?, MathOverflow, https://mathoverflow.net/q/50557 (version: 2010-12-28).
[3] C. W. Curtis and I. Reiner, Representation Theory of Finite Groups and Associative Algebras, Pure and Applied Mathematics, Vol. XI, Interscience Publishers, New York-London, 1962.
[4] E. D. Davis, Overrings of commutative rings. II. Integrally closed overrings, Trans. Amer. Math. Soc. 110 (1964), 196–212.
[5] R. Gilmer and J. Ohm, Integral domains with quotient overrings, Math. Ann. 153 (1964), 97–103.
[6] O. Goldman, On a special class of Dedekind domains, Topology 3 (1964), no. suppl. 1, 113–118.
[7] E. Hecke, Lectures on the theory of algebraic numbers, volume 77 of Graduate Texts in Mathematics, Springer-Verlag, New York-Berlin, 1981.
[8] A. W. Knapp, Advanced algebra, Cornerstones, Birkhäuser Boston, Inc., Boston, MA, 2007.
[9] D. Lorenzini, An invitation to arithmetic geometry, volume 9 of Graduate Studies in Mathematics, American Mathematical Society, Providence, RI, 1996.
[10] D. Ramakrishnan and R. J. Valenza, Fourier analysis on number fields, volume 186 of Graduate Texts in Mathematics, Springer-Verlag, New York, 1999.

Alexander Stasinski, Department of Mathematical Sciences, Durham University, Durham, DH1 3LE, UK
E-mail address: alexander.stasinski@durham.ac.uk