A UNIFORM PROOF OF THE FINITENESS OF THE CLASS GROUP OF A GLOBAL FIELD

ALEXANDER STASINSKI

Abstract. We give a definition of a class of Dedekind domains which includes the rings of integers of global fields and give a proof that all rings in this class have finite ideal class group. We also prove that this class coincides with the class of rings of integers of global fields.

1. Introduction.

1.1. **Background.** The starting point of algebraic number theory is to define an (algebraic) *number field* K as a finite field extension of $\mathbb{Q}$ and the ring $\mathbb{Z}_K$ of *algebraic integers* in K as all the elements in K that satisfy a monic polynomial equation with coefficients in $\mathbb{Z}$ (This is called the *integral closure* of $\mathbb{Z}$ in K.) Unlike the situation in $\mathbb{Z}$, unique factorization of elements in $\mathbb{Z}_K$ into irreducibles can fail. Nevertheless, $\mathbb{Z}_K$ is an example of a *Dedekind domain*, that is, an integral domain in which every nonzero proper ideal is, uniquely, a product of prime ideals.

One can develop a parallel theory of finite extensions K, called (algebraic) *function fields*, of the field $\mathbb{F}_q(t)$, which is the field of fractions of the ring of polynomials $\mathbb{F}_q[t]$ over a finite field $\mathbb{F}_q$. The analogue of $\mathbb{Z}_K$ is then the ring of elements in K that satisfy a monic polynomial equation with coefficients in $\mathbb{F}_q[t]$. These rings are also Dedekind domains and their theory can to a large extent be developed in parallel with that of the rings $\mathbb{Z}_K$. For this reason, it is sometimes convenient to use the term *global field* for either a number field or a function field.

One of the most fundamental problems about rings of integers in global fields is the study of the (failure of) unique factorization. This is encoded in the *(ideal) class group* of the ring, which is trivial if and only if unique factorization holds. A important result in algebraic number theory is that the class group of $\mathbb{Z}_K$ is finite. Similarly, it is known that the class group of a ring of integers in a function field is finite. One can define the ideal class group $Cl(R)$ of any Dedekind domain R as the equivalence classes of nonzero ideals where two ideals I, J are said to be equivalent if $aI = bJ$, for some nonzero $a, b \in R$, and the group operation is induced by multiplication of ideals.

1.2. **The main results.** In [6], 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 article we answer these questions in the affirmative. More precisely, we introduce a class (G) of Dedekind domains (see Definition 2) that contains the rings of integers of global fields. We then give a uniform (i.e., not case by case) proof that any ring of class (G) has finite ideal class group. We also give a known argument showing how to deduce the finiteness of the class group of any overring of a ring of class (G).

The proof of the finiteness of the class group that we give is essentially that of R. Swan [17, Theorem 3.9] and I. Reiner [16, (26.3)] (modulo some exercises) for rings of integers in global fields. The contribution here is that we axiomatize properties of a Dedekind domain sufficient for the proof to go through and that we show that these properties in fact characterize rings of integers in global fields. This shows in particular that the finiteness of the class groups of global fields can be proved uniformly without adeles and without methods from the geometry of numbers. This fact does not seem to have been widely known. Indeed, Clark writes in [6] that "[...] 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 [15, 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 the fact that a determinant is a homogeneous polynomial in the entries of a matrix (see the proof of Lemma 6). This idea is present in [17, p. 53], [16, (26.3)] and [7, (20.10)] but can be traced back to Zassenhaus [18] in the number field case and Higman–McLaughlin [12] in the function field case. By contrast, the standard nonadelic and nongeometric proof of the finiteness of the class group in the number field case (see, e.g., [14, V, Section 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 show that the class (G) coincides with the class of global fields. This uses the Artin–Whaples axiomatization of global fields and shows that the quasi-triangle inequality condition in Definition 2, despite its simplicity and elementary nature, implies the product formula for absolute values.

2. Basic PIDs and rings of class (G).

All rings are commutative with identity. Let $\mathbb{N}$ denote the set of positive integers. We use the standard acronym PID for "principal ideal domain." A ring R is called a *finite quotient domain* or is said to *have finite quotients* if for every nonzero ideal I of R, the quotient R/I is a finite ring. If R is a finite quotient domain, $I \subseteq R$ a nonzero ideal, and $x \in R$ is nonzero, we write $N_R(I) = |R/I|$ and $N_R(x) = |R/xR|$. We also define $N_R(0) = 0$. The function $N_R : R \to \mathbb{N} \cup \{0\}$ is called the *ideal norm* on R. It is known that if R is a finite quotient Dedekind domain, then N_R is multiplicative (see [14, Lemma V.3.5]).

Definition 1. We call a PID A a *basic PID* if it is not a field and if the following conditions are satisfied:

(1) A is a finite quotient domain;
(2) there exists a constant $c \in \mathbb{N}$ such that for each $m \in \mathbb{N}$,

$$\#\{x \in A \mid N_A(x) \leq c \cdot m\} \geq m$$

(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").

There exist PIDs for which the first and second conditions in Definition 1 hold but for which the third condition fails. Take, for instance, the PID $A = \mathbb{Z}[\sqrt{2}]$. Then $u = 1 + \sqrt{2}$ is a unit in A and $\overline{u} = 1 - \sqrt{2}$. 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 $N_A(u^r) + N_A(\overline{u}^r) = 2$, since u^r and $\overline{u}^r$ are units. Thus the third condition in Definition 1 fails for A even though A is a finite quotient domain that satisfies the second condition since it has infinitely many units.

Another example of a finite quotient PID A where the second condition holds but the third condition fails is the localization $\mathbb{Z}_{(p)}$ of $\mathbb{Z}$ at a prime p, that is, the subring of $\mathbb{Q}$ consisting of fractions a/b, $a, b \in \mathbb{Z}$, where $p \nmid b$. Here $\pm 1 + p^n$ is a unit for every $n \in \mathbb{N}$, so $N_A(1 + p^n) + N_A(-1 + p^n) = 1 + 1 = 2$, while $N_A(1 + p^n + (-1 + p^n)) = N_A(2)N_A(p)^n$, which grows with n.

Definition 2. Let A be a basic PID. We call a Dedekind domain B a *ring of class (G) (over A)* if B is an A-algebra that is finitely generated and free as a module over A.

Since free modules over a PID are torsion-free, we may and will consider A as a subring of B via the embedding $a \mapsto a \cdot 1$. Our goal in the next section is to prove that any ring B of class (G) has finite ideal class group. The terminology "(G)" is provisional ("G" for global), because it will turn out that the class (G) is equal to the class of rings of integers in global fields (see Corollary 13).

Definition 3. By *global field* we mean either a finite extension of $\mathbb{Q}$ or a finite separable extension of some $\mathbb{F}_q(t)$, where t is transcendental over $\mathbb{F}_q$. By a *ring of integers* of a global field K we mean either the integral closure in K of $\mathbb{Z}$ (in the number field case) or the integral closure in K of $\mathbb{F}_q[t]$, for some $t \in K$ transcendental over $\mathbb{F}_q$ (in the function field case).

Note that in the function field case, there is no unique ring of integers, as, for instance, one can also take the integral closure of $\mathbb{F}_q[t^{-1}]$.

Proposition 4. *Let B be a ring of integers of a global field. Then B is a ring of class (G) over $\mathbb{Z}$ or $\mathbb{F}_q[t]$, respectively.*

Proof. First, it is straightforward to check that $\mathbb{Z}$ is a basic PID. Indeed, all its proper quotients $\mathbb{Z}/n$ are finite, $N_{\mathbb{Z}}(n) = |n|$ (the absolute value of n) so $\#\{x \in \mathbb{Z} \mid N_{\mathbb{Z}}(x) \leq m\} = 2m + 1 \geq m$ and $N_{\mathbb{Z}}(x + y) = |x + y| \leq |x| + |y| = N_{\mathbb{Z}}(x) + N_{\mathbb{Z}}(y)$, thanks to the usual triangle inequality.

Next, let $A = \mathbb{F}_q[t]$. For any $f(t) \in A$ we have $N_A(f(t)) = q^{\deg(f)}$, so A is a finite quotient domain and

$$\begin{aligned}\#\{x \in A \mid N_A(x) \leq m\} &= \#\{x \in A \mid \deg(x) \leq \lfloor \log_q(m) \rfloor\} \\ &= q^{\lfloor \log_q(m) \rfloor + 1} > q^{\log_q(m)} = m,\end{aligned}$$

so the second property in Definition 1 is satisfied for A. Furthermore, for $f(t), g(t) \in A$ we have

$$\begin{aligned}N_A(f(t) + g(t)) &= q^{\deg(f+g)} = q^{\max\{\deg f, \deg g\}} \leq q^{\deg f} + q^{\deg g} \\ &= N_A(f(t)) + N_A(g(t)),\end{aligned}$$

so A is a basic PID. Thus both $\mathbb{Z}$ and $\mathbb{F}_q[t]$ satisfy Definition 1 with $c = C = 1$.

It is well known that B is a Dedekind domain and is free of finite rank over $\mathbb{Z}$ or $\mathbb{F}_q[t]$, respectively (see [14, Theorem I.4.7] for the number field case and [14, Theorem X.1.7] for the function field case; note that if the extension of fraction fields is finite and separable, which is always the case for number fields, this follows with a classical proof, but for function fields, where separability may fail, it requires a separate proof.). Thus, in either case, B is a ring of class (G). □

3. Norm estimates and finiteness.

Throughout this section, let B be a ring of class (G) 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_α 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 $N_{L/K}(B) \subseteq A$ (see, e.g., [14, Corollary IV.2.4]).

The following lemma is a consequence of [14, Proposition IV.6.9 and Proposition 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 (see, e.g., [1, Section 5.3]).

Lemma 5. *For any nonzero $\alpha \in B$, 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

$$B/\alpha B \cong A/p_1 A \oplus \cdots \oplus A/p_n A,$$

where n is the rank of B over A, and $p_i \in A$ are some nonunits 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_α identified with its matrix with respect to some chosen basis).

Now observe that for any $m_1, \dots, m_k \in A$, we have

$$|A/m_1 \cdots m_k A| = |A/m_1 A| \cdots |A/m_k A|,$$

which follows from the Chinese remainder theorem (see, e.g., [1, Corollary 2.25]), combined with the fact that for any irreducible element $m \in A$ and $i \in \mathbb{N}$, we have $|m^i A/m^{i+1} A| = |A/mA|$ (the map $A \to m^i A$ given by $1 \mapsto m^i$ induces an isomorphism $A/mA \to m^i A/m^{i+1} A$).

Thus

$$\begin{aligned} N_A(N_{L/K}(\alpha)) &= |A/N_{L/K}(\alpha) A| = |A/\det(T_\alpha) A| = |A/p_1 A| \cdots |A/p_n A| \\ &= |B/\alpha B| = N_B(\alpha). \end{aligned}$$

□

Lemma 6. *Let $x_1, \dots, x_n$ be a basis for B over A. Let $\alpha \in B$ and write $\alpha = c_1 x_1 + \cdots + c_n x_n$, with $c_i \in A$. Then there exists a homogeneous polynomial $f(T_1, \dots, T_n)$ over A of degree n such that*

$$N_{L/K}(\alpha) = f(c_1, \dots, c_n).$$

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 $1 \le i, j, k \le n$, let $r_{ij}^{(k)} \in A$ be such that

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

Then

$$\begin{aligned} \alpha x_i = c_1 x_i x_1 + \cdots + c_n x_i x_n &= c_1 \sum_{k=1}^{n} r_{i1}^{(k)} x_k + \cdots + c_n \sum_{k=1}^{n} r_{in}^{(k)} x_k \\ &= \sum_{k=1}^{n} \Big(\sum_{j=1}^{n} c_j r_{ij}^{(k)} \Big) x_k, \end{aligned}$$

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

Moreover, write $f(c_1, \ldots, c_n) = a_1 c_1^{n_{1,1}} \cdots c_n^{n_{1,n}} + \cdots + a_k c_1^{n_{k,1}} \cdots c_n^{n_{k,n}}$, where $a_i \in A$, $k, n_{i,j} \in \mathbb{N}$ and $\sum_{j=1}^{n} n_{i,j} = n$, for every i. By Lemma 5 and the quasi-triangle inequality for N_A, there exists a constant $C_0 \in \mathbb{N}$ such that

$$\begin{aligned} N_B(\alpha) &= N_A(N_{L/K}(\alpha)) = N_A(f(c_1, \ldots, c_n)) \\ &\le C_0 \big(N_A(a_1) N_A(c_1)^{n_{1,1}} \cdots N_A(c_n)^{n_{1,n}} + \cdots \\ &\quad + N_A(a_k) N_A(c_1)^{n_{k,1}} \cdots N_A(c_n)^{n_{k,n}} \big) \\ &\le C_0 k \cdot \max_i \{N_A(a_i)\} (\max_i \{N_A(c_i)\})^n. \end{aligned}$$

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

Theorem 7. *Suppose that B is a ring of class (G) over A. Then there exists a constant $C \in \mathbb{N}$ such that for any ideal I in B, there exists a nonzero element $\alpha \in I$ such that*

$$N_B(\alpha) \le C \cdot N_B(I).$$

Hence the ideal class group of B is finite.

Proof. Let $x_1, \ldots, x_n$ be a basis for B over A. Let m be the unique positive integer such that $m^n \le N_B(I) < (m+1)^n$. The fact that A is a basic PID (the second property) says that there exists a $c \in \mathbb{N}$ such that for every m, $\#\{x \in A \mid N_A(x) \le cm\} \ge m$. Thus, for every m, the set

$$S_m := \{x \in A \mid N_A(x) \le 2cm\}$$

has at least $m+1$ elements. Hence the set

$$S_m x_1 + \cdots + S_m x_n$$

has at least $(m+1)^n$ distinct elements. Since $(m+1)^n > |B/I|$, there exist two distinct elements s and t in the set $S_m x_1 + \cdots + S_m x_n$ that 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 $a_i, b_i \in S_m$. Then

$$s - t = \sum_{i=1}^{n} (a_i - b_i) x_i$$

is a nonzero element of I and by the third property of Definition 1, there is a $C_0 \in \mathbb{N}$ such that

$$N_A(a_i - b_i) \leq C_0(N_A(a_i) + N_A(b_i)) \leq C_0 2 \cdot 2cm.$$

Thus Lemma 6 implies that there is a $C_1 \in \mathbb{N}$ such that

$$N_B(s-t) \leq C_1 \cdot \max_i \{N_A(a_i - b_i)\}^n \leq C_1(C_0 4cm)^n,$$

and thus

$$\frac{N_B(s-t)}{N_B(I)} \leq \frac{C_1(C_0 4cm)^n}{m^n} = C_1(C_0 4c)^n.$$

Taking $\alpha = s - t$ and $C = C_1(C_0 4c)^n$ thus proves the first assertion of the theorem.

A well-known argument now implies the finiteness of the class group of B (see, e.g., [14, Lemmas V.3.8–3.9]). We give the argument here for the convenience of the reader. If I is an ideal of B, we write $[I]$ for the corresponding ideal class in the class group $Cl(B)$. We will first show that any ideal class $\mathfrak{c} \in Cl(R)$ contains an ideal I such that $N(I) \leq C$. Let J be an ideal of B such that $\mathfrak{c} = [J]$.

By the first assertion of the theorem, there exists a nonzero $\alpha \in J$ and a $C \in \mathbb{N}$ such that $N(\alpha) \leq C \cdot N(J)$. Since $\alpha B \subseteq J$, the unique factorization of ideals in B implies that we have $\alpha B = IJ$, for some ideal I. Since $[\alpha B]$ is the trivial ideal class,

$$[I] = [J]^{-1} = \mathfrak{c}^{-1},$$

and by the multiplicativity of N,

$$N(J)N(I) = N(\alpha) \leq C \cdot N(J),$$

so $N(I) \leq C$. We have thus shown what we wanted for $\mathfrak{c}^{-1}$. But $\mathfrak{c} \in Cl(B)$ was arbitrary, so it holds for all $\mathfrak{c}$. Now, since there are only finitely many ideals of norm below a given bound (see, e.g., [14, Lemma V.3.7]) we conclude that there can only be finitely many classes $\mathfrak{c} \in Cl(B)$. □

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

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 8. *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., [5, Lemma 1-1]). Since the class group of D is finite, hence torsion, a result independently due to Davis [8, Theorem 2], Gilmer and Ohm [9, Cor. 2.6], and Goldman [10, §1, Corollary (1)] implies that R is the localization of D at a multiplicative subset of D. Then, by a straightforward argument (see [5, Proposition 1-2, Corollary 1-3]), the class group of R is a quotient of the class group of D, hence is finite. □

The class of overrings of rings of class (G) includes all S-integer rings, for any finite set S of places containing the Archimedean ones. On the other hand, by Theorem 11 it will follow that a ring of S-integers is not of type (G) unless it is a ring of integers of a global field.

4. Rings of class (G) and global fields.

For the reader's convenience, we state a few definitions and results from Artin's book [2, Chapter 1].

Definition 9. An *absolute value* (called "valuation" in [2, Chapter 1]) of a field K is a function $|\cdot|: K \to \mathbb{R}$, $x \mapsto |x|$, satisfying the following conditions:

(1) $|x| \geq 0$ and $|x| = 0$ if and only if $x = 0$;
(2) $|xy| = |x| \cdot |y|$;
(3) there exists a constant $c \in \mathbb{R}$, $c \geq 1$ such that if $|x| \leq 1$, then $|1 + x| \leq c$.

Note that the third condition is equivalent to $|\cdot|$ satisfying the quasi-triangle inequality (cf. the third condition in Definition 1). Indeed, let c be as in the third condition above and let $x, y \in K$. If either $x = 0$ or $y = 0$, the quasi-triangle inequality is trivially satisfied, so we may assume that $x \neq 0$, $y \neq 0$, and without loss of generality $|x/y| \leq 1$. Then $|1 + x/y| \leq c \leq 2c(1 + |x/y|)$, so $|x + y| \leq C(|x| + |y|)$, with $C = 2c$. Conversely, if $C \in \mathbb{R}$ is a positive number such that $|x+y| \leq C(|x|+|y|)$ holds for all $x, y \in K$, then in particular $|1+x| \leq C(1+|x|)$, and by making C larger if necessary, we can take $C \geq 1$. Thus, if $|x| \leq 1$, we obtain $|1 + x| \leq 2C$, so the third condition in Definition 9 holds with $c = 2C$.

The trivial absolute value is the one for which $|x| = 1$ for all nonzero $x \in K$. One defines two absolute values $|\cdot|_1$ and $|\cdot|_2$ to be *equivalent* if for any $x \in K$, $|a|_1 < 1$ if and only if $|\cdot|_2 < 1$. It turns out that every absolute value is equivalent to one for which the usual triangle inequality holds.

Let K be a field and $|\cdot|_v$ and absolute value of K. The absolute value $|\cdot|_v$ is said to be *non-Archimedean* if for all $x, y \in K$,

$$|x + y|_v \leq \max\{|x|_v, |y|_v\};$$

otherwise $|\cdot|_v$ is said to be *Archimedean.* We call $|\cdot|_v$ *discrete* if $|K|_v$ is a discrete subset of $\mathbb{R}$. If $|\cdot|_v$ is non-Archimedean, $\mathcal{O}_v = \{x \in K \mid |x|_v \leq 1\}$ is a ring (called the *valuation ring* at v), $\mathfrak{p}_v = \{x \in K \mid |x|_v < 1\}$ is a maximal ideal of $\mathcal{O}_v$, and the field

$$\bar{k}_v = \mathcal{O}_v/\mathfrak{p}_v$$

is called the *residue class field* at v.

Let Σ be a set of nonequivalent and nontrivial absolute values of K. Consider the set $k_0 = \{x \in K \mid |x|_v \leq 1 \text{ for all } v \in \Sigma\}$. It is not hard to show that k_0 is a field if and only if Σ contains no Archimedean prime (see [2, Chapter 12, Section 1]). In this case we may consider k_0 as a subfield of each $\bar{k}_v$.

We will use the following fundamental result, due to Artin and Whaples [3].

Theorem 10. *Suppose that K is a field with a set Σ of mutually nonequivalent and nontrivial absolute values such that the following two conditions hold:*

(1) *For every $x \in K^\times$, $|x|_v = 1$ for all but a finite number of $v \in \Sigma$ and*

$$\prod_{v \in \Sigma} |x|_v = 1;$$

(2) *there is at least one $v \in \Sigma$ such that either v is Archimedean or v is discrete and $\bar{k}_v$ is finite.*

Then K is a global field.

A comment on the proof of this theorem. The proof of [2, Chapter 12, Theorem 3] shows that under the conditions of Theorem 10, if Σ has at least one Archimedean absolute value, then K is a number field and otherwise K is a finite extension of $k_0(t)$, for some t transcendental over k_0. In the latter case, k_0 is a subfield of the finite field $\overline{k}_v$, so k_0 itself is finite and thus K is a global function field.

We now come to the main result of the present section.

Theorem 11. *Let A be a finite quotient PID such that its ideal norm N_A satisfies the quasi-triangle inequality. Then the field of fractions K of A is a global field and A is a ring of integers of K.*

Proof. The ideal norm N_A extends to K via $N_A(a/b) = \frac{N_A(a)}{N_A(b)}$, for $a, b \in A$ and it is immediately checked that N_A on K satisfies the quasi-triangle inequality. Thus N_A on K is an absolute value. We also have $\mathfrak{p}$-adic absolute values for every nonzero prime ideal $\mathfrak{p}$ of A. Indeed, for $a \in A$, let $v_\mathfrak{p}(a)$ denote the largest integer n such that $\mathfrak{p}^n$ divides the ideal aA, and define

$$|a|_\mathfrak{p} = |A/\mathfrak{p}|^{-v_\mathfrak{p}(a)}.$$

Just like N_A, the function $|\cdot|_\mathfrak{p} : a \mapsto |a|_\mathfrak{p}$ extends to K via $|a/b|_\mathfrak{p} = \frac{|a|_\mathfrak{p}}{|b|_\mathfrak{p}}$, and this defines an absolute value on K. Note that N_A is not equivalent to any of the absolute values $|\cdot|_\mathfrak{p}$ because if $p \in A$ is a generator of a prime ideal $\mathfrak{p}$, we have $|p|_\mathfrak{p} = |A/\mathfrak{p}|^{-1} < 1$, while $N_A(p) = |A/\mathfrak{p}| > 1$.

We will now verify that K together with the absolute values N_A and $|\cdot|_\mathfrak{p}$, where $\mathfrak{p}$ runs through the prime ideals of A, satisfies the conditions of Theorem 10.

Condition 1: Since A is not a field (by the definition of basic PID), it has a nonzero proper ideal, so the ideal norm N_A is not the trivial absolute value on K. For any nonzero $a, b \in A$, there are only finitely many prime elements of A that divide a or b, so $|a/b|_\mathfrak{p} = 1$ for all but finitely many $\mathfrak{p}$. Set $|x|_\infty := N_A(x)$ for $x \in K$ and let $\Sigma_f = \{\mathfrak{p} \mid \mathfrak{p} \neq (0) \text{ prime ideal of } A\}$ and $\Sigma = \Sigma_f \cup \{\infty\}$. Note that Σ_f is nonempty since A is not a field. For a nonzero $a \in A$, let $aA = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ be the prime ideal factorization, where $e_i = v_{\mathfrak{p}_i}(a)$. Then

$$\begin{aligned}\prod_{i\in\Sigma} |a|_i &= |\mathfrak{p}_1^{e_1}|_{\mathfrak{p}_1} \cdots |\mathfrak{p}_r^{e_r}|_{\mathfrak{p}_r} \cdot |a|_\infty = |A/\mathfrak{p}_1|^{-e_1} \cdots |A/\mathfrak{p}_r|^{-e_r} \cdot |A/aA| \\ &= |A/\mathfrak{p}_1|^{-e_1} \cdots |A/\mathfrak{p}_r|^{-e_r} \cdot |A/\mathfrak{p}_1|^{e_1} \cdots |A/\mathfrak{p}_r|^{e_r} = 1,\end{aligned}$$

where for the penultimate equality we have used the Chinese remainder theorem and the fact that $|A/\mathfrak{p}^n| = |A/\mathfrak{p}|^n$, for any prime $\mathfrak{p}$ and $n \in \mathbb{N}$ (see [14, Lemma V.3.4]). Thus also $\prod_i |a/b|_i = 1$ for any nonzero $a, b \in A$.

Condition 2: Let $\mathfrak{p} \in \Sigma_f$. Then $|\cdot|_\mathfrak{p}$ is discrete since its values are of the form $|A/\mathfrak{p}|^n$, $n \in \mathbb{Z}$. Moreover, the valuation ring $\mathcal{O}_\mathfrak{p}$ contains A, so by [13, Theorem 2.3] $\mathcal{O}_\mathfrak{p}$ is a finite quotient domain. In particular, $\overline{k}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}/\mathfrak{p}$ is finite. Thus Theorem [3] implies that K is a global field.

By [2, Chapter 12, Corollary 1 and Theorem 4] the set $\{|\cdot|_v \mid v \in \Sigma\}$ consists of all the nontrivial absolute values on K (up to equivalence). Since $x \in K$ lies in A if and only if $v_\mathfrak{p}(x) \geq 0$ for all $\mathfrak{p} \in \Sigma_f$, we have

$$A = \{x \in K \mid |x|_\mathfrak{p} \leq 1 \text{ for all } \mathfrak{p} \in \Sigma_f\} = \bigcap_{\mathfrak{p}\in\Sigma_f} \mathcal{O}_\mathfrak{p}. \tag{1}$$

If K is a number field, let $\mathcal{O}_K$ be its ring of integers. If K is a function field, we define $\mathcal{O}_K$ as follows. As noted just before Theorem 10, k_0 is a subfield of any $\bar{k}_\mathfrak{p}$, so k_0 is finite. Moreover, (1) implies that $k_0 \subset A$. Let $t \in A$ be an element such that $t \notin k$ (such an element exists since A is not a field); then $N_A(t) > 1$ (otherwise $|x|_\mathfrak{p} \leq 1$ for all $\mathfrak{p} \in \Sigma$, hence $t \in k_0$). By the proof of [2, Chapter 12, Theorem 3], K is a finite extension of the field of fractions $k_0(t)$ of $k_0[t]$. In this case, let $\mathcal{O}_K$ denote the integral closure of $k_0[t]$ in K.

It remains to show that in either case we have $A = \mathcal{O}_K$. Let $A_0 = \mathbb{Z}$ in case K is a number field and let $A_0 = k_0[t]$ otherwise. By [4, Corollary 5.22], $\mathcal{O}_K$ is the intersection of all the valuation rings of K containing A_0, where a valuation ring R of K is an integral domain with field of fractions K such that $x \in K$ implies $x \in R$ or $x^{-1} \in R$. It is clear that every $\mathcal{O}_\mathfrak{p}$ is a valuation ring of K containing A_0, so that by (1) we have $\mathcal{O}_K \subseteq A$. Conversely, we claim that every valuation ring R of K containing A_0 equals some $\mathcal{O}_\mathfrak{p}$. Indeed, let R be a valuation ring of K containing A_0. Then R is integrally closed [4, Proposition 5.18], so $\mathcal{O}_K \subseteq R$. If $\mathfrak{m}$ is the maximal ideal of R, then $\mathfrak{q} := \mathcal{O}_K \cap \mathfrak{m}$ is a prime ideal of $\mathcal{O}_K$, and as R is a local ring [4, Proposition 5.18], we have $\mathcal{O}_{K,\mathfrak{q}} \subseteq R$, where $\mathcal{O}_{K,\mathfrak{q}}$ is the localization of $\mathcal{O}_K$ at the prime ideal $\mathfrak{q} = \mathcal{O}_K \cap \mathfrak{p}$. Since $\mathcal{O}_K$ is a Dedekind domain, $\mathcal{O}_{K,\mathfrak{q}}$ is a discrete valuation ring, hence a valuation ring, so by [4, Theorem 5.21] we must have $\mathcal{O}_{K,\mathfrak{q}} = R$. Now, since A is a PID it is integrally closed (and A contains A_0), so we must have $\mathcal{O}_K \subseteq A$. Let $\mathfrak{p}$ be a prime ideal of A such that $\mathfrak{q} = \mathcal{O}_K \cap \mathfrak{p}$ (i.e., $\mathfrak{p}$ can be any prime ideal dividing the ideal $\mathfrak{q}A$). Then $\mathcal{O}_K \subseteq A \subseteq \mathcal{O}_\mathfrak{p}$, so $\mathcal{O}_{K,\mathfrak{q}} \subseteq \mathcal{O}_\mathfrak{p}$ and by [4, Theorem 5.21] $\mathcal{O}_{K,\mathfrak{q}} = \mathcal{O}_\mathfrak{p}$ and thus $R = \mathcal{O}_\mathfrak{p}$. It thus follows from (1) and [4, Corollary 5.22] that $A = \mathcal{O}_K$. □

Let B be a ring of class (G) over the basic PID A, let K be the fraction field of A, and let L be the fraction field of B. With this notation, we have the following result.

Lemma 12. *The field extension L/K is of finite degree and B is the integral closure of A in L. On the other hand, let L'/K be a finite separable extension and let B' be the integral closure of A in L'. Then B' is a ring of class (G) over A.*

Proof. Let $S = A \setminus \{0\}$. Then (by a simple argument) $S^{-1}B$ is finitely generated as a vector space over $S^{-1}A = K$. Thus $S^{-1}B$ is an integral domain that is a finite-dimensional vector space, 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., [14, Proposition 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.

Moreover, it is well known that B' is a Dedekind domain that is finitely generated over A (see, e.g., [14, Theorem I.4.7 and Theorem I.6.2]). Since B' is torsion-free, it is free over A and thus B' is a ring of class (G) over A. □

Corollary 13. *Let A be a finite quotient PID such that its ideal norm N_A satisfies the quasi-triangle inequality. Let B be a Dedekind domain which is a finitely generated and free A-module. Then B is a ring of integers of a global field. In particular, if A is a basic PID and B is of class (G) over A, then B is a ring of integers of a global field.*

Proof. Let K and L be the fraction field of A and B, respectively. By Lemma 12 L is a global field and B is the integral closure of A in L. By Proposition 11, A is the integral closure in K of A_0, where A_0 is either $\mathbb{Z}$ or $\mathbb{F}_q[t]$, for some $t \in K$. Let C be the integral closure of A_0 in L. Since $A_0 \subseteq A$ we trivially have $C \subseteq B$. By the transitivity of integrality [14, Proposition I.2.18] applied to $A_0 \subseteq A \subseteq B$, we have that B is integral over A_0, hence $B \subseteq C$ and so $B = C$. We have proved that B is the integral closure of $\mathbb{Z}$ or $\mathbb{F}_q[t]$ in the global field L and thus B is a ring of integers in L. □

One may ask whether there exists a Dedekind domain B that is finitely generated and free over a PID A with finite quotients and such that B has infinite class group. Theorem 7 and Corollary 13 show that if such an example exists, then the quasi-triangle inequality must fail for ideal norm N_A. We note that Goldman [10] and Heitmann [11] have given examples of Dedekind domains with finite quotients and infinite class groups, but we do not know whether these examples are finitely generated and free over some PID.

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

Acknowledgement. I wish to thank Pete L. Clark and D. Lorenzini for pointing out inaccuracies in a previous version and for comments that helped to improve the exposition.

References

[1] W. A. Adkins and S. H. Weintraub, *Algebra: An approach via module theory*, volume 136 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, 1992.
[2] E. Artin, *Algebraic numbers and algebraic functions*, Gordon and Breach Science Publishers, New York-London-Paris, 1967.
[3] E. Artin and G. Whaples, *Axiomatic characterization of fields by the product formula for valuations*, Bull. Amer. Math. Soc. **51** (1945), no. 7, 469–492.
[4] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.
[5] L. Claborn, *Dedekind domains and rings of quotients*, Pacific J. Math. **15** (1965), 59–64.
[6] 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).
[7] 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.
[8] E. D. Davis, *Overrings of commutative rings. II. Integrally closed overrings*, Trans. Amer. Math. Soc. **110** (1964), 196–212.
[9] R. Gilmer and J. Ohm, *Integral domains with quotient overrings*, Math. Ann. **153** (1964), 97–103.
[10] O. Goldman, *On a special class of Dedekind domains*, Topology **3** (1964), no. suppl. 1, 113–118.
[11] R. C. Heitmann, *PID's with specified residue fields*, Duke Math. J. **41** (1974), no. 3, 565–582.
[12] D. G. Higman and J. E. McLaughlin, *Finiteness of class numbers of representations of algebras over function fields.*, Mich. Math. J. **6** (1959), 401–404.
[13] K. B. Levitz and J. L. Mott, *Rings with finite norm property*, Canadian J. Math. **24** (1972), 557–565.

[14] D. Lorenzini, *An invitation to arithmetic geometry*, volume 9 of *Graduate Studies in Mathematics*, American Mathematical Society, Providence, RI, 1996.
[15] D. Ramakrishnan and R. J. Valenza, *Fourier analysis on number fields*, volume 186 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, 1999.
[16] I. Reiner, *Maximal orders*, Academic Press, London-New York, 1975, london Mathematical Society Monographs, No. 5.
[17] R. G. Swan, *K-theory of finite groups and orders*, Lecture Notes in Mathematics, Vol. 149, Springer-Verlag, Berlin-New York, 1970.
[18] H. Zassenhaus, *Neuer beweis der endlichkeit der klassenzahl bei unimodularer aequivalenz endlicher ganzzahliger substitutionsgruppen*, Abh. Math. Semin. Univ. Hamb. **12** (1938), 276–288.

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