Elliptic Dedekind domains revisited

L'Enseignement Mathématique (2) 55 (2009), 213–225

ELLIPTIC DEDEKIND DOMAINS REVISITED

by Pete L. CLARK*)

ABSTRACT. We give an affirmative answer to a 1976 question of M. Rosen: every abelian group is isomorphic to the class group of an elliptic Dedekind domain R. We can choose R to be the integral closure of a PID in a quadratic field extension. In particular, this yields new and — we feel — simpler proofs of theorems of L. Claborn and C. R. Leedham-Green.

1. INTRODUCTION

Terminology: For a scheme X, $\operatorname{Pic} X$ denotes the Picard group of isomorphism classes of line bundles on X. In the case $X = \operatorname{Spec} R$, we write simply $\operatorname{Pic}(R)$. When R is a Dedekind domain, $\operatorname{Pic}(R)$ is the *ideal class group* of R.

A celebrated 1966 theorem of Luther Claborn asserts that for any abelian group A whatsoever, there exists a Dedekind domain R whose ideal class group $\operatorname{Pic}(R)$ is isomorphic to A [3]. A different proof was given in 1972 by C. R. Leedham-Green [9], which shows that R may be taken to be the integral closure of a PID in a quadratic field extension. Claborn's proof requires familiarity with the divisor class group of a Krull domain. Leedham-Green's proof is more elementary — in his own words, it is "based on a naive geometrical construction" — but is quite intricate.

*) Partially supported by National Science Foundation grant DMS-0701771.

Work of M. Rosen takes a completely different approach, based on the following facts:

FACT I. *For an elliptic curve E over a field k, the standard affine ring $R = k[E]$ is a Dedekind domain with* $\mathrm{Pic}(R)$ *isomorphic to the Mordell-Weil group* $E(k)$.

FACT II. *With $R = k[E]$ as above, for any subgroup $H \subset \mathrm{Pic}(R)$, there exists an overring R^H of R such that* $\mathrm{Pic}(R^H) \cong \mathrm{Pic}(R)/H$.

From these two facts it follows that any abelian group which is isomorphic to a quotient group of a Mordell-Weil group is the class group of some Dedekind domain. Rosen calls a Dedekind domain arising as an overring of the standard affine ring of some elliptic curve *elliptic*.

In [11], Rosen shows that any finitely generated abelian group is the class group of the coordinate of some (not necessarily standard) affine elliptic curve over some number field k. In [12], Rosen uses Serre's open image theorem to show that every countably generated abelian group is the class group of an elliptic Dedekind domain. His method does not work for uncountable groups, and accordingly he asks whether every abelian group is the class group of an elliptic Dedekind domain.

Our main result gives an affirmative answer to this question.

MAIN THEOREM. *Let A be any abelian group.*

a) *There is an elliptic Dedekind domain R with* $\mathrm{Pic}(R) \cong A$.

b) *We can take R to be the integral closure of a PID in a quadratic field extension.*

Our construction is inspired by Rosen's work and follows his general strategy in that it uses Facts I and II above to reduce to the problem of constructing a free abelian group of arbitrary rank as a quotient of some Mordell-Weil group. But there are also several differences. First, we construct arbitrary free abelian groups as Mordell-Weil groups, whereas Rosen constructs a free abelian group of countable rank as the quotient of a Mordell-Weil group by its torsion subgroup. Second, whereas Rosen's construction takes k to be the maximal multiquadratic extension of $\mathbf{Q}$, ours does not[1]). Our field k is a

[1]) Nor could it, of course: the group of rational points of an elliptic curve over a countable field must be countable.

transfinitely iterated function field, and accordingly we make no use of Serre's open image theorem nor of any other deep arithmetic facts.

The proof of the Main Theorem occupies little more than a single page. However, our goal is to maximize the audience that can read and appreciate the argument rather than to minimize its length. To this end, we have included in §2 some expository material on class groups of overrings of Dedekind domains. We also discuss Dedekind domains in which every ideal class can be represented by at least one prime ideal — we call such a domain *replete* — as well as a weaker property that suffices for our applications. Our Theorem 14 on the repleteness and weak repleteness of elliptic Dedekind domains may be new. The proof of the Main Theorem is in §3.

2. Preliminaries

We wish to recall some results concerning the effect of passage to an overring on the class group, and on the connection between class groups of affine curves and the Jacobians of their projective completions. We could not resist mentioning a few interesting results which are closely related to these topics but not needed for the proof of the Main Theorem. For such results we explicitly state that they are not needed in the sequel, and we give references rather than proofs.

2.1 Basic definitions

For a Dedekind domain R, let $\Sigma(R)$ be the set of all nonzero prime ideals; we typically speak of elements of $\Sigma(R)$ as simply "primes". Consider the map

$$\Phi\colon \Sigma(R) \to \mathrm{Pic}(R), \qquad \mathfrak{p} \mapsto [\mathfrak{p}].$$

Since the group $\mathrm{Frac}(R)$ of fractional ideals of R is free abelian with $\Sigma(R)$ as a basis, Φ uniquely extends to a homomorphism $\mathrm{Frac}(R) \to \mathrm{Pic}(R)$, which is surjective, and whose kernel is the subgroup $\mathrm{Prin}(R)$ of principal fractional ideals.

If R and S are Dedekind domains, by a *morphism* of Dedekind domains we mean an injective ring homomorphism $\iota\colon R \hookrightarrow S$. If I is a fractional ideal of R, then the *push-forward* $I \in \mathrm{Frac}(R) \mapsto IS$ induces a homomorphism from $\mathrm{Frac}(R)$ to $\mathrm{Frac}(S)$, denoted ι_*. Since the push-forward of a principal fractional ideal remains principal, ι_* factors through to a homomorphism $\iota_*\colon \mathrm{Pic}(R) \to \mathrm{Pic}(S)$. For an ideal J of S, we denote by $\iota^*(J)$ the ideal $J \cap R$ of R.

2.2 Overrings

If R is an integral domain with field of fractions K, an *overring* of R is a ring S intermediate between R and K, i.e., $R \subseteq S \subseteq K$.

LEMMA 1. *Let $\iota: R \hookrightarrow S$, where R is a Dedekind domain and S is an overring.*

a) *For any $\mathfrak{P} \in \Sigma(S)$, $S_{\mathfrak{P}} = R_{\mathfrak{P} \cap R}$.*

b) *S is itself a Dedekind domain.*

c) *$\iota^*: \Sigma(S) \hookrightarrow \Sigma(R)$.*

d) *For all $\mathfrak{P} \in \Sigma(S)$, $\iota_*(\iota^*\mathfrak{P}) = \mathfrak{P}$.*

Proof. a) Put $\mathfrak{p} = \mathfrak{P} \cap R$. Since $\mathfrak{P}$ is a nonzero prime ideal in the overring S of R, there exist nonzero elements $x, y \in R$ such that $\frac{x}{y} \in \mathfrak{P}$. Then $0 \neq x = y(\frac{x}{y}) \in \mathfrak{p}$, so $\mathfrak{p}$ is a nonzero prime ideal of R. Thus $S_{\mathfrak{P}}$ contains the DVR $R_{\mathfrak{p}}$ and is properly contained in its fraction field, so $S_{\mathfrak{P}} = R_{\mathfrak{p}}$.

b) By the Krull-Akizuki Theorem [10, Thm. 11.7], S is a one-dimensional Noetherian domain; and by part a) the localization of S at every prime is a DVR, hence S is integrally closed and thus a Dedekind domain.

c) From part a), we have that there is no other prime $\mathfrak{P}'$ of S with $\iota^*(\mathfrak{P}') = \mathfrak{p}$, since localizations at distinct primes in a Dedekind ring are distinct DVRs.

d) First,

$$(\iota_*\iota^*(\mathfrak{P}))S_{\mathfrak{P}} = \mathfrak{p}S_{\mathfrak{P}} = \mathfrak{P}S_{\mathfrak{P}}.$$

By part c), $\iota_*(\iota^*(\mathfrak{P}))$ is not divisible by any prime other than $\mathfrak{P}$, so $\iota_*(\mathfrak{p}) = \mathfrak{P}$.

COROLLARY 2. *Let S be an overring of the Dedekind domain R. The prime ideals of S are identified, via ι^*, with the prime ideals $\mathfrak{p}$ of R such that $\mathfrak{p}S \subsetneq S$.*

We can explicitly describe all overrings of a Dedekind domain R. For an arbitrary subset $W \subset \Sigma(R)$, put $R_W := \bigcap_{\mathfrak{p} \in W} R_{\mathfrak{p}}$, the intersection taking place in the fraction field K. For the sake of simplifying some later formulas, we also define

$$R^W = R_{\Sigma(R) \setminus W}.$$

Evidently R_W is an overring of R, hence is itself a Dedekind domain. Conversely:

THEOREM 3. *Let R be a Dedekind domain with fraction field K, and let $R \subset S \subset K$ be an overring. Let W be the set of all primes $\mathfrak{p}$ of R such that $\mathfrak{p}S \subsetneq S$. Then*

$$S = R_W = \bigcap_{\mathfrak{p} \in W} R_{\mathfrak{p}} .$$

Proof. Not needed in the sequel; see e.g. [8, Cor. 6.12].

The reader may be more used to thinking about generating overrings by *localization*: if R is a domain and $T \subset R$ a multiplicatively closed set, then $R[T^{-1}]$ is an overring of R. Probably the reader knows that every overring of $\mathbf{Z}$ is obtained by localization; in fact this is true for overrings of any PID R. For this it suffices to exhibit $R[\frac{x}{y}]$ as $R[\frac{1}{z}]$. The key point here [2]) is that since R is a UFD we may assume that x and y are relatively prime, and then there exist $a, b \in R$ with $ax + by = 1$, so that $\frac{1}{y} = \frac{ax+by}{y} = a\left(\frac{x}{y}\right) + b\left(\frac{y}{y}\right) \in R[\frac{x}{y}]$. But in general, not all overrings are realizable by localization:

THEOREM 4. *Let R be a Noetherian domain, and consider the following properties:*

(i) *Every overring of R is integrally closed.*

(ii) *Every overring of R is obtained by localizing at a multiplicative subset.*

Then (i) *holds if and only if R is a Dedekind domain, and* (ii) *holds if and only if R is a Dedekind domain with torsion class group.*

Proof. Not needed in the sequel; see [5] or [6].

The following result explains the importance of overrings in the study of class groups of Dedekind domains.

THEOREM 5 (Claborn [2]). *Let R be a Dedekind domain, and $S = R^W$ be an overring of R. There exists a short exact sequence*

$$0 \longrightarrow H \longrightarrow \mathrm{Pic}(R) \xrightarrow{\iota_*} \mathrm{Pic}(S) \longrightarrow 0 ,$$

where $H = \langle \Phi(W) \rangle$ is the subgroup generated by classes of primes $\mathfrak{p}$ with $\mathfrak{p}S = S$.

Proof. Since $\iota_* \circ \iota^* = 1_{\Sigma(S)}$, ι_* is surjective on prime ideals; *a fortiori* the induced map on class groups is surjective. Clearly each prime $\mathfrak{p}$ with

[2]) The fact that there is no ring strictly intermediate between a DVR and its fraction field, which was used in the proof of Lemma 1, is an (even) easier special case.

$\mathfrak{p}S = S$ lies in the kernel. Conversely, suppose I is a fractional ideal of R in the kernel of ι_*, so that there exists x in the fraction field with $IS = xS$. Then $xI^{-1}S = S$, so that xI^{-1} is a product of primes $\mathfrak{p}$ with $\mathfrak{p}S = S$.

Thus one can realize certain quotients of the Picard group of R by passing to a suitable overring S. In general however, not every subgroup of $\mathrm{Pic}(R)$ is generated by classes of prime ideals. This brings us to the next section.

2.3 Replete Dedekind rings

We say that a Dedekind domain R is *replete* if the map Φ is surjective, i.e., if every ideal class is represented by a prime ideal.

Proposition 6. *Let R be a replete domain, and let $H \subset \mathrm{Pic}(R)$ be any subgroup. Then there exists an overring S of R such that $\mathrm{Pic}(S) \cong \mathrm{Pic}(R)/H$.*

Proof. Indeed, if R is replete, then H is generated by a set W of prime ideals of R. Then take S to be the overring $R^W = \bigcap_{\mathfrak{p} \in \Sigma(R) \setminus W} R_{\mathfrak{p}}$. By Theorem 5, $\mathrm{Pic}(R^W) \cong \mathrm{Pic}(R)/H$.

For the proof of Proposition 6 to go through, it suffices that R have the property that any subgroup H of $\mathrm{Pic}(R)$ is generated by classes of prime ideals. Let us call a domain with this property *weakly replete*.

Corollary 7. *An overring of a weakly replete domain is weakly replete.*

Proof. This follows easily from Theorem 5.

Examples. Trivially, a PID is replete. The repleteness of the ring of integers in a global field is a weak version of the Chebotarev Density Theorem. We will see in §2.4 that the standard affine ring of an elliptic curve is weakly replete but not necessarily replete. Examples of domains which are not weakly replete seem harder to come by. In [4], Claborn exhibits for each $n \in \mathbf{Z}^+$ a Dedekind domain R_n whose class group is cyclic of order n and such that $[\mathfrak{p}] = [\mathfrak{q}]$ for all $\mathfrak{p}, \mathfrak{q} \in \Sigma(R_n)$, as well as a Dedekind domain R with $\mathrm{Pic}(R) \cong \mathbf{Z}$ such that for all $\mathfrak{p} \in \Sigma(R)$, $[\mathfrak{p}] = \pm 1$.

A *repletion* of a Dedekind domain R is a replete Dedekind domain S together with an injective ring homomorphism $\iota: R \hookrightarrow S$, such that $\iota_*: \mathrm{Pic}(R) \xrightarrow{\sim} \mathrm{Pic}(S)$.

THEOREM 8 (Claborn). *For a Dedekind domain R, let R^1 denote the localization of $R[t]$ at the multiplicative set generated by all monic polynomials. Then R^1 is Dedekind and the composite map $\iota\colon R \to R[t] \to R^1$ is a repletion.*

Proof. Not needed in the sequel; see [1, Cor. 2.5].

COROLLARY 9 (Claborn). *For any Dedekind domain R, and any subgroup $H \subset \mathrm{Pic}(R)$, there exist a Dedekind domain S and a homomorphism of Dedekind domains $\iota\colon R \to S$ making the following sequence exact:*

$$0 \longrightarrow H \longrightarrow \mathrm{Pic}(R) \xrightarrow{\iota_*} \mathrm{Pic}(S) \longrightarrow 0\,.$$

Thus every quotient group of $\mathrm{Pic}(R)$ is the class group of some Dedekind domain.

Proof. This follows immediately from Theorem 8 and Proposition 6.

2.4 AFFINE DOMAINS, GEOMETRIC DOMAINS, AND ELLIPTIC DOMAINS

Let k be a field. To a pair (C, O), where $C_{/k}$ is a complete, nonsingular geometrically integral curve and $O \in C(k)$ is a rational point, we attach the rational function field $k(C)$ and *standard affine ring* $k[C^o]$, the subring of $k(C)$ consisting of all functions which are regular on all points except (possibly) O. Note that $k[C^o]$ is the coordinate ring of the affine algebraic curve $C^o = C \backslash O$. The ring $k[C^o]$ is a nonsingular Noetherian domain of dimension one, i.e., a Dedekind domain. Consider the map which sends a degree 0 divisor $\sum_P n_P[P]$ on C to the divisor $\sum_{P \neq O} n_P[P]$ (of degree $-n_O$) on C^o. Upon quotienting out by principal divisors, this gives an isomorphism

$$J(C)(k) = \mathrm{Pic}^0(C) \xrightarrow{\sim} \mathrm{Pic}(k[C^o])\,, \tag{1}$$

where $J(C)$ is the Jacobian of C. Thus the class group of a standard affine domain is canonically isomorphic to the group of k-rational points on a certain (Jacobian) abelian variety.

When $C = E$ has genus one, the automorphism group acts transitively on the set of k-rational points, so the affine curve E^o is independent of the choice of O. In this case, we simplify the notation $k[E^o]$ to $k[E]$.

The following special case of (1) is already interesting:

COROLLARY 10. *For an elliptic curve $E_{/k}$, the following are equivalent:*

(i) *The standard affine ring $k[E]$ is a PID.*

(ii) *E has trivial Mordell-Weil group: $E(k) = 0$.*

Later we shall exhibit $E_{/k}$ such that $E(k) = 0$, i.e., "elliptic PID's" exist! In general, let us say that a Dedekind domain R is *affine* if it is of the form $k[C^o]$ for some nonsingular, geometrically integral affine curve C^o over a field k. Write C for the nonsingular projective model of C^o. As long as $C \setminus C^o$ contains at least one k-rational point, a well-known argument using Riemann-Roch shows that the affine domain $k[C^o]$ is an overring of some standard affine domain.

THEOREM 11 (Rosen). *Let $C^o = C \setminus S$ be a nonsingular, geometrically integral affine curve over a field k. Let $D^0(S)$ be the subgroup of* $\mathrm{Div}(C)$ *consisting of degree 0 divisors supported on S, and let $P(S)$ be the principal divisors in $D^0(S)$. Let d be the least positive degree of a divisor supported on S (note that $d = 1$ if and only if S contains at least one k-rational point), and let i be the least positive degree of a divisor on C. Then there is an exact sequence*

$$(2) \qquad 0 \to D^0(S)/P(S) \longrightarrow \mathrm{Pic}^0(C) \longrightarrow \mathrm{Pic}(C^o) \longrightarrow Z(d/i) \longrightarrow 0,$$

where $Z(d/i)$ is a cyclic group of order d/i.

Proof. Not needed in the sequel; see [11].

Rosen remarks that Theorem 11 was, in essence, already known to F.K. Schmidt in the 1930's. Nevertheless, one cannot help but feel that it is not as widely known as it should be. It has many consequences, some amusing and some important. First:

EXAMPLE. Let k be a field of characteristic different from 2, and let $C^o = C \setminus S$ be the affine curve with coordinate ring $R_\circ = k[C^o] = k[x,y]/(x^2 + y^2 - 1)$. Here S is a degree 2 divisor consisting of a pair of points ∞_1, ∞_2 which are (resp. are not) *each* k-rational if -1 is (resp. is not) a square in k. We conclude:

THEOREM 12. *Let k be a field of characteristic different from 2, and let $R_\circ$ be the Dedekind domain $k[x,y]/(x^2 + y^2 - 1)$. Then:*

(i) *If -1 is a square in k, then $R_\circ$ is a UFD (equivalently, a PID).*

(ii) *If -1 is not a square in k, then $R_\circ$ is not a UFD: rather* $\mathrm{Pic}(R_\circ) \cong \mathbf{Z}/2\mathbf{Z}$.

In particular, taking $k = \mathbf{R}$, the ring $R_\circ = \mathbf{R}[\cos\theta, \sin\theta]$ of real trigonometric polynomials is not a UFD. H.F. Trotter in [14] gives an

appealingly direct proof of this fact by showing that the familiar identity

$$\sin^2\theta = (1+\cos\theta)(1-\cos\theta)$$

is a non-unique factorization into irreducibles. (Notice that $\mathbf{Z}/2\mathbf{Z}$ is also the Picard group of topological $\mathbf{R}$-line bundles on the unit circle!) On the other hand, taking $k = \mathbf{C}$, $R_\circ \cong \mathbf{C}[e^{i\theta}, (e^{i\theta})^{-1}]$ is the ring of complex trigonometric polynomials, which is, in accordance with Theorem 12, a PID.

Using (2) and the fact that every elliptic curve over $\overline{\mathbf{Q}}$ has infinite rank, Rosen deduces:

THEOREM 13 (Rosen). *For any finitely generated abelian group A, there is a number field k and a (not necessarily standard) affine elliptic curve E^o over k such that* $\mathrm{Pic}(k[E^o]) \cong A$.

The claim that in Theorem 13 we can always take $k = \mathbf{Q}$ is equivalent to the existence of elliptic curves $E_{/\mathbf{Q}}$ of arbitrarily large rank, a notorious open problem.

A Dedekind domain is *geometric* if it is an overring of an affine Dedekind domain. In other words, a geometric Dedekind domain is the ring of all functions on a complete curve $C_{/k}$ which are regular on the complement of some fixed, but possibly infinite, subset of closed points of C. Finally, an *elliptic* Dedekind domain is an overring of the standard affine domain of an elliptic curve $E_{/k}$.

THEOREM 14. *Let $E_{/k}$ be an elliptic curve with equation $y^2 = P(x) = x^3 + Ax + B$.*

a) *The standard affine ring $k[E]$ is weakly replete (hence so are all of its overrings).*

b) *If k is algebraically closed, $k[E]$ is not replete.*

c) *Suppose k does not have characteristic 2 and $k[E]$ is not replete. Then for all $x \in k$, there exists $y \in k$ with $y^2 = P(x)$.*

Proof. Each point $P \neq O$ on $E(k)$ corresponds to a prime ideal in the standard affine ring $k[E]$; according to the isomorphism of (1), every nontrivial element of $\mathrm{Pic}(k[E])$ arises in this way. This proves part a). Part b) is similar: if k is algebraically closed, then by Hilbert's Nullstellensatz every prime ideal of $k[E]$ corresponds to a k-valued point $P \neq O$ on $E(k)$, which under (1) corresponds to a nontrivial element of the class group. Therefore the trivial

class is not represented by any prime ideal. Under the hypotheses of part c), there exists an $x \in k$ such that the points $(x, \pm\sqrt{P(x)})$ form a Galois conjugate pair. Therefore the divisor $(x, \sqrt{P(x)}) + (x, -\sqrt{P(x)})$ represents a closed point on the curve E, in other words a nonzero prime ideal of $k[E]$. But the corresponding point on $E(k)$ is $(x, \sqrt{P(x)}) + (x, -\sqrt{P(x)}) = O$.

To sum up: since every abelian group A is a quotient of a free abelian group $FA(\kappa)$ of some rank κ, and the standard affine domain $k[E]$ attached to an elliptic curve $E_{/k}$ is weakly replete, in order to realize A as the Picard group of an elliptic Dedekind domain it suffices to find k and E such that $E(k) \cong FA(\kappa)$. This we handle in the next section, along with the claim that the domain can be taken to be the integral closure of a PID in a quadratic extension.

3. Proof of the Main Theorem

PROPOSITION 15. *Let K be a field of characteristic 0 and $E_{/K}$ an elliptic curve. Let $K(E)$ be the function field of E. Then there is a short exact sequence*

$$0 \longrightarrow E(K) \longrightarrow E(K(E)) \longrightarrow \mathrm{End}_K(E) \longrightarrow 0.$$

Here $\mathrm{End}_K(E) \cong \mathbf{Z}^{a(E)}$, where $a(E) = 2$ if E has K-rational CM, and otherwise $a(E) = 1$. Since $\mathrm{End}_K(E)$ is free abelian, we have $E(K(E)) \cong E(K) \bigoplus \mathbf{Z}^{a(E)}$.

Proof. $E(K(E))$ is the group of rational maps from the nonsingular curve E to the complete variety E (the group law is pointwise addition). But every rational map from a nonsingular curve to a complete variety is everywhere defined, so $E(K(E))$ is the group of all morphisms $E \to E$ under pointwise addition. The constant morphisms form a subgroup isomorphic to $E(K)$, and every map of curves from E to itself differs by a unique constant from a map of elliptic curves $(E, O) \to (E, O)$, i.e., an endomorphism of E.

Now take $E_{/\mathbf{Q}} : y^2 + y = x^3 - 49x - 86$, so $E(\mathbf{Q}) = 0$ [7, Theorem H]. This elliptic curve has nonintegral j-invariant $\frac{2^{12}3^3}{37}$, so does not have complex multiplication. So defining $K_0 = \mathbf{Q}$ and $K_{n+1} = K_n(E_{/K_n})$, Proposition 15 gives

$$E(K_n) \cong \bigoplus_{i=1}^{n} \mathbf{Z}.$$

Now define $K_\infty = \lim_{n\to\infty} K_n$; what can we say about $E(K_\infty)$? We have the following technical result:

LEMMA 16 ("Continuity Lemma"). *Let K be a field, $(K_i)_{i\in I}$ be a directed system of field extensions of K, and $E_{/K}$ an elliptic curve. Then there is a canonical isomorphism*

$$\lim_I E(K_i) = E(\lim_I K_i)\,.$$

Proof. E.g. by abstract nonsense: this holds for any representable contravariant functor from the category of affine K-schemes to the category of abelian groups.

Therefore $E(K_\infty) = \lim_n E(K_n) = \bigoplus_{n\in\mathbf{Z}^+} \mathbf{Z}$, recovering Rosen's Theorem.

Now given an uncountable set κ, choose ω an ordinal of the same cardinality. We define the field K_ω by transfinite induction: $K_0 = \mathbf{Q}$, for an ordinal $o < \omega$, $K_{o+1} = K_o(E_{/K_o})$, and for a limit ordinal o, $K_o = \lim_{o'<o} K_{o'}$. By the Continuity Lemma, we have $E(K_o) = \lim_{o'\in o} E(K_{o'})$.

An isomorphism from $E(K_o)$ to $\bigoplus_{o'\in o} \mathbf{Z}$ can be built up by transfinite induction as well; this amounts to the following elementary exercise (cf. [13, p. 105]):

FACT. *For an abelian group A, the following are equivalent:*

(i) *A is free abelian.*

(ii) *A has a well-ordered ascending series with all factors A_{s+1}/A_s infinite cyclic.*

Thus for a given abelian group $A = \mathbf{Z}[\kappa]/H$, we have constructed a field k, an elliptic curve $E_{/k}$, and an overring R of the affine domain $k[E]$ such that $\mathrm{Pic}(R) \cong \mathbf{Z}[\kappa]/H \cong A$, which proves part a) of the Main Theorem.

As for the second part, let σ be the automorphism of the function field $k(E)$ induced by $(x, y) \mapsto (x, -y)$, and notice that σ corresponds to inversion $P \mapsto -P$ on $E(k) = \mathrm{Pic}(k[E])$. Let $S = R^\sigma$ be the subring of R consisting of all functions which are fixed by σ. Then $k[E]^\sigma = k[x]$ is a PID, and S is an overring of $k[x]$, hence also a PID. More precisely, S is the overring of all functions on the projective line which are regular away from the point at infinity and the x-coordinates of all the elements in H (note that since H is a subgroup, it is stable under inversion). Finally, to see that R is the integral

closure of S in the separable quadratic field extension $k(E)/k(x)$, it suffices to establish the following simple result.

LEMMA 17. *Let L/K be a finite Galois extension of fields, and S a Dedekind domain with fraction field L. Suppose that for all $\sigma \in \mathrm{Gal}(L/K)$, $\sigma(S) = S$. Then S is the integral closure of $R := S \cap K$ in L.*

Proof. Since S is integrally closed, it certainly contains the integral closure of R in L. Conversely, for any $x \in S$, $P(t) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \big(t - \sigma(x)\big)$ is a monic polynomial with coefficients in $(S \cap K)[t]$ satisfied by x.

REMARK. It is possible to avoid the use of an elliptic curve with trivial Mordell-Weil group: since we are, in general, passing to a quotient anyway, we can just mod out by $E(k)$. In fact, at the expense of introducing minor complications, one can make the argument go through starting with any elliptic curve E over any field k whatsoever.

ACKNOWLEDGEMENTS. The topic of class groups of Dedekind domains came up in the lectures and final student projects of a course taught by the author in Spring of 2008 at the University of Georgia. I wish to thank the students in that course, especially Jim Stankewicz and Nathan Walters, for their interest and insight.

REFERENCES

[1] CLABORN, L. Dedekind domains and rings of quotients. *Pacific J. Math. 15* (1965), 59–64.

[2] —— Dedekind domains: Overrings and semi-prime elements. *Pacific J. Math. 15* (1965), 799–804.

[3] —— Every abelian group is a class group. *Pacific J. Math. 18* (1966), 219–222.

[4] —— Specified relations in the ideal group. *Michigan Math. J. 15* (1968), 249–255.

[5] DAVIS, E. D. Overrings of commutative rings. II. Integrally closed overrings. *Trans. Amer. Math. Soc. 110* (1964) 196–212.

[6] GILMER, R. and J. OHM. Integral domains with quotient overrings. *Math. Ann. 153* (1964), 97–103.

[7] KOLYVAGIN, V. A. On the Mordell-Weil and Shafarevich-Tate groups for Weil elliptic curves. *Math. USSR-Izv. 33* (1989), 473–499.

[8] LARSEN, M. D. and P. J. MCCARTHY. *Multiplicative Theory of Ideals*. Pure and Applied Mathematics *43*. Academic Press, New York-London, 1971.

[9] LEEDHAM-GREEN, C. R. The class group of Dedekind domains. *Trans. Amer. Math. Soc. 163* (1972), 493–500.

[10] MATSUMURA, H. *Commutative Ring Theory*. Translated from the Japanese by M. Reid. Second edition. Cambridge Studies in Advanced Mathematics *8*. Cambridge University Press, Cambridge, 1989.

[11] ROSEN, M. S-units and S-class group in algebraic function fields. *J. Algebra 26* (1973), 98–108.

[12] —— Elliptic curves and Dedekind domains. *Proc. Amer. Math. Soc. 57* (1976), 197–201.

[13] SCOTT, W. R. *Group Theory*. Second edition. Dover Publications, Inc., New York, 1987.

[14] TROTTER, H. F. An overlooked example of nonunique factorization. *Amer. Math. Monthly 95* (1988), 339–342.

(Reçu le 22 juin 2008)

Pete L. Clark

Department of Mathematics
Boyd Graduate Studies Research Center
University of Georgia
Athens, GA 30602-7403
U. S. A.
e-mail : pete@math.uga.edu