PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 57, Number 2, June 1976

ELLIPTIC CURVES AND DEDEKIND DOMAINS

MICHAEL ROSEN

ABSTRACT. Some results are obtained on the group of rational points on elliptic curves over infinite algebraic number fields. A certain naturally defined class of Dedekind domains, elliptic Dedekind domains, are described and it is shown that every countable abelian group can be realized as the class group of an elliptic Dedekind domain.

Introduction. Let E be an elliptic curve defined over a field K. Let S be a set of K rational points on E and $R_S(E)$ the ring of K rational functions on E having all their poles in S. Then $R_S(E)$ is a Dedekind domain. We call such a ring an elliptic Dedekind domain. What abelian groups arise as class groups of such rings? In [6] it is shown that every finitely generated abelian group arises in this way. In this paper we extend this result as follows.

THEOREM A. *Every countable abelian group can be realized as the class group of an elliptic Dedekind domain.*

The proof of Theorem A is dependent on the following theorem which is of independent interest.

THEOREM B. *Let E be an elliptic curve defined over an algebraic number field k. Let K/k be a solvable algebraic extension, possibly infinite. Assume E has no complex multiplications. Then the torsion subgroup of $E(K)$ is finite and modulo torsion $E(K)$ is a free abelian group.*

The proof of Theorem B is dependent on deep results of J.-P. Serre on division points of elliptic curves (see [7] and [8]). It is related to, and in fact inspired by, results of B. Mazur [4].

L. Claborn has shown [1] that any abelian group can be realized as the class group of a Dedekind domain. The same result may be true for elliptic Dedekind domains. The main stumbling block for our methods is that Proposition 1 of this paper is not true if the hypothesis of countability is removed. Hopefully an adequate substitute can be found.

1. **A result on abelian groups.** We need a proposition on abelian groups which is essentially due to L. Pontryagin [5].

By the rank of an abelian group we mean the maximal number of linearly

Received by the editors September 29, 1975.
AMS (MOS) subject classifications (1970). Primary 14K15, 13F05.
Key words and phrases. Elliptic curves, rational points, Dedekind domains, class group.

independent elements in the group. For example, the integers Z and the rational numbers Q have rank one. Any torsion group has rank zero.

PROPOSITION 1. *Let A be a countable abelian group. Suppose every subgroup of finite rank is finitely generated. Then A_t, the torsion subgroup of A, is finite and A/A_t is free.*

PROOF. A_t has rank zero and is therefore finitely generated. A finitely generated torsion abelian group is finite.

Let $B = A/A_t$. B is torsion free. Let $B_1 \subseteq B$ have finite rank. Then A_1, the inverse image of B_1 in A, also has finite rank and so is finitely generated. Thus B_1 is finitely generated and torsion free and so free.

We are reduced to showing: if B is a countable, torsion free abelian group with every subgroup of finite rank free, then B is free. This is a result of L. Pontryagin. We include a proof for completeness.

Let $\{b_1, b_2, b_3, \dots\}$ be a maximal linearly independent set in B. Let $B_m = \{b \in B | b, b_1, b_2, \dots, b_m$ are linearly dependent$\}$. Then $B_1 \subseteq B_2 \subseteq B_3 \subseteq \cdots$ is an ascending chain of subgroups of finite rank and $B = \cup_m B_m$. In fact, B_m has rank m and so, by hypothesis, is free of rank m. B_m/B_{m-1} is easily seen to be torsion free and so is free of rank one. Thus $B_m = B_{m-1} + Zc_m$ (direct sum) for some $c_m \in B_m$. It follows that $\{c_1, c_2, c_3, \dots\}$ is a free basis for B.

2. **Elliptic curves.** Let E be an elliptic curve defined over an algebraic number field k. Let $\bar{k}$ denote the algebraic closure of k and for each prime l, let $E^{(l)}$ be the points of l power order and E_l the points of order dividing l in $E(\bar{k})$.

Let $k^{(l)} = k(E^{(l)})$ be the field obtained by adjoining the coordinates of all the points in $E^{(l)}$ to k. Finally, let $k_l = k(E_l)$.

Suppose E has no complex multiplications. Then Serre has shown

(i) For all but finitely many l, $G(k_l/k)$ is isomorphic to $\mathrm{Gl}_2(Z/lZ)$.

(ii) For all but finitely many l, $G(k^{(l)}/k)$ is isomorphic to $\mathrm{Gl}_2(Z_l)$.

(iii) For all l, $G(k^{(l)}/k)$ is isomorphic to an open subgroup of $\mathrm{Gl}_2(Z_l)$.

(iv) If we consider $E^{(l)}$ has a $G(k^{(l)}/k)$ module, then the only proper invariant submodules are finite.

The proofs are contained in [7] and [8]. A good reference is Lang's book [3] where he states and proves these theorems in a special case (nonintegral j invariant). See Chapter 17, Theorems 2 and 3, of that book.

PROPOSITION 2. *Let E be an elliptic curve without complex multiplications defined over a number field k. Let K be a solvable, possibly infinite, algebraic extension. Then the torsion subgroup $E(K)_t$ of $E(K)$ is finite.*

PROOF. Suppose $G(k_l/k) \approx \mathrm{Gl}_2(Z/lZ)$ and that $l \geqslant 5$. By Serre's result (i) these conditions are fulfilled for all but finitely many primes l. If l satisfies these conditions, we claim the l-primary component of $E(K)_t$ is zero.

As is well known $PSl_2(Z/lZ)$ is nonabelian and simple when $l \geqslant 5$. Thus $Gl_2(Z/lZ)$ is not solvable when $l \geqslant 5$.

Now suppose $a \in E(K)$, $la = 0$, and $a \neq 0$. Let $\sigma \in G(\bar{k}/k)$. Then $a^\sigma \in E(K)$ since K/k is Galois. By our choice of l, $G(\bar{k}/k)$ acts transitively on E_l and so $E_l \subset E(K)$. But then $G(K/k)$ maps onto $G(k_l/k)$. Since $G(K/k)$ is solvable and $G(k_l/k)$ is not, we have a contradiction.

To complete the proof we need only show that the l-primary component of $E(K)_t$ is finite for all l.

Let $E(K)^{(l)} = E(K) \cap E^{(l)}$. To begin with, we claim $E(K)^{(l)}$ is a proper subgroup of $E^{(l)}$. If not, $E^{(l)} \subset E(K)$ and thus $G(K/k)$ maps onto $G(k^{(l)}/k)$ which is isomorphic to an open subgroup of $Gl_2(Z_l)$ by Serre's result (iii). Such a subgroup cannot be solvable because its Lie algebra is the same as the Lie algebra of $Gl_2(Z_l)$ which is simple. Thus $E(K)^{(l)}$ is a proper subgroup of $E^{(l)}$. It is clearly invariant under $G(k^{(l)}/k)$ since K/k is a Galois extension. Thus by Serre's result (iv) it must be finite.

PROPOSITION 3. *Let A be an abelian variety defined over a number field k. Let K/k be a Galois extension of k, possibly infinite. If $A(K)_t$ is finite, then $A(K)/A(K)_t$ is free.*

PROOF. We wish to apply Proposition 1. Let $B \subset A(K)$ be a subgroup of finite rank. Our task is to show that B is finitely generated.

Since B has finite rank, there exist elements $b_1, b_2, \ldots, b_n \in B$ such that $B/(b_1, b_2, \ldots, b_n)$ is torsion where $(b_1, b_2, \ldots, b_n)$ is the subgroup of B generated by $b_1, b_2, \ldots, b_n$. Let K_0 be the field obtained by adjoining the coordinates of $b_1, b_2, \ldots, b_n$ to k. Let $B_0 = A(K_0)$ and $B_1 = B + B_0$. B_0 is finitely generated by the Mordell-Weil theorem. Thus B_1 has finite rank and $B_1/B_0 \approx B/B \cap B_0$ is torsion. We will be done if we can show B_1/B_0 is finite.

Let m be the order of $A(K)_t$. Suppose $b \in B_1$, $\sigma \in G(K/K_0)$, and $h \in Z$ such that $hb \in B_0$. Then $(hb)^\sigma = hb$ and $h(b^\sigma - b) = 0$. Thus $b^\sigma - b \in A(K)_t$ and $m(b^\sigma - b) = 0$. It follows that $mb \in B_0$ and so $B_1/B_0 \subseteq m^{-1}B_0/B_0$. The latter group is finite. Thus B is finitely generated.

Since $A(K)$ is a countable group, Proposition 1 applies and this completes the proof.

Theorem B of the introduction is a direct consequence of Propositions 2 and 3.

The proofs of Propositions 2 and 3 are generalizations of work of B. Mazur (Propositions 6.11 and 6.12 of [4]). He considers Γ extensions K/k of number fields and shows $A(K)_t$ is finite when A is an elliptic curve without complex multiplications and when A is any abelian variety of complex multiplication type providing K/k is the cyclomatic Γ extension.

DEFINITION. Ω will denote the field obtained from the rational numbers Q by adjoining the square roots of all the integers. Clearly Ω/Q is an infinite abelian extension.

PROPOSITION 4. *Let E be an elliptic curve defined over Q. Then $E(\Omega)$ has infinite rank.*

PROOF. This is Theorem 2.2 of the paper of G. Frey and M. Jarden [2]. The statement of the theorem is that $E(\overline{Q})$ has infinite rank but they remark directly after the proof that $E(\Omega)$ already has infinite rank.

PROPOSITION 5. *Let E be an elliptic curve defined over Q without complex multiplications. Then $E(\Omega)_t$ is finite and $E(\Omega)/E(\Omega)_t$ is a free abelian group of infinite rank.*

PROOF. This is an immediate consequence of Propositions 2,3, and 4.

REMARK. There are plenty of elliptic curves over Q without complex multiplication. It is well known that if $y^2 = 4x^3 - ax - b$ is an elliptic curve over Q with complex multiplication, then $j = 12^3a^3/a^3 - 27b^2$ is an integer. So, for example, consider $y^2 = 4x^3 - x - 1$. For this curve $j = -432/7 \notin Z$ and therefore there are no complex multiplications.

3. **Dedekind domains.** The following theorem and its corollary constitute a sharper version of Theorem A.

THEOREM C. *Let E be an elliptic curve defined over Q and without complex multiplication. Let $R = \Omega[x,y]$ where $y^2 = 4x^3 - ax - b$ is the Weierstrass equation for E.*

Then R is a Dedekind domain and its class group modulo torsion is a free abelian group of infinite rank.

COROLLARY. *Let A be a countable abelian group. Then A is isomorphic to the class group of an elliptic Dedekind domain lying between R and its quotient field.*

PROOF. R is the ring of Ω rational functions on E having poles only at infinity. It is standard that such a ring is a Dedekind domain.

We claim that the class group of R is isomorphic to $E(\Omega)$. Let P_0 denote the point at infinity on E. By the Riemann-Roch theorem every Ω-rational divisor class of degree zero is uniquely represented by a divisor of the form $P - P_0$ where P is an Ω-rational point. For $P \in E(\Omega)$, $P \neq P_0$, let $\mathfrak{P} = \{r \in R | \operatorname{ord}_p r \geqslant 0\}$. $\mathfrak{P}$ is a prime ideal of R. If $P \in E(\Omega)$, $P \neq P_0$, map P to the ideal class of $\mathfrak{P}$. Map P_0 to the principal class. This map from $E(\Omega)$ to the ideal class group of R is an isomorphism. The proof is relatively easy. For the details of this process see [6].

The statement of the theorem is now a direct consequence of Proposition 5.

Let C denote the class group of R. To prove the corollary notice that the structure of C allows us to construct a homomorphism from C onto A. Let B denote the kernel. Let S be a set of points P in $E(\Omega)$ such that the corresponding ideal classes $\overline{\mathfrak{P}}$ generate B. Let R_S be the subring of K, the quotient field of R, described by $\operatorname{ord}_p r \geqslant 0$ for all $P \notin S \cup \{P_0\}$. The natural map from the class group of R to the class group of R_S is onto and one easily sees that the kernel is B. Consequently, the class group of R_S is isomorphic to A.

BIBLIOGRAPHY

1. L. Claborn, *Every abelian group is a class group*, Pacific J. Math. **18** (1966), 219–222. MR **33** #4085.

2. G. Frey and M. Jarden, *Approximation theory and the rank of abelian varieties over large algebraic fields*, Proc. London Math. Soc. (3) **28** (1974), 112–128. MR **49** #2765.

3. S. Lang, *Elliptic functions*, Addison-Wesley, Reading, Mass., 1973.

4. B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266.

5. L. Pontryagin, *Theory of topological commutative groups*, Ann. of Math. (2) **35** (1934), 361–388; Russian transl., Uspehi Mat. Nauk **2** (1936), 177–195.

6. M. Rosen, *S-units and S-class groups in algebraic function fields*, J. Algebra **26** (1973), 98–108. MR **48** #6119.

7. J.-P. Serre, *Abelian l-adic representations and elliptic curves*, Benjamin, New York, 1968. MR **41** #8422.

8. ———, *Propriétés galoissience des pointes d'orde fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.

DEPARTMENT OF MATHEMATICS, BROWN UNIVERSITY, PROVIDENCE, RHODE ISLAND 02912