FROM INVERSE PICARD TO INVERSE MORDELL-WEIL

PETE L. CLARK

1. Four Inverse Problems

For any scheme X, its Picard group $\operatorname{Pic} X = H^1(X, \mathcal{O}_X^\times)$ classifies line bundles on X up to isomorphism. In particular restricting to the case of an integral affine scheme $\operatorname{Spec} R$, we get the notion of the Picard group of the domain R, i.e., invertible fractional ideals modulo principal fractional ideals. This group was first considered in the case of a Dedekind domain R, and in this case calling it the Picard group is perhaps slightly pretentious: one could equally well call it the **ideal class group** $\operatorname{Cl} R$. But by any name this is an important invariant of R lying at the border of algebra and arithmetic.

Number theorists are especially interested in the case of $R = \mathbb{Z}_K$ the ring of integers of a number field K, in which case $\operatorname{Pic} R$ is finite and its cardinality is the **class number** of K. Questions about the Picard groups of number rings are both classical and deep. Suppose for instance we ask which finite commutative groups arise as the Picard group of $\mathbb{Z}_K$ for a) an imaginary quadratic field or b) a real quadratic field. The answer says a lot about what we know and what we do not know about these two simplest classes of number fields: in the case of imaginary quadratic fields, not all commutative groups can arise. For instance, there are only finitely many values of K such that the class group can be isomorphic to $(\mathbb{Z}/2\mathbb{Z})^K$, and conditionally on GRH these values are precisely $0, 1, 2, 3, 4$. On the other hand, so far as we know every finite commutative group should serve as the Picard group of infinitely many real quadratic fields, but even proving that the trivial group occurs infinitely often seems just as out of reach to us as it was to Gauss in 1800 (who conjectured it).

Let me mention in passing that the following is – while not precisely the key question in this area – still very much open.

Question 1. *(Inverse Picard Problem for Number Fields) Which commutative groups G occur up to isomorphism as the Picard group of a number ring $\mathbb{Z}_K$?*

(As above, the conjectural answer is "all of them, even as K ranges over all real quadratic fields". Good luck with that!)

Now consider not just number rings but **all Dedekind domains**.

Question 2. *(Inverse Picard Problem) Which commutative groups G occur up to isomorphism as the Picard group of some Dedekind domain?*

This question was first answered by L. Claborn in 1966. A second proof was given in 1972 by C. Leedham-Green. Following up on some techniques and ideas of a 1976 paper of Mike Rosen, I gave a third answer to this question in 2008.

If for a number theorist the most natural class of Dedekind domains are the number rings, for an algebraic geometer the most natural class is probably the coordinate ring of a regular, integral affine curve $C^\circ_{/\mathbb{C}}$. In particular, suppose that the projective completion C of C° is obtained by adding a single point "at infinity": then there is an easy isomorphism

$$\operatorname{Pic} C^\circ \xrightarrow{\sim} (\operatorname{Pic}^0 C) = \operatorname{Jac}(C)(\mathbb{C}) \cong (S^1)^{2g(C)}.$$

By the way this shows that the Picard group can be a lot bigger than a finite group: here it is an uncountably infinite compact Lie group.

More generally, if C° is a regular, integral affine curve over an arbitrary field k with projective completion C, there is a natural map $\operatorname{Pic}^0 C \to \operatorname{Pic} k[C^\circ]$ with finitely generated kernel and finite cokernel which can be explicitly described: I learned of this result in 2008 from a 1973 paper of Mike Rosen and wished I had seen it before: it deserves to be better known!

Especially, for any elliptic curve $E_{/k}$ we have the notion of the "standard affine model" E^{circ} corresponding to an affine Weierstrass equation, and in this case again we simply have

$$E(k) = \operatorname{Pic}^0 E \xrightarrow{\sim} \operatorname{Pic} k[E^\circ].$$

Again, number theorists are most interested in the groups $E(k)$ when k is a number field, which once again have a very special and restricted structure, the relevant finiteness theorem being the Mordell-Weil theorem: for any number field k, the group $E(k)$ of k-rational points on E is finitely generated.

Again, I doubt I have to tell you that the behavior of these Mordell-Weil groups $E(k)$ is a big open problem in the field. Here the most attractive case is probably $k = \mathbb{Q}$, in which the possible torsion subgroups were classified by Barry Mazur in 197X. The free part of the Mordell-Weil group – i.e., the rank – is considerably more mysterious. It is pretty widely believed that for elliptic curves over $\mathbb{Q}$ the rank can be arbitrarily large, but if you ask if we believe it should assume every possible value already the experts get nervous (or at least I do). And once again the following problem ought to be much easier but is still wide open.

Question 3. *(Inverse Mordell-Weil Problem for Number Fields) Which finitely generated commutative groups G occur up to isomorphism as the Mordell-Weil group $E(k)$ of some elliptic curve defined over some number field k?*

(Presumably all of them? Let me know if you have any idea how to do it!)

So of course what I am leading up to is the following question.

Question 4. *(Inverse Mordell-Weil Problem) Which commutative groups G occur up to isomorphism as the group $E(k)$ of k-rational points of some elliptic curve E defined over some (arbitrary!) field k?*

If we allow ourselves to use the term "Mordell-Weil group" for the group of rational points of any elliptic curve defined over any field and allow ourselves to identify isomorphic commutative groups, then we may rephrase XXX more succicntly as **Which commutative groups are Mordell-Weil groups?**

2. Some answers

As above, every Mordell-Weil group is a Picard group, so we could answer both questions by showing that every commutative group is a Mordell-Weil group. Is this plausible?

Indeed it is not. Basic elliptic curve theory gives restrictions on the torsion subgroup of an elliptic curve over any field, namely for any $n \in \mathbb{Z}^+$, $E(k)[n]$ is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^2$, so $E(k)[\text{tors}] \hookrightarrow (\varinjlim \mathbb{Z}/n\mathbb{Z})^2 = (\mathbb{Q}/\mathbb{Z})^2$. On the other hand, by considering say the genus theory of binary quadratic fields it follows that there is no similar bound on the torsion subgroup of a Picard group.

However, as was first shown by Claborn in his 1966 paper, the class of Picard groups of Dedekind domains is more robust than that of Mordell-Weil groups in the following respect.

Theorem 1. *(Claborn) Any quotient of a Picard group is again a Picard group.*

My 2008 solution to the Inverse Picard Problem proceeded by establishing the following very special case of the Inverse Mordell-Weil Problem.

Theorem 2. *(*[PLC08]*) Every free abelian group is a Mordell-Weil group.*

Soon after seeing the proof of [PLC08], Bjorn Poonen reworked the argument so as to obtain a stronger result. Poonen's argument will be given in the next section.

Putting together Theorems 1 and 2 we deduce:

Theorem 3. *(*[Cl66], [LG72], [PLC08]*) A commutative group is a Picard group.*

In fact I want to discuss stronger versions of all of these results. First, the more geometric approach pioneered by Rosen and continued in my work allows replacement of Theorem 1 (whose proof uses some nontrivial commutative algebra) with the following more precise result.

Theorem 4. *Let k be a field and $E_{/k}$ an elliptic curve. Let $S \subset \operatorname{MaxSpec} k[E]$, and let $k(E)_S$ be the ring of functions on E which are regular away from S.*
a) We have $k[E] \subset k(E)_S \subset k(E)$.
b) The ring $k(E)_S$ is a Dedekind domain.
c) We have $\operatorname{Pic} k(E)_S = (\operatorname{Pic} k[E])/\langle S \rangle$.
d) Conversely, any subgroup H of $\operatorname{Pic} k[E]$ is of the form $\langle S \rangle$ for some $S \subset \operatorname{MaxSpec} k[E]$.

Proof. Part a) is clear from the definition.
Part b) follows from the Krull-Akizuki Theorem.
Part c) is a general fact about Picard groups of overrings of Dedekind domains, going back at least to a 1964 paper of O. Goldman.
As for part d), the issue is that in an arbitrary Dedekind domain R, an element of $\operatorname{Pic} R$ need not be the class of a *prime* ideal, and in fact L. Claborn [Cl68] constructs Dedekind domains with Picard group $\mathbb{Z}$ such that for all maximal ideals $\mathfrak{p}$ of R, the class $[\mathfrak{p}]$ of $\mathfrak{p}$ in $\operatorname{Pic} R$ is ± 1. This led me to define a Dedekind domain to be **replete** if every class in $\operatorname{Pic} R$ is the class of a prime and **weakly replete** if every subgroup H of $\operatorname{Pic} R$ is generated by classes of prime ideals. Weak repleteness is precisely

what you need to be sure that every quotient group of $\operatorname{Pic} R$ is the Picard group of some overring S of R. Claborn circumvents the issue that a general Dedekind domain R need not be replete by constructing a replete Dedekind domain R^1 with $\operatorname{Pic} R^1 \cong \operatorname{Pic} R$ and thus he gets Theorem 1. Happily, it is clear from the two canonical isomorphisms

$$E(k) = \operatorname{Pic}^0 E = \operatorname{Pic} k[E]$$

that the domain $k[E]$ is weakly replete. (If k is algebraically closed, then the Nullstellensatz implies that the trivial class in $\operatorname{Pic} k[E]$ is not the class of any maximal ideal, so $k[E]$ is not replete.) □

Thus combining Theorems 2 and 4 one gets a refined version of Claborn's Theorem: for any commutative group G, write it as quotient F/H for F a free commutative group. Then there exists a field k and an elliptic curve $E_{/k}$ with $E(k) \cong F$. Moreover, there exists a (possible infinite) subset S of the closed points of the affine elliptic curve E° such that subring $k(E)_S$ of all functions regular away from S and the origin is a Dedekind domain with Picard group $F/H \cong G$.

3. Towards a Solution of the Inverse Mordell-Weil Problem

It is natural to suspect that a commutative group G is a Mordell-Weil group iff $G[\text{tors}] \hookrightarrow (\mathbb{Q}/\mathbb{Z})^\times$. I can even sketch a proof of this conjecture, but unfortunately there is a certain technical snag that I do not yet know how to overcome. Let me begin by announcing that I do know how to prove some special cases.

Theorem 5. *Let G be a commutative group satisfying (T_1): $G[\text{tors}] \hookrightarrow (\mathbb{Q}/\mathbb{Z})^2$.*
a) If $G = G[\text{tors}]$, then it is a Mordell-Weil group.
b) (Poonen) If G is torsionfree, then it is a Mordell-Weil group.
c) If the short exact sequence $0 \to G[\text{tors}] \to G \to G/G[\text{tors}] \to 0$ splits, then G is a Mordell-Weil group.

Remark: Some reminders on the theory of $\mathbb{Z}$-modules: the exact sequence $G/G[\text{tors}]$ will definitely split when $G/G[\text{tors}]$ is a free commutative group (or equivalently, a projective $\mathbb{Z}$-module), a hypothesis is automatic when G is finitely generated. So every finitely generated group is a Mordell-Weil group (not necessarily over a number field, of course!). At the other extreme, the sequence certainly splits if $G[\text{tors}]$ is a divisible group (equivlently, an injective $\mathbb{Z}$-module). Since the torsion subgroup of a divisible commutative group is divisible, we get that all divisible groups G satisfying (T_1) are Mordell-Weil groups. On the other hand, the sequence certainly does not have to split and "usually doesn't" in some sense.

Proof. a) Just the idea: take k to be a limit of modular function fields $\mathbb{C}(X(T))$ for modular curves $X(T)$ attached to finite subgroups $T \subset (\mathbb{Q}/\mathbb{Z})^2$.
b) For clarity we will first prove the special case of G a free commutative group. Begin with an elliptic curve $E_{/k}$ with $\operatorname{End}(E) = \mathbb{Z}$, $E(k) = 0$ (for instance we may take $k = \mathbb{Q}$) and let κ be any set. For each finite subset S of κ, let k_S be the function field of the $|S|$-dimensional abelian variety $E^S = E \times \ldots \times E$. Then $E(k_S)$ is the group of all rational maps $E^S \to E$. But every rational map from a nonsingular variety into an abelian variety is everywhere defined [AV, Thm. 3.2], so $E(k_S)$ can be identified with the set of all k-morphisms $E^S \to E$. This group fits in a short exact sequence

$$0 \to E(k) \to E(k_S) \to \operatorname{Hom}_{\text{AV}}(E^S, E) \to 0,$$

the last term being the group of abelian variety homomorphisms $E^S \to E$, which is isomorphic to $\mathbb{Z}^S$.

Now suppose we have finite subsets $S \subset S' \subset \kappa$. There is then an evident (projection) morphism $E^{S'} \to E^S$, which induces a homomorphism of function fields $k(E^S) \hookrightarrow k(E^{S'})$. We therefore have a directed system of fields $\{k_S\}$, and since E is a finite type scheme we get

$$E(\lim_S k_S) = \lim_S E(k_S) = \lim_S \mathbb{Z}^S = \mathbb{Z}[\kappa].$$

Now start again with $E_{/k}$ with $E(k) = 0$. Let G be any **torsionfree** abelian group, and let $\{H_i\}$ be the set of all finitely generated subgroups of G, directed under inclusion. Then each H_i is free abelian of finite rank, hence (non-canonically) isomorphic to $\mathbb{Z}^{S_i}$ for some finite set S_i. The functor which takes a k-algebra R to $\mathrm{Hom}(H_i, E_{/R}(R))$ is representable by an abelian variety, say A_i, which is (non-canonically) isomorphic to E^{S_i}. Again if $H_i \subset H_{i'}$ there are canonical maps $A_{i'} \to A_i$. Therefore the now familiar limiting argument gives

$$E(\lim_i k(A_i)) = \lim_i E(k(A_i)) = \lim_i \mathrm{Hom}(\mathrm{Hom}(H_i, E), E)) = \lim_i H_i = G.$$

c) In general, if one starts with an elliptic curve $E_{/k_0}$ with $\mathrm{End}(E) = \mathbb{Z}$ and a torsionfree abelian group G and performs the above construction with E, then one gets an elliptic curve E with $E(k) \cong E(k_0) \times G$. In particualr, if $E(k_0)$ is a torsion group, this gives the split extension of G by $E(k_0)[\mathrm{tors}]$. □

Moreover, Poonen provided a strategy for a proof of the general case, which I have fleshed out somewhat (but not completely!).

Let G be a commutative group satisfying condition (T_1).

Lemma 6. *G injects into the direct sum of $(\mathbb{Q}/\mathbb{Z})^2$ and a $\mathbb{Q}$-vector space.*

Proof. The $\mathbb{Z}$-module $(\mathbb{Q}/\mathbb{Z})^2$ is divisible, hence injective. Therefore the inclusion $G[\mathrm{tors}] \hookrightarrow (\mathbb{Q}/\mathbb{Z})^2$ extends to a homomorphism $\alpha : G \to (\mathbb{Q}/\mathbb{Z})^2$. Moreover, tensoring with $\mathbb{Q}$ gives a homomorphism $\beta : G \to G \otimes \mathbb{Q}$. The natural map $(\alpha, \beta) : G \to (\mathbb{Q}/\mathbb{Z})^2 \times (G \otimes \mathbb{Q})$ is an injection. □

Now we start with the "arithmetically generic elliptic curve": let $k = \mathbb{Q}(a, b)$ be a rational function field in two independent indeterminates, and let

$$E_{/k} : y^2 = x^3 + ax + b.$$

Observe that $E(k) = 0$. As above, we can find an extension field L of k such that

$$E(L) = (\mathbb{Q}/\mathbb{Z})^2 \oplus (G \otimes \mathbb{Q}).$$

We CLAIM moreover that for any finitely generated subgroup H of $E(L)$, we have $E(k(H)) = H$. Then the same limiting argument allows us to realize any subgroup of $E(L)$ as a Mordell-Weil group – in particular G.

But how do we prove the claim?!? (Poonen suggested that something very much like this was proven in Alice Silverberg's PhD thesis. Unfortunately Alice Silverberg disagreed.) It comes down to some extremely plausible beliefs about adjoining rational points to "maximally generic" elliptic curves. I don't really know how to prove these facts **nor** am I completely convinced that proofs don't already exist

in the literature, so I haven't really given it my full attention. Any ideas will be warmly appreciated!

Final remark: When this problem is finished, it is natural to consider various analogues: what are the Mordell-Weil groups in characteristic p? Presumably the only restriction is

$$(T_{1,p}) : G[\text{tors}] \hookrightarrow (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^2 \times \mathbb{Q}_p/\mathbb{Z}_p.$$

What about supersingular Mordell-Weil groups?

More interestingly, what about Mordell-Weil groups of higher dimensional abelian varieties? Again one can predict the answer, but the following question is one that I find both puzzling and intriguing: what is the abelian variety analogue of the maximally generic elliptic curve $E_{a,b}$?

References

[AV] J. Milne, *Abelian varieties*, course notes available at `http://wwww.jmilne.org` .

[Cl65a] L. Claborn, *Dedekind domains and rings of quotients*. Pacific J. Math. 15 (1965), 59–64.

[Cl65b] L. Claborn, *Dedekind domains: Overrings and semi-prime elements*. Pacific J. Math. 15 (1965), 799–804.

[Cl66] L. Claborn, *Every abelian group is a class group*. Pacific J. Math. 18 (1966), 219–222.

[Cl68] L. Claborn, *Specified relations in the ideal group*. Michigan Math. J. 15 (1968), 249–255.

[PLC08] P.L. Clark, *Ellitpic Dedekind domains revisited*. Enseign. Math. (2) 55 (2009), 213-225.

[Go64] O. Goldman, *On a special class of Dedekind domain*. Topology 3 (1964) suppl. 1, 113-118.

[LG72] C.R. Leedham-Green, *The class group of Dedekind domains*. Trans. Amer. Math. Soc. 163 (1972), 493–500.

[LM] M.D. Larsen and P.J. McCarthy, *Multiplicative theory of ideals*. Pure and Applied Mathematics, Vol. 43. Academic Press, New York-London, 1971.

[M] H. Matsumura, *Commutative ring theory*. Translated from the Japanese by M. Reid. Second edition. Cambridge Studies in Advanced Mathematics, 8. Cambridge University Press, Cambridge, 1989.

[Ro73] M. Rosen, *S-units and S-class group in algebraic function fields*. J. Algebra 26 (1973), 98–108.

[Ro76] M. Rosen, *Elliptic curves and Dedekind domains*. Proc. Amer. Math. Soc. 57 (1976), 197–201.