RABINOWITSCH TIMES SIX

PETE L. CLARK

Abstract. We give an analogue of the Rabinowitsch Criterion with $\mathbb{Z}$ replaced by the polynomial ring $k[t]$ over a field of characteristic different from 2. In fact we expose three different proofs of the Rabinowitsch Criterion – using Dedekind-Hasse norms, binary quadratic forms and the Minkowski bound on ideal classes – and adapt each to prove our Polynomial Rabinowitsch Criterion. Whereas there are precisely seven cases in which the classical Rabinowitsch Criterion holds, working over an arbitrary ground field gives us much more latitude: e.g. recent results about genus one curves yield infinitely many instances in which the Rabinowitsch Criterion is satisfied over $k = \mathbb{Q}$. Finally we take a geometric perspective and relate the Rabinowitsch Criterion to the Mordell-Weil group of the Jacobian of the associated hyperelliptic curve.

Contents

1. Introduction

1.1. **Terminology.** Let R be a domain. An element $p \in R$ is **prime** if (p) is a nonzero prime ideal; an element x is **irreducible** if $x = yz$ implies that exactly one of y and z is a unit. Prime elements are irreducible, and in a unique factorization domain (henceforth UFD) the converse holds. In a UFD an element is **composite** if it is neither zero, a unit, nor a prime element.

1.2. **The Rabinowitsch Criteria.** Consider – as Euler did – the polynomial $x^2 + x + 41$. For $x = 0, 1, \ldots, 39$, $x^2 + x + 41$ is a prime number. That is a lot of prime values for such a simple polynomial! What do we make of this? G.Y. Rainich (né Rabinowitsch) gave an answer [Ra13] by establishing the equivalence of (i) and (ii) in the following result.

Theorem 1.1. *(Rabinowitsch Criterion)*
Let $C \in \mathbb{Z}^+$, let $\Delta = 1 - 4C$, let $\tau = \frac{1+\sqrt{\Delta}}{2}$, and let

$$\mathcal{O}_\Delta = \mathbb{Z}[\tau] = \mathbb{Z}[t]/(t^2 + t + C).$$

The following are equivalent:
(i) The ring $\mathcal{O}_\Delta$ is a PID.
(ii) For all $0 \leq x \leq C - 2$, the integer $x^2 + x + C$ is not composite.
(ii′) For all $x \in [0, \lfloor \sqrt{\frac{|\Delta|}{12}} \rfloor]$, the integer $x^2 + x + C$ is not composite.
(iii) For all primes $p \leq C - 1$, Δ is not a square modulo p.
(iii′) For all primes $p \leq \sqrt{\frac{|\Delta|}{3}}$, Δ is not a square modulo p.

Remark 1.2. *Let $C > 1$. Then $(C-1)^2 + (C-1) + C = C^2$ is composite, so in (i) $\implies$ (ii), the bound $x \leq C - 2$ is best possible in all cases.*

In February 2016 my colleague Paul Pollack asked for an analogue of Theorem 1.1 over a polynomial ring $k[t]$. Here is my answer.

Theorem 1.3. *(Polynomial Rabinowitsch Criterion)*
*Let k be a field of characteristic not 2. Let $\Delta \in k[t]$ be **definite**: either $\deg \Delta$ is odd*

or the leading coefficient of Δ is not a square in k. The following are equivalent:
(i) The ring $\mathcal{O}_\Delta = k[t][\sqrt{\Delta}] = k[t,x]/(x^2-\Delta)$ is a PID.
(ii) For all $x \in k[t]$ with $\deg x < \deg \Delta$, the polynomial $x^2 - \Delta$ is not composite.
(ii′) For all $x \in k[t]$ with $\deg x < \lceil \frac{\deg \Delta}{2} \rceil$, the polynomial $x^2 - \Delta$ is not composite.
(iii) For all primes p with $\deg p < \deg \Delta$, Δ is not a square modulo p.
(iii′) For all primes p with $\deg p \leq \lceil \frac{\deg \Delta}{2} \rceil$, Δ is not a square modulo p.

Remark 1.4. *When k is finite, (i) $\iff$ (ii) in Theorem 1.3 is a result of W. Hu* [Hu98, Cor. 1]*. His proof is different from (all of) ours: cf. Remark 7.5.*

The main thrust of Theorems 1.1 and 1.3 is the equivalence (i) $\iff$ (ii). Of these, (i) $\implies$ (ii) is more straightforward: it is a familiar theme that many number theoretic problems become easily solvable under the assumption that a certain ring of integers has unique factorization. The implication (ii) $\implies$ (i) is more interesting: by checking that some elements do not factor, we deduce that a ring is a PID. There is however one famous instance in which the knowing the class group of a ring of integers is *equivalent* to knowing the solution to a more elementary Diophantine problem: Gauss composition in quadratic fields. And indeed Gauss composition is part of the picture here, as we shall see.

Although the Rabinowitsch Criterion is not obscure, neither is it standard: I know of no "canonical" proof. To answer Pollack's question I began by searching the literature for different proofs of (ii) $\implies$ (i) in Theorem 1.1. I found three different arguments. The first, of [Fe85], uses Dedekind-Hasse norms. This is perhaps the most elementary, the only ingredient being a standard Diophantine approximation result due to Dirichlet which follows from the Pigeonhole Principle. The second, of [Gr], and uses the interpretation of the class group of a quadratic order in terms of binary forms. Later I found that a proof of this kind was given (much) earlier by H.H. Mitchell [Mi26, §3]. The last uses the Minkowski bound on ideal classes and has been exposed by many authors, e.g. by Ribenboim [Ri88].

In this paper we will give three proofs of (ii) $\implies$ (i) in the Rabinowitsch Criterion, using Dedekind-Hasse norms, binary quadratic forms and the Minkowski bound. Then we carry over all three to proofs of (ii) $\implies$ (i) in the Polynomial Rabinowitsch. (Thus "six Rabinowitsches.") This is a lot of iterated proving, but it seems enlightening to pursue all three function field analogues. In the first case we use Dedekind-Hasse norms: the Diophantine approximation is replaced by a (known, elementary) result about approximating elements of $k((\frac{1}{t}))$ by rational functions. In the second case it is interesting to see when we can work with binary quadratic forms over an arbitrary PID and when we need features particular to $\mathbb{Z}$ and $k[t]$. In the third case we establish a function field Minkowski bound. When k is finite this was done by Hu using methods which are very faithful to Minkowski's geometry of numbers, but for the general case we use the Riemann-Roch Theorem. In this way we make contact with arithmetic geometry: we are able to make use of yet another equivalent criterion for $\mathcal{O}_\Delta$ to be a PID in terms of the index of the hyperelliptic curve $C_\Delta : y^2 = \Delta(x)$ and the Mordell-Weil group of its Jacobian.

The implication (ii′) $\implies$ (ii) is also striking: if $x^2 - \Delta$ cannot be factored for x in a certain range of values, then it cannot be factored for x in a much larger range of values. The method of proof is (ii′) $\implies$ (i) $\implies$ (ii). In fact all of our proofs of (ii) $\implies$ (i) are nearly proofs of (ii′) $\implies$ (i), but over $\mathbb{Z}$ the constant in the first proof is a bit better than the ones obtained from the second and third proofs.

1.3. **Acknowledgments.** I am grateful to my colleague Paul Pollack for suggesting the problem to me. (It was the evening of the first Sunday of February, 2016, when many others were watching a Nietzschean sporting event.) He also introduced me to Ono numbers, and the proofs of the theorems of Möller and Sasaki in §9.2 follow sketches from a problem set in his Spring 2016 algebraic number theory course. His arguments seem simpler and shorter than the original proofs.

2. Rabinowitsch I and II: Following Fendel

The plan of the section is as follows. First we will give a complete exposition of Fendel's proof [Fe85] of the implications (i) $\implies$ (ii) and (ii$'$) $\implies$ (i) in Theorem 1.1. The implication (i) $\implies$ (ii$'$) requires very little in the way of setup and is done in §2.1. The proof of (ii$'$) $\implies$ (i) needs two preliminaries: the first is a discussion of Dedekind-Hasse norms and their relation to PIDs, which is done in §2.2. The second is a basic result on Diophantine approximation, given in §2.3. The proof of (ii$'$) $\implies$ (i) is then given in §2.4.

For the remainder of the section our task is to adapt the above arguments to give the corresponding implications (i) $\implies$ (ii) and (ii$'$) $\implies$ (i) in Theorem 1.3. The proof of (i) $\implies$ (ii$'$) is given in §2.5, a basic result on polynomial Diophantine approximation is given in §2.6 and the proof of (ii$'$) $\implies$ (i) is given in §2.7.

2.1. **Proof of (i) $\implies$ (ii) in Rabinowitsch's Criterion.** We put $C \in \mathbb{Z}^+$, $\Delta = 1-4C$, $\tau = \frac{1+\sqrt{\Delta}}{2}$, $\mathcal{O}_\Delta = \mathbb{Z}[\tau]$. We may view $\mathbb{Z}[\tau]$ as a subring of $\mathbb{C}$; for $z \in \mathbb{C}$, we denote by $|z|$ *the square* of the usual Euclidean absolute value: that is,

$$|x+yi| = x^2+y^2.$$

If for $x, y \in \mathbb{Z}$ we put $q_\Delta(x,y) = x^2+xy+Cy^2$ then we have

$$q_\Delta(x,y) \coloneqq x^2+xy+Cy^2 == (x+y\tau)(x+y\overline{\tau}) = |x+y\tau|.$$

In fact every element of $\mathcal{O}_\Delta$ is of the form $x+y\tau$ for unique $x, y \in \mathbb{Z}$, so $x+y\tau \mapsto q_\Delta(x,y)$ gives a **norm map**

$$|\cdot| : \mathcal{O}_\Delta \to \mathbb{N}.$$

The norm enjoys the following properties:
- For all $\alpha, \beta \in \mathcal{O}_\Delta$, we have $|\alpha\beta| = |\alpha||\beta|$.
- Forall $\alpha \in \mathcal{O}_\Delta$, we have $|\alpha| = 0 \iff \alpha = 0$.
- For all $\alpha \in \mathcal{O}_\Delta$, we have $|\alpha| = 1$ iff $\alpha \in \mathcal{O}_\Delta^\times$.

Lemma 2.1. *For a prime number p, the following are equivalent:*
(i) There are $x, y \in \mathbb{Z}$ such that $q_\Delta(x,y) = p$.
(ii) As an element of the domain $\mathcal{O}_\Delta$, p is not irreducible.

Proof. (i) $\implies$ (ii): By assumption $p = q_\Delta(x,y) = (x+y\tau)(x+\overline{y}\tau)$. We have $|x+y\tau| = |x+y\overline{\tau}| = p$, so $x+y\tau$ and $x+y\overline{\tau}$ are not units.
(ii) $\implies$ (i): If $p = \alpha\beta$ with α, β nonunits, then $p^2 = |p| = |\alpha\beta| = |\alpha||\beta|$. and $|\alpha|, |\beta| > 1$. This implies $p = |\alpha| = |\beta|$. If $\alpha = x+y\tau$, then $p = |\alpha| = q_\Delta(x,y)$. □

Lemma 2.2. *If $\alpha \in \mathcal{O}_\Delta \setminus \mathbb{Z}$, we have $|\alpha| \geq C$.*

Proof. We may write $\alpha = x+y\tau$ with $y \neq 0$, and then we have

$$|\alpha| = x^2+xy+Cy^2 = (x+\frac{y}{2})^2 + \frac{-\Delta}{4}y^2.$$

Since $y \neq 0$, $y^2 \geq 1$. If $y^2 = 1$, then y is odd, $x + \frac{y}{2} \in \frac{1}{2}\mathbb{Z} \setminus \mathbb{Z}$ so

$$|\alpha| \geq (1/2)^2 + \frac{4C-1}{4} = C.$$

Otherwise $y^2 \geq 4$ and

$$|\alpha| \geq \frac{-\Delta}{4}t^2 \geq -\Delta = 4C - 1 > C. \qquad \square$$

Proposition 2.3. *a) If $p < C$ is a prime number, then p is irreducible in $\mathcal{O}_\Delta$.*
b) If $\mathcal{O}_\Delta$ is a UFD, then for all $x \in \mathbb{Z}$, the integer $q_\Delta(x,1) = |x+\tau| = x^2 + x + C$ has no prime factor smaller than C.

Proof. a) By contraposition: if a prime number p is reducible in $\mathcal{O}_\Delta$, then by Lemma 2.1 there is $\alpha = x + y\tau \in \mathcal{O}_\Delta$ such that $|\alpha| = q_\Delta(x,y) = p$. If $\alpha \in \mathbb{Z}$ then $y = 0$ and $q_\Delta(x,y) = x^2 \neq p$. So $\alpha \in \mathcal{O}_\Delta \setminus \mathbb{Z}$, and Lemma 2.2 gives $p = |\alpha| \geq C$.
b) By contradiction: suppose there is a prime number $p < C$ such that

$$p \mid x^2 + x + C = (x+\tau)(x+\overline{\tau}).$$

By part a), p is irreducible in $\mathcal{O}_\Delta$, but by assumption $\mathcal{O}_\Delta$ is a UFD so it follows that $p \mid x + \tau$ or $p \mid x + \overline{\tau}$, which is absurd. $\square$

Theorem 2.4. *If $\mathcal{O}_\Delta$ is a UFD, then $x^2 + x + 2$ is prime for all $0 \leq x \leq C - 2$.*

Proof. Let $0 \leq x \leq C-2$. Then $x^2 + x + C < (C-1)^2 + (C-1) + C = C^2$. If $x^2 + x + C$ were composite, it would have a prime factor $p < C$, contradicting Proposition 2.3b). $\square$

Since PIDs are UFDs, Theorem 2.4 shows (i) $\implies$ (ii) in Rabinowitsch's Criterion.

2.2. **Dedekind-Hasse Norms.** Let R be a domain. A map $|\cdot| : R \to \mathbb{N}$ is a **multiplicative norm** if
(MN0) For all $x, y \in R$, we have $|xy| = |x||y|$.
(MN1) For all $x \in R$, we have $|x| = 0 \iff x = 0$.
(MN2) For all $x \in R$, we have $|x| = 1 \iff x \in R^\times$.

Henceforth by "norm" we will mean a multiplicative norm. If $|\cdot|$ is a norm on R and K is the fraction field of R, then we extend $|\cdot|$ to a map from K to $\mathbb{Q}^{\geq 0}$ by

$$\left|\frac{x}{y}\right| = \frac{|x|}{|y|}.$$

One sees easily that this is well-defined and is the unique extension such that $|xy| = |x||y|$ for all $x, y \in K$. (Note that $|x| \in \mathbb{Z}$ need not imply that $x \in R$.)

Example 2.5. *a) The standard absolute value is a norm on $\mathbb{Z}$.*
*b) As above, for $C \in \mathbb{Z}^+$ and $\Delta = 1 - 4C$, the map $|\cdot| : \mathcal{O}_\Delta \to \mathbb{N}$ given by $|x + y\tau| = x^2 + xy + C$ is a norm. We call it the **complex norm**.*
c) Let k be any field, and let $R = k[t]$. For $f(t) \in R[t]$, let $\deg f$ denote the degree, with the convention $\deg 0 = -\infty$. Then $|f| = 2^{\deg f}$ is a norm.
d) Let R be any UFD. A norm $|\cdot|$ sends each prime element π to an integer $n_\pi \geq 2$ such that $n_\pi = n_{\pi'}$ if π and π' are associates (i.e., generate the same principal ideal). Thus if $\{\pi_i\}_{i \in I}$ is a set of prime elements such that each prime element is associate to exactly one π_i, knowing the numbers n_{π_i} for all $i \in I$ determines the norm. Conversely, any function $\{\pi_i\}_{i \in I} \to \mathbb{Z}^{\geq 2}$ extends to a unique norm.

Let R be a domain with fraction field K. A norm $|\cdot|$ on R is **Euclidean** if for all $x \in K$, there is $y \in R$ such that $|x - y| < 1$. Writing $x = \frac{a}{b}$ with $a, b \in R$, this is equivalent to: there exist $q, r \in R$ with $a = qb + r$ and $|r| < |b|$. This recovers the standard definition of a Euclidean function restricted to the class of *multiplicative* norms. Recall that a domain admitting a Euclidean functions is a PID: if I is a nonzero ideal of R and x is any element of I of minimal nonzero norm then $I = \langle x \rangle$.

Example 2.6. *a) The standard norm on $\mathbb{Z}$ is Euclidean. So $\mathbb{Z}$ is a PID.*
b) For $C \in \{1, 2, 3\}$, the complex norm on $\mathcal{O}_{1-4C}$ is Euclidean: see e.g. [CJ14, Cor. 5.2]*. So $\mathcal{O}_{-3}$, $\mathcal{O}_{-7}$ and $\mathcal{O}_{-11}$ are PIDs. For $C \geq 4$ the complex norm on $\mathcal{O}_{1-4C}$ is not Euclidean, but the Rabinowitsch Criterion shows that $\mathcal{O}_{-19}$, $\mathcal{O}_{-43}$, $\mathcal{O}_{-163}$ are PIDs. Motzkin showed that none of them admit a Euclidean function* [Mo49]*.*
c) For any field k, the norm $|f| = 2^{\deg f}$ on $k[t]$ is Euclidean. So $k[t]$ is a PID.
d) Let $R = \mathbb{Z}[\frac{1+\sqrt{69}}{2}] = \mathbb{Z}[\tau]$. The most natural norm on R is the absolute value of the field norm. It is not Euclidean. Nevertheless, R admits a Euclidean function [Cl94]*. I believe it is not known whether R admits a Euclidean* norm*.*

So we cannot establish the Rabinowitsch Criterion using Euclidean norms. But consider the following modification. Let R be a domain with fraction field K. A **Dedekind-Hasse norm** is a norm $|\cdot|$ on a domain R with fraction field K is a norm such that: for all $x \in K \setminus R$, there are $a, b \in R$ such that $0 < |ax - b| < 1$. A Euclidean norm is a Dedekind-Hasse norm: take $a = 1$.

Proposition 2.7. *Let R be a domain, and let $|\cdot|$ be a norm on R.*
a) The following are equivalent:
(i) R is a PID.
(ii) The norm $|\cdot|$ is a Dedekind-Hasse norm.
b) A domain admits a Dedekind Hasse norm iff it is a PID.

Proof. a) (i) $\implies$ (ii): If R is a PID any $x \in K \setminus R$ we may write $x = \frac{p}{q}$ with $\gcd(p, q) = 1$ and thus there are $a, b \in R$ such that $ap - bq = 1$. Dividing by q gives

$$|ax - b| = |a\frac{p}{q} - b| = |\frac{1}{b}| \in (0, 1).$$

(ii) $\implies$ (i): Let I be a nonzero ideal of R, let d be a nonzero element of I of minimal norm. We claim $I = \langle d \rangle$: if not, there is $x \in I$ such that $\frac{x}{d} \in K \setminus R$, and then there are $a, b \in R$ such that $0 < |\frac{ax}{d} - b| < 1$. Thus $0 < |ax - bd| < |d|$ and $ax - bd \in I$ has a smaller nonzero norm than d: contradiction.
b) That a domain which admits a Dedekind-Hasse norm is a PID follows immediately from part a). Conversely, every PID is a UFD and every UFD admits a norm function, so by part a) every PID admits a Dedekind-Hasse function. □

2.3. **Diophantine Approximation.** Following Fendel [Fe85], we will show (ii) $\implies$ (i) in Rabinowitsch's Criterion by showing that the complex norm is a Dedekind-Hasse norm on $\mathcal{O}_\Delta$. For this we need a standard result on Diophantine Approximation.

Proposition 2.8. *(Dirichlet's Diophantine Approximation) Let $y \in \mathbb{R}$ and let $Q \in \mathbb{Z}$ with $Q \geq 2$. Then there are $p, q \in \mathbb{Z}$ such that $1 \leq q \leq Q - 1$ and*

$$|qy - p| \leq \frac{1}{Q}.$$

Proof. For $x \in \mathbb{R}$, there is a unique real number $x' \in [0,1)$ such that $x - x' \in \mathbb{Z}$. Consider the finite sequence $y', (2y', \ldots, ((Q-1)y)'$. We divide the interval $[0,1]$ up into Q subintervals $[0, \frac{1}{Q}], [\frac{1}{Q}, \frac{2}{Q}], \ldots, [\frac{Q-1}{Q}, 1]$. If for some $1 \leq q \leq Q-$ we have $(q\alpha)' \in [0, \frac{1}{Q}] \cup [\frac{Q-1}{Q}, 1]$, then there is an integer p such that $|qy - p| \leq \frac{1}{Q}$ and we're done. Otherwise we have a sequence of length $Q-1$ and $Q-2$ subintervals, so by the Pigeonhole Principle there are $1 \leq i < j \leq Q-1$ such that $|(iy)' - (jy)'| \leq \frac{1}{Q}$, so there is an integer p with $|(j-i)y - p| \leq \frac{1}{Q}$. Taking $q = j - i$, we're done. □

Corollary 2.9. *Let $\tau = \frac{1+\sqrt{\Delta}}{2}$, let $R = \mathbb{Z}[\tau] = O_\Delta$ and $K = \mathbb{Q}[\tau]$. For $\alpha \in K$ there is $q \in \mathbb{Z}$ with $1 \leq q \leq \sqrt{\frac{|\Delta|}{3}}$ and $\beta \in R$ such that $|q\alpha - \beta| < 1$.*

Proof. Let $\alpha = x + y\tau$ with $x, y \in \mathbb{Q}$ and put $Q = \lfloor \sqrt{\frac{|\Delta|}{3}} \rfloor + 1$. Applying Proposition 2.8 with these values of y and Q, we get $p, q \in \mathbb{Z}$ such that $1 \leq q \leq Q-1$ and $|qy - p| \leq \frac{1}{Q}$. Let $c = qy - p$, and let $r \in \mathbb{Z}$ be such that $|qx + c/2 - r| \leq \frac{1}{2}$. Finally, put $\beta = r + p\tau$. Then:

$$|q\alpha - \beta| = |q(x + y\tau) - (r + p\tau)| = |(qx - r) + (qy - p)\tau| = |(qx - r) + c\tau|$$

$$= \left(qx - r + \frac{c}{2}\right)^2 + \frac{|\Delta|}{4}c^2 \leq \frac{1}{4} + \frac{|\Delta|}{4}\frac{1}{Q^2} < \frac{1}{4} + \frac{|\Delta|}{4}\frac{3}{|\Delta|} = 1. \qquad \square$$

We immediately deduce the following known (cf. Example 2.5a)) result.

Corollary 2.10. *The complex norm is a Euclidean norm on $\mathcal{O}_{-3} = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$.*

2.4. **Proof of (ii′) $\implies$ (i) in the Rabinowitsch Criterion.** We return to the setup of §2.1. Let $K = \mathbb{Q}[\tau]$ be the fraction field of $\mathbb{Z}[\tau] = \mathcal{O}_\Delta$. For $\alpha \in K$ we define the **denominator** d_α of α to be the least $d \in \mathbb{Z}^+$ such that $d\alpha \in \mathcal{O}_\Delta$.

Lemma 2.11. *Let $C > 1$. Let $K = \mathbb{Q}[\tau]$. For $\gamma \in K \setminus \mathcal{O}_\Delta$, let t be the denominator of γ, and suppose $t \leq \sqrt{\frac{|\Delta|}{3}}$. If $t\gamma \in \mathcal{O}_\Delta$ and $t \mid |t\gamma|$, then $|x + \tau|$ is composite for some $x \in \mathbb{Z}$ with $0 \leq x < \frac{t}{2}$.*

Proof. Write $t\gamma = a + b\tau$ with $a, b \in \mathbb{Z}$. Suppose a prime ℓ divides b and t. Then

$$\ell \mid t \mid |t\gamma| = a^2 + ab + Cb^2,$$

so $\ell \mid a$. But this means that $\frac{t}{\ell}\gamma \in \mathcal{O}_\Delta$, contradicting the definition of the denominator. so $\gcd(b, t) = 1$. Thus there are $y \in \mathbb{Z}$ with $by \equiv 1 \pmod{t}$ and $x \in \mathbb{Z}$ with $xy \equiv a \pmod{t}$; we may moreover choose x such that $\frac{-t}{2} \leq x < \frac{t}{2}$. Then

$$|ty\gamma| = |ay + by\tau| \equiv |x + \tau| \pmod{t}.$$

Since $t \mid |t\gamma| \mid |ty\gamma|$, it follows that $t \mid |x + \tau| = x^2 + x + C$. Since $t \leq \sqrt{\frac{|\Delta|}{3}} < C$, we have $t \neq |x + \tau|$. Since t is the denominator of an element γ which is not in R, we have $t > 1$: thus $|x + \tau|$ is composite. If $x \in [\frac{-t}{2}, 0)$, then $x^* = 1 - x \in [0, \frac{t}{2}]$. Moreover we calculate $|x + \alpha| = |x^* + \alpha|$, so $|x^* + \alpha|$ is also composite. □

Theorem 2.12. *Let $C \geq 2$, and suppose that $x^2 + x + C$ is prime for all $x \in [0, \lfloor \sqrt{\frac{|\Delta|}{12}} \rfloor]$. Then $\mathcal{O}_\Delta$ is a PID.*

Proof. We will show the complex norm is a Dedekind-Hasse norm: let $\alpha \in K \setminus \mathcal{O}_\Delta$. We must find $\gamma, \beta \in \mathcal{O}_\Delta$ such that $0 < |\gamma\alpha - \beta| < 1$. By Lemma 2.11 there is an integer $t \in [1, \sqrt{\frac{|\Delta|}{3}}]$ and $\beta \in \mathcal{O}_\Delta$ with $|t\alpha - \beta| < 1$, and as above we are done unless $t\alpha \in \mathcal{O}_\Delta$, so assume this. Consider $\eta = t\overline{\alpha} \in \mathcal{O}_\Delta$. We have

$$\eta\alpha = \frac{|t\alpha|}{t} \in \mathbb{Q},$$

so we may choose $\beta \in \mathbb{Z}$ such that $|\eta\alpha - \beta| < 1$. (The complex norm restricted to $\mathbb{Q}$ is the square of the usual absolute value on $\mathbb{Q}$, but the condition of being less than one is preserved.) So again we are done unless $\eta\alpha \in \mathcal{O}_\Delta \cap \mathbb{Q} = \mathbb{Z}$, in other words, unless $t \mid |t\alpha|$. The preceding Lemma now finishes the proof! □

Corollary 2.10 and Theorem 2.12 give (ii′) $\implies$ (i) in the Rabinowitsch Criterion.

2.5. **Proof of (i) $\implies$ (ii) in the Polynomial Rabinowitsch Criterion.** Let k be a field of characteristic different from 2. Let $R = k[t]$. As in Example 2.6 above, for $f \in R$ we write $\deg f$ for the degree of f and $|f| = 2^{\deg f}$ (again note $\deg 0 = -\infty$, $|0| = 0$): this is a Euclidean norm.

Let $\Delta \in k[t]^\bullet$, and put $D = \deg \Delta$. We say Δ is **indefinite** if $\deg \Delta$ is even and the leading (i.e., highest degree) term of Δ is a square; otherwise Δ is **definite**. From now on we assume that Δ is definite and of positive degree.

Proposition 2.13. *Let $\Delta \in k[t]$ be definite, and put $q_\Delta(x, y) = x^2 - \Delta y^2$.*
a) For all $x, y \in k[t]$, we have

$$\deg q_\Delta(x, y) = \max(2 \deg x, 2 \deg y + \deg \Delta).$$

b) If $y \neq 0$, then $\deg q_\Delta(x, y) \geq D$.

Proof. a) We consider cases.
Case 1: Suppose $\deg \Delta$ is odd. Then $\deg x^2$ is even and $\deg \Delta y^2$ is odd, so the highest degree term does not cancel and

$$\deg x^2 - \Delta t^2 = \max(\deg x^2, \deg \Delta y^2) = \max(2 \deg x, 2 \deg y + \deg \Delta).$$

Case 2: Suppose the leading coefficient of Δ is not a square. Then the leading coefficient of x^2 is a square whereas the leading coefficient of Δy^2 is not, so again the highest degree term does not cancel.
b) Since $\deg y \neq -\infty$, we have $\deg q_\Delta(x, y) \geq 2 \deg y + \deg \Delta \geq \deg \Delta = D$. □

Henceforth we fix a definite $\Delta \in k[t]$. Let $\mathcal{O}_\Delta = R[\Delta] = \{x + y\Delta \mid x, y \in R\}$ and let $K = \{x + y\Delta \mid x, y \in k(t)\}$ be the fraction field of $\mathcal{O}_\Delta$. Then $K/k(t)$ is a quadratic field extension which – since the characteristic of k is not 2 – is Galois, with nontrivial automorphism $x + y\sqrt{\Delta} \mapsto \overline{x + y\sqrt{\Delta}} = x - y\sqrt{\Delta}$. Thus the norm map in the sense of field theory is

$$N : K \to k(t),\ \alpha = x + y\sqrt{\Delta} \mapsto \alpha\overline{\alpha} = x^2 - \Delta y^2 = q_\Delta(x, y).$$

Moreover $N(\mathcal{O}_\Delta) \subset k[t]$ and for $\alpha \in \mathcal{O}_\Delta$ we have $\alpha \in \mathcal{O}_\Delta^\times \iff N(\alpha) \in k[t]^\times = k^\times$. We define the "complex norm"

$$|\cdot| : \mathcal{O}_\Delta \to \mathbb{Q}^{\geq 0},\ \alpha = x + y\Delta \mapsto 2^{\deg N(\alpha)} = 2^{\deg(x^2 - \Delta y^2)}.$$

This is indeed a norm function on $\mathcal{O}_\Delta$ in the sense of §2.2. As in the general case, we extend it multiplicatively to a norm function on K.

Lemma 2.14. *For an irreducible polynomial $p \in k[t]$, the following are equivalent:*
(i) There are $x, y \in k[t]$ and $u \in k^\times$ such that $q_\Delta(x,y) = up$.
(ii) As an element of the domain $\mathcal{O}_\Delta$, p is reducible (i.e., not irreducible).

Proof. (i) $\implies$ (ii): We have

$$up = q_\Delta(x,y) = (x + y\sqrt{\Delta})(x - y\sqrt{\Delta}) = N(x + y\Delta) = N(x - y\Delta).$$

The elements $x \pm y\Delta$ do not lie in $\mathcal{O}_\Delta^\times$ because then up (hence also p) would lie in $k[t]^\times$, contrary to our assumption. Thus up (hence also p) is reducible in $\mathcal{O}_\Delta$.
(ii) $\implies$ (i): if $p = (x + y\sqrt{\Delta})(z + w\sqrt{\Delta})$ with $x + y\Delta, z + w\Delta \in \mathcal{O}_\Delta \setminus \mathcal{O}_\Delta^\times$, then

$$p^2 = N(p) = N(x + y\sqrt{\Delta})N(z + w\sqrt{\Delta}).$$

The elements $N(x+y\sqrt{\Delta})$,$N(z+w\sqrt{\Delta})$ are not units of the UFD $k[t]$, so the only other possibility is that each of $N(x + y\sqrt{\Delta})$ and $N(z + w\sqrt{\Delta})$ is associate to p, i.e., $N(x + \Delta) = up$ with $u \in k[t]^\times = k^\times$. □

Proposition 2.15.
a) If $p \in k[t]$ is irreducible and $\deg p < \deg \Delta$, then p is irreducible in $\mathcal{O}_\Delta$.
b) If $\mathcal{O}_\Delta$ is a UFD, then for all $x \in k[t]$, the polynomial $q_\Delta(x,1)$ has no irreducible factor of degree less than D.

Proof. a) By contraposition: if p is irreducible, then by Lemma 2.14 there is $\alpha = x + y\Delta \in \mathcal{O}_\Delta$ such that $q_\Delta(x,y) = up$ for some $u \in k^\times$. Since up is not a square in $k[t]$, $y \neq 0$, and thus by Proposition 2.13b) we have $\deg p = \deg up = \deg q_\Delta(x,y) \geq D$.
b) By contradiction: suppose there is an irreducible polynomial p of degree less than D such that $p \mid q_\Delta(x,1) = x^2 - \Delta = (x + \sqrt{\Delta})(x - \sqrt{\Delta})$. By part a), p is irreducible in $\mathcal{O}_\Delta$; since $\mathcal{O}_\Delta$ is a UFD, it follows that $p \mid \pm\Delta$, which is absurd. □

Theorem 2.16.
If $\mathcal{O}_\Delta$ is a UFD, then $x^2 - \Delta$ is irreducible for all $x \in k[t]$ with $\deg x < \deg \Delta$.

Proof. If $\deg x < \deg \Delta$, then $\deg x^2 - \Delta < 2 \deg \Delta$. If $x^2 - \Delta$ is reducible, then some irreducible factor has degree less than $\deg \Delta$, contradicting Proposition 2.15b). □

2.6. **Polynomial Diophantine Approximation.**

Proposition 2.17. *(Polynomial Diophantine Approximation) Let $a \in k(t)$ and let $Q \in \mathbb{N}$. There are $p, q \in k[t]$ such that $0 \leq \deg q \leq Q$ and $\deg(qa - p) < -Q$.*

Proof. FIRST PROOF: Apply Theorems 2.9 and 4.3 of [Cl16].
SECOND PROOF: Let $k((\frac{1}{t}))$ be the field of "formal finite-headed Laurent series." An element $a \in k((\frac{1}{t}))^\times$ can be written in the form $a = \sum_{n \geq N} a_n t^{-n}$ with $a_n \in k$ and $a_N \neq 0$, and we set $\delta(a) = N$ and $\delta(0) = \infty$. We have $k(t) \subset k(\frac{1}{t}))$, and if $x \in k(t)^\times$ then $\delta(x) = -\deg x$. Thus we may establish the result by showing that for all $a \in k((\frac{1}{t}))$ there are $p \in k[t]$, $q \in k[t]^\bullet$ with $\deg(q) \leq Q$ such that $\delta(qa - p) \geq Q + 1$. Let $\mathcal{P}_{\leq Q} \subset k[t]$ be the polynomials of degree at most Q, and consider the map $L : \mathcal{P}_{\leq Q} \to k^Q$ defined as follows: for $q \in \mathcal{P}_{\leq Q}$, write

$$qa = \sum_{n \geq N} a_n t^{-n}$$

and put

$$L(q) = (a_1, \ldots, a_Q).$$

The map L is k-linear. Since $\dim \mathcal{P}_{\le Q} = Q+1 > Q = \dim k^Q$, there is $q \in \mathcal{P}^\bullet_{\le Q}$ such that $L(q) = 0$. The principal part

$$p = \sum_{n=N}^{-1} a_n t^{-n}$$

of qa is a polynomial, and

$$qa - p = \sum_{n=Q+1}^{\infty} a_n t^{-n}$$

and thus

$$\delta(qa-p) \ge Q+1. \qquad \square$$

Remark 2.18. *Proposition 2.17 stands in close analogy to Dirichlet's Diophantine Approximation. In the former case, although our present application concerned the approximation of rational numbers, it was more natural to approximate all real numbers. Of course $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to the standard absolute value, which is extended from a multiplicative norm on $\mathbb{Z}$. In our case the norm $2^{\deg} = 2^{-\delta}$ is the norm associated to the discrete valuation δ on $k(t)$, and $k((\frac{1}{t}))$ is nothing else than the completion of $k(t)$ under this norm. And again, though here we will only need to approximate elements of $k(t)$, it is more natural to work with the complete field $k((\frac{1}{t}))$. Finally, the proof of Dirichlet's Diophantine Approximation used the pigeonhole principle, here we use the fact that $n+1$ vectors in k^n are linearly dependent. When k is finite this follows from the usual pigeonhole principle.*

2.7. **Proof of (ii′) $\implies$ (i) in the Polynomial Rabinowitsch Criterion.**

Lemma 2.19. *Let K be the fraction field of $\mathcal{O}_\Delta$. For $\alpha \in K$ there is $q \in k[t]$ such that $\deg q \le \lceil \frac{\deg \Delta}{2} \rceil$ and $\beta \in \mathcal{O}_\Delta$ such that $\deg N(q\alpha - \beta) < 0$.*

Proof. Let $\alpha = x + y\sqrt{\Delta}$ with $x, y \in k(t)$. Apply Proposition 2.17 with $Q = \lceil \frac{\deg \Delta}{2} \rceil$ and $a = y$: we get $p, q \in k[t]$ with $0 \le \deg q \le Q$ and $\deg(qy - p) < -Q$. Choose $z \in k[t]$ such that $\deg(qx - z) < 0$ and put $\beta = z + p\sqrt{\Delta}$. Then

$$N(q\alpha - \beta) = N((qx-z) + (qy-p)\sqrt{\Delta}) = (qx-z)^2 - \Delta(qy-p)^2$$

has negative degree since $(qx - z)$ does and

$$\deg \Delta(qy-p)^2 < -2Q + \deg \Delta = -2\lceil \frac{\deg \Delta}{2} \rceil + \deg \Delta \le 0. \qquad \square$$

Theorem 2.20. *Suppose that for all $x \in k[t]$, if $\deg x < \lceil \frac{\deg \Delta}{2} \rceil$ then $x^2 - \Delta$ is not composite. Then $\mathcal{O}_\Delta$ is a PID.*

Proof. We will show the complex norm is a Dedekind-Hasse norm. Let $\alpha \in K \setminus \mathcal{O}_\Delta$. We must find $\gamma, \beta \in \mathcal{O}_\Delta$ such that $) < |\gamma\alpha - \beta| < 1$, or equivalently that $N(\gamma\alpha - \beta)$ has negative degree. By Lemma 2.19 there is $t \in k[t]$ of degree at most $\lceil \frac{\deg \Delta}{2} \rceil$ and $\beta \in \mathcal{O}_\Delta$ such that $N(t\alpha - \beta)$ has negative degree, and as above we are done unless $t\alpha \in \mathcal{O}_\Delta$, so assume this. Without loss of generality we may assume that t is the denominator of γ (and thus that $t > 1$). Consider $\eta = t\overline{\alpha} \in \mathcal{O}_\Delta$. We have

$$\eta\alpha = \frac{N(t\alpha)}{t} \in k(t),$$

so we may choose $\beta \in k[t]$ such that $N(\eta\alpha - \beta)$ has negative degree. So again we are done unless $\eta\alpha \in \mathcal{O}_\Delta \cap k(t) = k[t]$: in other words, unless $t \mid N(t\alpha)$. We may assume without loss of generality that t is minimal in the sense that there is no proper divisor t' of t such that $t\alpha \in \mathcal{O}_\Delta$ (otherwise replace t with a proper divisor). Write $t\gamma = a + b\sqrt{\Delta}$ with $a, b \in k[t]$. We claim b and t are relatively prime in $k[t]$: indeed, if ℓ is an irreducible polynomial dividing both b and t then

$$\ell \mid t \mid N(t\gamma) = a^2 - \Delta b^2,$$

so $\ell \mid a$ and thus $\left(\frac{t}{\ell}\right)\gamma \in \mathcal{O}_\Delta$, contradicting the minimality of t. Thus there are $y \in k[t]$ with $by \equiv 1 \pmod{t}$ and $x \in k[t]$ with $xy \equiv a \pmod{t}$; we may moreover choose x such that $\deg x < \deg t$. Then

$$N(ty\gamma) = N(ay + by\sqrt{\Delta}) \equiv N(x + \sqrt{\Delta}) \pmod{t}.$$

Since $t \mid |t\gamma| \mid |ty\gamma|$, it follows that $t|N(x+\sqrt{\Delta}) = x^2 - \Delta$. Since $\deg x^2 - \Delta \geq \deg \Delta$ and $\deg x < \deg t \leq \lceil \frac{\deg \Delta}{2} \rceil$, we have $t \neq N(x + \sqrt{\Delta})$. Since $\gamma \in K \setminus \mathcal{O}_\Delta$, $t \notin k[t]^\times$. Thus we have found $x \in k[t]$ with $\deg x < \lceil \frac{\deg \Delta}{2} \rceil$ such that $N(x + t)$ is composite, contradicting our hypothesis. □

3. Interlude: Some quadratic number theory

3.1. **Quadratic Orders Over a PID.** Let R be a PID of characteristic not 2, with fraction field K. Let L/K be a quadratic field extension. For any $\alpha \in L \setminus K$ we have $L = K[\alpha]$; after scaling α by an element of $R^\bullet$, we may assume that α is integral over R, i.e., the minimal polynomial $f(t) = t^2 + bt + c$ of α over K has coefficients in R. We define the **discriminant** of α as

$$\Delta(\alpha) = b^2 - 4c \in R,$$

so (because $2 \in K^\times$) we have $L = K(\sqrt{\Delta(\alpha)})$. Since

$$R[\alpha] \cong R[t]/(t^2 + bt + c)$$

as an R-module $R[\alpha]$ is free of rank 2. Conversely, any R-subalgebra $\mathcal{O} of\ L$ which is free of rank 2 as an R-module is of the form $R[x]$ for some $x \in L$ which is integral over R. Such a ring $\mathcal{O}$ is called an R-order in L, and a **quadratic R-order** is an R-order in a quadratic field extension of K. Let $\mathcal{O}_L$ be the integral closure of R in L, which is a Dedekind domain. Because $\mathrm{char}(R) \neq 2$, L/K is separable and $\mathcal{O}_L$ is an R-order in L. It is moreover the unique maximal R-order in L.

The discriminant $\Delta(\alpha)$ is the discriminant of the discriminant of the trace form of $R[\alpha]$ with respect to the R-basis $1, \alpha$. It follows that if for $\beta \in \mathcal{O}_L$ we have $R[\alpha] = R[\beta]$ then there is a unit $u \in R^\times$ such that $\Delta(\beta) = u^2\Delta(\alpha)$. Conversely, for $u \in R^\times$ we have $\Delta(u\alpha) = u^2\Delta(\alpha)$. So the discriminant of a quadratic order ought really to be viewed as an element of the quotient monoid $R^\bullet/R^{\times 2}$. Here we will take the approach of speaking of "a discriminant" of a quadratic order, keeping the above discussion in mind.

Proposition 3.1. *Let R be a PID, let $\mathcal{O} = R[\alpha]$ a quadratic R-order, let $f = t^2 + bt + c \in R[t]$ be the minimal polynomial of α, and let $p \in R^\bullet$ be a prime element. We suppose that* $\mathrm{char}(R/pR) \neq 2$. *The following conditions are equivalent:*
(i) p is a prime element of $\mathcal{O}$.
(ii) The polynomial f is irreducible in $(R/pR)[t]$.

(iii) $\Delta(\alpha) = b^2 - 4ac$ *is not a square in* R/pR.
When they hold, we say p *is* ***inert in*** $\mathcal{O}$. *If* $\mathcal{O} = \mathcal{O}_L$ *we say* p *is* ***inert in*** L.

Proof. Observe that R/pR is a field and that $\mathcal{O}/p\mathcal{O} \cong (R/pR)[t]/(f)$.
(i) $\iff$ (ii): The ring $R/pR[t]$ is a UFD, and thus p is a prime element of $\mathcal{O}$ iff $\mathcal{O}/p\mathcal{O}$ is a domain iff f is irreducible in $(R/pR)[t]$.
(ii) $\iff$ (iii): Since $\mathrm{char}(R/pR) \neq 2$, the quadratic polynomial $f \in R/pR[t]$ is irreducible iff it has no root in $R/pR[t]$ iff $\Delta(\alpha)$ is not a square in R/pR. □

3.2. **Reduction to the Maximal Order.** Theorem 1.1 is often stated only when $C \in \mathbb{Z}^+$ is such that $1 - 4C$ is squarefree, in which case $\mathcal{O}_{1-4C}$ is the full ring of integers of the $\mathbb{Q}(\sqrt{1-4C})$. This is not necessary – if we follow Fendel the issue does not even arise. However, for the subsequent proofs, non-maximal orders engender technical complications that we prefer to evade rather than surmount.

Proposition 3.2. *a) Let* $C \in \mathbb{Z}+$. *Each of conditions (i) and (ii) in the Rabinowitsch Criterion implies that* $1 - 4C$ *is squarefree.*
b) Let $\Delta \in k[t]$ *be definite and of positive degree. Each of conditions (i) and (ii′) in the Rabinowitsch Criterion implies that* Δ *is squarefree.*

Proof. a) Let $\mathcal{O}$ be the quadratic $\mathbb{Z}$-order of discriminant $\Delta = 1-4C$. We may write $\Delta = \mathfrak{f}^2\Delta_K$, where $\mathfrak{f} \in \mathbb{Z}^+$ is odd and Δ_K is squarefree. Our task is to show that if $\mathfrak{f} > 1$ then neither condition (i) nor condition (ii) of the Rabinowitsch Criterion holds. First, if $\mathfrak{f} > 1$ then as above $\mathcal{O}_\Delta$ is not integrally closed in its fraction field, so it cannot be a PID: condition (i) does not hold. Moreover, since the odd number $\mathfrak{f}$ divides Δ, the quadratic polynomial $x^2 + 2 + \frac{1-\Delta}{4}$ has a root modulo $\mathfrak{f}$, so there is $x \in [0, \mathfrak{f} - 1]$ such that $\mathfrak{f} \mid x^2 + x + \frac{1-\Delta}{4}$. A calculation shows that $\mathfrak{f} - 1 \leq C - 2$ and $\mathfrak{f} < x^2 + x + \frac{1-\Delta}{4}$, so there is $x \in [0, C-2]$ such that $x^2 + x + C$ is composite: condition (ii) does not hold.
b) Let $\mathcal{O}_\Delta$ be the quadratic $k[t]$-order of discriminant Δ, and suppose $\Delta = \mathfrak{f}^2\Delta_K$ with $\deg \mathfrak{f} \geq 1$. Then as above $\mathcal{O}_\Delta$ is not integrally closed hence not a PID: condition (i) does not hold. Moreover, evaluating at 0 gives the composite polynomial $\mathfrak{f}^2\Delta_K$, so condition (ii′) does not hold. □

3.3. **Inertness Lemmas.** Let R be a PID, let $x \in R$, and let $p \in R^\bullet$ be a prime element. We will write $\left(\frac{x}{p}\right) = -1$ if x is not a square in the field $R/(p)$. This condition depends only on the ideal (p), and thus when $R = \mathbb{Z}$ it agrees with the usual Legendre symbol.[1]

Lemma 3.3. *(Inertness Lemma)*
Let $C \in \mathbb{Z}^{\geq 2}$, *and put* $\Delta = 1 - 4C$.
a) Let $1 \leq c < C$, *and suppose that for all* $x \in [0, c-1]$ *the integer* $x^2 + x + C$ *is prime. Then for all prime numbers* $p \leq c$ *we have* $\left(\frac{\Delta}{p}\right) = -1$.
b) Supose that for all prime numbers $p < C$ *we have* $\left(\frac{\Delta}{p}\right) = -1$. *Then for all* $x \in [0, C-2]$, *the integer* $x^2 + x + C$ *is prime.*

Proof. a) By contraposition: suppose there is a prime number $p \leq c$ such that Δ is a square modulo p. Then there is $x \in [0, p-1]$ such that $p \mid x^2 + x + C$ and

$$x^2 + x + C \geq C > c \geq p,$$

[1]We could also define $\left(\frac{x}{p}\right) = 0$ if $p \mid x$ and $\left(\frac{x}{p}\right) = 1$ if x is a nonzero square in $R/(p)$, but **beware**: $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$ holds for all $x, y \in R$ iff $R/(p)$ has at most 2 square classes.

so $x^2 + x + C$ is not prime.
b) By contraposition: suppose there is $x \in [0, C-2]$ such that $x^2 + x + C$ is not prime; since $C > 1$, there is a prime number $p \leq \sqrt{(C-2)^2 + (C-2) + C} < \sqrt{(C-1)^2 + (C-1) + C} = C$ such that $p \mid x^2 + x + C$ and thus $\left(\frac{\Delta}{p}\right) \neq -1$. □

Lemma 3.4. *(Polynomial Inertness Lemma) Let $\Delta \in k[t]$ be definite, $\deg \Delta \geq 2$.*
a) Let $c < \deg \Delta$ and suppose that for all $x \in k[t]$ with $\deg x < c$, the polynomial $x^2 - \Delta$ is prime. Then for all primes $p \in k[t]$ with $\deg p \leq c$ we have $\left(\frac{\Delta}{p}\right) = -1$.
b) Suppose that for all $x \in k[t]$ with $\deg x < \lceil \frac{\deg \Delta}{2} \rceil$ the polynomial $x^2 - \Delta$ is prime. Then for all primes $p \in k[t]$ with $\deg p \leq \lceil \frac{\deg \Delta}{2} \rceil$ we have $\left(\frac{\Delta}{p}\right) = -1$.

Proof. a) By contraposition: suppose there is a prime $p \in k[t]$ with $\deg p \leq c$ such that Δ is a square modulo p. By polynomial division, there is $x \in k[t]$ with $\deg x < \deg p$ such that $p \mid x^2 - \Delta$. Since $\deg x^2 - \Delta \geq \deg \Delta > c \geq \deg p$, the polynomial $x^2 - \Delta$ is not prime.
b) By contraposition: suppose there is a prime $p \in k[t]$ with $\deg p \leq \lceil \frac{\deg \Delta}{2} \rceil$ such that $\left(\frac{\Delta}{p}\right) \neq -1$, i.e., Δ is a square modulo p. By polynomial division there is $x \in k[t]$ with $\deg x < \deg p \leq \lceil \frac{\deg \Delta}{2} \rceil$ such that $p \mid x^2 - \Delta$, and

$$\deg(x^2 - \Delta) \geq \deg \Delta > \lceil \frac{\Delta}{2} \rceil,$$

so $x^2 - \Delta$ is not prime. □

4. Rabinowitsch III and IV: Following Granville

4.1. **Binary quadratic forms over a PID.** Let R be a PID, of characteristic not 2, with fraction field K. By a binary quadratic form over R we mean a polynomial $f(x, y) = ax^2 + bxy + cy^2 \in R[x, y]$. The **discriminant** of a binary quadratic form f is $\Delta(f) = b^2 - 4ac$. Put

$$A_f = \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix} \in M_2(K)$$

and viewing (x, y) as a column vector, we have

$$q(x, y) = (x, y)^T A_f (x, y)$$

and

$$\operatorname{disc} f = -4 \det A_f.$$

Two binary quadratic forms $q, q' \in R[x, y]$ are **widely equivalent** (resp. **narrowly equivalent**) if there is $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(R)$ (resp. $\mathrm{SL}_2(R)$) such that $q'(x, y) = q(ax + by, cx + dy)$. If q and q' are widely equivalent, then $\Delta(q') \equiv \Delta(q) \pmod{R^{\times 2}}$ (resp. $\Delta(q') = \Delta(q)$). We say q **represents** $z \in R$ if there are $(x, y) \in R^2$ such that $q(x, y) = z$. We say q **primitively represents** $z \in R$ if there are $(x, y) \in R^2$ with $\langle x, y \rangle = R$ such that $q(x, y) = z$. If z is squarefree then all representations of z are primitive.

Proposition 4.1.
a) For $a, \Delta \in R$, the following are equivalent:
(i) There are $b, c \in R$ such that $ax^2 + bxy + cy^2$ has discriminant Δ.
(ii) Some binary quadratic form of discriminant Δ primitively represents a.

(iii) The image of Δ in $R/4aR$ is a square.
b) If a quadaratic form $q(x,y) \in R[x,y]$ primitively represents a, then q is narrowly equivalent to $ax^2+bxy+cy^2$ for some $b,c \in R$.

Proof. a) (i) $\implies$ (ii): $q(x,y) = ax^2+bxy+cy^2$ has discriminant Δ and $q(1,0) = a$.
(ii) $\implies$ (iii): Suppose there is $q(x,y) = Ax^2+Bxy+Cy^2$ with $B^2-4AC = \Delta$ and $\alpha, \gamma \in R$ such that $\langle \alpha, \gamma \rangle = R$ and

$$a = A\alpha^2 + B\alpha\gamma + C\gamma^2.$$

Since R is a PID there are $\beta, \delta \in R$ such that $\alpha\delta - \beta\gamma = 1$. Put

$$x = \alpha X + \beta Y,\ y = \gamma X + \delta Y.$$

Then

$$f(x,y) = f(\alpha X + \beta Y, \gamma X + \delta Y) = aX^2 + bXY + cY^2$$

for some $b, c \in R$. Then $\Delta = b^2 - 4ac \equiv b^2 \pmod{a}$.
(iii) $\implies$ (i): There are $b, c \in R$ such that $b^2 - \Delta = 4ac$.
b) This follows from the proof of (ii) $\implies$ (iii). □

We say that $\Delta \in R$ is a **quadratic discriminant** if Δ is a square modulo $4R$. We justify the terminology as follows: if there is a binary quadratic form $f = ax^2+bxy+cy^2 \in R[x,y]$ of discriminant Δ, then $b^2-4ac = \Delta$, so Δ is a square in $R/4R$. The converse is also true: indeed, if Δ is a square modulo $4R$ then there are $b, c \in R$ such that $b^2 - 4c = \Delta$, so $x^2+bxy+cy^2$ has discriminant Δ.

Henceforth we suppose that Δ is a quadratic discriminant which is not a square in R (hence also is not a square in K, since R is integrally closed). Let $L = K(\sqrt{\Delta})$. As above, there is an element $\tau \in L$ satisfying a monic polynomial relation $\tau^2+b\tau+c = 0$ with $b, c \in R$ and $b^2 - 4c = \Delta$. We put $\mathcal{O}_\Delta = R[\tau] = R \cdot 1 \oplus R \cdot \tau$, so $\mathcal{O}_\Delta$ is a quadratic R-order in L whose discriminant in the more general algebraic sense (i.e., the discriminant of the trace form) is the class of Δ in $R/R^{\times 2}$.

There is a standard right action of $\mathrm{GL}_2(R)$ on binary quadratic forms: if $M = \left[\begin{array}{cc} \alpha & \beta \\ \gamma & \delta \end{array} \right] \in \mathrm{GL}_2(R)$ and $f(x,y) = ax^2+bxy+cy^2$,

$$(f \circ M)(x,y) = f(\alpha x + \beta y, \gamma x + \delta y).$$

$$(f \circ M)(x,y) = (x,y)^T M^T A_f M (x,y) = (M(x,y))^T A_f (M(x,y)),$$

so

$$\mathrm{disc}(f \circ M) = \det(M)^2 \,\mathrm{disc}(f).$$

If $R = \mathbb{Z}$ then the natural (right) $\mathrm{GL}_2(R)$-action preserves discriminants, but in general it only preserves the class of the discriminant in $R/R^{\times 2}$. The classical way to get an action which preserves the discriminant is to restrict to $\mathrm{SL}_2(R)$. Here we will use the **twisted action**: for $f \in \mathrm{GL}_2(R)$, we put

$$(f \bullet M)(x,y) = \frac{1}{\det M}(f \circ M)(x,y),$$

and thus

$$\mathrm{disc}(f \bullet M) = \mathrm{disc}\, f.$$

We say that two binary quadratic forms are **twisted equivalent** if they lie in the same twisted $\mathrm{GL}_2(R)$-orbit and write $f \equiv g$. Let $C(\Delta)$ denote the set of twisted equivalence classes of binary quadratic forms of discriminant Δ.

Example 4.2. *Using the matrix* $M = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, *we find that* $f(x,y) = ax^2 + bxy + cy^2$ *is twisted equivalent to* $f' = -ax^2 + bxy - cy^2$, *although these two forms are in general not widely equivalent: e.g. over* $\mathbb{Z}$, f *is positive-definite iff* f' *is negative-definite. From the classical perspective this is a bit strange, but in a context in which we do not have notions of "positive" and "negative," this behavior is desirable.*

Thus twisted equivalent quadratic forms need not represent the same elements of R, which motivates the following definition of González-Avilés: $a \in R$ is **quasi-represented** (resp. **primitively quasi-represented**) by the binary quadratic form $f(x,y) \in R[x,y]$ if there are $u \in R^\times$ and $(x,y) \in R^2$ (resp. there are $u \in R^\times$ and $(x,y) \in R^2$ with $\langle x, y \rangle = R$) such that

$$f(x,y) = ua.$$

The following simple result may be left to the reader.

Lemma 4.3.
a) For a binary quadratic form $f \in R[x,y]$ *and* $a \in R$, *the following are equivalent:*
(i) f *quasi-represents* a.
(ii) Every g *which is twisted equivalent to* f *quasi-represents* a.
(iii) Some g *which is twisted equivalent to* f *represents* a.
b) The results of part a) continue to hold when each instance of "represented" is replaced by "primitively represented."

A binary quadratic form $f \in R[x,y]$ is **principal** if it quasi-represents 1.F

Let L/K be a quadratic field extension. Denote by $x \mapsto \overline{x}$ the nontrivial field automorphism. Let $\mathcal{O}_L$ be the integral closure of R in L. There is a norm function from ideals of $\mathcal{O}_L$ to ideals of R, $N(I) = I\overline{I} \cap R$. This function is multiplicative, so it is characterized by its restriction to prime ideals, which is as follows: let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_L$, and let $(p) = \mathfrak{p} \cap R$. If $p\mathcal{O}_L = \mathfrak{p}\overline{\mathfrak{p}}$ then $N(\mathfrak{p}) = (p)$, whereas if $pR = \mathfrak{p}$ is a prime ideal, then $N(\mathfrak{p}) = (p^2)$.

Theorem 4.4. *Let* R *be a PID of characteristic not* 2 *with fraction field* K, *let* L/K *be a quadratic field extension, let* $\mathcal{O}_L$ *be the integral closure of* R *in* L, *and let* Δ *be a discriminant of* $\mathcal{O}_L$. *To a nonzero ideal* $I = \langle \alpha, \beta \rangle$ *of* $\mathcal{O}_L$, *we associate the quadratic form*

$$\Phi(I)(x,y) = \frac{\alpha\overline{\alpha}x^2 + (\alpha\overline{\beta} + \overline{\alpha}\beta)xy + \beta\overline{\beta}y^2}{N(I)}.$$

The above notation is slightly abusive: $N(I)$ *is an* ideal *of the PID* R, *and our claim is that it has a (unique) generator such that* $\operatorname{disc}\Phi(I) = \Delta$.[2] *To a quadratic form* $f(x,y) = ax^2 + bxy + cy^2 \in R[x,y]$ *of discriminant* Δ, *we associate the* $\mathcal{O}_L$*-ideal*

$$\Psi(f) = \left\langle a, \frac{-b + \sqrt{\Delta}}{2} \right\rangle.$$

[2]The ambiguity in the choice of Δ corresponds precisely to the ambiguity in the choice of a generator for $N(I)$.

a) For all ideals I of $\mathcal{O}_L$, $\Phi(I) \in R[x,y]$ has discriminant Δ.
b) If $f_1 \equiv f_2$, then $[\Psi(f_1)] = [\Psi(f_2)]$ in $\operatorname{Pic} \mathcal{O}_L$.
c) If $[I_1] = [I_2] \in \operatorname{Pic} \mathcal{O}_L$, then $\Phi(I_1) \equiv \Phi(I_2)$.
d) The induced maps $\overline{\Phi} : C(\Delta) \to \operatorname{Pic} \mathcal{O}_L$ and $\overline{\Psi} : \operatorname{Pic} \mathcal{O}_L \to C(\Delta)$ are mutually inverse bijections.

Proof. This is morally a special case of much more general results of Kaplansky [Ka68], Kneser [Kn82] and Wood [Wo11], although some translation is required. But the result is plainly implied by Example 4.4 in [O'D15], which treats arbitrary quadratic orders over a PID (here we have restricted to maximal orders). The special case $R = \mathbb{F}_q[t]$ is due to González-Avilés [Go92]. □

Corollary 4.5. *Maintain the notation of the previous result.*
a) For a form f of discriminant Δ, f is principal iff $\Psi(f)$ is a principal $\mathcal{O}_L$-ideal.
b) Two principal forms of discriminant Δ are twisted equivalent.
c) Every binary quadratic form of discriminant Δ is principal iff $\mathcal{O}_L$ is a PID.

Proof. a) Suppose f is principal. According to the theorem we may adjust f within its twisted equivalence class, and thus we may assume $a \in R^\times$. Then $\Psi(f) = \langle a, \frac{-b+\sqrt{\Delta}}{2} \rangle = \langle \frac{-b+\sqrt{\Delta}}{2} \rangle = \mathcal{O}_L$. Suppose $\Psi(f)$ is principal. Again we may adjust within the equivalence class and thus may assume $\Psi(f) = \mathcal{O}_L$, in which case evaluating $\Phi(\Psi(f)) = \Phi(\mathcal{O}_L)$ at $(1,0)$, we get 1.
b) This follows immediately from part a) and Theorem 4.4b).
c) This follows from part b): the principal forms form a full twisted equivalence class which corresponds to the equivalence class of principal ideals. □

The following consequence is a key one for us.

Corollary 4.6. *Let $f \in R[x,y]$ be a binary quadratic form of discriminant $\Delta \in R \backslash R^2$. Suppose the quadratic R-order $\mathcal{O}$ of discriminant Δ is a PID. If f primitively quasi-represents $a \in R$, then f primitively represents each $b \mid a$.*

Proof. Since f primitively quasi-represents a, it primitive represents ua for some $u \in R^\times$ and thus Δ is a square modulo $\langle 4ua \rangle = \langle 4a \rangle$. If b divides a, then Δ is also a square modulo $4b$, so some binary quadratic form g of discriminant Δ primitively represents b. But since $\mathcal{O}$ is a PID, by Corollary 4.5 all binary quadratic forms of discriminant Δ lie in the same twisted equivalence class, so $f \equiv g$ and thus f primitively quasi-represents a. □

4.2. **In the presence of a Euclidean norm.** If $(R, |\cdot|)$ is a normed PID and $f(x,y) \in R[x,y]$ is a binary quadratic form, we define the **minimum** $\min(f)$ to be the minimum value of $|q(x,y)|$ as (x,y) ranges over elements of $(R^2)^\bullet$. If $\Delta(f)$ is not a square in R, then $\min(f) \geq 1$. All three notions of equivalence preserve the minimum, and we have $\min(f) = 1$ iff f is principal.

Proposition 4.7. *Let R be a domain of chracteristic not 2, and let $|\cdot|$ be a Euclidean norm on R. Let $f \in R[x,y]$ be a quadratic form with $\Delta(f) \in R \setminus R^2$.*
a) The form q is properly equivalent to a form $ax^2 + bxy + cy^2$ with $|a| = \min(f)$, $|b| < |2a|$ and $|a| \leq |c|$.
b) If $R = \mathbb{Z}$, then f is properly equivalent to a form $ax^2+bxy+cy^2$ with $|a| = \min(f)$ and $|b| \leq |a| \leq |c|$. Moreover, if $a \geq 1$ then f is properly equivalent to a form

$ax^2 + bxy + cy^2$ with $a = \min(f)$, $0 \leq b \leq 2a - 1$ and $|a| \leq |c|$.
c) If $2 \in R^\times$, then f is properly equivalent to a form $ax^2 + bxy + cy^2$ with $|a| = \min(f)$ and $|b| < |a| \leq |c|$.

Proof. a) By definition of the minimum, f represents some $a \in R$ with $|a| = \min(f)$, and every representation of such an a by f is primitive. So by Proposition 4.1, f is narrowly equivalent to a form $f' = ax^2 + b'xy + c'y^2$ with $|a| = \min(f)$. Now for any $q \in R$, consider the matrix

$$T_q = \begin{bmatrix} 1 & q \\ 0 & 1 \end{bmatrix} \in \mathrm{SL}_2(R).$$

Applying T_q to f we get a form $ax^2 + (2qa + b')xy + Cy^2$ for some $C \in R$. Because the norm is Euclidean, there are $q, r \in R$ such that $b' = q(-2a) + r$ with $|r| < |2a|$. This gives us a properly equivalent form $ax^2 + bxy + cy^2$ with $|a| = \min(f)$ and $|b| < |2a|$. Since $c = f(0, 1)$ and $|a| = \min(q)$, we necessarily have $|a| \leq |c|$.
b) In $\mathbb{Z}$, when we divide by $2a$ we can take the remainder to lie in $[-|a|, |a|]$, so to have norm at most $|a|$. Moreover, if $a \geq 1$ we can take the remainder in $[0, 2a - 1]$.
c) If $2 \in R^\times$ then $|2a'| = |2||a'| = |a'|$. □

Let $\Delta \in R \setminus R^2$. If $\mathcal{O}_\Delta = R[\frac{1+\sqrt{\Delta}}{2}]$, we put

$$f_\Delta = x^2 + xy + \left(\frac{1 - \Delta}{4}\right) y^2.$$

If $\mathcal{O}_\Delta = R[\sqrt{\Delta}]$, we put

$$f_\Delta = x^2 - \left(\frac{\Delta}{4}\right) y^2.$$

In either case, f_Δ has discriminant Δ and represents 1.

Corollary 4.8. *Let R be $\mathbb{Z}$ or $k[t]$, and let $f(x, y) \in R[x, y]$ have nonsquare discriminant Δ and represent 1. Then f is narrowly equivalent to f_Δ.*

Proof. First suppose $R = \mathbb{Z}$. By Binary Reduction, f is narrowly equivalent to $g = x^2 + bxy + cy^2$ with $b \in \{0, 1\}$. Moreover $b \equiv \Delta \pmod 2$, so if $\Delta \equiv 1 \pmod 4$ then $b = 1$ and since $\Delta = b^2 - 4ac = 1 - 4c$, we have $c = \frac{1-\Delta}{4}$ and thus $g = f_\Delta$. Similarly, if $\Delta \equiv 0 \pmod 4$ then $b = 0$ so $c = \frac{-\Delta}{4}$ and $g = f_\Delta$.
Now suppose $R = k[t]$. By Binary Reduction, f is narrowly equivalent to $G = x^2 + cy^2$, and again equating discriminants gives $c = \frac{-\Delta}{4}$. □

4.3. **Granville's Proof of the Rabinowitsch Criterion.** Let $C \in \mathbb{Z}^+$ and $\Delta = 1 - 4C$, and let $f(x, y) = x^2 + xy + Cy^2$.

(i) $\implies$ (ii): Suppose $\mathcal{O}_\Delta$ is a PID. Seeking a contradiction, let $x \in [0, C - 2]$ be such that $m = x^2 + x + C$ is composite, and let p be a prime divisor of m. Then

$$p \leq \sqrt{m} < \sqrt{(C-1)^2 + (C-1) + C} = \sqrt{C^2} = C.$$

Since $m = f(x, 1)$, the form f primitively represents m. By Corollary 4.6 f primitively quasi-represents p: here, that means f primitively represents $\pm p$, and since f is positive definite, the plus sign plays: there are $x, y \in \mathbb{Z}$ such that

$$p = x^2 + xy + Cy^2 = (x + \frac{y}{2})^2 + \frac{-\Delta}{4} y^2.$$

As in the proof of Lemma 2.2, this implies $p \geq C$: contradiction.
(ii) $\implies$ (i) Suppose there is a nonprincipal form of discriminant Δ. By binary reduction, there is then a form $f = ax^2 + bxy + cy^2$ of discriminant Δ with $|a| \geq 2$ and $|b| \leq |a| \leq |c|$. Then

$$|\Delta| = -\Delta = 4ac - b^2 = 4|a||c| - |b|^2 \geq 4|a| \cdot |a| - |a|^2 = 3|a|^2,$$

so

$$|a| \leq \sqrt{\frac{|\Delta|}{3}}.$$

Let p be the smallest prime factor of $|a|$. Since f primitively represents a, Δ is a square modulo $4a$, hence is also a square modulo p.

Because there are only finitely many reduced forms of a given discriminant, we may easily check that every form of discriminant -3 is principal, and thus we may assume $C \geq 2$ and thus $\Delta \leq -7$. If $p = 2$ then since Δ is an odd square modulo 8 we have $\Delta \equiv 1 \pmod 8$ and $C = \frac{1-\Delta}{4}$ is even and $f(0) = 0^2 + 0 + C = C$ is composite. Otherwise p is odd, hence there is an odd x such that $x^2 \equiv \Delta \pmod p$. We may take $n_1 \in [0, p-1]$ such that $(2n_1 + 1)^2 \equiv \Delta \pmod p$, hence

$$p \mid 4n_1^2 + 4n_1 + 1 - \Delta = 4(n_1^2 + n_1 + C),$$

so $p \mid n_1^2 + n_1 + C$. If $n_1^2 + n_1 + C$ were prime then we'd have

$$\sqrt{\frac{|\Delta|}{3}} \geq |a| \geq p = n_1^2 + n_1 + C \geq C = \frac{1-\Delta}{4},$$

an equality which does not hold since $\Delta < -3$. So there is $n_1 \leq p - 1 < p \leq |a| \leq \sqrt{\frac{|\Delta|}{3}}$ with $f(n_1) = n_1^2 + n_1 + C$ composite.

4.4. **Proof of the Polynomial Rabinowitsch Criterion.** Let $\Delta \in k[t]$ be of positive degree and definite. Suppose, by way of contradiction, that every binary quadratic form $f(x, y) \in k[t, x, y]$ of discriminant Δ is principal and that there is $x \in k[t]$ with $\deg x < \deg \Delta$ such that $m = x^2 - \Delta$ is composite. Then m has an irreducible factor p satisfying

$$\deg p \leq \frac{1}{2} \deg m = \frac{1}{2} \deg(x^2 - \Delta) < \deg \Delta.$$

Since $m = f_\Delta(x, 1)$, it is primitively represented by a form of discriminant Δ, we have that Δ is a square modulo m (since $2 \in R^\times$, we have $mR = 4mR$) and thus is also a square modulo p, so p is represented by some quadratic form f of discriminant Δ. Since every form of discriminant Δ is principal, there is $u \in k^\times = k[t]^\times$ such that $uf_\Delta = x^2 - \frac{\Delta}{4}$ represents p, hence so does $x^2 - \Delta$. But because Δ is definite, $\deg(x^2 - \Delta) \geq \deg \Delta > \deg p = \deg(u^{-1}p)$: contradiction.

Now suppose that there is a nonprincipal form of discriminant Δ. By binary reduction there is then a form $f = ax^2 + bxy + cy^2$ of dsicriminant Δ with $\deg a \geq 1$ and $\deg b < \deg a \leq \deg c$. Then

$$\deg \Delta = \deg(ac - b^2) = \deg(ac) = \deg a + \deg c \geq 2 \deg a,$$

i.e.,

$$\deg a \leq \frac{1}{2}(\deg \Delta).$$

Let p be an irreducible factor of a. Since f primitively represents a, Δ is a square modulo a and thus also a square modulo p. By Euclidean division, there is $x \in k[t]$ with $\deg x < \deg p$ such that

$$p \mid x^2 - \Delta.$$

By Proposition 2.14 we have

$$\deg(x^2 - \Delta) \geq \deg \Delta \geq 2 \deg a \geq 2 \deg p > \deg p,$$

so $x^2 - \Delta$ is composite and

$$\deg x < \deg p \leq \frac{1}{2} \deg \Delta.$$

5. Rabinowitsch V and VI: Following Minkowski

5.1. **Minkowski Bounds and Applications.**

Theorem 5.1. *Let $K/\mathbb{Q}$ be an imaginary quadratic field with discriminant Δ. Then every class in $\operatorname{Pic} \mathcal{O}_K$ has an integral representative I with*

$$|I| := \#\mathcal{O}_K/I \leq \sqrt{\frac{|\Delta|}{3}}.$$

Proof. For a number field F with $[F : \mathbb{Q}] = n$, discriminant Δ_F and precisely s distinct embeddings $\iota : F \hookrightarrow \mathbb{C}$ with $\iota \neq \bar{\iota}$, Minkowski showed that every class in $\operatorname{Pic} \mathcal{O}_F$ has an integral representative I with

$$|I| \leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \sqrt{|\Delta_F|}.$$

For our imaginary quadratic field K this gives

$$|I| \leq \frac{2}{\pi} \sqrt{|\Delta|}.$$

In the imaginary quadratic case, this bound comes from using the Minkowski Convex Body Theorem to get a lower bound on the lattice constant of a 2-dimensional disk. But the exact value of the lattice constant of a 2-dimensional disk is known; this amounts to the theory of reduction of positive definite binary forms. Using this exact value gives the stated upper bound: see e.g. [Ma, Cor. 4.2]. Since

$$0.57735 \approx \frac{1}{\sqrt{3}} < \frac{2}{\pi} \approx 0.6366,$$

this is a (modest) improvement over the Minkowski bound. □

Theorem 5.2. *Let $\Delta \in k[t]$ be definite and of positive degree, and let $\mathcal{O}_\Delta = k[t, \sqrt{\Delta}]$ be the imaginary quadratic order of discriminant Δ. We assume that Δ is squarefree, so $\mathcal{O}_\Delta$ is a Dedekind domain. Then every class in $\operatorname{Pic} \mathcal{O}_\Delta$ has an integral representative I with*

$$\dim_k \mathcal{O}_K/I \leq \left\lceil \frac{\deg \Delta}{2} \right\rceil.$$

Proof. A more precise result, Theorem 7.4, will be proven later on. □

We can now give a third proof that (ii) $\implies$ (i) in the Rabinowitsch Criterion.

Theorem 5.3. *Let $C \in \mathbb{Z}^+$, and suppose that for all $x \in [0, \sqrt{\frac{|\Delta|}{3}} - 1]$ the integer $x^2 + x + C$ is not composite. Then the ring $\mathcal{O} = \mathbb{Z}[\frac{1+\sqrt{1-4C}}{2}]$ is a PID.*

Proof. Let $\Delta = 1 - 4C$ and $K = \mathbb{Q}(\sqrt{\Delta})$.
Step 1: Suppose $C = 1$, so $\Delta = -3$. Then our hypothesis holds, vacuously. Moreover, since Δ is squarefree, $\mathcal{O} = \mathcal{O}_K$ is the ring of integers of K. So it suffices to show that $\operatorname{Pic} \mathcal{O}_K$ is trivial, which is immediate from Theorem 5.1.
Step 2: Suppose $C \geq 2$. Then $\sqrt{\frac{|\Delta|}{3}} < C$, so by our hypothesis Lemma 3.3 applies with $c = \sqrt{\frac{|\Delta|}{3}}$, and we get that $\left(\frac{\Delta}{p}\right) = -1$ for all primes $p \leq \sqrt{\frac{|\Delta|}{3}}$.

Proposition 3.2a) gives $\mathcal{O} = \mathcal{O}_K$. So to show that $\mathcal{O}$ is a PID it is enough to show that the class group $\operatorname{Pic} \mathcal{O}_K$ is trivial. Let $[I] \in \operatorname{Pic} \mathcal{O}_K$, and choose a representative I with $|I| \leq \sqrt{\frac{|\Delta|}{3}}$. We may factor $I = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, and then for all i we have

$$|\mathfrak{p}_i| \leq \prod_{i=1}^{r} |\mathfrak{p}_i| = |I| \leq \sqrt{\frac{|\Delta|}{3}}.$$

So let $\mathfrak{p}$ be a prime ideal with $|\mathfrak{p}| \leq \sqrt{\frac{|\Delta|}{3}}$. Then $\mathfrak{p} \cap \mathbb{Z} = (p)$ for a prime number p. We claim $\mathfrak{p} = p\mathcal{O}_K$; indeed, if not then p is split or ramified, and $p = |\mathfrak{p}| \leq \sqrt{\frac{|\Delta|}{3}}$, so $\left(\frac{\Delta}{p}\right) = -1$, contradiction. Thus $\mathfrak{p} = p\mathcal{O}_K$ is principal and $\mathcal{O}_K$ is a PID. □

Theorem 5.4. *Let* $\deg \Delta \geq 2$. *Then in the Polynomial Rabinowitsch Criterion, condition (ii′) implies condition (i).*

Proof. The proof is parallel to that of Theorem 5.3 and is left to the reader. □

5.2. **End of the proof of the Rabinowitsch Criterion.** Let $R = \mathbb{Z}$. In Theorem 1.1 we have proved (i) $\implies$ (ii) twice: in §2.1 and §4.2. Clearly (ii) $\implies$ (ii′). Lemma 3.3a) gives (ii′) $\implies$ (iii′). And our proof of Theorem 5.3 shows that (iii′) $\implies$ (i). Thus the proof of Theorem 1.1 is complete.

Let $R = k[t]$. In Theorem 1.3 we have proved (i) $\implies$ (ii) twice: in §2.4 and §4.3. Clearly (ii) $\implies$ (ii′). Lemma 3.4a) gives (ii′ $\implies$ (iii′). And our proof of Theorem 5.4 shows that (iii′) $\implies$ (i). Thus the proof of Theorem 1.3 is complete – or rather it will be once we prove Theorem 7.4, which implies Theorem 5.2.

6. Satisfying the Rabinowitsch Criterion I: Elementary Examples

6.1. **Satisfying the Classical Rabinowitsch Criterion.** Over $\mathbb{Z}$, checking the Rabinowitsch Criterion for a given Δ is straightforward. One readily sees that it holds for $\Delta = -3, -7, -11, -19, -43, -67, -163$. As we saw in §4, this is equivalent to showing that every binary quadratic form of discriminant Δ is principal for these values of Δ, and in this form these results were well known to Gauss. In fact, Gauss famously conjectured that the above values of Δ are the only (negative, congruent to 1 (mod 4)) values of Δ such that $\mathcal{O}_\Delta$ is a PID. This class number one problem was resolved affirmatively by Heegner, Baker and Stark.

We turn now to the Polynomial Rabinowitsch Criterion. In contrast to the classical case, there are certainly infinitely many pairs (k, Δ) for which it holds. As we will seee, the examples become more interesting as $\deg \Delta$ increases. In the remainder of this section we examine the case of small degree by elementary methods. In the next section we will incorporate arithmetic geometry, which will allow us to say more and will also give rise to some open problems.

6.2. **Degree 0 and 1.** Let $\Delta \in k[t]$ be definite, and suppose the Rabinowitsch Criterion holds for Δ. Then plugging in $x = 0$ we get that Δ is not composite. If $\deg \Delta = 0$ then $\Delta \in k = k[t]^\times$; if $\deg \Delta \geq 1$ this implies that $\Delta \in k[t]$ is irreducible.

• Suppose $\deg \Delta = 0$. Then condition (ii) of Theorem 1.3 holds (clearly) and condition (iii) holds (vacuously). So the Rabinowitsch Criterion holds and $\mathcal{O}_\Delta$ is a PID. This is easily seen directly: here $l = k[\sqrt{\Delta}]$ is a quadratic field extension of k and $\mathcal{O}_\Delta = k[t, \sqrt{\Delta}] = l[t]$ is a polynomial ring over l, hence a PID.

• Suppose $\deg \Delta = 1$. Then for all $x \in k[t]$ with $\deg x < \deg \Delta$, x is constant, so $\deg(x^2 - \Delta) = 1$, so $x^2 - \Delta$ is prime, so condition (ii) holds. Moreover condition (iii) holds vacuously. So the Rabinowitsch Criterion holds and $\mathcal{O}_\Delta$ is a PID. Again, this is easily seen directly: if $\Delta = at + b$ then

$$\mathcal{O}_\Delta = k[t, \sqrt{at+b}] \cong k[\sqrt{t}] \cong k[t],$$

so again $\mathcal{O}_\Delta$ is simply a univariate polynomial ring over a field.

• Suppose $\deg \Delta = 1$ and $k = \mathbb{C}$ (or any algebraically closed field of characteristic not 2). Then for *all* $x \in k[t]$ with $\deg x = d \geq 1$, we have $\deg(x^2 - \Delta) = 2d \geq 2$, so $x^2 - \Delta$ is composite. Thus the degree bounds in conditions (ii) and (ii′) are sharp.

From now on we assume $\deg \Delta \geq 2$. This makes things more interesting:

Proposition 6.1. *Let $\Delta \in k[t]$ be definite, of degree at least 2. Then $\mathcal{O}_\Delta$ is* not *isomorphic to $k[t]$ or to $l[t]$ for any quadratic field extension l/k.*

Proof. The result is clear if $\mathcal{O}_\Delta$ is not a PID, so we may assume that the Rabinowitsch Crtierion holds for Δ. Condition (iii) of Theorem 1.3 implies that $\mathcal{O}_\Delta$ has no degree one primes: i.e., there is no prime ideal $\mathfrak{p}$ of $\mathcal{O}_\Delta$ such that $\mathcal{O}_\Delta/\mathfrak{p} = k$. Since $k[t]/(t) \cong k$, this shows that $\mathcal{O}_\Delta$ is not isomorphic to $k[t]$. If $\mathcal{O}_\Delta$ were isomorphic to $l[t]$ for some quadratic field extension l/k, then since $l \otimes_k l \cong l \times l$ is not a domain, $\mathcal{O}_\Delta \otimes_k l = l[x,y]/(y^2 - \Delta(x))$ is not a domain, which implies that Δ is a square in $l[x]$. But $\Delta \in k[x]$ is irreducible of degree at least 2 and k does not have characteristic 2, so this is impossible. □

6.3. **Degree 2 and 3.** For $\Delta \in k[t]$, we put

$$C^\circ(k) = \{(x,y) \in k^2 \mid y^2 = \Delta(x)\}.$$

Theorem 6.2. *Let $\Delta \in k[t]$ be definite and of degree at least 2.*
a) If the Polynomial Rabinowitsch Criterion holds for Δ, then $C^\circ(k) = \varnothing$.
b) If $\deg \Delta \leq 3$, the Polynomial Rabinowitsch Criterion holds for Δ iff $C^\circ(k) = \varnothing$.

Proof. a) By contrapositive: suppose $(x,y) \in C^\circ(k)$. Viewing y as a degree zero element of $k[t]$ we have $y^2 - \Delta(x) = 0$. Thus $y^2 - \Delta(t) \in k[t]$ is a polynomial of degree at least 2 with a root in k, so it is reducible.
b) Since $\deg \Delta \leq 3$, condition (iii′) of Theorem 1.3 is that $y(t)^2 - \Delta(t)$ is irreducible for all $y \in k[t]$ with $\deg y \leq 1$. Suppose not: then, since $\deg \Delta \leq 3$ there is $x \in k$ is such that $y(x)^2 - \Delta(x) = 0$ and $(x, y(x)) \in C^\circ(k)$, a contradiction. □

Example 6.3. *Let $k = \mathbb{R}$. For $g \in \mathbb{N}$, let $\Delta_g = -t^{2g+2} - 1$, a definite polynomial. Sign considerations show*

$$\{(x,y) \in \mathbb{R}^2 \mid y^2 = -x^{2g+2} - 1\} = \varnothing.$$

When $g = 0$ we have $\deg \Delta_g = 2 \leq 3$, so by Theorem 6.2 the Rabinowitsch Criterion holds for $\Delta = -t^2 - 1$. When $g \geq 1$ we have $\deg \Delta_g \geq 4$ so the result does not apply. In fact for $k = \mathbb{R}$ the Rabinowitsch Criterion never holds when $\deg \Delta \geq 3$: taking $x = t^{\deg \Delta - 1}$, we have $\deg x = 2 \deg \Delta - 2 > \deg \Delta > 2$, so $\deg x^2 - \Delta = 2 \deg \Delta - 2 > 2$ and thus $x^2 - \Delta$ is reducible for degree reasons alone.

Example 6.4. *Let $k = \mathbb{F}_3$, $\Delta = t^3 - t - 1$. For all $x \in \mathbb{F}_3$, $x^3 - x - 1 \notin \mathbb{F}_3^{\times 2}$, so*

$$\{(x, y) \in \mathbb{F}_3^2 \mid y^2 = x^3 - x - 1\} = \varnothing.$$

Thus the Rabinowitsch Criterion shows that

$$\mathcal{O}_\Delta = \mathbb{F}_3[x, y]/(y^2 - x^3 + x + 1)$$

is a PID.

Let us now look more concretely at the case $\deg \Delta = 2$.[3] Let $\Delta = at^2 + bt + c$ with $a \in k \setminus k^2$. After the harmless change of variables $t \mapsto \frac{t-b}{2a}$ we may assume $b = 0$. Then Condition (i) of Theorem 1.3 holds iff for all $x \in k$, the polynomial

$$x^2 - \Delta = -at^2 + (x^2 - c)$$

is irreducible. Away from characteristic 2, a quadratic polynomial is irreducible iff its discriminant is not a square, so the criterion holds iff

$$\forall x \in k, a(x^2 - c) \notin k^2.$$

Example 6.5. *Let $(k, \leq)$ be an ordered field, and let $\Delta = at^2 + c$ with $a \in k \setminus k^2$.*
a) If $a, c < 0$ are negative, then the Rabinowitsch Criterion holds for Δ.
b) If every positive element of k is a square (e.g. $k = \mathbb{R}$), then Δ definite forces $a < 0$, and the Rabinowitsch Criterion holds for Δ iff $c < 0$.

Example 6.6. *Let q be an odd prime power, let k be a finite field of order q, and let $\Delta = at^2 + c$ with $a \in k \setminus k^2$. Recall $[k^\times : k^{\times 2}] = 2$. As x ranges over all elements of k, $x^2 - c$ takes on $\frac{q+1}{2}$ values, so for some x, $x^2 - c$ is either 0 or a nonsquare and thus $a(x^2 - c) \in k^2$. Thus the Rabinowitsch Criterion does not hold for Δ.*

Proposition 6.7. *Let $\Delta = at^2 + c$ with $a \in k \setminus k^2$. The Rabinowitsch Criterion holds for Δ iff the quaternion algebra $\left(\frac{a,c}{k}\right)$ is a division algebra.*

We omit the proof: we will not rehearse the theory of quaternion algebras, and a reader who knows this theory will have no difficulty proving this result.

Thus for a field k, the Rabinowitsch Criterion holds for some degree 2 polynomial $\Delta \in k[t]$ iff k admits some division quaternion algebra. In particular this holds if k is $\mathbb{Q}$, $\mathbb{F}_p(t)$, $\mathbb{Q}_p$, $\mathbb{F}_p((t))$ or any finite extension thereof. It does not hold over $\mathbb{F}_q$. This is our first sign that an infinite ground field makes things more interesting.

7. A Geometric Approach

7.1. **Jacobians.** We begin by recalling the following result of M. Rosen.

Theorem 7.1. *(Rosen* [Ro73]*) Let $C^\circ = C \setminus S$ be a regular, 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 I_∞ be the least positive degree of a divisor supported on S (note that $I_\infty = 1$ if and*

[3]The reader who knows the classification of plane conics may move on to the next section.

only if S contains at least one k-rational point), and let I be the ***index*** *of C: the least positive degree of a divisor on C. Then there is an exact sequence*

$$0 \to D^0(S)/P(S) \to \mathrm{Pic}^0(C) \to \mathrm{Pic}(C^o) \to \mathbb{Z}/(I_\infty/I)\mathbb{Z} \to 0. \tag{1}$$

The following result, though a mouthful, follows immediately from Theorem 7.1.

Theorem 7.2. *Let k be a field of characteristic different from 2, let $\Delta \in k[t]$ be definite and squarefree of positive degree, which we write in the form $2g+1$ or $2g+2$ for $g \in \mathbb{N}$. Let $\mathcal{O}_\Delta = k[x,y]/(y^2 - \Delta)$, and let C be the complete, regular curve with affine model*

$$C : y^2 = \Delta(x).$$

Let $\pi : C \to \mathbb{P}^1$ be the degree 2 branched covering induced by $(x,y) \mapsto x$. Let $J(C)$ be the Jacobian of C, an abelian variety of dimension g.
a) Suppose $\deg \Delta = 2g+1$. Then the covering π is ramified over the point $\infty = [1:0] \in \mathbb{P}^1(k)$, so there is a unique k-rational point O such that $\pi(O) = \infty$. Moreover the ring $\mathcal{O}_\Delta$ is naturally identified with the coordinate ring $k[C^\circ]$ of the regular affine curve $C^\circ = C \setminus \{O\}$. We have canonical isomorphisms

$$J(C)(k) = \mathrm{Pic}^0 C \xrightarrow{\sim} \mathrm{Pic}\, k[C^\circ] = \mathrm{Pic}\, \mathcal{O}_\Delta.$$

Thus the Rabinowitsch Criterion holds for Δ iff $J(C)(k) = \{0\}$.
b) Suppose $\deg \Delta = 2g+2$. Then the covering π is unramified over the point $\infty \in \mathbb{P}^1(k)$, and the definiteness condition that the leading coefficient of Δ is not a square in k means precisely that ∞ is inert in $k(C)$: that is, there are two geometric points $O_1 \neq O_2$ for which $\pi(O_1) = \pi(O_2) = \infty$, each with residue field a quadratic extension l/k, and conjugate under the nontrivial element of $\mathrm{Aut}(l/k)$. The ring $\mathcal{O}_\Delta$ is naturally identified with the coordinate ring $k[C^\circ]$ of the regular affine curve $C^\circ = C \setminus \{O_1, O_2\}$. Let $I(C)$ be the ***index*** *of the hyperelliptic curve $C_{/k}$, i.e., the least positive degree of a K-rational divisor on K. Then $I(C) \in \{1,2\}$. If C has a k-rational point then $I(C) = 1$; the converse holds if $g \leq 1$ but not (in general) when $g \geq 2$. We have a short exact sequence*

$$0 \to J(C)(k) \to \mathrm{Pic}\, \mathcal{O}_\Delta \to \mathbb{Z}/I(C)\mathbb{Z} \to 0. \tag{2}$$

c) Thus, when $\deg \Delta = 2g+2$, the following are equivalent:
(i) The Rabinowitsch Criterion holds for Δ.
(ii) We have $I(C) = 2$ and $J(C)(k) = \{0\}$.

Proposition 7.3. *Let $\Delta_1, \Delta_2 \in k[t]$ be definite and satisfying the Rabinowitsch Criterion. Suppose $\mathcal{O}_{\Delta_1}$ and $\mathcal{O}_{\Delta_2}$ are isomorphic k-algebras. Then $\deg \Delta_1 = \deg \Delta_2$.*

Proof. Suppose $\deg \Delta_1 \leq \deg \Delta_2$. We have seen that if $\deg \Delta_1 \in \{0,1\}$ then $\deg \Delta_1 = \deg \Delta_2$, so suppose $\deg \Delta_1 \geq 2$. Since $\mathcal{O}_{\Delta_1}$ is isomorphic to $\mathcal{O}_{\Delta_2}$, the hyperelliptic curves $y^2 = \Delta_1(x)$ and $y^2 = \Delta_2(x)$ have isomorphic affine coordinate rings, so the corresponding complete regular models C_1 and C_2 are isomorphic over k, and in particular have the same genus g. So either $\deg \Delta_1 = \deg \Delta_2$ or $\deg \Delta_1 = 2g+1$ and $\deg \Delta_2 = 2g+2$. But then the complete curve C_1 has a k-rational point and the complete curve C_2 does not: contradiction. □

7.2. **Minkowski Constants For Hyperelliptic Curves.** For a smooth, projective integral curve $C_{/k}$ we denote linear equivalence of divisors by $\sim$. For a smooth,

affine integral curve $C^\circ_{/k}$ we denote linear equivalence of divisors by $\sim_\circ$. In the latter case, divisors correspond to fractional ideals in the affine coordinate ring $k[C^\circ]$ and the classes of $\sim_\circ$ are the ideal classes in the usual number theoretic sense.

Theorem 7.4. *Let k be a field, let $C_{/k}$ be a smooth, projective integral curve of genus g, and let $\pi : C \to \mathbb{P}^1$ be a degree 2 morphism such that there is a unique closed point O lying over $\infty \in \mathbb{P}^1$ ("definite case"). Let C° be the affine curve $C \setminus \{O\}$, and let $\mathcal{O} = k[C^\circ]$ be its affine coordinate ring, a Dedekind domain. Let*

$$M(\mathcal{O}) = \begin{cases} g, & \text{if } \deg O = 1 \\ g, & \text{if } \deg O = 2, \ C \text{ has index 2 and } g \text{ is even} \\ g+1, & \text{if } \deg O = 2, \ C \text{ has index 2 and } g \text{ is odd} \\ g+1, & \text{if } \deg O = 2, \text{ and } C \text{ has index 1.} \end{cases}$$

Let $D \in \operatorname{Div} C^\circ$ be a divisor. Then there is an effective divisor D' such that $D \sim_\circ D'$ and $\deg D' \leq M(\mathcal{O})$. Equivalently, every class in $\operatorname{Pic} \mathcal{O}$ has an integral representative I with $\dim_k \mathcal{O}/I \leq M(\mathcal{O})$.

Proof. Let

$$\eta : \operatorname{Div}^0 C \hookrightarrow \operatorname{Div} C^\circ$$

be the injective group homomorphism $\sum_P n_P[P] \mapsto \sum_{P \neq O} n_P[P]$, and let

$$\overline{\eta} : \operatorname{Pic}^0 C \hookrightarrow \operatorname{Pic} C^\circ$$

be the induced injective homomorphism.

Case 1: Suppose $\deg \Delta = 2g+1$. Then $\deg O = 1$, so we may define

$$\iota_1 : \operatorname{Div} C^\circ \mapsto \operatorname{Div}^0 C, \ \sum_{P \neq O} n_P[P] \mapsto \sum_{P \neq O} n_P[P] - \left(\sum_P n_P \right) [O].$$

The homomorphism ι_1 is the inverse of the isomorphism η, and it induces the inverse isomorphism $\overline{\iota_1} : \operatorname{Pic} C^\circ \to \operatorname{Pic}^0 C$. Let $D \in \operatorname{Div} C^\circ$. Then $\iota_1(D) + g[O]$ has degree g, so by Riemann-Roch, there is an effective D' such that $\iota_1(D) + g[O] \sim D'$. Write $D' = k[O] + D''$ where the support of D'' is disjoint from $[O]$ and $0 \leq k \leq g$, so

$$\deg D'' = g - k \leq g.$$

Then

$$\iota_1(D) \sim D' - g[O] = D'' + (k-g)[O] = \iota_1(D'').$$

Thus $\overline{\iota_1}(D - D'') = 0$, so $D \sim D''$.

Case 2: Suppose $\deg \Delta = 2g+2$, C has index 2 and g is even. Then $\deg O = 2$. Moreover, since C has index 2, if $\sum_{P \neq O} n_P[P] \in \operatorname{Div} C^\circ$ then $\sum_P n_P$ is even, so we may define a homomorphism

$$\iota_2 : \operatorname{Div} C^\circ \mapsto \operatorname{Div}^0 C, \ \sum_{P \neq O} n_P[P] \mapsto \sum_{P \neq O} n_P[P] - \left(\frac{\sum_P n_P}{2} \right) [O].$$

The maps η and ι_2 are mutually inverse, and we have $\overline{\iota_2} : \operatorname{Pic} C^\circ \xrightarrow{\sim} \operatorname{Pic}^0 C$. Let $D \in \operatorname{Pic} C^\circ$. We may argue as in Case 1, using $\iota_2(D) + \frac{g}{2}[O]$ in place of $\iota_1(D) + g[O]$, to get that D is linearly equivalent to an effective divisor of degree at most g.

Case 3: Suppose $\deg \Delta = 2g+2$, C has index 2 and g is odd. We may argue as in Case 2, using $\iota_2(D) + \frac{g+1}{2}[O]$ in place of $\iota_2(D) + \frac{g}{2}[O]$, to get that D is linearly equivalent to an effective divisor of degree at most $g+1$.

Case 4: Suppose $\deg \Delta = 2g+2$ and C has index 1. Then $E = \eta(\mathrm{Div}^0 C)$ is the index 2 subgroup of divisors of even degree.
Step 1: We can define $\iota_2 : E \to \mathrm{Div}^0 C$ as in Case 2 above, and now $\eta : \mathrm{Div}^0 C \to E$ and $\iota_2 : E \to \mathrm{Div}^0 C$ are mutually inverse isomorphisms and $\overline{\iota_2} : \overline{E} \to \mathrm{Pic}^0 C$ is an isomorphism. The argument of Case 2 now shows that every divisor D on C° of even degree is linearly equivalent to an effective divisor of degree at most $g+1$.
Step 2: Since every element of $\mathrm{Pic}\, C^\circ$ is represented by an effective divisor, we may suppose that D is a divisor with $d = \deg D$ odd and greater than $g+1$, and we must show that D is linearly equivalent to an effective divisor on C° of degree at most $g+1$. Let $O^\circ = \pi^*([0])$ be the pullback of $0 \in \mathbb{P}^1$, so $[O] \sim [O^\circ]$. Let D_1 be a divisor on C° of degree 1. Then $\deg(D - D_1)$ is even, so by Step 1 there is an effective divisor D' on C° of even degree $d' \leq g$ such that $D - D_1 \sim_\circ D'$. Put

$$\delta_g = \begin{cases} 1 & g \text{ is odd} \\ 0 & g \text{ is even} \end{cases}.$$

Thus we have

$$D - D_1 \sim D' + \frac{d-1-d'}{2}[O^\circ] \sim_\circ D' + \frac{g-\delta_g-d'}{2}[O^\circ],$$

because the last two divisor classes differ by a multiple of $[O]$. Thus

$$D \sim_\circ D_1 + D' + \frac{g-\delta_g-d'}{2}[O^\circ].$$

The right hand side has degree $g+1-\delta_g \in \{g, g+1\}$. By Riemann-Roch, it is linearly equivalent to an effective divisor D'' of degree $g+1-\delta_g$, which may have $[O]$ in its support, but as above we may replace $[O]$ with $[O']$ without changing the effectivity or the linear equivalence class, finally arriving at an effective divisor of degree $g+1-\delta_g \leq g+1$ on C°. □

Thus in all cases we have

$$M(\mathcal{O}) \leq g+1 = \left\lceil \frac{\deg \Delta}{2} \right\rceil,$$

establishing Theorem 5.2.

Remark 7.5. *When k is finite of odd order, Theorem 7.4 is due to W. Hu* [Hu99]. *Because every curve over a finite field has index 1, our Cases 2 and 3 do not arise. His approach is very much in the spirit of the classical geometry of numbers: in fact he works with any curve C endowed with a map $\pi : C \to \mathbb{P}^1$ such that the closed points lying over ∞ have degrees 1 or 2 and uses a Minkowski-style embedding of $k[C^\circ]$ as a lattice in the locally compact group $\mathbb{F}_q((\frac{1}{t}))^r \times \mathbb{F}_{q^2}((\frac{1}{t}))^s$.*

Example 7.6. *Suppose $\deg \Delta = 2$. Above we saw that the Rabinowitsch Criterion holds iff $C^\circ(k) = \varnothing$. In geometric terms, C is a genus zero curve, so $J(C) = (0)$. By Theorem 7.2, the Rabinowitsch Criterion holds iff C has index 2. By Riemann-Roch, a genus zero curve of index 1 has a rational point, so C has index 2 iff $C(k) = \varnothing$ iff $C^\circ(k) = \varnothing$. When $C(k) = \varnothing$ we have equality in Case 2 of Theorem 7.4 and when $C(k) \neq \varnothing$ we have equality in Case 4 of Theorem 7.4.*

Example 7.7. *Suppose $\deg \Delta = 3$. Above we saw that the Rabinowitsch Criterion holds iff $C^\circ(k) = \varnothing$. In geometric terms C is a genus one curve with a k-rational point O so C is its own Jacobian and $C(k) = \mathrm{Pic}^0 C \cong \mathrm{Pic}\, C^\circ$. By Riemann-Roch,*

a genus one curve of index 1 *has a rational point, so* C *has index* 2 *iff* $C^\circ(k) = \varnothing$. *When* $C^\circ(k) \neq \varnothing$ *we have equality in Case 1 of Theorem 7.4.*

Example 7.8. *Suppose* $\deg \Delta = 4$. *Above we saw that* $C^\circ(k) = \varnothing$ *is necessary but not sufficient for the Rabinowitsch Criterion to hold. In geometric terms,* C *is a genus one curve without a* k*-rational point, so its Jacobian* $J(C)$ *is an elliptic curve, which may still have nonzero Mordell-Weil group: indeed, when* $k = \mathbb{R}$, *the group of rational points on an elliptic curve is isomorphic to either* S^1 *or* $S^1 \times \mathbb{Z}/2\mathbb{Z}$ *and we have equality in Case 3 of Theorem 7.4.*

8. Satisfying the Rabinowitch Criterion II: Using Geometry

8.1. Some Cases of Failure of the Polynomial Rabinowitsch Criterion.

Theorem 8.1. *Let* q *be an odd prime power, and let* $\Delta \in \mathbb{F}_q[t]$ *be definite of degree at least* 2. *If the Rabinowitsch Criterion holds for* Δ, *then* $(q, \deg \Delta) = (3, 3)$.

Proof. Step 1: Suppose $\deg \Delta = 2$, so $g = 0$. The Weil bounds give $\#C^\circ(\mathbb{F}_q) = \#C(\mathbb{F}_q) = q + 1$, so C has index 1 and the Rabinowitsch fails.
Step 2: Now assume $g \geq 1$. The Weil bounds give $\#\operatorname{Pic}^0 C = \#J(C)(\mathbb{F}_q) \geq (\sqrt{q} - 1)^{2g}$, so if $q \neq 3$ then[4] $\operatorname{Pic}^0 C$ is nonzero and the Rabinowitsch Criterion fails.
Step 3: Suppose $q = 3$. If $\deg \Delta = 4$ then C has genus one. The Weil bounds give

$$\#C(\mathbb{F}_q) \geq (\sqrt{3} - 1)^2 > 0,$$

so $\#C^\circ(\mathbb{F}_q) = C(\mathbb{F}_q) \neq \varnothing$ and the Rabinowitsch Criterion fails. If $\deg \Delta \geq 5$ then $g \geq 2$ and if the Rabinowitsch Criterion holds there would be a curve $C_{/\mathbb{F}_3}$ of genus $g \geq 2$ with $J(C)(\mathbb{F}_q) = (0)$. This was ruled out in [LMQ75]. □

The case of $\deg \Delta = 3$ over $\mathbb{F}_3$ *cannot* be eliminated: as we saw in Example 6.4, the Rabinowitsch Criterion holds for $\Delta = t^3 - t - 1$ over $\mathbb{F}_3$. A straightforward calculation shows that $y^2 = x^3 - x - 1$ is up to isomorphism the only elliptic curve over $\mathbb{F}_3$ with trivial Mordell-Weil group. This implies that if $\Delta_1, \Delta_2 \in \mathbb{F}_3[t]$ are degree 3 polynomials for which the Rabinowitsch Criterion holds, then $\mathcal{O}_{\Delta_1} \cong \mathcal{O}_{\Delta_2}$.

A field k is **ample** if for every smooth, geometrically integral variety $V_{/k}$ with $V(k) \neq \varnothing$, we have that $V(k)$ Zariski-dense in $V(\overline{k})$. Ample fields include:
(i) $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}_p$, $\mathbb{F}_p((t))$.
(ii) Algebraically closed fields and real-closed fields.
(iii) Pseudo-algebraically closed (PAC) fields and pseudo-real closed (PRC) fields.
(iv) Fields which are complete (or Henselian) for a nontrivial valuation.
(v) Algebraic extensions of ample fields.

The following fields are *not* ample:
(i) Finite fields.
(ii) Fields which are finitely generated over their prime subfield.
(iii) Fields K which admit a subfield k such that K/k is finitely generated and of positive transcendence degree.

Theorem 8.2. *Let* k *be an ample field, and let* $\Delta \in k[t]$ *be definite, squarefree and of degree at least* 3. *Then the Rabinowitsch Criterion does not hold for* Δ.

[4]Because we have assumed q is odd, $q = 2$ and $q = 4$ are excluded.

Proof. Since $\deg \Delta \geq 3$, we have $g \geq 1$ and thus the Jacobian of the curve

$$C : y^2 = \Delta(x)$$

is a nontrivial abelian variety, so $J(C)(k)$ is infinite. In fact, Moret-Bailly has shown [MB-MO] that for a nontrivial abelian variety A defined over an ample field k, the Mordell-Weil group $A(k)$ is not finitely generated. By Theorem 7.2, the ring $\mathcal{O}_\Delta$ is not a PID: in fact, its class group is not finitely generated. □

8.2. **More Satisfaction of the Polynomial Rabinowitsch Criterion.**

Theorem 8.3. *Let k be a number field.*
a) The conditions of Theorem 1.3 hold for some degree three $\Delta \in k[t]$.
b) The conditions of Theorem 1.3 hold for some degree four, definite $\Delta \in k[t]$.

Proof. a) By a result of Mazur and Rubin [MR10, Cor. 1.11], there is an elliptic curve $E_{/k}$ with $E(k) = (0)$, given by a Weierstrass equation $y^2 = \Delta(x)$. By Theorem 6.2, the domain $\mathcal{O}_\Delta$ is a PID.
b) Again, there is an elliptic curve $E_{/k}$ with $E(k) = (0)$. By a result of Sharif [Sh12] there is a genus one curve C of index 2 with Jacobian elliptic curve E. By Riemann-Roch, C has an effective divisor of degree 2 which yields a degree 2 map $\pi : C \to \mathbb{P}^1$. By Riemann-Hurwitz, C is given by an equation $y^2 = \Delta(x)$ with $\Delta \in k[t]$ squarefree of degree 4, and Δ is definite because $C(k) = \varnothing$. □

8.3. **Two Conjectures.**

Conjecture 8.4. *Let k be a field which is infinite and finitely generated over its prime subfield. Then for each $d \geq 2$, there is an infinite sequence $\{\Delta_n\}_{n=1}^\infty$ such that each $\Delta_n \in k[t]$ is definite, of degree d, satisfies the Rabinowitsch Criterion, and such that the k-algebras $\{\mathcal{O}_{\Delta_n}\}_{n=1}^\infty$ are pairwise nonisomorphic.*

Conjecture 8.5. *Let κ be a field of characteristic different from 2, and let $k = \kappa(a_0, \ldots, a_{2g+2})$ be a rational function field in $2g+3$ independent indeterminates.*
a) The polynomial

$$\Delta_{2g+1} = t^{2g+1} + a_{2g}t^{2g} + \ldots + a_1 t + a_0 \in k[t]$$

satisfies the Rabinowitsch Criterion.
b) The polynomial

$$\Delta_{2g+2} = a_{2g+2}t^{2g+2} + a_{2g+1}t^{2g+1} + \ldots + a_1 t + a_0 \in k[t]$$

satisfies the Rabinowitsch Criterion.

9. Final Remarks

9.1. **(No) History.** We do not purport to give a survey, historical or otherwise, of Theorem 1.1. But I feel compelled to mention that this result, published by Rabinowitsch in 1913, already appears in a 1912 paper of Frobenius [Fr12]. Perhaps I should have spoken throughout of the **Frobenius-Rabinowitsch Criterion**; I admit to being partially motivated by considerations of equidistribution.

Parts of Theorem 1.1 have also appeared in papers of Mitchell [Mi26], Lehmer [Le36], Szekeres [Sz74] and Ayoub-Chowla [AC81].

9.2. **Variants and Refinements of the Rabinowitch Criteria.** Theorem 1.1 is the first of many results relating prime values of quadratic polynomials over $\mathbb{Z}$ to the arithmetic of quadratic fields. The literature contains many variants and refinements, and it seems to me that most (or all) of these ought to have analogues over $k[t]$. Such a systematic pursuit would be a length undertaking, and we do not attempt it here. Rather we single out two such classes of results.

First, there is an analogue of Theorem 1.1 for real quadratic fields due to Mollin and Williams [MW88]. Analogues of the Mollin-Williams Criterion over real quadratic function fields over an odd order finite field $\mathbb{F}_q$ have been given by Feng-Hu [FH99] and Bae [Ba12]. The real quadratic case involves continued fractions and their function field analogues (which appear in the thesis of Emil Artin). Can the results of Feng-Hu and Bae be extended to an arbitrary ground field k?

Now we consider a refinement of Theorem 1.1, following T. Ono.

For a PID R, we define a function $\Omega_R : R^\bullet \to \mathbb{N}$, as follows: if $x = p_1 \cdots p_r$ is a product of prime elements $p_1, \ldots, p_r$, we put $\Omega_R(x) = r$.

Let $C \in \mathbb{Z}^{\geq 2}$ and $\Delta = 1 - 4C$. We define the **Ono number**

$$\mathrm{Ono}_\Delta = \max_{x \in [0, C-2]} \Omega_{\mathbb{Z}}(x^2 + x + C) \in \mathbb{Z}^+.$$

Observe that condition (i) in the Rabinowitsch Criterion is: $\mathrm{Ono}_\Delta \leq 1$. Thus one can seek refinements of Theorem 1.1 which relate the Ono number to the structure of the class group $\mathrm{Pic}\, \mathcal{O}_\Delta$.

Meanwhile, let k be a field of characteristic not 2, and let $\Delta \in k[t]$ be definite of positive degree. We define the **polynomial Ono number**

$$\mathrm{Ono}_\Delta = \sup_{\deg x < \deg \Delta} \Omega_{k[t]}(x^2 - \Delta) \in \mathbb{Z}^+.$$

If $\deg \Delta = 0$ then $\mathrm{Ono}_\Delta = 0$. Observe that condition (i) in Theorem 1.3 is: $\mathrm{Ono}_\Delta = 1$. When $\deg \Delta = 1$ the conditions of Theorem 1.3 always hold and $\mathrm{Ono}_\Delta = 1$. From now on we assume $\deg \Delta \geq 2$, in which case we have

$$1 \leq \mathrm{Ono}_\Delta \leq 2 \deg \Delta - 2.$$

For a commutative group $(G, +)$ the **Davenport constant** $D(G)$ is the least $n \in \mathbb{Z}^+$ such that for any $x_1, \ldots, x_n \in G$ there is a nonempty subset $J \subset \{1, \ldots, n\}$ such that $\sum_{i \in J} x_i = 0$, or ∞ if there is no such n. If G is finite, then $D(G) \leq \#G$ with equality if G is cyclic, while $D(G) = \infty$ for all infinite G [CA, Prop. 23.14].

Theorem 9.1.
a) (Möller [Mö76]*) Let $C \in \mathbb{Z}^+$ be such that $\Delta = 1 - 4C$ is squarefree. Then*

$$\mathrm{Ono}_\Delta \leq D(\mathrm{Pic}\, \mathcal{O}_\Delta).$$

b) Let $\Delta \in k[t]$ be definite and squarefree. Then

$$\mathrm{Ono}_\Delta \leq D(\mathrm{Pic}\, \mathcal{O}_\Delta).$$

Proof. a) Let $\tau = \frac{1+\sqrt{\Delta}}{2}$. For $x \in [0, C-2]$, we have

$$|x + \tau| = x^2 + x + C < C^2.$$

Then $x+\tau$ is irreducible in $\mathcal{O}_\Delta$: indeed, if not, there is $\alpha \in \mathcal{O}_\tau$ with $\alpha \mid x+\tau$ and $|\alpha| \in (1, C)$; evidently $\alpha \notin \mathbb{Z}$, so Lemma 2.2 gives $|\alpha| \geq C$, contradiction. Let $\langle x+\tau \rangle = \mathfrak{p}_1 \cdots \mathfrak{p}_d$ be the factorization of $\langle x+\tau \rangle$ into prime ideals. We have $d \leq D(\operatorname{Pic} \mathcal{O}_\Delta)$ [CA, Prop. 23.13]. On the other hand,

$$|x+\tau|\mathcal{O}_\Delta = (x+\tau)\overline{(x+\tau)}\mathcal{O}_\Delta = \mathfrak{p}_1\overline{\mathfrak{p}_1} \cdots \mathfrak{p}_d\overline{\mathfrak{p}_d}.$$

Let $(p_i) = \mathfrak{p}_i \cap \mathbb{Z}$. If p_i were inert in $\mathcal{O}_\Delta$ then $\mathfrak{p}_i = \langle p_i \rangle$, contradicting the fact that $x+\tau$ is not divisible by any nonunit elements of $\mathbb{Z}$. So we have $\mathfrak{p}_i\overline{\mathfrak{p}_i} = p_i\mathcal{O}_\Delta$ for all $1 \leq i \leq d$. It follows that there is $u \in \mathbb{Z}^\times$ with

$$x^2 + x + C = |x+\tau| = up_1 \cdots p_d$$

and thus

$$\Omega_{\mathbb{Z}}(x^2+x+C) = d \leq D(\operatorname{Pic} \mathcal{O}_\Delta).$$

b) The above proof carries over with Proposition 2.10 in place of Lemma 2.2. □

Corollary 9.2. *Let $\Delta \in k[t]$ be definite and squarefree, of degree $2d \geq 2$. Suppose the regular projective model $C_{/k}$ of the hyperelliptic curve $y^2 = \Delta(x)$ has index 2 and $J(C)(k) = 0$. Then $\operatorname{Ono}_\Delta = 2$.*

Proof. By Theorem 7.2 we have $\operatorname{Pic} \mathcal{O}_\Delta \cong \mathbb{Z}/2\mathbb{Z}$. Thus $\mathcal{O}_\Delta$ is not a PID, so the Rabinowitsch Criterion fails and $\operatorname{Ono}_\Delta > 1$. On the other hand, $D(\operatorname{Pic} \mathcal{O}_\Delta) = D(\mathbb{Z}/2\mathbb{Z}) = 2$, so by Theorem 9.1 we have $\operatorname{Ono}_\Delta \leq 2$. □

Theorem 9.3.
a) (Sasaki [Sa86]*) Let $C \in \mathbb{Z}^+$ be such that $\Delta = 1 - 4C$ is squarefree. Then*

$$\operatorname{Ono}_\Delta = 2 \iff \#\operatorname{Pic} \mathcal{O}_\Delta = 2.$$

b) Let $\Delta \in k[t]$ be definite and squarefree. Then

$$\operatorname{Ono}_\Delta = 2 \iff \#\operatorname{Pic} \mathcal{O}_\Delta = 2.$$

Proof. a) By Theorems 1.1 and 9.1a), $\#\operatorname{Pic} \mathcal{O}_\Delta = 2$ implies $\operatorname{Ono}_\Delta = 2$, so suppose $\operatorname{Ono}_\Delta = 2$. This implies $\Delta \leq -15$. By Theorem 1.1, $\mathcal{O}_\Delta$ is not a PID so there are nonprincipal prime ideals. By Theorem 5.1, $\operatorname{Pic} \mathcal{O}_\Delta$ is generated by prime ideals $\mathfrak{p}$ with norm at most $\sqrt{\frac{|\Delta|}{3}}$ and which are nonprincipal, and thus if $\mathfrak{p}$ lies over $p \in \mathbb{Z}$ then (p) is not inert in $\mathcal{O}_\Delta$. It is enough to show that for any two such nonprincipal $\mathfrak{p}$ and $\mathfrak{q}$ lying over primes (p) and (q) of $\mathbb{Z}$, we have that $\mathfrak{pq}$ is principal.

Suppose first that $\mathfrak{p} \cap \mathbb{Z} = \mathfrak{q} \cap \mathbb{Z} = (p)$. If (p) ramifies in K then $\mathfrak{p} = \mathfrak{q}$ is the unique prime of norm (p) and $\mathfrak{pq} = p^2\mathcal{O}_\Delta$ is principal. If $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ with $\mathfrak{p}_1 \neq \mathfrak{p}_2$ and $\mathfrak{p} \neq \mathfrak{q}$, then $\{\mathfrak{p}, \mathfrak{q}\} = \{\mathfrak{p}_1, \mathfrak{p}_2\}$ so $\mathfrak{pq} = \mathfrak{p}_1\mathfrak{p}_2 = p^2\mathcal{O}_\Delta$ is principal. Finally suppose $\mathfrak{p} = \mathfrak{q}$. Since $\mathfrak{p}$ splits in $\mathcal{O}_\Delta$ the polynomial x^2+x+C has distinct roots modulo (p), hence by Hensel's Lemma it has a root modulo (p^2). So there is x with $|x| < |p| \leq \sqrt{\frac{|\Delta|}{3}} \leq C-2$ such that $p^2 \mid x^2+x+C$. The inequalities imply $|x| \leq C-2$, so our assumption $\operatorname{Ono}_\Delta = 2$ gives

$$p^2 = x^2 + x + C = |x+\tau|.$$

Since $p \nmid x+\tau$, the ideal $(x+\tau)\mathcal{O}_\Delta$ has norm (p^2) and is not $p\mathcal{O}_\Delta$, so we must have

$$(x+\tau)\mathcal{O}_\Delta = \mathfrak{p}_1\mathfrak{p}_2.$$

Now suppose $\mathfrak{p} \cap \mathbb{Z} = (p)$ and $\mathfrak{q} \cap \mathbb{Z} = (q)$ with $p \neq q$. The polynomial $x^2 + x + C$ has roots modulo (p) and modulo (q) hence (by the Chinese Remainder Theorem) also modulo (pq); using $\mathrm{Ono}_\Delta = 2$ as above we get x with $|x| \leq C - 2$ such that

$$pq = x^2 + x + C = |x + \tau|.$$

The only ideals of $\mathcal{O}_\Delta$ of norm (pq) are $\mathfrak{pq}$, $\overline{\mathfrak{p}}\mathfrak{q}$, $\mathfrak{p}\overline{\mathfrak{q}}$ and $\overline{\mathfrak{p}}\overline{\mathfrak{q}}$. Since $\mathfrak{p}\overline{\mathfrak{p}} = p\mathcal{O}_\Delta$ and $\mathfrak{q}\overline{\mathfrak{q}} = q\mathcal{O}_\Delta$, this shows that $\mathfrak{pq}$ is principal.
b) The above proof carries over with Theorem 1.3 in place of Theorem 1.1, Theorem 9.1b) in place of Theorem 9.1a) and Theorem 5.2 in place of Theorem 5.1. □

Example 9.4. *Suppose $R = \mathbb{Z}$ or $k[t]$ and Δ is a definite discriminant such that $\mathrm{Pic}\,\mathcal{O}_\Delta \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. (When $R = k[t]$, this occurs if $\deg \Delta$ is odd and $(JC_\Delta)(k) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. If $\deg \Delta$ is even and $(JC_\Delta)(k) = \mathbb{Z}/2\mathbb{Z}$, it occurs iff the sequence (2) splits.) Then $D(\mathrm{Pic}\,\mathcal{O}_\Delta) = 3 = \mathrm{Ono}_\Delta$.*

When $R = \mathbb{Z}$, Guo and Qin show, conditionally on the Extended Riemann Hypothesis, that if $\mathrm{Ono}_\Delta = 3$ then $\mathrm{Pic}\,\mathcal{O}_\Delta \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ iff precisely three prime ideals of $\mathbb{Z}$ ramify in $\mathcal{O}_\Delta$ [GQ10]*. It may be interesting to investigate the $k[t]$ case.*

9.3. **Euclidean Rings and Dedekind-Hasse Norms.** Let R be a domain. A **Euclidean function** $\varphi : R^\bullet \to \mathbb{N}$ is a function such that for all $a \in R$ and $b \in R^\bullet$, there are $q, r \in R$ such that $a = qb + r$ and either $r = 0$ or $\varphi(r) < \varphi(b)$. (This is the same as the definition of a *Euclidean norm* given in §2.2 except that multiplicativity is not required.) A domain is **Euclidean** if it admits a Euclidean function.

An interesting aspect of the approach to Theorem 1.1 via Dedekind-Hasse norms is that the quadratic order $\mathcal{O}_\Delta$ can be a PID even when (i) the complex norm is not Euclidean and (ii) there is no Euclidean function on $\mathcal{O}_\Delta$, multiplicative or otherwise. In the $R = \mathbb{Z}$ case, the PID $\mathcal{O}_\Delta$ is Euclidean for the complex norm when $\Delta \in \{-3, -7, -11\}$ and admits no Euclidean function when $\Delta \in \{-19, -43, -67, -163\}$.

A similar phenomenon holds in the polynomial ring case. The following result is due to M.L. Brown and makes crucial use of work of Leitzel-Madan-Queen [LMQ75] that we encountered in §8.1 above.

Theorem 9.5. *(Brown* [Br91]*) Let $C^\circ = C \setminus S$ be a regular, geometrically integral affine curve over a field k, and let $k[C^\circ]$ be its affine coordinate ring. Then $k[C^\circ]$ is Euclidean iff it is a PID satisfying one of the following conditions:*
(i) k is infinite and C is isomorphic over k to the projective line $\mathbb{P}^1$.
(ii) k is finite and $k[C^\circ]$ is not *isomorphic to one of the following PIDs:*
a) $\mathbb{F}_2[x,y]/(y^2 + y + x^3 + x + 1)$.
b) $\mathbb{F}_3[x,y]/(y^2 - x^3 + x + 1)$.
c) $\mathbb{F}_4[x,y]/(y^2 + y + x^3 + \eta)$, where η generates the multiplicative group $\mathbb{F}_4^\times$.
d) $\mathbb{F}_2[x,y]/(y^2 + y + x^5 + x^3 + 1)$.

Corollary 9.6. *Let k be a field of characteristic not 2, and let $\Delta \in k[t]$ be definite of degree at least 2. Suppose that the Rabinowitsch Criterion holds for Δ. Then the ring $\mathcal{O}_\Delta = k[x,y]/(y^2 - \Delta)$ is a non-Euclidean PID.*

Proof. Let C be the associated complete, smooth hyperelliptic curve.

Suppose k is infinite. If $\deg \Delta$ is even, then by Theorem 7.2, the curve C has index 2 and thus is not isomorphic to $\mathbb{P}^1$, so $\mathcal{O}_\Delta = k[C^\circ]$ is not Euclidean by Theorem 9.5. If $\deg \Delta$ is odd, then C has genus at least one, so again is not isomorphic to $\mathbb{P}^1$ and $\mathcal{O}_\Delta$ is not Euclidean.

Suppose k is finite. Then $I(C) = 1$, so $\deg \Delta$ is odd by Theorem 7.2. Since $\mathcal{O}_\Delta$ is a PID, by Theorem 7.2 we have $J(C)(k) = 0$. Then [LMQ75, Thm. 2] gives $\mathcal{O}_\Delta \cong \mathbb{F}_3[x,y]/(y^2 - x^3 + x + 1)$, so $\mathcal{O}_\Delta$ is not Euclidean by Theorem 9.5. □

In particular the results of §8.2 give examples of non-Euclidean PIDs, and many more examples of non-Euclidean PIDs are implied by Conjectures 8.4 and 8.5.

The statement that a domain is a PID iff it admits a Dedekind-Hasse norm appears in the literature (e.g. [Gr97]), but the refined statement that in a PID *every* multiplicative norm is a Dedekind-Hasse norm apparently does not. (To be sure, no new ideas are required for the proof.) This seems to be an advantage of Dedekind-Hasse norms over Euclidean norms: they need not be cleverly chosen.

Though Dedekind-Hasse norms show up in the literature, they have rarely been put to substantial use. Fendel's proof of Theorem 1.1 is a major exception; another is an unpublished preprint of Lemmermeyer [Le12], which bears some relation both to Fendel and to the considerations of the present work.

Several recent papers implicitly or explicitly claim that the best way to show that, say, $\mathbb{Z}[\frac{1+\sqrt{-163}}{2}]$ is a PID is to construct a Dedekind-Hasse norm. In fact Gauss knew a better way at the end of the 18th century (binary quadratic forms) and Minkowski knew a better way at the end of the 19th century (bounds on ideal classes). This provided impetus for the latter approaches to Theorems 1.1 and 1.3.

That the "base PIDs" $\mathbb{Z}$ and $k[t]$ are Euclidean plays a key role in all the proofs of Theorems 1.1 and 1.3. It should be possible to develop analogous results over certain other norm-Euclidean domains, e.g. over $R = \mathbb{Z}[\sqrt{2}]$.

9.4. **Characteristic 2.** There is no fundamental need to exclude the case in which k has characteristic 2. In Theorem 7.4 it is permitted for k to have characteristic 2, and thus the argument in §5 gives a version of (iii′) $\implies$ (i) in Theorem 1.3 that is valid without such a restriction. However, the rest of our treatment is built around discriminants of quadratic field extension and quadratic forms, and in characteristic 2 one should replace these with analogous invariants of Artin-Schreier and Dickson.

9.5. **Work of Bevelacqua.** Just before this paper was submitted for publication, A.J. Bevelacqua published a note containing the following result.

Theorem 9.7. *(Bevelacqua* [Be16]*) Let k be a field, and let $\Delta \in k[x]$ be definite of degree 2 or 3. Let $\delta \in k$, and let*

$$P(x,y) = y^2 - \delta y - \Delta(x) \in k[x,y].$$

Let R be the domain $k[x,y]/(P)$. Then:
a) The domain R is not *Euclidean.*
b) The domain R is a PID iff there is no $(x,y) \in k^2$ such that $P(x,y) = 0$.

Theorem 9.7b) recovers Theorem 6.2b) and extends it to characteristic 2. Theorem 9.7a) is a consequence of the work of Leitzel-Madan-Queen [LMQ75] and Brown [Br91] – indeed, when the characteristic of k is not 2 it is a special case of Corollary 9.6, and here at least it is straightforward to extend the argument to characteristic 2. However, whereas the proof of Theorem 9.5 uses some sophisticated arithmetic geometry, the proof of Theorem 9.7 is entirely elementary.

References

[AC81] R.G. Ayoub and S. Chowla, *On Euler's polynomial*. J. Number Theory 13 (1981), 443-445.

[Ba12] S. Bae, *Real quadratic function fields of Richaud-Degert type with ideal class number one*. Proc. Amer. Math. Soc. 140 (2012), 403-414.

[Be16] A.J. Bevelacqua, *A Family of Non-Euclidean PIDs*. Amer. Math. Monthly 123 (2016), 936-939.

[Br91] M.L. Brown, *Euclidean rings of affine curves*. Math. Z. 208 (1991), 467-488.

[CA] P.L. Clark, *Commutative Algebra*. `math.uga.edu/~pete/integral2015.pdf`.

[CJ14] P.L. Clark and W.C. Jagy, *Euclidean quadratic forms and ADC-Forms II: integral forms*. Acta Arithmetica 164 (2014), 265–308.

[Cl94] D.A. Clark, *A quadratic field which is Euclidean but not norm-Euclidean*. Manuscripta Math. 83 (1994), 327-330.

[Cl09] P.L. Clark, *Elliptic Dedekind domains revisited*. Enseign. Math. (2) 55 (2009), 213-225.

[Cl16] P.L. Clark, *Abstract geometry of numbers: linear forms*. `http://alpha.math.uga.edu/~pete/GoN_Linear_Forms.pdf`

[Fe85] D. Fendel, *Prime-producing polynomials and principal ideal domains*. Math. Mag. 58 (1985), no. 4, 204-210.

[FH99] K. Feng and W. Hu, *On real quadratic function fields of Chowla type with ideal class number one*. Proc. Amer. Math. Soc. 127 (1999), 130101307.

[Fr12] F.G. Frobenius, *Über quadratische Formen, die Primzahlen darstellen, Sitzungesber. d. Königl. Akad. d. Wiss. zu Berlin* (1912), 966–980.

[Go92] C.D. González, *Class numbers of quadratic function fields and continued fractions*. J. Number Theory 40 (1992), 38-59.

[GQ10] X. Guo and H. Qin, *Imaginary quadratic fields with Ono number 3*. Comm. Algebra 38 (2010), 230-232.

[Gr] A. Granville, *Binary quadratic forms*. `http://www.dms.umontreal.ca/~andrew/Courses/Chapter4.pdf`

[Gr97] J. Greene, *Principal ideal domains are almost Euclidean*. Amer. Math. Monthly 104 (1997), 154-156.

[Hu98] W. Hu, *On imaginary quadratic function fields with the ideal class group to be exponent* ≤ 2. Chinese Sci. Bull. 43 (1998), 2055-2059.

[Hu99] W. Hu, *On Minkowski constant of function fields*. Northeast. Math. J. 15 (1999), 69-75.

[Ka68] I. Kaplansky, *Composition of binary quadratic forms*. Studia Math. 31 (1968), 523-530.

[Kn82] M. Kneser, *Composition of binary quadratic forms*. J. Number Theory 15 (1982), 406-413.

[Le36] D.H. Lehmer, *On the function* $x^2 + x + A$, Sphinx 6 (1936), 212–214.

[Le12] F. Lemmermeyer, *An application of the Dedekind-Hasse criterion*. `http://arxiv.org/pdf/1205.1147.pdf`

[LMQ75] J.R.C. Leitzel, M.L. Madan and C.S. Queen, *Algebraic function fields with small class number*. J. Number Theory 7 (1975), 11-27.

[Ma] J. Martinet, *On the Minkowski constants for class groups*. `http://jamartin.perso.math.cnrs.fr/Othertexts/classmink.pdf`

[Mi26] H.H. Mitchell, *On classes of ideals in a quadratic field*. Ann. of Math. (2) 27 (1926), 297-314.

[MB-MO] L. Moret-Bailly, `http://mathoverflow.net/questions/108543/over-which-fields-does-the-mordell-weil-theorem-hold`.

[Mo49] T. Motzkin, *The Euclidean Algorithm*. Bull. Amer. Math. Soc. 55 (1949), 1142–1146.

[Mö76] H. Möller, *Verallgeminerung eines Satzes von Rabinowitsch ber imaginär-quadratische Zahlkörper*. J. Reine Angew. Math. 285 (1976), 100-113.

[MR10] B. Mazur and K. Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem*. Invent. Math. 181 (2010), 541-575.

[MW88] R.A. Mollin and H.C. Williams, *On prime valued polynomials and class numbers of real quadratic fields*. Nagoya Math. J. 112 (1988), 143-151.

[O'D15] E. O'Dorney, *Rings of small rank over a Dedekind domain and their ideals*. `http://arxiv.org/abs/1508.02777`.

[Ra13] G. Rabinowitsch, *Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörpern*. J. Reine Angew. Math. 142 (1913), 153-164.

[Ri88] P. Ribenboim, *Euler's famous prime-generating polynomial and the class number of imaginary quadratic fields*. Enseign. Math. (2) 34 (1988), 23-42.

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

[Sa86] R. Sasaki, *On a lower bound for the class number of an imaginary quadratic field*. Proc. Japan Acad. Ser. A Math. Sci. 62 (1986), no. 1, 37-39.

[Sh12] S. Sharif, *Period and index of genus one curves over global fields*. Math. Ann. 354 (2012), 1029-1047.

[Sz74] G. Szekeres, *On the number of divisors of* $x^2 + x + A$. Collection of articles dedicated to K. Mahler on the occasion of his seventieth birthday. J. Number Theory 6 (1974), 434-442.

[Wo11] M.M. Wood, *Gauss composition over an arbitrary base*. Adv. Math. 226 (2011), 1756-1771.