THE THEORY OF THE ENTIRE ALGEBRAIC FUNCTIONS

TAYLOR DUPUY AND EHUD HRUSHOVSKI

Abstract. Let A be the integral closure of the polynomials withing the ring of algebraic functions in one variable. We show that A interprets the ring of integers.

1. Introduction

For an integral domain A, let A^{int} denote the integral closure of A within the algebraic closure of the field of fractions of A. Thus $\mathbb{Z}^{int}$ is the ring of algebraic integers. Our motivation is the theorem of [3], that the theory of $\mathbb{Z}^{int}$ is decidable (see also [4], [2].) There is a well-established analogy, going back to Leibniz and Euler, between integers and polynomials; rational numbers and rational functions; algebraic numbers and algebraic functions. The analogue of $\mathbb{Z}^{int}$ would appear to be $\mathbb{C}[t]^{int}$, the ring of algebraic functions that are entire, i.e. holomorphic as functions on the associated Riemann surface. It is thus natural to ask as to the decidability of this ring. The answer turns out to go the other way:

Theorem 1.1. *Let* k *be a field of positive Kroneker dimension. Let* $\mathrm{k}[t]^{int}$ *be the integral closure of* $\mathrm{k}[t]$ *in* $\mathrm{k}(t)^{alg}$. *Then* $Th(\mathrm{k}[t]^{int}, +, \cdot, t)$ *interprets* $Th(\mathbb{N}, +, \cdot)$. *In particular,* $(\mathrm{k}[t]^{int}, +, \cdot)$ *is undecidable.*

Recall that the *Kronecker dimension* $Kr.dim.(k)$ of a field k is defined to be 0 for a finite field k, 1 for $k = \mathbb{Q}$, and in general $Kr.dim.(k) := Kr.dim(F) + tr.deg._F(k)$, where F is the prime field of k. Thus the only fields k left out are those algebraic over a finite field. In fact for such fields, it was proved in [4] that $\mathrm{k}[t]^{int}$ is is decidable.

In the finite field case, the first and fundamental principle is is that of glueing. Given finitely many primes $p_1, \ldots, p_k$ of $\mathrm{k}(t)$, and elements $a_1, \ldots, a_k$ of $\mathrm{k}[t]$, in some finite extension L it is possible to find an integer that is close to a_i at primes above p_i, and a unit at any other prime. This is no longer possible when k is a non-algebraic field; the obstruction to glueing on $\mathrm{k}(C)$ in this sense is measured by the Jacobian of C up to torsion, and related $\mathbb{Q}$-vector spaces. An interesting structure becomes interpretable, consisting of the direct limit of all Jacobians, along with a filtration according to supports. However, the field of coefficients $\mathbb{Q}$ turns out to be interpretable within it. It remains a very interesting open problem to find a decidable setting capturing the essential geometry here.

Throughout this paper, k is a field of positive Kronecker dimension. Note that in Theorem 1.1 we may assume k is algebraically closed, since changing k to k^{alg} does not change the ring $\mathrm{k}[t]^{int}$.

2. Definable systems of class groups

Let k be an algebraically closed field. Fix an algebraic closure $\mathrm{k}(t)^{alg}$ of the field of rational functions $\mathrm{k}(t)$. Let $\mathrm{k}[t]^{int}$ be the integral closure of $\mathrm{k}[t]$ in $\mathrm{k}(t)^{alg}$. Let $\mathcal{I}$ be the set finite extension fields of $\mathrm{k}(t)$, contained in $\mathrm{k}(t)^{alg}$. This is a directed partially ordered set, under inclusion. Each $i \in \mathcal{I}$ is the function field of a smooth projective curve C_i, over k (we will also denote this field by k_i.) Given $i \leq j \in \mathcal{I}$ there is a unique morphism $p_{ji} : C_j \to C_i$ of curves, corresponding to the given inclusion of function fields; the p_{ji} form a directed system. The smallest element, with function field $\mathrm{k}(t)$, is $C_0 \cong \mathbb{P}^1$. We fix an element $\infty_t \in C_0(\mathrm{k})$, the pole of t. For any i, if $C = C_i$ denote $C_{af} = C_{i,af} = C \setminus p_{i0}^{-1}(\infty_t)$.

Lemma 2.1. *Any finitely generated ideal of* $\mathrm{k}[t]^{int}$ *is* 2*-generated as an ideal. For any curve* C*, any function* $C_{af}(\mathrm{k}) \to \mathbb{N}$ *with finite support has the form* $p \mapsto \min(v_p(f), v_p(g))$ *for some* $f, g \in \mathrm{k}[t]^{int}$*.*

Proof. It suffices to prove this for a cofinal family of finitely generated subring, namely for the affine coordinate rings R of the affine curves C_{af}. Any ideal I of R has the form $\{f : v_{p_k}(f) \geq m_k, k = 1, \ldots, m\}$ for some $p_1, \ldots, p_k \in C(\mathrm{k})$ and $m_1, \ldots, m_k \in \mathbb{N}$. Since the localizations are regular local rings, and using the Chinese remainder theorem, we may find $g \in R$ with $v_{p_k}(g) = m_k$. Now g may have additional zeroes at some additional points $q_1, \ldots, q_l$. But by the independence of valuations, there exists h with $v_{p_i}(h) \geq m_i$ and $v_{q_i}(h) = 0$. Now it is clear that g, h generate I. The second statement is proved in the same way. □

Let C be a curve along with a dominant morphism to $\mathbb{P}^1_k$ (corresponding to an element of the index set $\mathcal{I}$.) Let $\mathbb{B}(C)$ be the Boolean algebra of finite or cofinite subsets of $C_{af}(\mathrm{k})$, $\mathbb{B}_f(C)$ the ideal of finite subsets, $D(C)$ the group of functions $C(\mathrm{k}) \to \mathbb{Z}$ with support in C_{af}.

Let $Div(C)$ be the free Abelian group on $C(\mathrm{k})$, viewed as the group of functions $C(\mathrm{k}) \to \mathbb{Z}$ with finite support. $Div_0(C)$ the subgroup of elements of coefficient sum 0, and $J(C)$ the Jacobian of C, quotient of $Div_0(C)$ by the principal divisors. Let $\rho = \rho_C : Div_0(C) \to J(C)$ be the natural map.

For $b \in \mathbb{B}_f(C)$, let b^* be the finite subset of $C(\mathrm{k})$ consisting of b along with the points at ∞, $b^* = (C(\mathrm{k}) \setminus C_{af}(\mathrm{k})) \cup b$.

$Div(C)_b$ be the free Abelian group on b^*, and let $J_b(C) = \rho(Div_0(C) \cap Div(C)_b)$.

Let $H(C) = J(C)/J_0(C)$. Then ρ induces a homomorphism $\rho : D(C) \to H(C)$: choose some element of $Div_0(C)$ extending a given $d \in D(C)$, and map d to the image under ρ of that element; this is well-defined modulo $J_0(C)$. Let $D_{pr}(C)$

denote the kernel of $\rho : D(C) \to H(C)$; it is the group of affine divisors $(f)_{af}$ of elements f of i, $(f)_{af}(p) := v_p(f)$, v_p being the valuation corresponding to p. So we have an exact sequence:

$$0 \to D_{pr}(C) \to D(C) \to H(C) \to 0$$

Consider now a pair $i \leq j \in \mathfrak{I}$.

There is a natural map

$$p^{ij} : D(C_i) \to D(C_j), \quad d \mapsto p^{ij}(d), \quad p^{ij}(d)(q) = r(q)d(q|k_i) \tag{1}$$

where $r(q)$ is the ramification degree of j over i with respect to the valuation q.

This is a homomorphism of partially ordered groups. The multiplicities are defined so as to have, for any $f \in i = \mathrm{k}(C_i)$,

$$p^{ij}(f)_{af} = (f \circ p_{ji})_{af}$$

so $p_{ij}(D_{pr}(C_i)) \subseteq D_{pr}(C_j)$. Thus p^{ij} also induces a homomorphism

$$p^{ij} : H(C_i) \to H(C_j) \tag{2}$$

Finally, we have a natural embedding $p^{ij} : \mathbb{B}_f(C_i) \to \mathbb{B}_f(C_j)$, the pullback; it is compatible with $p^{ij} : D(C_i) \to D(C_j)$ and the support maps $supp : D(C_i) \to \mathbb{B}_f(C_i)$, taking an element to its support.

Let $\mathbb{B}, \mathbb{B}_f, D, H, J, H_b$ be the direct limits along $\mathfrak{I}$ of $\mathbb{B}(C_i), \mathbb{B}_f(C_i), D(C_i), H(C_i), J(C_i)$. The transition maps from i to j are (1),(2), and $supp \circ p_{ij} : B_{i,af} \to B_{j,af}$. $\mathbb{B}$ is a Boolean algebra with maximal ideal $\mathbb{B}_f$. These direct limits come with the maps $p^{i\infty} : D(C_i) \to D$, $p^{i\infty} : J(C_i) \to J$, etc.

Lemma 2.2. *J and H are torsion-free divisible abelian groups; so are the H_b*

Proof. Let us show that J is torsion-free. We have to show that for any i, with $C = C_i$, any torsion element of $J(C)$ maps to 0 in $J(C')$ for an appropriate covering curve $C' \to C$. Let $\tau \in Div_0(C)$ represent a torsion element of $J(C)$; so there is a function $f \in \mathrm{k}(C)$ with $(f) = m\tau$. Let $j = i(g)$ with $g^m = f$. Then $(g^m) = mp^{ij}(\tau)$ so $(g) = p^{ij}(t)$, thus τ pulls back to 0 in $J(C')$.

A similar argument works for H, and more generally for J/J_b, for any $b \in \mathbb{B}_f$. In this case we have $(f) = m\tau + \upsilon$ with υ supported above b, and so $(g) = \tau + \upsilon'$ with υ' still supported above b.

Each $J(C)$ and $H(C)$ is already divisible, hence J and H are divisible. Since $H/H_b = J/J_b$ is torsion-free, it follows that H_b is divisible too. □

We thus view J, H, H_b as $\mathbb{Q}$-vector spaces.

We remark that D is also a $\mathbb{Q}$-vector space. Each $D(C)$ is torsion-free, hence so is D. And any element of D attains an n'th root with the same support in some (sufficiently ramified) covering.

We will keep in mind that at the limit we are working with $\mathbb{Q}$-vector spaces, so that our interest in the approximations $H(C)$ will always be modulo torsion.

We fix an element of $\mathfrak{I}$ corresponding to a curve C_1, and denote it by 1; the corresponding function field is k_1. We may take C_1 to be an elliptic curve; this is not essential but will simplify notation in Lemma 2.7, and will suffice for interpreting $\mathbb{Q}$ with parameters from $F(t)^{alg}$, F being the prime field.

We consider from now on only elements $j \in \mathfrak{I}$ with $j \geq 1$.

For any $j \geq 1$ we also have a morphism in the opposite direction,

$$p_{1j*} : D(C_j) \to D(C_1), \quad p_{1j*}(e)(p) = \sum_{q|k_1=p} r(q)e(q)$$

Note that $p_{1j*}p^{1j}$ is multiplication by $n = [k_j : k_1]$.

We have induced homomorphisms between $J(C_j)$ and $J(C_1)$, as well as $H(C_j)$ and $H(C_1)$ denoted by the same letters. We still have $p_{1j*}p^{1j} = [\cdot n]$ with $n = [k_j : k_1]$. Thus on $H(C_j)$ we have $\ker p_{1j*} \cap Im(p^{1j})$ torsion. On the other hand $\ker p_{1j*} + Im(p^{1j}) = H(C_j)$ (as in Lemma 2.6 below.) Note that for $j \leq k$, $p^{jk}(\ker p_{1j*}) \subset \ker p_{1k*}$. Let $H_1 = p^{1\infty}(H(C_1)) \cong \mathbb{Q} \otimes H(C_1)$ be the image of $H(C_1)$ in H, and let ${H_1}^{\perp} = \lim_j \ker p_{1j*}$. Then ${H_1}^{\perp}, H_1$ are complementary $\mathbb{Q}$-subspaces of H.

Fix $b \in \mathbb{B}_f$. An element of H has many representatives in D. We let $H(b)$ be the set of elements of H having some representative supported on b. More formally:

Definition 2.3. For $b \in \mathbb{B}_f(C_i)$, $i \leq j$, let $H(j; b) = \rho(D(j; b))$, where $D(j; b)$ is the set of elements of $D(C_j)$ supported on (a subset of) $\operatorname{supp} p^{ij}b$.

The $H(j; b)$ (or their pullbacks to the Jacobian of C_j) are our fundamental geometric objects. We have already considered $H(C_j)$, which is the limit of $H(j; b)$ over all $b \in \mathbb{B}_f(C_i)$.

For fixed $b \in \mathbb{B}_f(C_i)$ we now consider $H(b)$ be the limit of the $H(j; b)$ over j. This is a $\mathbb{Q}$-subspace of H. [1]

Lemma 2.4. *Let k be a finitely generated field of positive Kronecker dimension. Let C, D be pointed curves over k, and $p : D \to C$ a finite morphism of degree > 1. Let $A = J(C)$, $B = J(D)$ be the Jacobians. We have a dominant morphism $\sum : C^g \to A$, where g is the genus of C. Let $a \in A(k)$, $d \in B(k^{alg})$. Then there exist $b = (b_1, \ldots, b_g)$ and $c = (c_1, \ldots, c_g)$ in $C(k^{alg})^g$ such that $(\sum b_i) + a = (\sum c_i)$, and $Aut(k^{alg}/k(a, b, c, d))$ acts transitively on $p^{-1}(b_i)$, as well as on $p^{-1}(c_i))$, for each $i \leq g$.*

Proof. Let $p_1 : C \to \mathbb{P}^1$ be a dominant morphism. Let $k' = k(b'_1, \ldots, b'_g)$ with $b' = (b'_1, \ldots, b'_g)$ a generic element of C^g. Let $t'_i = p_1(b'_i)$; then $k(t'_1, \ldots, t'_g)$ is a purely transcendental extension of k. Let $c = (c'_1, \ldots, c'_g) \in C(k')^g$ be such that $\sum b'_i + a = \sum c'_i$.

[1] There will be no risk of confusion, as finite sets and curves are denoted by different letters, such as b and C.

If $e_i', e_i'' \in p^{-1}(b_i)$, then $(e_1', \ldots, e_g')$ is a generic element of D^g over $k(d)$ as is $(e_1'', \ldots, e_g'')$; so there exists a field automorphism fixing $k(d)$ and taking each $e_i \mapsto e_i''$; this field automorphism fixes $k(b', c', d)$. Similarly, $Aut(k(b', c', d)^{alg}/k(b', c', d)$ acts transitively on each $p^{-1}(c_i')$.

Let L' be a finite normal field extension of $k(t_1', \ldots, t_g')$ with $d \in B(L')$, and such that:

(1) Each b_i' and c_i' lie in L'; we have $b_i' + a = c_i'$, and $p_1(b_i') = t_i$; $d \in L$; moreover,
(2) all elements of $D(k(t_1', \ldots, t_g')^{alg})$ lying above some b_i' or c_i', belong to L'.
(3) $Aut(L'/k(b', c', d)$ acts transitively on each $p^{-1}(b_i)$ and $p^{-1}(c_i)$.

By [1] Theorem 13.4.2, k is a Hilbertian field, and in fact we may embed $k(t_1', \ldots, t_g')$ in an elementary extension k^* of k, in such a way that k^* is a regular field extension of $k(t_1', \ldots, t_g')$, i.e. it is linearly disjoint from $k(t_1', \ldots, t_g')^{alg}$ over $k(t_1', \ldots, t_g')$. It follows that the compositum $L'k^*$ is a normal extension of k^* with automorphism group $G = Aut(L'k^*/k^*) = Aut(L'/k(t_1', \ldots, t_g')$.

Recall the the set of field extensions of a given degree of any field is interpretable in it; applying this to $L'k^*/k^*$, it is easy to write a formula $\psi(u_1, \ldots, u_g)$ such that $k^* \models \psi(t_1', \ldots, t_g')$, and such that ψ asserts the existence of a finite field extension having the properties above. Since $k \prec k^*$, there exist $t_1, \ldots, t_g \in k$ with $k \models \psi(t_1, \ldots, t_g)$; hence there exist a finite field extension L and elements $b_i, c_i \in B(L)$ having the properties (1-3) above.

□

2.5. **The subspaces $H(b)$.** Say $b = \{\beta_1, \ldots, \beta_k\} \subset C_1(\mathrm{k})$. Let $H_1(b)$ be the subspace of H generated by the images of $\beta_1, \ldots, \beta_k$. Let $H_1^\perp(b)$ be the subspace of H generated by the differences $x - y$ where $p_{j1}(x) = p_{j1}(y) = \beta_i$ for some $i \leq k$. Note that $H_1(b) \leq H_1$, while $H_1^\perp(b) \leq {H_1}^\perp$.

Lemma 2.6. $H(b) = H_1(b) \oplus H_1^\perp(b)$.

Proof. The sum is direct since $H_1 \cap {H_1}^\perp = 0$. To show that $H_1(b) \oplus H_1^\perp(b) = H(b)$, consider an element of $D(C_j)$ supported above b. It is a linear combination of singleton elements of C_j, supported above some $\beta = \beta_l$. So it suffices to show that such an e lies in $H_1(b) + H_1^\perp(b)$. Say $n = [C_j : C_1]$. Then $ne = p^{1j}(\beta) - \sum_{p_{j1}(y)=\beta}(y - e)$, and each $y - e \in H_1^\perp(b)$. This exhibits ne as the difference of an element of $H_1(b)$ and one of $H_1^\perp(b)$. Since by definition these are $\mathbb{Q}$-subspaces, we have also $e \in H_1(b) + H_1^\perp(b)$. □

We now take a closer look at the interaction of the subspaces $H(b)$.

Lemma 2.7. *Assume C_1 has genus one, and $k = k^{alg}$ has positive Kronecker dimension. Fix j; so we have a covering $p = p_j : C_j \to C_1$.*

Let $\beta_1 \in C_1(k)$. Then there exists $\beta_2 \in C_1(k)$ such that, letting $\beta_3 = \beta_1 - \beta_2$, statements (1-3) below hold.

(1) $H(j;\beta_1) \cap (H_1^\perp(j;\beta_2) + H_1^\perp(j;\beta_3))$ *is torsion.*
(2) $H_1^\perp(j;\beta_1) \cap (H(j;\beta_2) + H(j;\beta_3))$ *is torsion.*
(3) $p^{j\infty}H_1^\perp(j;\beta_1) \cap (H(\beta_2) + H(\beta_3)) = (0)$

Proof. We may choose a finitely generated subfield k_0 of k such that k_0 has positive Kronecker dimension, C_j, C_1, p are defined over k_0, and $\beta_1 \in C_1(k_0)$, as are the points δ of C_1 above $\infty = \infty_t$'.

Let $A = C_1 = J(C_1)$ and let $B = J(C_j)$ be the Jacobian variety of C_j. Choose β_1 as in Lemma 2.4 (with respect to $a = \beta_1, D = C_j, b$ an enumeration of $p^{-1}(a)$, in the notation of that lemma; note here $g = 1$.)

Let $a_1 \in B(k)$ represent an element of $H(j;\beta_1)$; in other words, a_1 is represented by a cycle on C_j whose support lies about $\delta \cup \beta_1$. Let $a_1 = a_2 + a_3$ such that for $i = 2, 3$, we have a_i supported above $\delta \cup \beta_i$, and $p(a_i)$ is supported above δ. We have to show that a_1 is torsion, modulo points supported above δ.

Note that $a_1 \in B(k_0^{alg})$, since $\delta \cup \beta_1 \subset C_j(k_0^{alg})$, and a_1 is supported on points above this finite set.

Let $K = k_0^{alg}(\beta_2) = k_0^{alg}(\beta_3)$, L the Galois hull over K of $K(a_2) = K(a_3)$, and $G = Aut(L/K)$, $m = |G|$. Then G acts on $B(L)$ and on $A(L)$, and we have a trace map (sum of conjugates) $tr : B(L) \to B(K)$. Since G fixes a_1 we have $tr(a_1) = ma_1$. On the other hand for $i = 2, 3$, any two elements of $p_{j1}^{-1}(\beta_i)$ are $Aut(L/K)$-conjugate; thus their difference has G-trace zero. Since a_2 and a_3 are sums of such differences, and points lying above δ, we have $tr(a_2)$ and $tr(a_3)$ supported above δ. Thus so is ma_1. This proves (1).

We now deduce (2,3) from (1).

For (2), assume $a_1 \in H_1^\perp(j;\beta_1)$. We apply the operator $Id - p^{1j}p_{j1*}$; it leaves a_1 fixed since $a_1 \in H_1^\perp(j;\beta_1)$, so that $p_{j1*}(a_1) = 0$; and takes a_2, a_3 to elements of $H_1^\perp(j;\beta_i)$, so that the previous paragraph applies.

The last point, (3), amounts to saying, for any $j' \geq j$, that

$$p^{jj'}H_1^\perp(j;\beta_1) \cap (H(j';\beta_2) + H(j';\beta_3))$$

is torsion. Let $a_1 \in H_1^\perp(j;\beta_1)$, $a_i \in H(j';\beta_i)$ for $i = 2, 3$ and suppose $p^{jj'}(a_1) = a_2 + a_3$. Applying $p_{j'j*}$, and using that $p_{j'j*}p^{jj'}(a_1) = da_1$ for appropriate d, we see that $da_1 \in H(j;\beta_2) + H(j;\beta_3)$ so a_1 is torsion.

□

Observe that Lemma 2.7 (3) implies that for any $j' \geq j$, $p^{jj'}H_1^\perp(j;\beta_1) \cap (H(j';\beta_2) + H(æ';beta_3)) = (0)$, but does not go as far as asserting the same of $H_1^\perp(j';\beta_1) \cap (H(j';\beta_2) + H(j';\beta_3))$. This is because even if β_1 is chosen to be generic over k_0, it cannot be chosen generic over all j'.

Example 2.8. Let C be a smooth projective curve over k. Let $a_1, \ldots, a_l$ be points of $C(\mathrm{k})$, such that some $f \in \mathrm{k}(C)$ has simple zeroes at the a_i and no other zeroes. Then there exists a (ramified) double covering $p : E \to C$ and points

$b_i, c_i \in p^{-1}(a_i)$ with distinct images in $\mathbb{Q}\otimes J(E)$, such that $\sum b_i = \sum c_i$ in $J(E)$. Thus the groups $H(a_i)_1^\perp$ are not in direct sum.

Proof. Choose a projective embedding of C, and find homogeneous polynomials f_0, f_1 such that $f = f_0/f_1$ on C. Choose $\alpha \in \mathrm{k}$ such that $4\alpha f^2 - 1$ has distinct roots in C, so that it is not a perfect square in $\mathrm{k}(C)$. Define $E \leq C \times \mathbb{P}^1$ by the equation:

$$f_0(x)y_1^2 + f_1(x)y_1y_0 + \alpha f_0(x)y_0^2 = 0$$

Because of the condition on the discriminant, E is an irreducible curve. Let $\pi : E \to C$ be the projection $(x, y) \mapsto x$. Consider the poles and zeroes of y_1/y_0 on E, i.e. the zeroes of y_1 and of y_0. When $f_1(x) = 0$ we may divide by $f_0(x)$ to obtain $y_1 = \pm\sqrt{\alpha}y_0$, two points that are not poles or zeroes of y_1/y_0. Thus we may restrict to $f_1(x) \neq 0$ and write

$$f(x)y_1^2 + y_1y_0 + \alpha f(x)y_0^2 = 0$$

When $f(a) = 0$ we find the equation $y_1y_0 = 0$, giving a pole and a zero of y lying above a; it is easy to check that E is smooth at these points, so these still give one pole and one zero of the normalization $\widetilde{E}$ of e. When $f(a) \neq 0$ we see that y_1/y_0 is integral over k so it has no poles over a. Passing to the normalization of E, we find no new poles, so we have a simple pole b_i and a zero c_i above each a_i, and as there are no further poles, there can be no further zeroes either. □

Notably, the hypothesis applies to almost all l-tuples $a_1, \ldots, a_l$ if l is at least than the genus of C. By considering $b_1 - c_1 = b_2 - c_2$ we see that $H(a_1) \cap H(a_2) \neq (0)$ even when a_1, a_2 are independent generics of a rational or elliptic curve.

3. Interpreting the rational field

We consider the structure $\mathcal{S}$ consisting of the Boolean algebra $\mathbb{B}$, the ideal $\mathbb{B}_f$, the partially ordered group D, the support map $D \to \mathbb{B}_f$, the group H and the homomorphism $\rho : D \to H$.

The following interpretation is implicit in [4] and [3].

Lemma 3.1. *(cf. [4]) $\mathcal{S}$ can be interpreted in $\mathrm{k}[t]^{int}$.*

Proof. Let $A = \mathrm{k}[t]^{int}$. The interpretation hinges on the interplay between ideals and radical ideals. Finitely generated ideals are uniformly definable as by Lemma 2.1 they are all 2-generated. As for radicals: since all prime ideals of A are maximal, the radical of an ideal, intersection of all prime ideals containing it, coincides with the Jacobson radical; the standard formula for the Jacobson radical of a definable ideal I shows that $\sqrt{I}$ is definable too.

$\mathbb{B}_f$ can be identified with the set of radicals of finitely generated ideals of $\mathrm{k}[t]^{int}$. Intersection in $\mathbb{B}_f$ corresponds to the radical of the sum of ideals; union to the intersection. The difference of two elements of $\mathbb{B}_f$ corresponds to the operation of (radical) ideals, mapping (I, J) to $\{x : Jx \subset I\}$. Given $\mathbb{B}_f$ with this structure,

the Boolean algebra $\mathbb{B}$ can be easily interpreted by adding a formal element 1 and defining the obvious structure on $\mathbb{B}_f \cup \{1-a : a \in \mathbb{B}_f\}$.

Let D^+ be the semigroup of non-negative elements of D. Define a map $\alpha : A^2 \to D^+$, $\alpha(a,b)(p) = \min(v_p(a), v_p(b))$; more precisely, define this at the level of each sufficiently large field i of the limit system, and check compatibility. By Lemma 2.1, α is surjective. We have to show that equality and the ordered group operations $+, \min$ pull back to definable sets on A^4. Indeed min corresponds to the sum of ideals, i.e. $\alpha(a'',b'') = \min(\alpha(a,b), \alpha(a',b'))$ iff $A(a,b,a',b') = A(a'',b'')$. Equality corresponds to equality of ideals. $+$ corresponds to product of ideals. The lattice-ordered group D is now easily definable as the set of differences $a-b$ with $a, b \in D^+$.

Observe that D is interpreted along with the structural map $\alpha : A^2 to D^+ \subseteq D$. In particular we can define $\beta(a) = \alpha(a,a)$ so that $\beta(a)(p) = v_p(a)$. We define H as D modulo the image of β.

The support map $D \to \mathbb{B}_f$ is obtained by factoring through D the map $A^2 \to \mathbb{B}_f$, taking (a_1, a_2) to the radical ideal generated by a_1, a_2.

□

Assume k has positive Kronecker dimension

Lemma 3.2. *Assume C_1 has genus 1. There exists a formula $\phi(x,y)$ such that for any $a \in H_1$, $\phi(x,a)$ defines $\mathbb{Q}a$ (a subspace of H.)*

Proof. We have a definable family Ξ_1 of $\mathbb{Q}$-subspaces of H, namely all the ones of the form $H(b)$ for $b \in \mathbb{B}_f$.

So $\Xi = \{U + V : U, V \in \Xi_1\}$ is also a uniformly definable family (actually $\Xi = \Xi_1$ since $H(b \cup b') = H(b) + H(b')$.)

For $a \in H$, let $\Phi(a)$ denote the intersection of all $U \in \Xi$ with $a \in U$. So $\Phi(a)$ is definable uniformly in a; it is a $\mathbb{Q}$-space; and $a \in \Phi(a)$. If $a \in H(C_1)$, we also write $\Phi(a)$ for $\Phi(\bar{a})$ where $\bar{a} = p_{1\infty}(a)$. Moreover we write $H(a)$ for $H(\pi_{1\infty}(\{a\}))$.

Claim . Let $a \in H(C_1)$. Then $\Phi(a) = \mathbb{Q}\bar{a}$.

Let $C_j \to C_1$ be some other curve, covering C_1. Let $b \in H(C_j)$, supported over (the support of) a, but such that there are no nonzero $m, m' \in \mathbb{Z}$ with $ma + m'b = 0$; i.e. $\bar{b}$ is not a rational multiple of $\bar{a}$. We have to show that $\bar{b} \notin \Phi(a)$.

Let $a' \in C_1$ be generic (over a, b and a base of definition for C_j), and let a"=a+a'. Then $a \in H(a') + H(a'')$. So we are done if we show

(*) $b \notin H(a') + H(a'')$.

(*) follows by combining Lemma 2.6 and Lemma 2.7. Suppose $b = b' + b''$, with $b' \in H(a')$ and $b'' \in H(a'')$. By Lemma 2.6 may subtract a scalar multiple of a from b, so as to have $b \in p^{j\infty} H_1^{\perp}(j; a)$. But then by Lemma 2.7 we have $b = 0$, contradicting that it is not a multiple of a. □

Proof of Theorem 1.1: interpreting $\mathbb{Q}$ with parameters. One can interpret a 2-dimensional vector space V over $\mathbb{Q}$, with the family of all subspaces of V. Choose a_1, a_2 linearly independent in $H(C_1)$. Let $V = \mathbb{Q}a_1 + \mathbb{Q}a_2$. Then V is definable, since $+$ is definable on H. Now letting b vary and considering $\phi(x, b) \cap V$, we obtain a family of subspces of V, including all one-dimensional subspaces of V.

It is easy to interpret $\mathbb{Q}$ in such a vector space, with a distinguished basis. [2] Now $(\mathbb{N}, +, \cdot)$ is interpretable by a theorem of J. Robinson, using the theory of quadratic forms over $\mathbb{Q}$.

Undecidability of $(\mathrm{k}[t]^{int}, +, \cdot)$ follows: Let T_0 be a non-recursive finitely axiomatizable theory, true in $(\mathbb{N}, +, \cdot)$. Let N_u be a uniformly definable family of rings in $\mathrm{k}[t]^{int}$, including at least one copy of $(\mathbb{N}, +, \cdot)$. Then $T_0 \vdash \theta$ iff $\mathrm{k}[t]^{int} \models (\forall u)(N_u \models \psi \to \theta)$. So $Th(\mathrm{k}[t]^{int})$ cannot be recursive.

□

3.3. **Extensions.** The use of an elliptic curve C_1 was convenient, but not necessary. To see this let g be the genus of C_1, and let us drop the assumption that $g = 1$.

Lemma 2.7 can be generalized as follows.

Lemma 3.4. *Let $p = p_j : C_j \to C_1$ be defined over a subfield k_0 of k. Let $\beta_{1,1}, \ldots, \beta_{1,m} \in C_1(k_0)$, let $\beta_{2,1}, \ldots, \beta_{2,g}$ be g elements of C_1 that are algebraically independent over k_0, and let $\beta_{3,1}, \ldots, \beta_{3,g}$ be elements of C_1 such that in the Jacobian J_1 we have*

$$\sum_{\nu=1}^{m} \beta_{1,\nu} = \sum_{\mu=1}^{g} \beta_{2,\mu} + \sum_{\mu=1}^{g} \beta_{3,\mu}$$

Then

$$p^{j\infty} H_1^{\perp}(j; \beta_1) \cap (H(\beta_2) + H(\beta_3)) = (0)$$

The proof is the same as of Lemma 2.7.

Using Lemma 3.4 in place of 2.7, the proof of Lemma 3.2 goes through for C_1 of any genus g, and thus for any curve C_j as well. We thus have, with no assumptions of genus:

Lemma 3.5. *Assume* k *has positive Kronecker dimension. There exists a formula $\phi(x, y)$ such that for any i and any $a \in H_i$, $\phi(x, a)$ defines $\mathbb{Q}a$ (a subspace of H.)*

[2] This is related to the fundamental theorem of projective geometry, but is an especially basic case, underlying the algebrization of Euclid by Descartes, [**?**]. We can take the universe of $\mathbb{Q}$ to be the x-axis, i.e. the line through $(0, 0)$ and $(1, 0)$. The bijection with the y axis can be defined by mapping a to b if the line through (a, b) is parallel to the line through the basis elements $(1, 0)$, $(0, 1)$. Multiplication $x \cdot y$ can be defined by considering lines parallel to the one through $(x, 0)$ and $(0, 1)$, and passing through $(0, y)$. By means of parallelograms it is easy to define when two segments on the x-axis have equal length, and then we immediately define addition.

In fact there is a simpler argument giving a stronger result, at least when the transcendence degree of k is infinite.

Lemma 3.6. *Assume* k *has infinite transcendence degree over the prime field. . There exists a formula $\phi(x, y)$ such that for any $a \in H$, $\phi(x, a)$ defines $\mathbb{Q}a$ (a subspace of H.)*

Proof. □

It follows that the various copies of $\mathbb{Q}$ we interpreted are all definably isomorphic (by embedding the two 2-dimensional geometries in a bigger one of dimension ≤ 4).

Proof of Theorem 1.1, interpreting $\mathbb{Q}$ in $(\mathrm{k}[t]^{int}, +, \cdot, t)$ without additional parameters. We have found a finite definable class P of parameters, such that for any $c \in P$ which we obtain uniformly a field K_c isomorphic to $\mathbb{Q}$, and such for any $c, c' \in P$ we obtain (with further parameters, by embedding the two 2-dimensional geometries in a bigger one of dimension ≤ 4) an isomorphism $K_c \to K_{c'}$. In this situation, by Remark 3.7 below, a copy of $\mathbb{Q}$ may also be interpreted without parameters. □

The next lemma is valid in any structure.

Remark 3.7. Assume:

(1) P is a definable set
(2) For $c \in P$, we have an interpretable structure Z_c in some finite language L, given uniformly in c.
(3) For $c, d \in P$ (and uniformly in c, d) there exists an isomorphism $Z_c \to Z_d$, definable possibly with additional parameters.
(4) Each Z_c has trivial automorphism group.

Then there exists a structure Z interpretable without parameters, and isomorphic to each Z_c.

Proof: Let $Z = \{(a, z) : a \in P, z \in Z_c\}/E$, where E is the equivalence relation: $(c, y)E(d, z)$ iff there exists a definable isomorphism $Z_c \to Z_d$ with $y \mapsto z$.

By assumption, for some formula $\phi(u, v, w, x, y)$, for any $c, d \in P$, for some e, $\phi(c, d, e, x, y)$ defines an isomorphism $Z_c \to Z_d$. Let $IS(c, d)$ be the (nonempty, definable) set of all e such that $\phi(c, d, e, x, y)$ defines an isomorphism $Z_c \to Z_d$. Note that $(c, f)E(d, g)$ iff for all $e \in IS(c, d)$ we have $\phi(c, d, e, f, g)$. Indeed if $\alpha : Z_c \to Z_d$ is an isomorphism with $\alpha(f) = g$, let $e \in IS(c, d)$ and let α' be the isomorphism $Z_c \to Z_d$ defined by $\phi(c, d, e, x, y)$; then by uniqueness of the isomorphism $Z_c \to Z_d$ assumed in (4), we have $\alpha = \alpha'$ so $\phi(c, d, e, f, g)$ holds. The other direction is clear.

Hence, E is definable.

Now pick $c \in P$; define $f_c : Z_c \to Z$ by $f_c(z) = (c, z)/E$. Clearly f_c is a bijection $Z_c \to Z$. Moreover, by definition of E, for any $c, d \in P$ we have that

$f_d^{-1} \circ f_c : Z_c \to Z_d$ is an isomorphism. Hence there exists a unique L-structure on Z such that each f_c is an isomorphism.

Question 3.8. Consider the structure $\mathcal{S}$ described above; view the support relation on $H \times B$ as a basic relation (asserting of (h, b) that there exists $d \in D$ with $\rho(d) = h$ and supported on b.) Is the universal theory of $\mathcal{S}$ decidable? With parameters allowed, the formula defining $\mathbb{Q}c$ is *universal*: $x \in \mathbb{Q}c$ iff for all $b \in B$, if c is supported on b then so is x. From this it follows formally that a 2-dimensional $\mathbb{Q}$-vector space $\mathbb{Q}c_1 + \mathbb{Q}c_2$ is defined by an $\exists\forall$-formula; but it seems likely that is can also be defined by a universal formula, perhaps stating that any supports for the c_i also jointly support x. One can guess that the field $\mathbb{Q}$ can also be interpreted by means of universal formulas.

Question 3.9. Can we also interpret $\mathbb{Q}$ within $\mathbb{B}_f$? Here example 2.8 is relevant. Let $B_{dep}(C)$ be the set of finite subsets of C, whose image in $\mathbb{Q} \otimes H(C)$ is $\mathbb{Q}^+$-linearly dependent. For $i \leq j$, note $B_{dep}(C_i) = (p^{ij})^{-1} H_{dep}(C_j)$. It is clear that the image of a dependent set is dependent. Conversely the norm of a function showing dependence of a full pullback on C_j, will already show dependence on C_i. Let $B_{dep} \subset \mathbb{B}_f$ be the limit of these sets. We can easily interpret $\mathbb{Q}$ in $(C, \mathbb{B}_f, B_{dep})$ for a fixed C, at least.

Question 3.10. Can one understand the theory of the ring $\mathrm{k}[t]^{int}$ relative to $\mathbb{B}, H$?

Question 3.11. The theory of $k[t]^{int}$ depends at most on the characteristic of k, and on the transcendence degree over the prime field. Does it in fact depend on the latter?

This could be the case if one can understand the theory of $\mathrm{k}[t]^{int}$ relative to the scalar field $\mathbb{Q}$. On the other hand if the constant field k is definable, the answer is yes and one has a strong form of undecidability by interpreting all finite subsets of k.

References

[1] Fried, Michael D.; Jarden, Moshe Field arithmetic. Third edition. Revised by Jarden. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], 11. Springer-Verlag, Berlin, 2008.

[2] A. Prestel, J. Schmid "Existentially closed domains with radical relations" J. Reine Angew. Math. , 407 (1990) pp. 178-201

[3] L. van den Dries, "Elimination theory for the ring of algebraic integers" J. Reine Angew. Math. , 388 (1988), pp. 189-205

[4] L. van den Dries, A. Macintyre, "The logic of Rumely's local-global principle" J. Reine Angew. Math. , 407 (1990) pp. 33-56