DIFFERENCE ALGEBRAIC GEOMETRY IN/FOR HRUSHOVSKI'S FROBENIUS PAPER.

ALICE MEDVEDEV

NOTATION

These notes are a commentary on, and refer to, the July 24, 2012 draft of Hrushovski's "The elementary theory of the Frobenius Automorphisms" posted on the arxiv.

If you see $\subset$, it's likely to be $\subseteq$. When A and B are sets with structure, $A \leq B$ means substructure (e.g. subring, or sub-difference-ring), while $A \trianglelefteq B$ is reserved for (not necessarily difference) ideals A of rings B.

Single, undecorated letters like b may stand for tuples; in that case, b_i are the entries in the tuple.

1. FLAVOURS OF IDEALS: DEFINITIONS, EXAMPLES, EASY LEMMAS

1.1. Definitions.

Definition 1. A difference ring *is a commutative ring with identity with an endomorphism σ. The usual signature for doing model theory is $L_{ring,\sigma} := \{+, \cdot, 0, 1, \sigma\}$.*

A homomorphism of $L_{ring,\sigma}$-structures is a ring homomorphism, and the isomorphism type of its image is determined by its kernel. An ideal I is a kernel of an $L_{ring,\sigma}$-homomorphism iff I is closed under σ; such an ideal is a difference ideal.

Example 2. ***Difference polynomial rings.***

Let $\mathbb{N}[\sigma] := \{\sum_{i=0}^{m} m_i \sigma^i : m, m_i \in \mathbb{N}\}$, and order it by setting $\sigma > n$ for all $n \in \mathbb{N}$, and requiring the ordering to respect addition and multiplication.
For $\nu := \sum_{i=0}^{m} m_i \sigma^i \in \mathbb{N}[\sigma]$, we write $x^\nu := \prod_{i=0}^{m} (\sigma^i(x))^{m_i}$.
For a difference ring R, the difference polynomial ring *$R[x]_\sigma$ is the set of formal finite R-linear combinations of x^ν, also known as the polynomial ring over R in variables $x, \sigma(x), \sigma^2(x), \ldots$. For multiple variables, $Rx, y_\sigma := (R[x]_\sigma)[y]_\sigma$.*
`In the paper,` $\mathbb{N}[\sigma]$ `is somehow ordered, but the order is ?never? defined.`

Lemma 3. *All the properties of difference ideals $I \trianglelefteq R$ of difference rings (R, σ) that we care about are equivalent to properties of the quotient difference ring R/I.*

ideal $I \trianglelefteq R$	*quotient ring* R/I
algebraically prime $ab \in I \Rightarrow a \in I \vee b \in I$	*(algebraically) integral domain* *no zero-divisors*
radical $\forall n \in \mathbb{N}\, a^n \in I \Rightarrow a \in I$ $\Leftrightarrow, a^2 \in I \Rightarrow a \in I$	*algebraically reduced* *no nilpotents*
perfect $\forall \nu \in \mathbb{N}[\sigma]\, a^\nu \in I \Rightarrow a \in I$ $\Leftrightarrow, a\sigma(a) \in I \Rightarrow a \in I$	*perfectly reduced* $\forall \nu \in \mathbb{N}[\sigma]\, a^\nu = 0 \Rightarrow a = 0$ *no* σ-nilpotents
reflexive $\sigma(a) \in I \Rightarrow a \in I$	*transformally reduced* *endomorphism* σ *is injective*
well-mixed $ab \in I \Rightarrow a\sigma(b) \in I$	well-mixed $ab = 0 \Rightarrow a\sigma(b) = 0$
transformally prime *algebraically prime and reflexive*	difference domain *integral domain with injective endomorphism*

Proof. Let us show that the two definitions of "perfect" are equivalent. Suppose that $c\sigma(c) \in I \Rightarrow c \in I$. First, we show that I is well-mixed:

$$ab \in I \Rightarrow \sigma(a)\sigma(b) \in I \Rightarrow I \ni \sigma(a)\sigma(b)a\sigma^2(b) = (a\sigma(b))\sigma(a\sigma(b)) \Rightarrow I \ni a\sigma(b).$$

The first implication is from "difference", the second is from "ideal", and the last uses $c\sigma(c) \in I \Rightarrow c \in I$ with $c = a\sigma(b)$. Then we show that I is radical:

$$a^2 \in I \Rightarrow a\sigma(a) \in I \Rightarrow a \in I$$

the first implication uses I is well-mixed and the second uses $c\sigma(c) \in I \Rightarrow c \in I$ with $c = a$. Finally, suppose that $\prod_j (\sigma^{n_j}(a))^{m_j} \in I$. Since I is an ideal, we may replace all m_j by their maximum M, and assume that the n_j are $0, 1, 2, \ldots 2^N$. Since I is radical, we may replace M by 1. Using $c\sigma(c) \in I \Rightarrow c \in I$ with $c = \prod_{j=0}^{2^{N-1}} \sigma^j(a)$, we may replace N by $(N-1)$ until at $N = 1$ we get $a\sigma(a) \in I$, and then use $c\sigma(c) \in I \Rightarrow c \in I$ with $c = a$. □

Corollary 4. *Perfect implies well-mixed and radical and reflexive.*

The converse of the Corollary is also true.

Lemma 5. *If* $I \trianglelefteq R$ *is a well-mixed, radical, reflexive ideal of a difference ring* R*, then* I *is perfect.*

Proof. Take $a \in R$ such that $a\sigma(a) \in I$. Since I is well-mixed, $\sigma(a)\sigma(a) \in I$. Since I is radical, $\sigma(a) \in I$. Since I is reflexive, $a \in I$. □

Lemma 6. *An algebraically prime difference ideal is always well-mixed; it is perfect iff it is reflexive. A difference ring* (R, σ) *where* R *is an integral domain is always well-mixed.*

Proof. This first part is immediate, and the second is a consequence of the first. □

1.2. **Examples.**

Example 7. ***(prime difference ideal, well-mixed but not reflexive.)*** *Consider a difference field* (k, id) *and a polynomial difference ring* $R := k[x]_\sigma$ *and a difference ideal* I *generated by* $\sigma(x)$*. This* I *consists of difference polynomials*

$\sum_\nu a_\nu x^\nu$ in which each ν includes $\sigma^m(x)$ for some $m \geq 1$. The quotient is isomorphic to the (not difference!) polynomial ring $k[x]$, with σ fixing coefficients and sending x to 0. In particular, the quotient is an integral domain, so the ideal is prime, so (see Lemma 6) it is well-mixed. However, it is clearly not reflexive, as it contains $\sigma(x)$ but not x.

Example 8. ***(radical, reflexive, not well-mixed.)*** *Consider a difference field (k, id), the polynomial difference ring $R := k[x]_\sigma$ and a difference ideal I generated by $x\sigma(x)$. This I consists of difference polynomials $\sum_\nu a_\nu x^\nu$ in which each ν includes two consecutive powers of σ. This ideal is clearly reflexive: including two consecutive powers of σ is invariant under σ^{-1} whenever σ^{-1} is defined. It is also radical: take a polynomial $p \in k[x]_\sigma$, drop all terms with consecutive powers of σ, take a least leftover monomial $a_\nu x^\nu$ in the sense of some lexicographic ordering, and $(a_\nu x^\nu)^m$ will not cancel with anything in $p(x)^m$, and will have no consecutive powers of σ. On the other hand, $x\sigma^2(x) \notin I$, so I is not well-mixed; and $x\sigma(x) \in I$ but $x \notin I$, so I is also not perfect.*

Example 9. ***(well-mixed, not radical, not reflexive.)*** *Consider the well-mixed ideal I_{wm} generated by $I \trianglelefteq R$ from the previous example. As $x\sigma(x) \in I$, it must be that $x\sigma^m(x) \in I_{wm}$ for all m, so whenever ν includes two distinct powers of σ, the difference monomial $x^\nu \in I_{wm}$. On the other hand, as $\sigma(x)x \in I$, it must be that $\sigma(x)\sigma(x) \in I_{wm}$, so whenever ν includes $(\sigma^m(x))^n$ for some $m \geq 1$ and $n \geq 2$, the difference monomial $x^\nu \in I_{wm}$. These monomials (all except x^n and $(\sigma^m(x))^1$)* generate I_{wm} as a k-vector space. *It is clear that this ideal is neither radical, nor reflexive.*

Example 10. ***(no proper well-mixed ideals)****. Fix a field k, let the ring $R := \{f : \mathbb{Z} \to k\}$ be the product of countably many copies of k, and define $\sigma(f(x)) := f(x+1)$ to be the shift operator. Consider $\xi_o, \xi_e \in R$, the characteristic functions of the sets of odd and even integers, respectively. Note that $\sigma(\xi_o) = \xi_e$ and $\sigma(\xi_e) = \xi_o$ and $\xi_o\xi_e = 0$. Suppose that $I \trianglelefteq R$ is a well-mixed difference ideal. Since $\xi_e\sigma(\xi_e) = 0 \in I$, by well-mixedness if I also $I \ni \sigma(\xi_e)^2 = \xi_o^2 = \xi_o$. In like manner, $\xi_e \in I$. But then $1 = \xi_o + \xi_e \in I$, so $I = R$!*

2. VERY EASY DIFFERENCE COMMUTATIVE ALGEBRA

2.1. operations that preserve properties, and generation.

Remark 11. *All of the properties of difference ideals in Lemma 3 are properties of quotients, so given two difference ideals $I_1 \leq I_2 \trianglelefteq R$, the ideal I_2/I_1 of the quotient R/I_1 has each property if and only if the ideal I_2 of R does.*

Remark 12. *Since all the properties are universal, they pass to subrings: given an ideal $I \trianglelefteq R$ and a subring $R' \leq R$, the ideal $I' := I \cap R'$ of R' inherits all of these properties. For the same reason, they are preserved under unions of chains, either of ideals inside a fixed ring, or of pairs $\{(I_i \trianglelefteq R_i\}_i$.*

Lemma 13. *If $I \trianglelefteq R$ has one of the properties listed in Lemma 3, then so does $\sigma^{-1}(I) \trianglelefteq R$.*

Proof. Let $I_2 := \sigma^{-1}(I) \trianglelefteq R$ and let $I_1 := \ker(\sigma) \trianglelefteq R$. By Remark 11, it suffice to show that the ideal I_2/I_1 of the quotient R/I_1 has the property. That is, we need to show that $\sigma(\sigma^{-1}(I))$ has the property in $\sigma(R)$. This follows from Remark 12, as $\sigma(\sigma^{-1}(I)) = I \cap \sigma(R)$. □

Remark 14. *Except for "prime" and "transformally prime", each of these properties is a matter of being closed under certain operations. Thus, for any set A there exists a unique smallest ideal with the desired property containing A, and these properties are preserved under intersections. Given a difference ideal $I \trianglelefteq R$, the same thing is obtained by generating in R starting with I, or by generating in R/I starting with $\{0\}$ and then taking the preimage in R.*

As usual, $\sqrt{I}$ is the radical ideal generated by a difference ideal I. This preserves all σ properties of I.

Lemma 15. *If I is a difference ideal, so is $\sqrt{I}$.*
If I is well-mixed (resp. reflexive), then so is $\sqrt{I}$.
If I is perfect, $\sqrt{I} = I$.

Proof.

$$a \in \sqrt{I} \Rightarrow a^n \in I \Rightarrow \sigma(a^n) \in I \Rightarrow \sigma(a) \in \sqrt{I}$$

$$ab \in \sqrt{I} \Rightarrow a^n b^n \in I \Rightarrow a^n \sigma(b^n) \in I \Rightarrow a\sigma(b) \in \sqrt{I}$$

$$\sigma(a) \in \sqrt{I} \Rightarrow \sigma(a^n) \in I \Rightarrow a^n \in I \Rightarrow a \in \sqrt{I}$$

The last follows immediately from Corollary 4: a perfect difference ideal is already radical. □

On the other hand, the well-mixed ideal generated by a radical difference ideal need not remain radical - see Example 9. Furthermore, the generating procedures for any of the σ properties might generate the whole ring, even starting from a proper ideal!

The paper's notation for generating well-mixed and perfect ideals is less than satisfying:

- $\sqrt[\sigma]{I}$ is defined in the paper to be the first displayed equation in Lemma 16 below. If I is not a well-mixed ideal, $\sqrt[\sigma]{I}$ need not be a perfect ideal: indeed, it may fail to be an ideal by failing to be closed under addition.
- $rad_{wm}(R)$ is the well-mixed ideal generated by $\{0\}$ in R. It seems natural to write $rad^R_{wm}(I)$ for the smallest well-mixed ideal generated by an ideal I in a ring R, also known as the pre-image of $rad_{wm}(R/I)$ in R.

As far as I can tell, the notation $\sqrt[\sigma]{I}$ is only used in the paper for well-mixed I. It might be more natural to define $\sqrt[\sigma]{I}$ to be the perfect ideal generated by I. In Lemma 16 below, we reword Lemma 2.3 in the paper to avoid the notation $\sqrt[\sigma]{I}$, and to better match the way Lemma 2.3 is used in the paper, for example, in 2.11 p. 15 and 3.7 p. 19.

Lemma 16 (Alternate Lemma 2.3)**.** *If I is a well-mixed ideal, then the perfect ideal J_1 generated by I coincides with*

$$J_2 := \{a \in R : \prod_j (\sigma^{n_j}(a))^{m_j} \in I \textit{ for some } n_j, m_j\}$$

and with

$$J_3 := \{a \in R : (\sigma^n(a))^m \in I \textit{ for some } n, m\}.$$

Proof. Clearly, $J_1 \supseteq J_2 \supseteq J_3$, so it suffices to show that J_3 is a perfect difference ideal. By Lemma 15, $\sqrt{I}$ is also a well-mixed difference ideal, and by Lemma 13, $\sigma^{-n}(\sqrt{I})$ are also well-mixed and radical for all n. Now $J_3 = \cup_n \sigma^{-n}(\sqrt{I})$ is a union of a chain of well-mixed radical difference ideals, so it is itself a well-mixed radical difference ideal. It is clearly reflexive, so by Lemma 5, it is perfect. □

2.2. **localizations.** Most of the properties in Lemma 3 are also preserved under localizations. To obtain a difference structure $\sigma(\frac{a}{b}) := \frac{\sigma(a)}{\sigma(b)}$, one should only localize by multiplicative sets S closed under σ. However:

Example 17. ***(stupid localizing)*** *Consider the ring $R := k[x, \frac{1}{x}] \cong k[x,y]/(xy - 1)$ with σ fixing k and switching x and $\frac{1}{x}$, and consider the set $S := \{x^n : n \in \mathbb{N}\}$. On one hand, S is clearly not closed under σ. On the other hand, S consists of R-units, so $S^{-1}R = R$ inherits a perfectly good difference structure.*

Pleasantly, that does not happen when localizing at prime ideals.

Lemma 18. *Let $P \trianglelefteq R$ be an algebraically prime difference ideal, and let $S := R \backslash P$. The localization $R_P := S^{-1}R$ admit a difference structure compatible with that of R iff S is closed under σ, i.e. iff P is reflexive, i.e. iff P is transformally prime.*

Proof. Suppose $a \in S$ but $\sigma(a) \in P$. Denote the difference structure on $S^{-1}R$ by σ as well. Now in $S^{-1}R$,

$$1 = \sigma(1) = \sigma(a \cdot \frac{1}{a}) = \sigma(a) \cdot \frac{b}{c}$$

for some $b \in R$ and some $c \in S$. Thus, for some $s \in S$, we have $sc = s\sigma(a)b$ in R. But $sc \in S$ while $sb\sigma(a) \in P$, which are disjoint. □

In particular, σ will extend from an integral domain R to its field of fractions if and only if $S := R \setminus \{0\}$ is closed under σ, that is, if σ is injective on R. Together with the Remark 11 this proves the first part of Lemma 2.1.1 in the paper.

As usual, the set S should also be disjoint from an ideal whose properties we're studying. Since localization commutes with quotients, and all the properties in Lemma 3 are properties of quotients, we may and often do study the ideal is $\{0\}$ in R/I, thereby working with the ring properties in Lemma 3 instead of the ideal properties there.

Example 19. *Let R be the quotient of the polynomial difference ring $k[x,y]_\sigma$ by the difference ideal generated by xy. So, monomials with $\sigma^i(x)\sigma^i(y)$ for some i are zero in R, and the rest remain linearly independent over k. This ideal is clearly reflexive, so σ is injective on R. Let $S := \{\sigma^m(y^n) : n \geq 1,\ m \geq 17\}$ be the multiplicative set closed under σ generated by $\sigma^{17}(y)$. In $S^{-1}R$, $\sigma^{17}(x) = 0$ but $x \neq 0$.*

Lemma 20. *Suppose that R is a difference ring, that $S \subset R$ is closed under multiplication and σ, and that $0 \notin S$.*

1. *If R is an integral domain, then so is $S^{-1}R$.*
2. *If R has no nilpotents, then neither does $S^{-1}R$.*
3. *If R has no σ-nilpotents, then neither does $S^{-1}R$. ("perfect")*
4. *This may fail for "reflexive".*
5. *If R is well-mixed, then so is $S^{-1}R$.*
6. *If R is an difference domain, then so is $S^{-1}R$.*

Proof. The first two are standard, and the argument for "no nilpotents" generalizes to an argument for "no σ-nilpotents" as follows. Suppose that $\nu := \sum_j n_j \sigma^{m_j}$ and $(\frac{a}{b})^\nu = 0$ in $S^{-1}R$. Then $s(a^\nu) = 0$ in R for some $s \in S$. Then $(sa)^{1+\nu} = (sa^\nu)(as^\nu) = 0$, so $sa = 0$ since R has no σ-nilpotents. So $\frac{a}{b} = 0$ in $S^{-1}R$.

Example 19 is a counterexample for "reflexive".

For well-mixed, suppose that $\frac{a}{s_a}\frac{b}{s_b} = 0$ in $S^{-1}R$. Then $sab = 0$ in R for some $s \in S$. Since R is well-mixed, $sa\sigma(b) = 0$ as well, making $\frac{a}{s_a}\frac{\sigma(b)}{\sigma(s_b)} = 0$.

For difference domain (aka $\{0\}$ is transformally prime), we only need to show that σ remains injective in the localization. If $\sigma(\frac{a}{s_a}) = 0$ in $S^{-1}R$, then $\sigma(a) = 0$ in R as R is an integral domain, so $a = 0$ as σ is injective on R. $\square$

Lemma 21. *(Lemma 2.1, part 2) Given two difference rings $R' \leq R$ and an algebraically prime difference ideal $P \trianglelefteq R$, let $P' := P \cap R'$, an algebraically prime ideal of R'. Consider the two fields of fractions, K of R/P and K' of R'/P'. The natural map $\frac{a+P'}{b+P'} \mapsto \frac{a+P}{b+P}$ is an embedding of K' in K; we identify K' with its image under this embedding.*

If K is an algebraic extension of K', then P is a transformally prime ideal of R if and only if P' is a transformally prime ideal of R'.

Proof. First, we reduce to the case where $P = P' = \{0\}$. Let $R'_1 := R'/P' \leq R/P =: R_1$, and let $P_1 = P'_1 = \{0\}$. By Remark 11, P (resp. P') is transformally prime iff P_1 (resp. P'_1) is, and the fields K and K' are unchanged.

One direction of the Lemma is an instance of Remark 12. For the other, suppose that $\{0\}$ is a transformally prime ideal of R'. We need to show that $\{0\}$ must be a transformally prime ideal of R. By Lemma 18, it suffices to show that the field of fractions K of R admits a difference structure compatible σ on R.

Let $S := R' \setminus \{0\}$, a multiplicative subset of R closed under σ and not containing 0. Now $M := S^{-1}R$ admits a difference structure compatible σ on R. This M is a subring of the field of fractions K of R, containing the field of fractions K' of R'. Since K is algebraic over K', M is generated over K' by algebraic elements, so it is a field. So M is a subfield of K containing R, so $M = K$. $\square$

3. Annihilators: enough good ideals.

Definition 22. *For $I \subset R$, $Ann_R(a/I) := \{b \in R : ab \in I\}$ and $Ann(a) = Ann(a/\{0\})$. This is only used when $I \trianglelefteq R$. When R is clear, the subscript is dropped.*

Note that $b \in Ann(a/I)$ if and only if $a \in Ann(b/I)$, and $I \leq Ann(a/I)$ for any a. Since all our rings have identity, $Ann(a/I)$ is a proper ideal as long as $a \notin I$.

The proof of Lemma 2.5 in the paper proves the following generalization, and the references to that lemma later in the paper use this more general result.

Lemma 23. *Let R be a difference ring, $a \in R$, and $J \trianglelefteq R$ a well-mixed difference ideal; then $Ann(a/J)$ is a well-mixed ideal.*

Furthermore, let I be the smallest well-mixed ideal containing a and J; then $b^2 \in J$ for any $b \in I \cap Ann(a/J)$.

Proof. This is a search-and-replace generalization of the proof given for Lemma 2.5 in the paper.

$$cd \in Ann(a/J) \Rightarrow acd \in J \Rightarrow ac\sigma(d) \in J \Rightarrow c\sigma(d) \in Ann(a/J).$$

Suppose that $b \in Ann(A/J)$, so $a \in Ann(b/J)$. Now $Ann(b/J)$ is a well-mixed ideal containing a and J, so $I \subset Ann(b/J)$. So $b \in I$ implies $b \in Ann(b/J)$, which means $b^2 \in J$. □

Results 2.5 - 2.11 in the paper use annihilators to build difference ideals and transformally prime ideals in well-mixed rings, ensuring that there will be enough points on schemes. This section substantially reworks the presentation.

Lemma 2.6 has typos, and does not seem to be used anywhere. Judging by the proof, the ambiguous hypothesis "R is a well-mixed domain" should be "R is a well-mixed difference ring with no nilpotents"; and $I(a)$ should be $J(a)$ in the last line - that's a slightly stronger conclusion.

The following generalization of Lemma 2.7 in the paper appears in Zoe's notes about the paper. It clarifies the exposition immensely.

Lemma 24. *Fix a difference ring R and a multiplicative $S \subset R$ with $0 \notin S$ and $\sigma(S) \subset S$. Suppose that $I \trianglelefteq R$ is*

($\star$) *a well-mixed difference ideal of R, disjoint from S,*

and that I is maximal with respect to ($\star$). Then I is transformally prime.

Note that as long as S is disjoint from $rad_{wm}(R)$, such ideals I exist: $rad_{wm}(R)$ satisfies ($\star$), and ($\star$) is preserved in unions of chains.

Proof. This is a direct generalization of the proof of Lemma 2.7 in the paper.

First, let us show that I is reflexive, that is that $\sigma^{-1}(I) = I$. Since $\sigma^{-1}(I) \supset I$, it suffices to show that $\sigma^{-1}(I)$ satisfies ($\star$). If $a \in S \cap \sigma^{-1}(I)$, then $\sigma(a) \in I \cap \sigma(S) = I \cap S = \emptyset$, a contradiction. Thus, $\sigma^{-1}(I)$ is disjoint from S. If $ab \in \sigma^{-1}(I)$, then $\sigma(a)\sigma(b) \in I$. Since I is well-mixed, this puts $\sigma(a)\sigma^2(b) \in I$, and then $a\sigma(b) \in \sigma^{-1}(I)$.

It remains to show that I is prime. Suppose $ab \in I$, so $b \in Ann(a/I)$. By Lemma 23, $Ann(a/I)$ is a well-mixed ideal, and $I \subset Ann(a/I)$.

If $Ann(a/I) \cap S = \emptyset$, then $Ann(a/I)$ satisfies ($\star$). Then, by the maximality of I, it must be that $Ann(a/I) = I$, so $b \in I$.

Otherwise, there is some $b' \in Ann(a/I) \cap S$. If $c \in Ann(b'/I) \cap S$, then $cb' \in I \cap S$; but $I \cap S = \emptyset$, so $Ann(b'/I) \cap S = \emptyset$, and so $Ann(b'/I) \cap S$ satisfies ($\star$) and contains I. Then $Ann(b'/I) = I$, and a is in it. □

Alternately, if one is convinced that everything in the lemma is unaffected by quotienting by I and localizing at S, it suffices to prove the special case where $S = \{1\}$ and $I = \{0\}$ and R is well-mixed.

The following special case $S = \{1\}$ of Lemma 24 is all that is needed for Lemma 2.7 in the paper (Lemma 34 here).

Corollary 25. *If I is a proper well-mixed ideal of a well-mixed ring R, and there are no proper well-mixed J such that $I \lneq J \trianglelefteq R$, then I is transformally prime.*

Another special case of Lemma 24 gives a simple and correct proof of Lemma 2.11 in the paper; the proof given in the paper appears incorrect: algebraically prime difference ideals of Lemma 2.10 magically become transformally prime.

Lemma 26. *(Lemma 2.11 from the paper) In a well-mixed ring R, an element a is σ-nilpotent if and only if it is in all transformally prime ideals of R.*

Proof. Clearly, every transformally prime ideal $p \trianglelefteq R$ contains all σ-nilpotents. For the other direction, suppose that a is not σ-nilpotent. Then the multiplicative set $S := \{a^\nu : \nu \in \mathbb{N}[\sigma]\}$ is closed under σ and does not contain 0. The ideal $\sqrt{\{0\}}$ is well-mixed by Lemma 16, and disjoint from S. Find a ideal p that is proper, well-mixed, and disjoint from S and maximal with respect to these properties as in Lemma 24. By Lemma 24 p is transformally prime, and by construction $a \notin p$. $\square$

Thinking of a as a global function on $\mathrm{Spec}^\sigma(R)$, this says that if a isn't σ-nilpotent, then it is not everywhere locally equal to the constant function 0.

Lemmas 2.8 - 2.10 require a bit more commutative algebra, and achieve a more refined analog Lemma 2.10 of Lemma 2.11. Neither appears to follow from the other. Again, annihilators are used to obtain difference ideals. This time, we approximate a finitely-σ-generated difference ring by a sequence of finitely-ring-generated rings, and approximate the desired difference ideal by annihilators: the nth approximating annihilator agrees with the desired difference ideal on the nth approximation to the ring. Again, we may and do work in the quotient by the ideal I in the statement of Lemma 2.10 of the paper.

Lemma 27. *(Lemma 2.10 of the paper, for finitely-σ-generated rings.)*
Let R be a well-mixed ring with no nilpotents, finitely generated or finitely generated over a difference field k, as a difference field. Then $\{0\}$ is the intersection of algebraically prime difference ideals.

Proof. Take $0 \neq b \in R$; we need to find an algebraically prime difference ideal $p \trianglelefteq R$ with $b \notin p$.

Let a be the tuple of generators of R as a difference ring (maybe over k), and let S_n be the subring of R *ring*-generated by $\{\sigma^j(a_i) : 0 \leq j \leq n, 0 \leq i \leq m\}$ (maybe over k). Clearly $R = \cup_n S_n$.

The desired ideal p will be the union $\cup_n p_n$ of a chain of minimal prime ideals of S_n. In the finitely-ring-generated (maybe over k) and, therefore, Noetherian rings S_n, minimal primes are annihilators, and this will make p a difference ideal.

Construction details. We inductively build p_n, maintaining the following inductive hypotheses:

(1) $b \notin p_0$;
(2) $p_{n+1} \cap S_n = p_n$; and
(3) p_n is a minimal prime ideal of S_n.

Since each S_n is Noetherian, each has finitely many minimal prime ideals, whose intersection is the nilradical $\{0\}$: recall that the whole ambient ring R has no nilpotents. In S_0, there is a minimal prime ideal $p_0 \not\ni b$ because $b \neq 0$. Whenever $S_n \leq S_{n+1}$ are Noetherian rings and p_n is a minimal prime of S_n, some minimal prime p_{n+1} of S_{n+1} satisfies $p_{n+1} \cap S_n = p_n$. The proof given in Lemma 2.9 is correct, easy commutative algebra. From the second inductive hypothesis, $p \cap S_n = p_n$. From then third, p is an algebraically prime ideal of R.

Difference properties of p. For each n, we find $c_n \in S_n$ such that $p_n = Ann_R(c_n) \cap S_n$. List the minimal primes $q_1 = p_n, q_2, q_3, \ldots q_m$ of S_n, and let $b_i \in q_i \setminus p_n$ for $2 \leq i \leq m$. Let $c_n := \prod_{i=2}^m b_i$; then by `magical commutative algebra` $p_n = Ann_{S_n}(c_n) = Ann_R(c_n) \cap S_n$. By Lemma 2.5 (actually, Lemma 23), each $Ann_R(c_n)$ is a well-mixed ideal of R.

Suppose $e \in p$ and take n sufficiently large to have $e, \sigma(e) \in S_n$. Then $e \in p_n = Ann_r(c_n) \cap S_n$. Since $Ann_R(c_n)$ is a well-mixed ideal of R, now $\sigma(e) \in Ann_R(c_n)$. So $\sigma(e) \in Ann_r(c_n) \cap S_n = p_n \subset p$. Thus, p is a difference ideal of R. □

The idea of writing $R = \cup_n S_n$ as a union of Noetherian rings, finding an ideal $p \trianglelefteq R$ which is a union $p = \cup_n p_n$ of minimal primes $p_n \trianglelefteq S_n$, and observing as in the proof above that p must be an algebraically prime difference ideal is reused later in the paper. The collection of Noetherian rings S_n need not be a chain, but one must at least assume that any finite subset of R is contained in some S_n. Such an ideal p is called *cofinally prime*.

4. DIFFERENCE SCHEMES

We should assume that all rings in this section are well-mixed - otherwise $\mathrm{Spec}^\sigma(R)$ might be empty!

4.1. Definition and first properties of Spec^σ.

The following is approximately from the beginning of section 3.1 of the paper.

Definition 28. *The* difference spectrum $\mathrm{Spec}^\sigma(R)$ *of a difference ring R is defined to be the set of transformally prime ideals of R. It is made into a topological space in the following way: a* closed *subset of* $\mathrm{Spec}^\sigma(R)$ *is the set of elements of* $\mathrm{Spec}^\sigma(R)$ *extending a given ideal I. That is,* $\mathrm{Spec}^\sigma(R)$ *is the subset* $\{p \in \mathrm{Spec}(R) : \sigma^{-1}(p) = p\}$ *of the usual spectrum* $\mathrm{Spec}(R)$ *from algebraic geometry, and the topology is the subspace topology.*

Lemma 29. *If R is well-mixed,* $\mathrm{Spec}^\sigma(R)$ *is non-empty. The sets $V_I := \{p \in \mathrm{Spec}^\sigma : I \leq p\}$ for* perfect *ideals I are all the closed sets of* $\mathrm{Spec}^\sigma(R)$*. As topological spaces,* $\mathrm{Spec}^\sigma(R) \cong \mathrm{Spec}^\sigma(R/(\sqrt[\sigma]{0}))$.

Proof. By Lemma 24 with $S := \{1\}$, $\mathrm{Spec}^\sigma(R)$ is non-empty.

Any transformally prime ideal p that contains an ideal I also contains the perfect hull $\sqrt[\sigma]{I}$ of I, so $V_I = V_{\sqrt[\sigma]{I}}$.

Every transformally prime ideal p contains $\sqrt[\sigma]{0}$, and so does every perfect ideal I, so the two topological spaces have the same points and the same closed sets (see the first observation in Sections 2.1). □

As with quotients by the nilradical in the usual algebraic geometry, the difference schemes $\mathrm{Spec}^\sigma(R)$ and $\mathrm{Spec}^\sigma(R/(\sqrt[\sigma]{0})$ have different structure sheaves. We delay defining these and first prove a crucial topological property of difference spectra.

Lemma 30. *Suppose that R is a well-mixed difference ring, either finitely-σ-generated, or finitely-σ-generated over a difference field k. Then* $\mathrm{Spec}^\sigma(R)$ *is a Noetherian topological space.*

Proof. Since $\mathrm{Spec}^\sigma(R)$ and $\mathrm{Spec}^\sigma(R/(\sqrt[\sigma]{0})$ are isomorphic as topological spaces, we may assume that R has no σ-nilpotents. In particular, σ is injective on R, so that R is a difference ring in the sense of Cohn.

We want to show that $\mathrm{Spec}^\sigma(R)$ has no infinite descending chains on closed sets, or, equivalently, that R has no infinite ascending chains of perfect ideals. That is, we want to show that R is a *Ritt difference ring*(see Cohn Theorem II p.86).

If R is finitely-σ-generated, let R_0 be the subring of R generated by 1. It is a quotient of $\mathbb{Z}$ by a radical ideal, closed under σ, and Noetherian, so it is a Ritt difference ring. Otherwise, let $R_0 = k$, also closed under σ and Noetherian. Since R is finitely-σ-generated over R_0, it is also a Ritt difference ring by the Corollary on p.93 of Cohn. □

The following is an easy fact about Noetherian topological spaces.

Corollary 31. *Suppose that R is a well-mixed difference ring, either finitely-σ-generated, or finitely-σ-generated over a difference field k. Then $\mathrm{Spec}^\sigma(R)$ is a union of finitely many irreducible closed sets, that is closed sets which cannot be written as a union of two proper closed subsets.*

Properties of points in a Noetherian topological space can be proved by *Noetherian induction.*

Lemma 32. *Let $\mathcal{K}$ be a class of Noetherian topological spaces such that for any $X \in \mathcal{K}$ and any closed $Y \subset X$, $Y \in \mathcal{K}$.*

Let "rainy" be a property of points in spaces in $\mathcal{K}$ that passes up from closed subspaces; that is, whenever $p \in Y \subset X \in \mathcal{K}$ and Y is closed in X, if $p \in Y$ is rainy, then $p \in X$ is rainy.

Suppose that

base *whenever $\{p\} = X \in \mathcal{K}$, p is rainy; and that*

induct *for any $X \in \mathcal{K}$, there is a closed $Y \subset X$ such that all points in $X \setminus Y$ are rainy.*

Then all points in all spaces in $\mathcal{K}$ are rainy.

Definition 33. *The structure sheaf $\mathcal{O}_{\mathrm{Spec}^\sigma(R)}$ is a sheaf of difference rings is defined to have the same stalks R_p as the structure sheaf from the usual algebraic geometry. The coordinate ring of an open set U then consist of functions f on U such that*

- *the value $f(p)$ at a point p is in the stalk R_p at p; and*
- *f is everywhere locally given by ratios of elements of R.*

This topological space with this sheaf of difference rings is called an affine difference scheme *determined by R.*

As we noted in Section 2.2, σ extends canonically from R to the stalks R_p. The coordinate rings are then also difference rings. Furthermore, If R was well-mixed, then the stalks R_p also are well-mixed (Lemma 20), and then it is easy to see that so are the coordinate rings.

Beware that the obvious difference ring homomorphism from R to the global sections $\mathcal{O}_{\mathrm{Spec}^\sigma(R)}(\mathrm{Spec}^\sigma(R))$ **might might not be an isomorphism**!

Lemma 34. *(Lemma 2.7 from the paper.) If R is well-mixed, then the obvious difference ring homomorphism $\phi : R \to \mathcal{O}_{\mathrm{Spec}^\sigma(R)}(\mathrm{Spec}^\sigma(R))$ is injective. For non-zero $a \in R$, the set points where $\phi(a)$ is not locally constant and equal* 0 *is a non-empty closed subset of* $\mathrm{Spec}^\sigma(R)$.

Proof. The set of points where $\phi(a)$ is not locally constant and equal 0,

$$\{p \in \mathrm{Spec}^\sigma(R) : a_p \neq 0\} = \{p \in \mathrm{Spec}^\sigma(R) : Ann_R(a) \subset p\},$$

is the closed set corresponding to the ideal $Ann_R(a)$.

This set is non-empty iff $\phi(a) \neq 0$, iff there is some $p \in \mathrm{Spec}^\sigma(R)$ such that $Ann_R(a) \subset p$. By Lemma 23, $Ann_R(a)$ is a (proper) well-mixed difference ideal.

As "well-mixed" is preserved under unions of chains, there is a maximal (proper) well-mixed difference ideal p containing $Ann_R(a)$. By Lemma 25, p is transformally prime. □

As in algebraic geometry, $a \in p$ means that the value of the global section a at the point p is 0; and $a_p = 0$ means that the global section a is locally constant and equal to 0 on some neighborhood of p. So the geometric meaning of Lemma 2.7 is that for a non-zero $a \in R$, the set of points where a is locally-constant and zero is a proper open subset. `This smells like irreducible components to me...`

4.2. **Homomorphisms to difference fields, formulas, quantifier-free types.** The points of $\mathrm{Spec}^\sigma(R)$, transformally prime ideals of R, are the only points of $\mathrm{Spec}(R)$ at which the stalk of the structure sheaf of $\mathrm{Spec}(R)$ is a difference ring. They are also precisely the kernels of difference-ring homomorphisms from R to difference fields, so they encode isomorphism types of such homomorphisms onto their images. We explain this slogan in some detail.

Definition 35. *Given difference rings $S \leq R$ and a tuple $a \in R$,*

$$I_\sigma^R(a/S) := \{P(x) \in S[x]_\sigma : R \models P(a) = 0\} \trianglelefteq S[x]_\sigma.$$

Given a difference ring R and a tuple $a \in R$,

$$I_\sigma^R(a) := \pi^{-1}(I_\sigma^R(a/R_0)) \trianglelefteq \mathbb{Z}[x]_\sigma,$$

where R_0 is the subring of R generated by 1, and $\pi : \mathbb{Z} \to R_0$ is the ring unique homomorphism with $\pi(1) = 1$.

If R is generated as a difference ring by finitely many a_i, then $R \cong (\mathbb{Z}[x]_\sigma)/(I_\sigma^R(a))$.

If R is generated as a difference ring over a difference field k by finitely many a_i, then $R \cong (k[x]_\sigma)/(I_\sigma^R(a/k))$.

If $f : R \to S$ is a homomorphism of difference rings and $a \in R$ is some tuple, then $I_\sigma^R(a) \leq I_\sigma^S(f(a))$. If R, S, and f are over some difference field k, the same is true of the ideals over k: $I_\sigma^R(a/k) \leq I_\sigma^S(f(a)/k)$.

If $b \in L$ and L is a difference field, then $I_\sigma^L(b)$ is transformally prime; if L is over k, then $I_\sigma^L(b/k)$ is transformally prime.

If R is generated as a difference ring by a finite tuple a, a difference ring homomorphism $f : R \to L$ to a fixed difference field L is determined by $f(a)$, and the isomorphism type of $f : R \to f(R)$ is determined by $I_\sigma^L(f(a))$, a transformally prime difference ideal extending $I_\sigma^R(a)$. Conversely, given a transformally prime $J \trianglelefteq \mathbb{Z}[x]_\sigma)$ with $J \geq I_\sigma^R(a)$, the field of fractions of $L := (\mathbb{Z}[x]_\sigma))/J$ admits a homomorphism $f : R \to L$, given by $f(a) = x/J$. The same works over k.

Lemma 36. *Suppose that R is generated as a difference ring by a finite tuple a, and $b \in L$ is a tuple of the same length as a in some difference field L. There is a (necessarily unique) difference ring homomorphism $f : R \to L$ with $f(a) = b$ if and only if $I_\sigma^L(b) \geq I_\sigma^R(a)$.*

Similarly, if R is generated by a over a difference field k and L is over k, then such f over k exists if and only if $I_\sigma^L(b/k) \geq I_\sigma^R(a/k)$.

Since $I_\sigma^L(b)$ (resp., $I_\sigma^L(b/k)$) is transformally prime, it contains $I_\sigma^R(a)$ (resp., $I_\sigma^R(a/k)$) if and only if it contains the perfect closure of the same. Recall (see the proof of Lemma 30) that perfect ideals in $\mathbb{Z}[x]_\sigma$ or in $k[x]_\sigma$ are finitely generated as a perfect ideals.

Lemma 37. *Suppose that R is generated as a difference ring by a finite tuple a, and $b \in L$ is a tuple of the same length in a difference field L. Let $\{P_j : 1 \leq j \leq m\}$ generate (as a perfect ideal) the perfect closure of $I^R_\sigma(a)$, and let $\phi_{R,a}(x) := \wedge_{j=1}^m P(x) = 0$. There is a (necessarily unique) difference ring homomorphism $f : R \to L$ with $f(a) = b$ if and only if $L \models \phi_{R,a}(b)$.*

Similarly, if R is generated by a over a difference field k and L is over k, let P_j generate $I^R_\sigma(a/k)$ and again set $\phi_{R,a/k}(x) := \wedge_{j=1}^m P(x) = 0$. Then there is a (necessarily unique) difference ring homomorphism $f : R \to L$ over k with $f(a) = b$ if and only if $L \models \phi_{R,a/k}(b)$.

Slogan 38. *A finitely generated difference ring R together with a choice of generators corresponds to a quantifier-free formula; transformally prime ideals of R correspond to complete quantifier-free types in the theory of difference fields containing this formula.*

If R is instead finitely generated over a difference field k, then the formula is over k, and the types are in the theory of difference fields extending k.

4.3. **algebraically prime difference ideals.** Lemma 36 is just as true when L is an integral domain with a difference structure instead of a difference field, but the difference ideal $I^L_\sigma(b)$ is then only algebraically prime instead of transformally prime. Some of the deep/hard difference algebra in the paper requires this more general setting. One (but I think not the only) purpose is to work over $\mathbb{Z}$ in order to work across all positive characteristics. In this setting, *well-mixed* replaces *perfect* (see Lemma 27). One difficulty of this more general setting is that well-mixed ideals need not be finitely generated as well-mixed ideals, so there is no analog of Lemma 37.

5. Leftovers

5.1. **From Zoe's exp3.** Small leftovers that maybe should be folded in:

- Definition of "inversive", unique inversive closures: $I + \sigma(R) = R$ doesn't smell like an interesting property of ideals.
- Another corollary of Zoelem, going up/going down from minimal transformal primes; 1.11 in exp3.
- 1.12.1, 1.12.2, and 1.12.4: more quotations from Cohn.
- 1.13 about $[\sigma^k]V$, which I don't understand.

Section 2 of exp3 about dimensions might admit model-theoretic simplifications using my Section 4.2?