Assumptions:
- Fix a prime p.
- All rings are p-local, i.e. p is an element of the Jacobson radical.
- All ideals are finitely generated.

Distinguished Elements

Definition 1. Let $(A, \delta) \in \mathbf{Ring}_\delta$. An element $x \in A$ is said to be ***distinguished*** if $\delta(x) \in A^\times$. ⌟

Remark. An alternative definition exists, which states that $x \in A$ is distinguished if $(p, x, \delta(x)) = A$. We will almost exclusively look at distinguished elements which lie in $\mathrm{Rad}(A)$, in which case both definitions are equivalent.

Proposition 2. *Let $f: (A, \delta) \to (A', \delta')$ be a morphism in $\mathbf{Ring}_\delta$ and let $x \in A$ be distinguished. Then $f(x) \in A'$ is distinguished. In particular, if $(A, \delta) = (A', \delta')$ and $f = \varphi$, the p-locality of A implies that $x \in A$ is distinguished if and only if $\varphi(x) \in A$ is distinguished.*

Example 3. We discuss two examples:

- Let $A = \mathbb{Z}_{(p)}$ (localisation), with a delta structure given by $\delta: x \mapsto \frac{x - x^p}{p}$. Then $\delta(p) = 1 - p^{p-1} \in \mathbb{Z}_{(p)}^\times$. As $\delta(n) = \frac{n - n^p}{p}$ for any integer n and delta ring (A, δ), p is distinguished for any p-local delta ring. In particular (the case where the ring has p-torsion), zero divisors can be distinguished.
- Let $A = \mathbb{Z}_p[[q-1]]$, with a delta structure uniquely determined by $\delta(q) = 0$ (or $\varphi(q) = q^p$). Let $d = \frac{q^p - 1}{q - 1} = \sum_{i=0}^{p-1} q^i$, then d is mapped to the distinguished element p under the δ-map $A \to \mathbb{Z}_p$ given by $q \mapsto 1$. As the ring is $(q-1)$-adically complete, d is distinguished as well. ⌟

Lemma 4. *Let R be a perfect $\mathbb{F}_p$-algebra.*

(i) An element $d = \sum_{i \geq 0} [d_i] p^i \in W(R)$ is distinguished if and only if $d_1 \in R^\times$.

(ii) Distinguished elements in $W(R)$ are not zerodivisors.

(iii) For distinguished elements $d \in W(R)$, we get $(W(R)/d)[p^\infty] = (W(R)/d)[p]$.

Proof. (i) Let $d = \sum_{i \geq 0} [d_i] p^i \in W(R)$; we have $\varphi(d) = \sum_{i \geq 0} [d_i^p] p^i$ and $d^p = [d_0^p] \bmod p^2$. Hence $\delta(d) = \frac{\varphi(d) - d^p}{p} = [d_1^p] \bmod p$. As $p \in \mathrm{Rad}(W(R))$, the result follows.

(ii) Suppose $d \in W(R)$ is distinguished and $df = 0$ for some nonzero f. Then $0 = \delta(df) = d^p \delta(f) + \delta(d) f^p + p\delta(d)\delta(f) = f^p \delta(d) + \delta(f)\varphi(d)$. Multiplying with $\varphi(f)$ yields $f^p \varphi(f) \delta(d) = 0$, and as d is distinguished $f^p \varphi(f) = 0$. It follows that $f^{2p} = 0 \bmod p$, and as $W(R)/p$ is reduced, $f = 0 \bmod p$, say $f = pf'$. As $W(R)$ is p-torsionfree, $df' = 0$. We see that f must be zero, otherwise it would be an 'infinite power of p', which is not possible as $W(R)$ is p-adically separated.

(iii) It suffices to show that $(W(R)/d)[p^2] = (W(R)/d)[p]$. Hence, let $f, g \in W(R)$ such that $p^2 f = gd$; we show that $pf \in dW(R)$. As $gd \in p^2 W(R)$, the image $\delta(gd) = g^p \delta(d) + \delta(g)\varphi(d) \in pW(R)$. Multiplying this by $\varphi(g)$, we get that $g^p \delta(d) \varphi(g) \in pW(R)$. Again, as $\delta(d)$ is a unit, $g^{2p} = 0 \bmod p$, hence $g = 0 \bmod p$. This shows that $pf \in dW(R)$. □

Example 5 (Universal distinguished element)**.** We construct a universal p-local δ-ring equipped with a distinguished element. Localise $\mathbb{Z}\{d\}$ along the multiplicative subset generated by the elements $\{\delta(d), \varphi(\delta(d)), \varphi^2(\delta(d)), \dots\}$, then localise the resulting ring along $V(p)$. ⌟

As long as $x \in \mathrm{Rad}(A)$, we have the following:

The distinguishedness of x is purely dependent on the ideal (x).

Lemma 6. *Let $(A, \delta) \in \mathbf{Ring}_\delta$. Let $f \in \mathrm{Rad}(A)$ be distinguished and let $u \in A^\times$, then uf is distinguished.*

Proof. Plainly use the definition of δ to get

$$\delta(uf) = u^p\delta(f) + \delta(u)f^p + p\delta(f)\delta(u).$$

The first term is a unit and the latter two terms lie in $\mathrm{Rad}(A)$, hence $\delta(uf)$ is a unit, hence uf is distinguished. □

Lemma 7. *Let $(A, \delta) \in \mathbf{Ring}_\delta$. Let $f \in \mathrm{Rad}(A)$ and $h \in A$ be such that fh is distinguished, then f is distinguished and $h \in A^\times$.*

Proof. Another writing exercise:

$$\delta(fh) = f^p\delta(h) + \delta(f)h^p + p\delta(f)\delta(h).$$

By the same argument as in Lemma 6, $\delta(f)h^p$ is a unit. Of course this is only possible if f is distinguished and h is a unit. □

Proposition 8. *Let $(A, \delta) \in \mathbf{Ring}_\delta$ and let $f \in \mathrm{Rad}(A)$. Then f is distinguished if and only if $p \in (f, \varphi(f))$.*

Proof. ($\Longrightarrow$) This follows directly from $\varphi(f) = f^p + p\delta(f)$.
($\Longleftarrow$) We show that $(p, f, \delta(f)) = A$ (which is equivalent to showing that $\delta(f)$ is a unit, considering $p, f \in \mathrm{Rad}(A)$). Assume this is not the case; we may then even assume that $\delta(f) \in \mathrm{Rad}(A)$ (by replacing A with its localisation along $V(p, f, \delta(f)) \subseteq \mathrm{Spec}(A)$). However, the assumption $p \in (f, \varphi(f))$ implies the existence of $x, y \in A$ such that $xf + y\varphi(f) = p$. Rewriting this expression yields $p(1 - y\delta(f)) = f(x + yf^{p-1})$. However, the left hand side is now distinguished by Lemma 6 and the fact that $\delta(f) \in \mathrm{Rad}(A)$. Lemma 7 in turn implies that f must be distinguished, so the assumption that it was not distinguished was nonsense. □

We generalise this idea from principal ideals to *locally principal ideals.*
Definition 9. Let $R \in \mathbf{Ring}$. An ideal I is ***locally principal*** if $I_\mathfrak{m} = IR_\mathfrak{m}$ is principal for all maximal ideals $\mathfrak{m} \subseteq R$. ⌟
Corollary 10. *Let $(A, \delta) \in \mathbf{Ring}_\delta$ and let $I \subseteq A$ be an ideal such that $I \subseteq \mathrm{Rad}(A)$. Then the following are equivalent:*

(i) $p \in I + \varphi(I)A$;

(ii) There exists a faithfully flat δ-map $A \to A'$, where A' is a finite product of localisations of A along φ-stable multiplicative subsets and $IA' = (f)$ for some distinguished $f \in \mathrm{Rad}(A')$.

If both conditions are satisfied, then $p \in I^p + \varphi(I)A$.

Proof. There are elements $g_1, \dots, g_r \in R$ such that $(g_1, \dots, g_r) = A$ and all $I_{g_i} = IA_{g_i}$ are principal (this can be shown using compactness of $\operatorname{Spec}(A)$ and the fact that we can cover $\operatorname{Spec}(A)$ by distinguished opens on which I is trivial). Write $B = \prod_i A_{g_i}$, then the canonical map $A \to B$ is faithfully flat and IB is principal, say $IB = (f)$. Localise B along the closed subset $V(p, f) \subseteq \operatorname{Spec}(B)$; the resulting ring A' will be (p, f)-local and a finite product of localisations of A along φ-stable multiplicative subsets. Hence, it is will inherit a unique δ-structure from A such that $A \to A'$ is a δ-map. It remains to show that this map is faithfully flat. The composite of flat maps $A \to B \to A'$ is flat. It is faithfully flat as the induced map $\operatorname{Spec}(A') \to \operatorname{Spec}(A)$ is surjective: the image contains $V(p, I)$, hence all closed points as $(p, I) \subseteq \operatorname{Rad}(A)$ and it is closed under generalisation by flatness. The fact that f is distinguished follows from Proposition 8.

Suppose now that both conditions are satisfied. The property that $p \in I^p + \varphi(I)A$ may be checked after a faithfully flat base change, so assume $I = (f)$ is principal. Then $\delta(f)$ is a unit, and $\varphi(f) = f^p + p\delta(f)$ implies that $p \in (f^p, \varphi(f))$. □

Prisms

Definition 11. Define the category of δ-pairs $\mathscr{P}$: its objects are pairs (A, I), where $A \in \mathbf{Ring}_\delta$ and $I \subseteq A$ is an ideal; its morphisms $(A, I) \to (B, J)$ are δ-morphism $A \to B$ that map I into J. ⌟

Definition 12. A pair $(A, I) \in \mathscr{P}$ is a ***prism*** if

(i) I is locally principal, generated by a nonzerodivisor (i.e. I defines a Cartier divisor on $\operatorname{Spec} A$, I is invertible);

(ii) A is derived (p, I)-complete;

(iii) $p \in I + \varphi(I)A$. ⌟

Remark. Derived (p, I)-completeness of A means in particular that $(p, I) \subseteq \operatorname{Rad}(A)$, hence also $\varphi(I) \subseteq \operatorname{Rad}(A)$. The property $p \in I + \varphi(I)A$ can be interpreted in a geometric way: the closed subschemes $\varphi^{-1}V(I)$ and $V(I)$ of $\operatorname{Spec} A$ only meet in characteristic p.

Definition 13. A map $(A, I) \to (B, J)$ of prisms is ***(faithfully) flat*** if $A \to B$ is (p, I)-completely (faithfully) flat (which means that $A/(p, I) \to B \otimes^L_A A/(p, I)$ is (faithfully) flat). ⌟

Definition 14. A prism (A, I) is called

- ***perfect*** if A is perfect;
- ***bounded*** if A/I has bounded p-torsion;
- ***crystalline*** if $I = (p)$. ⌟

Example 15.
- A pair $(A, (p)) \in \mathscr{P}$ is a (crystalline, bounded) prism if and only if A is p-adically complete and p-torsionfree;
- Both cases in Example 3 give rise to a (bounded) prism $A, (d))$. [NB: We might need to complete A.] ⌟

Proposition 16. *Let $(A, I) \in$ **Prism**. The ideal $\varphi(I)A$ is principal, generated by a distinguished element.*

Proof. By Corollary 10, write $p = a + b$, with $a \in I^p$ and $b \in \varphi(I)A$. We show that $\varphi(I)A = bA$, in other words the map $A \to \varphi(I)A$ given by $1 \mapsto b$ is surjective. We may do so after faithfully flat base change, so by Corollary 10 we may assume that I is principal; say $I = (f)$ with $f \in \mathrm{Rad}(A)$ distinguished. After writing $a = xf^p$ and $b = \varphi(f)y$, it remains to prove that y is a unit. Suppose this is not the case, then we may assume $y \in \mathrm{Rad}(A)$ by localising along $V(p, f, y) \subseteq \mathrm{Spec}\, A$. Writing out $\varphi(f)$ we find that $p = a + b$ is equivalent to $p(1 - y\delta(f)) = f(f^{p-1}(x + y))$. The fact that p, f are distinguished and $y \in \mathrm{Rad}(A)$ imply (with Lemma 7) that $f^{p-1}(x + y)$ is a unit. This is impossible, as $f \in \mathrm{Rad}(A)$. □

The following corollary is now obvious.
Corollary 17. *If (A, I) is a perfect prism, then I is principal, generated by a distinguished element.*

Finally we discuss rigidity of prisms.
Theorem 18. *Let $(A, I) \to (B, J)$ be a morphism of prisms. Then $I \otimes_A B \cong J$. In particular, $IB = J$. Conversely, if B is a derived (p, I)-complete A-algebra with δ-structure, then $(B, IB) \in$ **Prism** if and only if $B[I] = 0$.*

Proof Sketch. As $I \otimes_A B, J$ are invertible, it suffices to show that $I \otimes_A B \to J$ is surjective, or equivalently that $IB = J$. By faithfully flat descent and Corollary 10, it suffices to prove the theorem for prisms (A, d) and (B, e), where $d \in \mathrm{Rad}(A)$ and $e \in \mathrm{Rad}(B)$ are distinguished. However, now $d = ex$ for some $x \in B$, which is a unit by Lemma 7. Hence, $(d)B = (e)$.

Note that $B[I] = 0$ if and only if the map $I \otimes_A B \to IB$ is an isomorphism. If (B, IB) is a prism $I \otimes_A B \to IB$ is an isomorphism by the previous part. If $I \otimes_A B \to IB$ is an isomorphism, then IB is invertible, and checking the definition yields that (B, IB) is a prism. □