PROBLEM SET #3

(1) Is $\mathbb{Z}[\sqrt[3]{37}]$ a regular ring? What about $\mathbb{Z}[\sqrt[3]{43}]$?

Proof. Write $R = \mathbb{Z}[\sqrt[3]{37} \cong \mathbb{Z}[x]/(x^3 - 37)$. First, we show that $R_{\mathfrak{p}}$ is regular for many primes $\mathfrak{p}$. The prime ideals of R correspond to prime ideals of $\mathbb{Z}[x]$ containing $(x^3 - 37)$. Note that $x^3 - 37$ is irreducible by Eisenstein's criterion, so it is prime. Then the prime ideals of $\mathbb{Z}[x]$ properly containing $(x^3 - 37)$ must be of the form $(p, g(x))$, where g is a polynomial that divides $x^3 - 37$ modulo p. For $R_{\mathfrak{p}}$ to not be regular, we must have $x^3 - 37 \in (p, g)^2 \subseteq (p, g^2)$. Then for degree reasons, g must be linear, so of the form $x - a$, and a must be a double root of $x^3 - 37$ in $\mathbb{F}_p$. But then $x - a$ divides $\frac{dg}{dx} = 3x^2$, so $a \equiv 0 \bmod p$ unless $p = 3$, but if 0 is a root of $x^3 - 37$ in $\mathbb{F}_p$, then $p = 37$, but $x^3 - 37 \notin (37, x)^2$, so we must have $p = 3$, and then $a \equiv 1 \bmod p$.

Thus, we reduce to checking whether $x^3 - 37 \in (3, x-1)^2$. We have $(3, x-1)^2 = (9, 3(x-1), (x-1)^2)$. By long division, write $x^3 - 37 = (x+2)(x-1)^2 + 3x - 39$. Then $3x - 39 = 3(x-1) - 36 = 3(x-1) - 4 \cdot 9$, so $x^3 - 37 \in (3, x-1)^2$, and $\mathbb{Z}[\sqrt[3]{37}]_{(3, 1+\sqrt[3]{37})}$ and hence $Z[\sqrt[3]{37}]$ are not regular.

For $S = \mathbb{Z}[\sqrt[3]{43}]$, everything is the same up to checking whether $x^3 - 43 \in (3, x-1)^2$. By long division, write $x^3 - 43 = (x+2)(x-1)^2 + 3x - 45$. Then $3x - 45 = 3(x-1) - 42 = 3(x-1) - 5 \cdot 9 + 3$, so $x^3 - 43 \equiv 3 \mod (3, x-1)^2$. But $3 \notin (3, x-1)^2$, so $x^3 - 43 \notin (3, x-1)^2$, and hence $\mathbb{Z}[\sqrt[3]{43}]$ is regular. □

(2) Let R be an A-algebra, $f(x_1, \ldots, x_n) \in A[x_1, \ldots, x_n]$ a polynomial with coefficients in A, and $r_1, \ldots, r_n, s_1, \ldots, s_n \in R$.
  (a) Prove the *chain rule* for the universal derivation: $d_{R|A}(f(r_1, \ldots, r_n)) = \sum_i \frac{df}{dx_i}(r_1, \ldots, r_n) dr_i$.
  (b) Prove the *Taylor expansion* formula: $f(r_1 + s_1, \ldots, r_n + s_n) = \sum_{\alpha \in \mathbb{N}^n} \frac{1}{|\alpha|!} \frac{d^{|\alpha|} f}{dx_1^{\alpha_1} \cdots dx_n^{\alpha_n}}(r_1, \ldots, r_n) s_1^{\alpha_1} \cdots s_n^{\alpha_n}$.

(3) Facts about p-bases/ p-degree:
  (a) Let L be a field of positive characteristic. Let T be a p-basis for L. Show that for any e, the set $T^{[<p^e]}$ is a basis for L.
  (b) Let $K \subseteq L$ be a finite extension of fields of positive characteristic. Show that $p\deg(K) = p\deg(L)$.
  (c) Let $L = K(x_1, \ldots, x_m)$ be a field of rational functions in m variables over K. Show that $p\deg(L) = p\deg(K) + m$.

Proof ideas. (a) By induction on e, with $e = 1$ as the definition. If the claim is true for e, so $T^{[<p^e]}$ is a basis for L/L^{p^e}, taking pth powers we have that $(T^p)^{[<p^e]}$ is a basis for $L^p/L^{p^{e+1}}$. But $T^{[<p^{e+1}]} = (T^p)^{[<p^e]} T^{[<p]}$ (i.e., the first set is the set of products of the two sets on the right-hand side), so from field theory, the left hand side is a basis for $L/L^{p^{e+1}}$.
  (b) Consider the diagram

$$\begin{tikzcd} & L & \\ L^p \arrow[ur] & & K \arrow[ul] \\ & K^p \arrow[ul] \arrow[ur] & \end{tikzcd}$$

From field theory $[L:K][K:K^p] = [L^p:K^p][L:L^p]$, and $[L^p:K^p] = [L:K]$, so $[K:K^p] = [L:L^p]$. Then $p\deg(K) = \log_p([K:K^p]) = \log_p([L:L^p]) = p\deg(L)$.

(c) Take a p-basis T for K. One checks that $T \cup \{x_1, \dots, x_m\}$ is a p-basis for L.

□

(4) Let k be a field of positive characteristic with a finite p-basis, R be a finitely generated k-algebra, and $\mathfrak{p} \subseteq \mathfrak{q}$ be prime ideals of R. Show that

$$\dim R_{\mathfrak{q}}/\mathfrak{p}R_{\mathfrak{q}} = p\deg(\kappa(\mathfrak{p})) - p\deg(\kappa(\mathfrak{q})).$$

Proof. We will show that $\dim(R/\mathfrak{p}) = p\deg(\kappa(\mathfrak{p})) - p\deg(k)$; the formula above then follows. We can replace R by $R/\mathfrak{p}$ and assume R is a domain and $\mathfrak{p} = 0$, Take a Noether normalization A for R. By part (2) of the previous problem, $p\deg(\kappa(\mathfrak{p})) = p\deg(\mathrm{frac}(R)) = p\deg(\mathrm{frac}(A))$. By part (3) of the previous problem, $p\deg(\mathrm{frac}(A)) = \dim(A) + p\deg(k) = \dim(R) + p\deg(k)$. The conclusion then follows. □

(5) Let K be a field.

(a) Let $R = K[x]$ be a polynomial ring in one variable and $M = R^{\oplus \mathbb{N}}$ be a free R-module on a countable basis. Compute the (x)-adic completion of M.

(b) Let $R = K[x_1, x_2, \dots]$ be a polynomial ring in countably many variables and $\mathfrak{m} = (x_1, x_2, \dots)$. Describe the elements of $\hat{R}^{\mathfrak{m}}$. Find an element in the maximal ideal of $\hat{R}^{\mathfrak{m}}$ that is *not* an element of $\mathfrak{m}\hat{R}^{\mathfrak{m}}$.

(6) Let $K \subseteq L$ be an extension of fields.

(a) Suppose that L is a finitely generated over K as fields. Show that L is formally unramified over K if and only if the extension is separable algebraic.

(b) Show that the finite generation hypothesis is strictly necessary in part (1).

Proof. (a) We just need to show that unramified implies separable algebraic. Any transcendental element is a p-independent set, which contradicts unramified, so unramified implies algebraic. Write $K \subseteq F \subseteq L$, with $F \subseteq L$ purely inseparable. By finite generation plus algebraic, this is finite. We can then choose some f with $f \in L \smallsetminus F$ and $f^p \in F$ using finiteness. Then f is p-independent in L over F, contradicting unramified.

(b) Take $K = \mathbb{F}_p(t)$ and $L = \bigcup_{e \in \mathbb{N}} \mathbb{F}_p(t^{1/p^e})$.

□