MATH 7220 Homework 9

Andrea Bourque

April 2022

1 Problem 17.1

Show that a discrete valuation ring is integrally closed in its fraction field.

Proof. We take the definition of a discrete valuation ring (DVR) A to be an integral domain with a discrete valuation ν on its fraction field K, such that $A = \{x \in K : \nu(x) \geq 0\}$. We will show that A is a principal ideal domain (PID). We use the facts that a PID is a unique factorization domain (UFD), and that any UFD is integrally closed. (First fact is found in Dummit and Foote, chapter 8, Theorem 14. Second is given as an example in Dummit and Foote Chapter 15 section 3; also found in the remarks after Proposition 5.12 in Atiyah-MacDonald.) Thus, a DVR is integrally closed from the chain of implications: DVR $\to$ PID $\to$ UFD $\to$ integrally closed.

Take a non-trivial ideal I in A. Since the set $\nu(I) \subset \mathbb{Z} \cup \{\infty\}$ is bounded below, we can take an element $t \in I$ of minimal valuation, so $\nu(x) \geq \nu(t)$ for any $x \in I$. Since I is non-trivial, $\nu(t) < \infty$, so $t \neq 0$. For any $x \in I$, $x/t \in K$ satisfies $\nu(x/t) = \nu(x) - \nu(t) \geq 0$, so $x/t \in A$. Then $x \in (t)$, so $I \subset (t)$. But since $t \in I$, $(t) \subset I$. Thus $I = (t)$. □

2 Problem 20.1

Let $A = \mathbb{Z}[x]$. Consider the maximal ideal $\mathfrak{m} = (p, x)$ for a prime number p. Describe the $\mathfrak{m}$-adic completion of A.

Proof. We claim that $\hat{A} = \mathbb{Z}_p[[x]]$, the formal power series over the p-adic integers. First, we show that the $\mathfrak{m}$-adic topology is the same as the topology determined by (p^n, x^n). This follows from the inclusions $(p, x)^{2n} \subset (p^n, x^n) \subset (p, x)^n$, where the first inclusion follows since for any $p^m x^{2n-m}$, either $m \geq n$ or $2n - m \geq n$. Thus the completion with respect to the filtration determined by (p^n, x^n) will be the same as the $\mathfrak{m}$-adic completion. Denote by A_n the ring $A/(p^n, x^n) = (\mathbb{Z}/p^n\mathbb{Z})[x]/(x^n)$. We wish to show $\varprojlim A_n = \mathbb{Z}_p[[x]]$.

Let (f_n) be a compatible sequence of elements in (A_n). In particular, write $f_n = a_{n,1} + a_{n,2}x + ... + a_{n,n-1}x^{n-1}$ where the $a_{m,n} \in \mathbb{Z}/p^m\mathbb{Z}$ and $(a_{n,n}, a_{n+1,n}, ...)$ is a compatible sequence. There is a unique way to turn the $a_{m,n}$ for fixed n into $\mathbb{Z}_p$ coefficients. We define $a_{m,n} = a_{n,n} \mod p^m$ for $m < n$ to give the element $a_n = (a_{1,n}, a_{2,n}, ...) \in \mathbb{Z}_p$. Then we define $f = a_1 + a_2 x + ... \in \mathbb{Z}_p[[x]]$. This construction gives a map $\varprojlim A_n \to \mathbb{Z}_p[[x]]$, sending (f_n) to f. We can similarly define a map $\mathbb{Z}_p[[x]] \to \varprojlim A_n$ by taking f to the sequence $f_n = f \mod (p^n, x^n)$. The two maps are inverse to each other. It is easy to see that the latter map is a morphism, since reduction mod an ideal preserves algebraic structure. Thus $\hat{A} = \varprojlim A_n \equiv \mathbb{Z}_p[[x]]$. □

3 Problem 21.1

Use Hensel's lemma to find a solution to $x^2 - 3 = 0$ in the 13-adic numbers. Give the expansion up to the 13^3 term.

Proof. First we solve $x^2 - 3 \equiv 0 \bmod 13$. Note that $x^2 - 3 \equiv x^2 - 16 = (x-4)(x+4) \equiv (x-4)(x-9)$, so we have $x \equiv 4, 9$. Since the question asks for "a" solution, we just focus on $x \equiv 4$. Since $2(4) \not\equiv 0 \bmod 13$, we can lift to the next root. We solve $(4 + 13t)^2 \equiv 3 \bmod 13^2$, or $13 + 104t \equiv 0 \bmod 13^2$. Then $1 + 8t \equiv 0 \bmod 13$, which gives $t = 8$. Next we look at $(108 + 13^2 t)^2 \equiv 3 \bmod 13^3$, or $676 + 1352t \equiv 0 \bmod 13^3$. This gives $4 + 8t \equiv 0 \bmod 13$, so $t = 6$. Thus we have $x = (4, 8, 6, ...)$. □

4 Problem 21.3

Show that any $u \equiv 1\ (8)$ in $\mathbb{Z}_2$ is a square in $\mathbb{Z}_2$.

Proof. We use the generalization of Hensel's lemma described in Problem 21.2. Let $f(X) = X^2 - u$. Suppose $x \in \mathbb{Z}_2$ satisfies $f(x) \equiv 0 \mod 2^n = 8$. Note $n = 3$. Then $x^2 \equiv 1 \mod 8$, from which we can only conclude $x \equiv 1 \mod 2$. However, this means that $k = \nu_2(f'(x)) = \nu_2(2x) = 1$. Then we have the condition $0 \leq 2k < n$. Therefore there is a solution to $f(y) = 0$ in $\mathbb{Z}_2$, meaning $u = y^2$ is a square. □