ON THE PRIME SPECTRUM OF $\mathbb{Z}_p[T]$

JUAN SERRATOS

Abstract. In 1966, David Mumford created photo of a so-called *arithmetic surface*: a drawing of $\operatorname{Proj}\mathbb{Z}[X,Y]$ in his book, *Lectures on Curves on an Algebraic Surface*. In following, he created a photo of $\operatorname{Spec}\mathbb{Z}[T]$ for his 1988 book, *The Red Book of Varieties and Schemes*. The photos present something that comes from the out the layers of abstraction in a clear and pleasant manner. Taking inspiration from Mumford, we create a drawing similar for $\operatorname{Spec}\mathbb{Z}_p[T]$, which has a lot of similarities with $\operatorname{Spec}\mathbb{Z}[T]$. In the end, we get that $\operatorname{Spec}\mathbb{Z}_p[T]$ is essentially a union $\operatorname{Spec}\mathbb{F}_p[T]$ and $\operatorname{Spec}\mathbb{Q}_p[T]$.

1. Introduction

1.1. **Mumford's picture.** The reason for this article is to create a photo of the prime spectrum of $\mathbb{Z}_p[T]$, in a satisfactory manner. There are a few difficulties in doing this because for a choice of prime p, we have a different situation of $\mathbb{Q}_p[T]$ for other primes, but this is expected. A central example of this surrounds the polynomial $f(T) = T^2+1$, which Mumford grounded his depiction of $\operatorname{Spec}\mathbb{Z}[T]$ with: For a prime p with $p \equiv 1 \pmod 4$, the polynomial $f(T)$ admits a solution in $\mathbb{Q}_p[T]$, meaning that it is reducible as $f(T)$ is quadratic, so we can't use $f(T) = T^2+1$ in a satisfactory way as Mumford did for $\operatorname{Spec}\mathbb{Z}[T]$.

Mumford's picture of $\operatorname{Spec}\mathbb{Z}[T]$, as shown in Figure 1.1, surrounds quotients of $\mathbb{Z}[T]$. Using a technique in algebraic geometry (which we'll use for $\operatorname{Spec}\mathbb{Z}_p[T]$ later), or instead doing this by hand, we find out that $\operatorname{Spec}\mathbb{Z}[T]$ is in bijection with $\operatorname{Spec}\mathbb{Z}/p\mathbb{Z}[T]$ and $\operatorname{Spec}\mathbb{Q}[T]$.[1] In relation to Mumford's picture, the points we depict are precisely all the points of $\operatorname{Spec}\mathbb{Z}[T]$, and we give *greater* importance to those that say more once modded out of $\mathbb{Z}[T]$. Additionally, Mumford has made the point of depicting the ideals of form (p) with some volume as they will contain the points below them on their respective horizontal line, and the same is true of (T^2+1) and (T); recall that when talking about geometry, we invert inclusions. For the maximal ideals in $\mathbb{Z}[T]$, we have $(p, f(T))$ where $f(T)$ is $\mathbb{F}_p$-irreducible and as we quotient them with $\mathbb{Z}[T]$ we get: $\mathbb{Z}[T]/(p, f(T)) = (\mathbb{Z}/p\mathbb{Z}[T])/(f(T)) = \mathbb{F}_p[T]/(f(T))$ which results in a field. We cannot depict these all so we just depict the linear polynomials $g(T)$, which are maximal as $\mathbb{Z}[T]/(p, g(T)) = \mathbb{F}_p[T]/(g(T)) = \mathbb{F}_p$, where this last "equality" comes from evaluation of $g(T) = T - a$ with $\varphi\colon \mathbb{F}_p[T] \to \mathbb{F}_p$ by $\varphi(f(T)) = f(a)$.

Mumford additionally wanted us to think of $\mathbb{A}^1_{\mathbb{Z}}$ as a union of the $\mathbb{A}^1_{\mathbb{F}_p}$ lines and $\mathbb{A}^1_{\mathbb{Q}}$ whereby $\mathbb{A}^1_{\mathbb{Q}}$ behaves as a horozontal line that interacts with the union of vertical lines of $\mathbb{A}^1_{\mathbb{F}}$, as outlined in his newest draft, *Algebraic Geometry II (a penultimate draft)* (see [Mum15, Pages $119-121$, §4.1]). The main interaction still deals with taking quotients and inspecting the results. For example, Mumford anchors this philosophy by passing $f(T) = T^2+1$ throughout the lines of $\mathbb{A}^1_{\mathbb{F}_p}$ in the vertical manner and comparing *significances* whether or not drawing big and empty circles ("blips"). He draws a blip, in respect to $f(T)$, on the $\mathbb{A}^1_{\mathbb{F}_7}$ line since $\mathbb{Z}_p[T]/(7, T^2+1) = (\mathbb{Z}/7\mathbb{Z}[T])/(T^2+1) = \mathbb{F}_7[T]^1/(T^2+1) = \mathbb{F}_{7^2}$; note that $f(T)$ remains irreducible in $\mathbb{F}_7[T]$ as it admits not roots. Whereas, he draws no blips on $\mathbb{A}_{\mathbb{F}_5}$ or $\mathbb{A}^1_{\mathbb{F}_2}$ as $\mathbb{Z}[T]/(2, T^2+1) = \mathbb{F}_2[T]/(T^2+1)$ and $\mathbb{Z}[T]/(5, T^2+1) = \mathbb{F}_5[T]/(T^2+1)$ are not even fields: $f(1) = (1)^2+1 \equiv 0 \pmod 2$ in $\mathbb{F}_2$ and $f(2) = (2)^2+1 \equiv 0 \pmod 5$ in $\mathbb{F}_5$, so neither remain irreducible after processing quotients.

Our main issue is in whether or not to stay close to Mumford's picture of $\operatorname{Spec}\mathbb{Z}[T]$ by also anchoring our depiction with $f(T) = T^2+1$ and considering the specific case of $p \not\equiv 1 \pmod 4$,

---

[1] As such we classify $\operatorname{Spec}\mathbb{Z}[T]$ as:

(i) (0),
(ii) (p) for p prime,
(iii) $(f(T))$ with $f(T)$ irreducible in $\mathbb{Z}[T]$, and
(iii) $(p, f(T))$ where p is prime and $f(T) \in \mathbb{F}_p[T]$ irreducible.

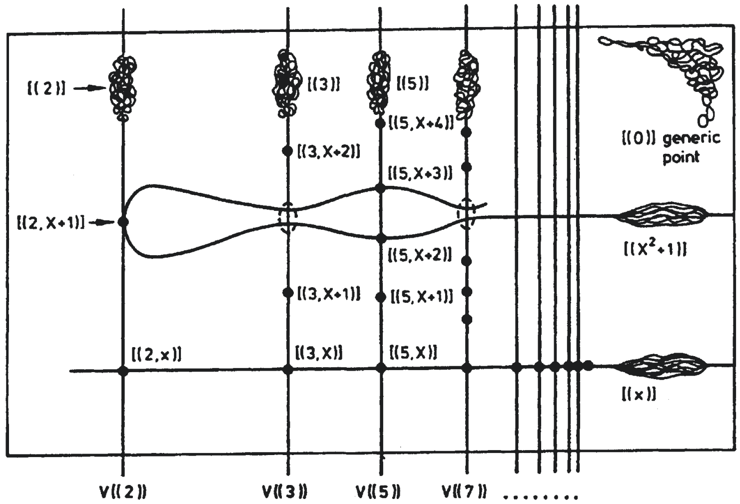

FIGURE 1. Depiction of $\operatorname{Spec}\mathbb{Z}[T]$ ([Mum99, Page. 75, §II.1]).

which is in some ways *unnatural* as we're also forcing the quotients $\mathbb{Z}[T]$ with $(p, f(T))$ to always result in a quadratic extension of $\mathbb{F}_p$. That is, for $p > 2$ and $p \not\equiv 1 \pmod 4$, we have $\mathbb{Z}[T]/(p, T^2+1) = \mathbb{F}_p[T]/(T^2+1) = \mathbb{F}_{p^2}$. For the interested reader, we draw $\operatorname{Spec}\mathbb{Z}_p[T]$ for $p \not\equiv 1 \pmod 4$ in §3.2. But we also want to make a more natural choice of a polynomial $\ell(T)$ which to anchor our depiction of $\operatorname{Spec}\mathbb{Z}_p[T]$; this is what we explain in §3.3.

Lastly, there a disappointing note: The intersection of $\operatorname{Spec}\mathbb{Q}_p[T]$ and $\operatorname{Spec}\mathbb{Q}[T]$ share a common quadratic polynomial, namely, for prime p, we have $q(T) = T^2 - p \in \operatorname{Spec}\mathbb{Q}_p[T] \cap \operatorname{Spec}\mathbb{Q}[T]$, yet in terms of our picture of $\operatorname{Spec}\mathbb{Z}_p[T]$, it isn't that fascinating. This is because $\mathbb{Z}_p[T]/(p, T^2-p) = (\mathbb{Z}_p/p\mathbb{Z}_p[T])/(T^2-p) = \mathbb{F}_p[T]/(T^2-p) = \mathbb{F}_p[T]/(T^2) = \mathbb{F}_p \times \mathbb{F}_p$; the polynomial $q(T)$ sees a desert of $\mathbb{A}^1_{\mathbb{Z}_p}$ as its water is not capable of stretching to form an oasis.

1.2. **Outline.** In the following section, we give some background to the *ring of p-adic integers* and as well as the *p-adic numbers*. It's essential to know two reformulations of Gauss' Lemma and Eisenstein, which we state and prove, to think about irreducibility of polynomials in $\mathbb{Z}_p[T]$. In addition, we state simply state Hensel's Lemma and refer the reader to online sources for the proof. In §3, we establish, somewhat quickly, what $\operatorname{Spec}\mathbb{Z}_p[T]$ is set-theoretically; this comes from a well-known technique from algebraic geometry in using fibres of maps, namely, we look at the fibres of the induced map $\pi\colon \operatorname{Spec}\mathbb{Z}_p[T] \to \operatorname{Spec}\mathbb{Z}_p$. Lastly, we present two depictions as outlined in the end of the previous section, and give some of our reasoning as to what the picture says and why it was chosen in such a way.

2. $\mathbb{Z}_p$ AND $\mathbb{Q}_p$

2.1. **Definitions and Basics.** One has many ways to start to talk about the p-adics. There's the more "analytic" construction that describes the p-adic numbers as being formal power series expressions, that is, $\mathbb{Q}_p := \{\sum_{k=n}^{\infty} a_n p^n \colon a_n \in \mathbb{F}_p\}$, and $\mathbb{Z}_p$ is the subring of $\mathbb{Q}_p$ for which the power series expressions begin at $n = 0$. For our purposes, we won't dedicate any more time this route, but instead we're going to describe $\mathbb{Z}_p$ as a projective limit and its discrete valuation ring description. The *ring of p-adic integers* is defined as the projective limit $\mathbb{Z}_p := \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ given by the sequence of of ring maps

$$\begin{tikzcd}
\mathbb{Z}_p \arrow[d] \arrow[dr] \arrow[drr] \arrow[drrr] & & & \\
\cdots \arrow[r] & \mathbb{Z}/p^3\mathbb{Z} \arrow[r] & \mathbb{Z}/p^2\mathbb{Z} \arrow[r] & \mathbb{Z}/p\mathbb{Z}
\end{tikzcd}$$

where the sequence of maps are given by $a + p^n \mapsto a + p^{n-1} \colon \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^{n-1}\mathbb{Z}$. By construction, since we're taking an inverse limit of ring $\mathbb{Z}/p^n\mathbb{Z}$ for $n \geq 1$, we have that $\mathbb{Z}_p$ will inherit a ring structure from its family of rings which constitute it. We have the following characterization:

$$\mathbb{Z}_p := \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \{(a_n)_{n\geq 1} \colon a_n \in \mathbb{Z}/p^n\mathbb{Z},\ a_{n+1} \equiv a_n \pmod{p^n}\}$$

That is, an element $x \in \mathbb{Z}_p$ is a sequence $x = (x_1, x_2, \ldots)$ whereby $x_{n+1} \equiv x_n \pmod{p^n}$ for all $n \geq 1$. For $x = (x_1, x_2, \ldots)$ and $y = (y_1, y_2, \ldots)$ in $\mathbb{Z}_p$, we write $x + y = (x_1 + y_1, x_2 + y_2, \ldots)$ and $xy = (x_1y_1, x_2y_2, \ldots)$, and our multiplicative identity is $1 = (1, 1, \ldots)$. Lastly, note here that we can embed $\mathbb{Z} \to \mathbb{Z}_p$ by mapping some $x \in \mathbb{Z}$ to $i(x) = (x, x, \ldots)$; that is, x can be represented as $(x \bmod p, x \bmod p^2, x \bmod p^3, \ldots)$. For example, for $x = 200 \in \mathbb{Z}$, we embed into $\mathbb{Z}_3$ as $(2, 2, 11, 38, 200, 200, \ldots)$.

Definition 2.1. The *field of p-adic numbers* $\mathbb{Q}_p$ is the field of fraction of $\mathbb{Z}_p$, i.e. $\mathbb{Q}_p := \mathbb{Z}_p[\frac{1}{p}]$.

Although we've characterized $\mathbb{Z}_p$ in this algebraic manner, we can once again (quite remarkably) go about this in a different (but equivalent) manner once again. We can describe $\mathbb{Z}_p$ in terms of *valuations*, which is incredibly fruitful and an inescapable tool. We should note here that these reformulations are isomorphic and have an added layer of also a homeomorphism between them. We recall the following definition:

Definition 2.2. A **discrete valuation** is a map $v \colon k \to \mathbb{Z} \cup \{+\infty\}$ on a field k satisfying:

(i) $v(xy) = v(x) + v(y)$,
(ii) $v(x + y) \geq \min\{v(x), v(y)\}$, and
(iii) $v(x) = \infty \Leftrightarrow x = 0$.

Before describing the p-adic valuation for the field $k = \mathbb{Q}$, we define it as a preliminary step for the integers. If $x \in \mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$, we define $v_p(x)$ to be the unique positive integer satisfying $x = p^{v_p(x)}x'$, where p does not divide x'. We extend this to $k = \mathbb{Q}$, by defining $v_p \colon \mathbb{Q}^* \to \mathbb{Z} \cup \{\infty\}$ by $v_p(\frac{a}{b}) = v_p(a) - v_p(b)$ where $\frac{a}{b} \neq 0$, for which this mapping is indeed a discrete valuation. Furthermore, we define the *p-adic absolute value* $|\cdot|_p \colon \mathbb{Q}^* \to \mathbb{R}_{\geq 0}$ by $x \mapsto |x|_p = p^{-v_p(x)}$ and $|0|_p = 0$. This absolute value is in fact *nonarchimedean*, meaning that it satisfies the usual absolute value axioms but has the stronger condition that $|x - y|_p \leq \max\{|x|_p, |y|_p\} \leq |x|_p + |y|_p$. One then defines a metric $d_p(x, y) = |x - y|_p$ with respect to the p-adic absolute value to give us a metric space, and the completion with respect to d_p is the field of p-adic numbers. We define the *ring of p-adic integers* as $\mathbb{Z}_p := \{x \in \mathbb{Q}_p \colon |x|_p \leq 1\} = \{x \in \mathbb{Q}_p \colon v_p(x) \geq 0\}$.

Lemma 2.1.

(i) For all $q \in \mathbb{Q}_p^*$, we have $q \in \mathbb{Z}_p$ or $q^{-1} \in \mathbb{Z}_p$.
(ii) The group of units of $\mathbb{Z}_p$ is $\mathbb{Z}^\times = \{a \in \mathbb{Z}_p \colon v_p(a) = 0\} = \{a \in \mathbb{Z}_p \colon |a|_p = 1\}$.

Proof. (i) Let q be nonzero in $\mathbb{Q}_p$. Then $v_p(1) = v_p(qq^{-1}) = v_p(q) + v_p(q^{-1}) = 0$, so we must have that either $v_p(q) \geq$ or $v_p(q^{-1}) \geq 0$, and thus $q \in \mathbb{Z}_p$ or $q^{-1} \in \mathbb{Z}_p$.

(ii) Let $q \in \mathbb{Z}_p$ with $q \neq 0$, so we have $v_p(q) \geq 0$. But $q \in \mathbb{Z}_p^\times$ if and only $q^{-1} \in \mathbb{Z}_p$, and so $v_p(q^{-1}) = -v_p(q) \geq 0$, and if and only if $v_p(q) = 0$. As $v_p(a) = 0$, then $|a|_p = 1$ since $|a|_p = \frac{1}{p^0} = 1$, and if $|x|_p = 1$, then $1 = p^{v_p(x)}$ so $v_p(x) = 0$. $\square$

Beyond $\mathbb{Z}_p$ being integral domain, it enjoys many other structural properties of rings. Consider the set $\mathfrak{m}_p = \{x \in \mathbb{Q}_p \colon |x|_p < 1\} \subset \mathbb{Z}_p$, which is an ideal of $\mathbb{Z}_p$ as $x, y \in \mathfrak{m}_p$ and $z \in \mathbb{Z}_p$ gives $|zx + y|_p \leq \max\{|zx|_p, |y|_p\}$ and $|zx|_p = |z|_p|x|_p \leq |x|_p < 1$ so $zx + y \in \mathfrak{m}_p$. We can show that $\mathfrak{m}_p$ is in fact maximal and unique, and thus makes $(\mathbb{Z}_p, \mathfrak{m}_p)$ a local ring. Before we show this, and a few other important qualities of $\mathbb{Z}_p$, note that any $a \in \mathbb{Z}_p$, can be written uniquely as $a = p^n t$ with $t \in \mathbb{Z}_p^\times$ and $n \in \mathbb{Z}_{\geq 0}$. Since if we let $n = v_p(a)$ then we can write $a = p^n t$ for some $p \nmid t$ by the fundamental theorem of arithmetic. As $p \nmid t$, then $v_p(t) = 0$, so $|t|_p = 1$, and thus by Lemma 2.1 $t \in \mathbb{Z}_p^\times$, and lastly uniqueness is clear by cancellation.

Theorem 2.1. The integral domain $\mathbb{Z}_p$ is a local principal ideal domain with unique maximal ideal $\mathfrak{m}_p = p\mathbb{Z}_p$ and every nonzero ideal of the form $I = p^n\mathbb{Z}_p$.

Proof. Let J be an ideal of $\mathbb{Z}_p$ with $\mathfrak{m}_p \subsetneq J \subset \mathbb{Z}_p$. Take $x \in J \setminus \mathfrak{m}_p$. As $x \in \mathbb{Z}_p$, then $|x|_p \leq 1$ but also since $x \notin \mathfrak{m}_p$ then we must have $|x|_p = 1$. So x is invertible, and thus $|x^{-1}|_p = \frac{1}{|x|_p} = 1$, meaning $x^{-1} \in \mathbb{Z}_p$. As J is an ideal, and $x \in J$, then $xx^{-1} = 1 \in J$, i.e. $J = \mathbb{Z}_p$. Hence $\mathfrak{m}_p$ is a maximal ideal of $\mathbb{Z}_p$. To show uniqueness, let $L \subsetneq \mathbb{Z}_p$ be a maximal ideal. Assume that L is distinct from $\mathfrak{m}_p$, i.e. there exists $x \in L \setminus \mathfrak{m}_p$. Then we get a contradiction (following the same argument as above), so there does not exist such an x in their difference. Thus $L \subset \mathfrak{m}_p$, but as L is maximal then we that either $L = \mathfrak{m}_p$ or $\mathfrak{m}_p = \mathbb{Z}_p$, and hence we conclude that $\mathfrak{m}_p = L$.

There's an easier way to conceive of $\mathfrak{m}_p$, namely $\mathfrak{m}_p = p\mathbb{Z}_p$. This is pretty easy to show as if we take some $x \in \mathfrak{m}_{\mathbb{Z}_p}$ then $|x|_p < 1$, i.e. $v_p(x) \geq 1$, meaning that we can write $x = p^{v_p(x)}y = p(p^{v_p(x)-1}y)$ with $p \nmid y$ and thus $x \in p\mathbb{Z}_p$. For the other inclusion, let $x \in p\mathbb{Z}_p$, then $x = py$ with $p \nmid y$ and $|y|_p \leq 1$. So, $|x|_p = |py|_p$ and $v_p(py) = 1$, so $|x|_p = \frac{1}{p} < 1$. Thus $x \in \mathfrak{m}_p$.

As $(p) \subset \mathbb{Z}_p$ is the generator of $\mathfrak{m}_p$, then every element $x \in \mathbb{Z}_p$ can be written uniquely as up^n where $u \in \mathbb{Z}_p^\times$. So, let $a \in I$ have minimal order, i.e $\min\{v_p(x) \colon x \in I\} = v_p(a)$. Then $a = p^n\ell$ with $\ell \in \mathbb{Z}_p^\times$, but then p^n divides all elements of I and $p^n \in I$, so $I = (p^n) = p^n\mathbb{Z}_p$. □

Corollary 2.1. $\mathbb{Z}_p$ is a regular local ring, meaning that $\dim \mathbb{Z}_p = 1$ and $\mathfrak{m}_p$ is generated by a single element.

Proposition 2.1. The sequence

$$0 \to \mathbb{Z}_p \to \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z} \to 0$$

is an exact sequence where $\mathbb{Z}_p \to \mathbb{Z}_p$ is multiplication by p^n and $\mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ where $a = (a_1, a_2, \ldots) \in \mathbb{Z}_p$ is mapped to the n-term, i.e. $a \mapsto a_n$.

Proof. Let $\varphi \colon \mathbb{Z}_p \to \mathbb{Z}_p$ be defined by $\varphi(a) = ap^n$. Then, for $a \neq 0$ in $\mathbb{Z}_p$ with $a = (a_1, a_2, \ldots)$, we have that $\varphi(a) = p^n a$ implies $(a_1p^n, a_2p^n) = (0, 0, \ldots)$, so a must be zero and thus $\ker\varphi = \{0\}$ and φ is injective. Denote $\chi_j \colon \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ to be the map where $a = (a_1, a_2, \ldots)$ and $\chi_j(a) = a_j$. This is map is surjective as if we take some $\ell \in \mathbb{Z}/p^n\mathbb{Z}$, then $\chi_j((\ell, 0, 0, \ldots)) = \ell$. Hence it remains to show that $\ker\chi = \operatorname{im}\varphi$. We have that $\operatorname{im}\varphi \subset \ker\chi$ as $\chi \circ \varphi(a) = \chi(p^n a) = p^n a_n = 0$. For $a = (a_1, a_2, \ldots) \in \ker\chi$, we have that $\chi(a) = a_j = 0$, meaning that $a_j \in p^n\mathbb{Z}_p$. Hence $\ker\chi = \operatorname{im}\varphi$ and our sequence is in fact exact. □

Corollary 2.2. $\mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p^n\mathbb{Z}$.

2.2. **Irreducibility in $\mathbb{Z}_p[T]$.** A polynomial $p(T) \in \mathbb{Z}_p[T]$ is of the form $p(T) = a_nT^n + a_{n-1}T^{n-1} + \cdots + a_1T + a_0$ where $a_i \in \mathbb{Z}_p$ for $0 \leq i \leq n$. Recall that for an integral domain A, a polynomial $p(T) \in A[T]$, which is nonzero and not a unit in $A[T]$, is said to *irreducible* whenever $p(T) = f(T)g(T)$, with $f(T), g(T) \in A[T]$, then either $f(T)$ or $g(T)$ is a unit in $A[T]$. (It is useful to remember the basic fact that, for an integral domain A, we have $(A[T])^\times = A^\times$.) For example, any linear polynomial, say, $L(T) = T - a$ is irreducible in $A[T]$; if we assume $L(T)$, which is $\deg L = 1$, and $L(T) = f(T)g(T)$ where $\deg f, g < \deg L = 1$, then we must have that both are nonzero constants, and hence $L(T)$ is irreducible. We should remember the following fact to further our discussion about $\mathbb{Z}_p[T]$, which was used throughout the entire introduction:

Lemma 2.2. Let $A[T]$ be a PID. The polynomial $p(T) \in A[T]$ is irreducible if and only if $A[T]/(p(T))$ is a field.

Proof. Assume that $p(T)$ is irreducible. Let $(p(T))$ be contained in the ideal $I = (q(T))$, and we assume $I \neq A[T]$. Then $p(T) = q(T)g(T)$ for some $g(T) \in A[T]$, so as $p(T)$ is irreducible, then either $q(T)$ or $g(T)$ is invertible. Assume, WLOG, $q(T)$ is invertible. Then there exists $f(T) \in A[T]$ such that $q(T)f(T) = 1$. But this implies that $1 \in I$ so $I = A[T]$, which is a contradiction. Thus $(p(T))$ cannot be contained in any other ideal of $A[T]$, so it is maximal and hence $A[T]/(p(T))$ is a field. For the backwards direction, let $A[T]/(p(T))$ be a field. Then $(p(T))$ is a maximal ideal. Assume that $p(T)$ is reducible, i.e. $p(T) = f(T)g(T)$ with $\deg f < p$ and $\deg g < p$. So, WLOG, we have $(p(T)) \subset (f(T))$. We cannot have that $(f(T)) = A[T]$, as then this would mean that $f(T)$ is invertible and consequentially mean that $p(T)$ is irreducible. Hence $(p(T))$ is not maximal and a contradiction. Therefore $p(T)$ is irreducible. □

From basic algebra, we learn Eisenstein's criterion and Gauss' Lemma. Both of these theorems provide an easier way to verify whether or not a given polynomial $p(T) \in \mathbb{Q}[T]$ is irreducible. In conjugation, these two are very strong together; that is, if we have that $f(T) \in \mathbb{Z}[T]$ is irreducible by applying Eisenstein, then if it is also primitive, it is also irreducible over $\mathbb{Q}[T]$. This primitive condition is necessary, relevant to our definition of irreducibility, as there is a difference between irreducibility in $\mathbb{Z}[T]$ and $\mathbb{Q}[T]$. For example, consider $f(T) = 2T^2 + 2 = 2(T+1)$; this is irreducible over $\mathbb{Q}[T]$ as 2 is a unit of $\mathbb{Q}$, but this polynomial is reducible over $\mathbb{Z}[T]$ as 2 is not a unit of $\mathbb{Z}$. In a similar vein, the element 2 is irreducible in $\mathbb{Z}[T]$, but not in $\mathbb{Q}[T]$ as 2 is once again just a unit. Now, as $\mathbb{Z}_p[T]$ and $\mathbb{Q}_p[T]$ are the objects most relevant to us, there are in fact analogues of Eisenstein and Gauss' Lemma for these such objects:

Proposition 2.2 (Eisenstein, [Gou20, Proposition 6.3.11])**.** Let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}_p[x]$ be such that

(i) $|a_n|_p = 1$,
(ii) $|a_i|_p < 1$ for $0 \leq i < n$, and
(iii) $|a_0|_p = \frac{1}{p}$.

Then $f(x)$ is irreducible over $\mathbb{Q}_p$.

Example 2.1. The polynomial $p(x) = x^2 - 3$ is irreducible over $\mathbb{Q}_3$. This polynomial is monic, so $a_n = 1$ and thus $|1|_3 = 1$ as $v_p(1) = 0$ in general, and $a_0 = -3$ is the only other term so we find $v_3(3) = 1$ meaning that $|3|_3 = \frac{1}{3^1} = \frac{1}{3} < 1$. Therefore $p(x)$ is irreducible in $\mathbb{Q}_3$. Moreover we can adjoin a root of $x^2 - 3$ to $\mathbb{Q}_3$ to get the extension $\mathbb{Q}_3(\sqrt{3})/\mathbb{Q}_3$.

Theorem 2.2 (Gauss' Lemma[2])**.** A non-constant polynomial $f(x) \in \mathbb{Z}_p[x]$ is irreducible in $\mathbb{Z}_p[x]$ if and only it is both irreducible in $\mathbb{Q}_p[x]$ and primitive in $\mathbb{Z}_p[x]$. In particular, if f is irreducible in $\mathbb{Z}_p[x]$, then it is irreducible in $\mathbb{Q}_p[x]$.

Hensel's lemma as given [Con]

3. The prime spectrum of $\mathbb{Z}_p[T]$

3.1. **An algebraic geometry technique.** Establishing $\operatorname{Spec} \mathbb{Z}_p[T]$ is somewhat difficult, even though we can formulate clearly what it *need be*; that is, we will see that $\operatorname{Spec} \mathbb{Z}_p[T]$ ends up looking like $\operatorname{Spec} \mathbb{Q}_p[T]$ and $\operatorname{Spec} \mathbb{Z}/p\mathbb{Z}[T]$. Now, to get down what $\operatorname{Spec} \mathbb{Z}_p[T]$ is, we employ a useful tool from algebraic geometry. For the injection $\varphi\colon \mathbb{Z}_p \to \mathbb{Z}_p[T]$, we can get a map on spectra, $\pi\colon \operatorname{Spec} \mathbb{Z}_p[T] \to \operatorname{Spec} \mathbb{Z}_p$ where $\mathfrak{p} \mapsto \varphi^{-1}(\mathfrak{p})$. To inspect the prime ideals of $\mathbb{Z}_p[T]$ amounts to looking at *fibres* of π. Luckily $\mathbb{Z}_p$ is a DVR, meaning that it only has two prime ideals, namely (0) and (p), so we only need to look at two fibres of π. For the map $\pi\colon \operatorname{Spec} \mathbb{Z}_p[T] \to \operatorname{Spec} \mathbb{Z}_p$ and a point $\mathfrak{q} \in \operatorname{Spec} \mathbb{Z}_p$,

$$(\operatorname{Spec} \mathbb{Z}_p[T])_{\mathfrak{q}} = \operatorname{Spec} \mathbb{Z}_p[T] \times_{\operatorname{Spec} \mathbb{Z}_p} \operatorname{Spec} \kappa(\mathfrak{q}),$$

where the canonical map $\operatorname{Spec} \kappa(\mathfrak{q}) \to \operatorname{Spec} \mathbb{Z}_p$ is given by composition $\operatorname{Spec} \kappa(\mathfrak{q}) \to \operatorname{Spec}(\mathscr{O}_{\operatorname{Spec} \mathbb{Z}_p, \mathfrak{q}}) \to \operatorname{Spec} \mathbb{Z}_q$. The reason this setup is useful is that we can apply the following lemma:

Lemma 3.1. Let $f\colon X \to Y$ be a morphism of schemes and let $y \in Y$. Then $X_y = X \times_Y \operatorname{Spec} \kappa(y)$ is homeomorphic to $f^{-1}(y)$ with the induced topology.

To find out $\operatorname{Spec} \mathbb{Z}_p[T]$ it amounts to checking $\operatorname{Spec} \kappa((0)) \times_{\mathbb{Z}_p} \operatorname{Spec} \mathbb{Z}[T] = \operatorname{Spec}(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathbb{Z}[T]) = \operatorname{Spec} \mathbb{Q}_p[T]$ and $\operatorname{Spec} \kappa((p)) \times_{\mathbb{Z}_p} \operatorname{Spec} \mathbb{Z}[T] = \operatorname{Spec}(\mathbb{Z}/p\mathbb{Z} \otimes_{\mathbb{Z}_p} \mathbb{Z}[T]) = \operatorname{Spec} \mathbb{Z}/p\mathbb{Z}[T]$. This follows from the fact that $\mathscr{O}_{\mathbb{Z}_p,(0)} \simeq (\mathbb{Z}_p)_{(0)} = \mathbb{Q}_p$ and the unique maximal ideal $\mathfrak{m} = (0)\mathbb{Z}_p = (0)$, so $\kappa((0)) = \mathbb{Q}_p/\mathfrak{m} = \mathbb{Q}_p$, and $\kappa((p)) = \mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$. Hence the prime ideals of $\operatorname{Spec} \mathbb{Z}_p[T]$ are in bijection with the prime ideals of $\mathbb{Z}/p\mathbb{Z}[x] \simeq \mathbb{F}_p[T]$ and $\mathbb{Q}_p[T]$. Thus it suffices to inspect $\operatorname{Spec} \mathbb{Z}/p\mathbb{Z}[T]$ and $\operatorname{Spec} \mathbb{Q}_p[T]$; this is what we will do in the rest of this paper.

Lemma 3.2. $\operatorname{Spec} \mathbb{Z}_p[T]$ is in bijection with $\operatorname{Spec} \mathbb{F}_p[T]$ and $\operatorname{Spec} \mathbb{Q}_p[T]$; that is, $\operatorname{Spec} \mathbb{Z}_p[T]$ consists of:

(i) (0),

---

[2] This is a special case of Gauss' lemma; this in general works over an unique factorization domain and it's corresponding field of fractions.

(ii) (p) for p prime,
(iii) $(f(T))$ with $f(T)$ irreducible in $\mathbb{Z}_p[T]$, and
(iii) $(p, f(T))$ where p is prime and $f(T) \in \mathbb{F}_p[T]$ irreducible.

Once again, finding some prime/maximal ideals of $\mathbb{A}_{\mathbb{Z}/p\mathbb{Z}}$ and $\mathbb{A}_{\mathbb{Q}_p}$ are not hard--in fact, by Lemma 2.1 we have found that $p(x) = x^2 \pm 2$ will generate a maximal ideal $(p(x))$ for $\mathbb{Q}_p$ for every p. Even easier are the maximal ideals of $\mathbb{A}_{\mathbb{Z}/p\mathbb{Z}}$ for a fixed p: We have $(p), (p, x), (p, x+1), \ldots, (p, x+(p-1))$ being the maximal ideals landing on $\mathbb{A}_{\mathbb{Z}/p\mathbb{Z}}$.

3.2. Drawing of $\operatorname{Spec} \mathbb{Z}_p[T]$ with $p \not\equiv 1 \pmod 4$.

3.3. Drawing of $\operatorname{Spec} \mathbb{Z}_p[T]$.

References

[Con] K. Conrad. *Hensel's Lemma*. https://kconrad.math.uconn.edu/blurbs/gradnumthy/hensel.pdf.

[Gou20] Fernando Q. Gouvêa. *p-adic numbers*. Springer Cham, third edition, 2020. UTX.

[Mum99] David Mumford. *The Red Book of Varieties and Schemes*. Springer Berlin, Heidelberg, 1999.

[Mum15] David Mumford. *Algebraic Geometry II (a penultimate draft)*. 2015.