IDEAL THEORY AND PRÜFER DOMAINS

FELIX GOTTI

Integer-Valued Polynomials I

The goal of this final lecture is to give a brief introduction to rings of integer-valued polynomials. Throughout this section, R is an integral domain with quotient field K. The ring

$$\operatorname{Int}(R) := \{p(x) \in K[x] \mid p(R) \subseteq R\}$$

is called the *ring of integer-valued polynomials* of R. We will conclude this lecture proving that the ring of integer-valued polynomial of a Dedekind domain with finite residue fields is a Prüfer domain. In particular, $\operatorname{Int}(\mathbb{Z})$ is a Prüfer domain. Here we will also describe the spectrum of $\operatorname{Int}(S, R)$.

Uniform Continuity and Stone-Weierstrass Theorem. Let R be a Noetherian ring, and let I be an ideal of R. By Krull Intersection Theorem, $\bigcap_{n \in \mathbb{N}} I^n = (0)$. Then we can define $w_I \colon R \to \mathbb{N}_0$ by $w_I(r) = \sup\{n \in \mathbb{N}_0 \mid r \in I^n\}$ if $r \neq 0$ and $w_I(0) = \infty$. Using w_I one can define a metric on R by setting $|r|_I := e^{-w_I(r)}$ and

$$d(r, s) = |r - s|_I = e^{-w(r-s)} \tag{0.1}$$

for all $r, s \in R$, with the convention $e^{-\infty} = 0$. With d defined as in (0.1), the ring R becomes a metric space; indeed, the following properties can be easily verified:

- $d(r, s) = 0$ if and only if $r = s$,
- $d(r, s) = d(s, r)$, and
- $d(r, t) \le \sup\{d(r, s), d(s, t)\} \le d(r, s) + d(s, t)$

for all $r, s, t \in R$. The topology on R induced by the distance d is called the I-adic topology, and R is a topological ring with respect to the I-adic topology.

Proposition 1. *Let R be a Noetherian domain, and let I be an ideal of R. Then every $f \in \operatorname{Int}(R)$ is uniformly continuous on R with respect to the I-adic topology.*

Proof. Take $f \in \operatorname{Int}(R)$, and fix $\epsilon > 0$. Then take $d \in R$ such that $df(x) \in R[x]$. By virtue of Artin-Rees Lemma, there is a $k \in \mathbb{N}_0$ such that $I^{n+k} \cap dR = I^n(I^k \cap dR)$ for every $n \in \mathbb{N}_0$. Now set $\delta := e^{-(n_0+k)}$, where $n_0 \in \mathbb{N}$ satisfies that $e^{-n_0} < \epsilon$. Now take $r, s \in R$ with $|r - s|_I < \delta$. It is not hard to verify that $r - s$ divides $d(f(r) - f(s))$ in R, that is, $d(f(r) - f(s)) \in (r - s)R$. This implies that $d(f(r) - f(s)) \in (r - s)R \subseteq I^{n_0+k}$, and so

$$d(f(r) - f(s)) \in I^{n_0+k} \cap dR = I^{n_0}(I^k \cap dR) \subseteq dI^{n_0}.$$

As a consequence, $f(r)-f(s) \in I^{n_0}$, and we see that $|f(r)-f(s)|_I \le e^{-n_0} < \epsilon$. Hence we conclude that f is uniformly continuous on R in the I-adic topology. $\square$

Corollary 2. *Every polynomial in* $\mathrm{Int}(\mathbb{Z})$ *is uniformly continuous as a function on* $\mathbb{Z}_p$ *with respect to the* p*-adic topology.*

For every compact subset K of $\mathbb{R}$, the ring of polynomials $\mathbb{R}[x]$ is dense in the metric space $C(K,\mathbb{R})$ consisting of all continuous real-valued functions on K with respect to the uniform convergence topology. This is known as the Stone-Weierstrass Theorem. A parallel result for the p-adic completion of $\mathbb{Q}$ was proved in 1944 by Dieudonné [3, Theorem 4]: $\mathbb{Q}_p[x]$ is dense in $C(K,\mathbb{Q}_p)$ for every compact subset K of $\mathbb{Q}_p$ with respect to the p-adic topology. Our next theorem is a related version of the Stone-Weierstrass Theorem for rings of integer-valued polynomials, due to Mahler [4, Theorem 1]. Since $\mathbb{Z}_p$ is the closure of $\mathbb{Z}$ in $\mathbb{Q}_p$ and $\mathbb{Z}_p$ is a complete metric space, by virtue of Proposition 1, every polynomial in $\mathrm{Int}(\mathbb{Z})$ uniquely extends as a continuous function to a function in $C(\mathbb{Z}_p,\mathbb{Z}_p)$. Thus, we can assume that $\mathrm{Int}(\mathbb{Z}) \subseteq C(\mathbb{Z}_p,\mathbb{Z}_p)$.

Theorem 3. *For each* $p \in \mathbb{P}$*, the ring of integer-valued polynomials* $\mathrm{Int}(\mathbb{Z})$ *is dense in* $C(\mathbb{Z}_p,\mathbb{Z}_p)$ *with respect to the uniform convergence topology.*

Proof. Fix $p \in \mathbb{P}$ and $n \in \mathbb{N}$, and then set $U_i := i + p^n\mathbb{Z}_p$ for every $i \in [\![0, p^n-1]\!]$. Note that for each U_i is a clopen ball in $\mathbb{Z}_p$ with respect to the p-adic topology and, in addition, $\mathbb{Z}_p$ is the disjoint union of all these balls. Now let $\chi_i \colon \mathbb{Z}_p \to \mathbb{Z}_p$ be the characteristic functions of U_i, that is, $\chi_i(x) = 1$ if $x \in U_i$ and $\chi_i(x) = 0$ otherwise. Clearly, $\chi_i \in C(\mathbb{Z}_p,\mathbb{Z}_p)$ for every $i \in [\![0,p^n-1]\!]$. We will argue now that each χ_i is an integral combination of the binomial functions $\binom{x}{0}, \dots, \binom{x}{p^n-1}$ modulo p. Since $\deg \binom{x}{k} = k < p^n$ for every $k \in [\![0,p^n-1]\!]$, it is not hard to argue that for every $a,b \in \mathbb{Z}$,

$$\Big| \binom{b}{k} - \binom{a}{k} \Big|_p \le p^{n-1}|b-a|_p \tag{0.2}$$

(see Exercise 2). Since $\mathbb{Z}_p$ is the closure of $\mathbb{Z}$ in $\mathbb{Q}_p$, we obtain that (0.2) also holds for every $a,b \in \mathbb{Z}_p$. Then if $a,b \in U_i$ for some $i \in [\![0,p^n-1]\!]$, then the fact that $v_p(b-a) \ge n$ ensures that

$$\Big| \binom{b}{k} - \binom{a}{k} \Big|_p \le p^{n-1}|b-a|_p \le p^{-1},$$

which means that $\binom{x}{k}$ is constant on U_i modulo p. Therefore for every $k \in [\![0,p^n-1]\!]$ there is a function $\delta_k \in C(\mathbb{Z}_p,\mathbb{Z}_p)$ such that

$$\binom{x}{k} = p\delta_k + \sum_{i=0}^{p^n-1} \binom{i}{k} \chi_i. \tag{0.3}$$

We can write the identity (0.3) using matrix notation as $B = pD + MX$, where B, D, and X are the column vectors $\big(\binom{x}{0}, \dots, \binom{x}{p^n-1}\big)^T$, $(\delta_0, \dots, \delta_{p^n-1})^T$, and $(\chi_0, \dots, \chi_{p^n-1})^T$, respectively, and M is the square matrix with entry $\binom{i}{k}$ in the position (k,i). Observe that M is upper triangular with 1's in its main diagonal. Thus, M is invertible, and $X = M^{-1}B - pM^{-1}D$. After unfolding this matrix identity, we find that for every $i \in [\![0, p^n-1]\!]$ there is a function $\sigma_i \in C(\mathbb{Z}_p, \mathbb{Z}_p)$ such that

$$\chi_i = p\sigma_i + \sum_{i=0}^{p^n-1} c_{ik}\binom{x}{k},$$

where $c_{ik} \in \mathbb{N}_0$ for every $k \in [\![0, p^n-1]\!]$. Since $\left\{\binom{x}{k} : k \in \mathbb{N}_0\right\}$ is a $\mathbb{Z}$-basis for $\operatorname{Int}(\mathbb{Z})$, every characteristic function can be approximated modulo p in $C(\mathbb{Z}_p, \mathbb{Z}_p)$ by an integer-valued polynomial.

Now suppose that $\phi_0 \in C(\mathbb{Z}_p, \mathbb{Z}_p)$. Since $\mathbb{Z}_p$ is compact, ϕ_0 is uniformly continuous and, therefore, we can take $n \in \mathbb{N}$ large enough so that ϕ_0 is constant modulo p on U_i for every $i \in [\![0, p^n-1]\!]$. Therefore ϕ_0 equals modulo p an integral linear combination of the characteristic functions $\chi_1, \dots, \chi_{p^n-1}$, and so we can take $f_0 \in \operatorname{Int}(\mathbb{Z})$ such that $\phi_0 = f_0 + p\phi_1$ for some $\phi_1 \in C(\mathbb{Z}_p, \mathbb{Z}_p)$. Now we can repeat the same argument for ϕ_1 to obtain $f_1 \in \operatorname{Int}(\mathbb{Z})$ and $\phi_2 \in C(\mathbb{Z}_p, \mathbb{Z}_p)$ such that $\phi_0 = f_0 + pf_1 + p^2\phi_2$. Continuing in this fashion, for every $n \in \mathbb{N}_0$ we find $f_0, \dots, f_n \in \operatorname{Int}(\mathbb{Z})$ and $\phi_{n+1} \in C(\mathbb{Z}_p, \mathbb{Z}_p)$ such that $\phi_0 = p^{n+1}\phi_{n+1} + \sum_{i=0}^n p^i f_i$. Hence for every $n \in \mathbb{N}$, there exists $g \in \operatorname{Int}(\mathbb{Z})$ such that $v_p(\phi_0(x) - g(x)) \ge n+1$ for every $x \in \mathbb{Z}_p$. This allows us to conclude that $\operatorname{Int}(\mathbb{Z})$ is dense in $C(\mathbb{Z}_p, \mathbb{Z}_p)$. □

Corollary 4. *Let $U_1, \dots, U_k$ be disjoint open subsets covering $\mathbb{Z}_p$, and let $c_1, \dots, c_k$ be nonnegative integers. Then there exists $f(x) \in \operatorname{Int}(\mathbb{Z})$ such that $v_p(f(x)) = c_i$ for all $x \in U_i$ and $i \in [\![1, k]\!]$.*

Proof. Set $n := 1 + \max\{c_i : i \in [\![1,k]\!]\}$. Now consider the function $\varphi = \sum_{i=1}^k p^{c_i}\chi_i$, where χ_i is the characteristic function of U_i. It is clear that $\varphi \in C(\mathbb{Z}_p, \mathbb{Z}_p)$. Therefore, Stone-Weierstrass Theorem guarantees the existence of $f \in \operatorname{Int}(\mathbb{Z})$ such that $|\varphi - f|_p < p^{-n}$, and so $v_p(p^{c_i} - f(x)) \ge n > c_i$ for all $x \in U_i$ and $i \in [\![1,k]\!]$. This implies that $v_p(f(x)) = c_i$ whenever $x \in U_i$ and $i \in [\![1,k]\!]$. □

Hensel's Lemma. In this subsection, we will discuss Hensel's lemma, which will be used to describe the spectrum of $\operatorname{Int}(\mathbb{Z})$ in the next subsection.

Lemma 5. *Let R be a commutative ring with identity, and let $f \in R[x]$. Then there exists $g(x,y) \in R[x,y]$ such that*

$$f(x+y) = f(x) + f'(x)y + g(x,y)y^2.$$

Proof. After writing $f(x) = \sum_{i=0}^n c_i x^i$ for some $c_0, \dots, c_n \in R$, we see that

$$f(x+y) = \sum_{k=0}^n c_k(x+y)^k = c_0 + \sum_{k=1}^n \left(c_k(x^k + kx^{k-1}y) + g_i(x,y)y^2\right),$$

where $g_i(x,y) \in R[x,y]$ for every $i \in [\![1,k]\!]$. Now we can set $g(x,y) = \sum_{k=1}^n g_i(x,y)$ to obtain the desired identity, namely,

$$f(x+y) = \sum_{k=0}^n c_k x^k + \left(\sum_{k=1}^n c_k k x^{k-1}\right) y + \left(\sum_{k=1}^n g_i(x,y)\right) y^2 = f(x) + f'(x)y + g(x,y)y^2.$$

□

We proceed to prove Hensel's Lemma.

Theorem 6 (Hensel's Lemma)**.** *Let f be a monic polynomial in $\mathbb{Z}_p[x]$, and suppose that $f(a) \equiv 0 \pmod{p\mathbb{Z}_p}$ but $f'(a) \not\equiv 0 \pmod{p\mathbb{Z}_p}$ for some $a \in \mathbb{Z}_p$. Then there exists a unique $r \in \mathbb{Z}_p$ such that $f(r) = 0$ and $r \equiv a \pmod{p\mathbb{Z}_p}$.*

Proof. Let us argue that there exists a sequence $(a_n)_{n \in \mathbb{N}_0}$ with terms in $\mathbb{Z}_p$ such that for every $n \in \mathbb{N}_{\geq 1}$,

$$a_n \equiv a_{n-1} \pmod{p^{n-1}\mathbb{Z}_p} \quad \text{and} \quad f(a_n) \equiv 0 \pmod{p^n \mathbb{Z}_p}. \tag{0.4}$$

We proceed by induction on n. For $n = 1$, both conditions in (0.4) clearly hold after taking $a_0 = a_1 = a$. Suppose, therefore, that we have found $a_0, a_1, \dots, a_n$ satisfying both conditions in (0.4) for some $n \in \mathbb{N}$. Since $f'(a) \not\equiv 0 \pmod{p\mathbb{Z}_p}$, the congruence equation $f'(a)x \equiv -f(a_n)/p^n \pmod{p\mathbb{Z}_p}$ has a solution t_n in $\mathbb{Z}_p$. Now it follows from Lemma 5 that

$$f(a_n + p^n t_n) = f(a_n) + f'(a_n)p^n t_n + z p^{2n} t_n^2$$

for some $z \in \mathbb{Z}_p$, and so $f(a_n + p^n t_n) \equiv f(a_n) + f'(a_n)p^n t_n \pmod{p^{n+1}\mathbb{Z}_p}$. Since $a_n \equiv a \pmod{p\mathbb{Z}_p}$, it follows that $f'(a_n)p^n t_n \equiv f'(a)p^n t_n \pmod{p^{n+1}\mathbb{Z}_p}$. Set $a_{n+1} := a_n + p^n t_n$. Because $f'(a)t_n \equiv -f(a_n)/p^n \pmod{p\mathbb{Z}_p}$, we see that a_{n+1} is a root of f modulo $p^{n+1}\mathbb{Z}_p$:

$$f(a_{n+1}) = f(a_n + p^n t_n) \equiv f(a_n) + f'(a)p^n t_n \equiv 0 \pmod{p^{n+1}\mathbb{Z}_p}.$$

Therefore $a_{n+1} \equiv a_n \pmod{p^n\mathbb{Z}_p}$ and $f(a_{n+1}) \equiv 0 \pmod{p^{n+1}\mathbb{Z}_p}$, as desired. At this point, we have produced a sequence $(a_n)_{n \in \mathbb{N}}$ whose terms satisfy the conditions in (0.4). The first condition in (0.4) ensures that $(a_n)_{n \in \mathbb{N}}$ is a Cauchy sequence in $\mathbb{Z}_p$. As $\mathbb{Z}_p$ is complete, $(a_n)_{n \in \mathbb{N}}$ converges. Let r denote the limit of $(a_n)_{n \in \mathbb{N}}$. Since for each $n \in \mathbb{N}$, the congruence equality $a_{n+k} \equiv a_n \pmod{p^n\mathbb{Z}_p}$ holds for every $k \in \mathbb{N}$, after taking limits we obtain $r \equiv a_n \pmod{p^n\mathbb{Z}_p}$ and, in particular, $r \equiv a \pmod{p\mathbb{Z}_p}$. Also, for each $n \in \mathbb{N}$, after applying f to both sides of $r \equiv a_n \pmod{p^n\mathbb{Z}_p}$, we obtain that $f(r) \equiv f(a_n) \equiv 0 \pmod{p^n\mathbb{Z}_p}$, that is, $f(r) \in \bigcap_{n \in \mathbb{N}} p^n\mathbb{Z}_p$. Hence $f(r) = 0$.

Finally, let us prove that r is the unique element of $\mathbb{Z}_p$ satisfying the desired properties. To do so, suppose that $r' \in \mathbb{Z}_p$ satisfies that $f(r') = 0$ and $r' \equiv a \pmod{p\mathbb{Z}_p}$. Proving that $r' = r$ amounts to verifying that $r' \equiv r \pmod{p^n\mathbb{Z}_p}$ for every $n \in \mathbb{N}$. We proceed by induction. It is clear that $r' \equiv r \pmod{p\mathbb{Z}_p}$. Assume that $r' \equiv r$

(mod $p^n\mathbb{Z}_p$) for some $n \in \mathbb{N}$, and write $r' = r + p^n z_n$ for some $z_n \in \mathbb{Z}_p$. Using Lemma 5 and the fact that $f(r') = f(r) = 0$, we see that

$$0 = f(r') = f(r + p^n z_n) \equiv f(r) + f'(r)p^n z_n = f'(r)p^n z_n \pmod{p^{n+1}}.$$

Hence $f'(r)z_n \in p\mathbb{Z}_p$. Because $p\mathbb{Z}_p$ is prime, the fact that $f'(r) \equiv f'(a) \not\equiv 0 \pmod{p\mathbb{Z}_p}$ ensures that $z_n \in p\mathbb{Z}_p$. Thus, $r' = r + p^n z_n \equiv r \pmod{p^{n+1}\mathbb{Z}_p}$. Hence $r' \equiv r \pmod{p^n\mathbb{Z}_p}$ for every $n \in \mathbb{N}$, which implies that $r' = r$. □

Example 7. Consider the polynomial $f(x) = x^2 + 5 \in \mathbb{Z}[x]$, which does not have any root in $\mathbb{Z}$ (indeed, $f(x)$ does not have any root in $\mathbb{R}$). We will use Hensel's Lemma to show that $f(x)$ has a root in $\mathbb{Z}_3$. This amounts to observing that 1 is a simple root of $f(x)$ modulo 3, that is, $f(1) \equiv 0 \pmod{3\mathbb{Z}_3}$ while $f'(1) = 2 \not\equiv 0 \pmod{3\mathbb{Z}_3}$. As a consequence, -5 is a square in $\mathbb{Z}_3$.

Spectrum of Int($\mathbb{Z}$). We are in a position now to describe the spectrum and the maximal spectrum of the ring Int($\mathbb{Z}$).

Theorem 8 (Spectrum of Int($\mathbb{Z}$))**.** *The following statements hold.*

1. *A nonzero prime ideal of* Int($\mathbb{Z}$) *lies over the ideal* (0) *in* $\mathbb{Z}$ *if and only if it has the form*
$$P_{q(x)} := \mathrm{Int}(\mathbb{Z}) \cap q(x)\mathbb{Q}[x],$$
for some irreducible polynomial $q(x) \in \mathbb{Q}[x]$*. In addition, for any two distinct monic irreducible polynomials* $q(x)$ *and* $r(x)$ *of* $\mathbb{Q}[x]$*, the ideals* $P_{q(x)}$ *and* $P_{r(x)}$ *are different.*
2. *A prime ideal of* Int($\mathbb{Z}$) *lies over the ideal* (p) *in* $\mathbb{Z}$ *for some* $p \in \mathbb{P}$ *if and only if it has the form*
$$M_{p,\alpha} := \{f \in \mathrm{Int}(\mathbb{Z}) : f(\alpha) \in p\mathbb{Z}_p\}$$
for some $\alpha \in \mathbb{Z}_p$*, in which case it is maximal. For any distinct pairs* (p, α) *and* (p', α')*, the ideals* $M_{p,\alpha}$ *and* $M_{p',\alpha'}$ *are different.*
3. *The ideal* $P_{q(x)}$ *is contained in* $M_{p,\alpha}$ *if and only if* $q(\alpha) = 0$*. Also, the maximal ideals of* Int($\mathbb{Z}$) *are precisely those of the form* $M_{p,\alpha}$*.*

Proof. (1) It is clear that $P_{q(x)}$ lies over (0) in $\mathbb{Z}$. Moreover, after setting $S = \mathbb{Z} \setminus \{0\}$, we see that the prime ideals of Int($\mathbb{Z}$) lying over (0) are precisely the prime ideals of Int($\mathbb{Z}$) that do not intersect S and, therefore, are in one-to-one correspondence with the prime ideals of $S^{-1}\mathrm{Int}(\mathbb{Z}) = \mathbb{Q}[x]$. Thus, the nonzero prime ideals of Int($\mathbb{Z}$) are precisely the $P_{q(x)}$, which are the contractions of the nonzero prime ideals of $\mathbb{Q}[x]$. The last statement follows immediately as two principal prime ideals $q(x)\mathbb{Q}[x]$ and $r(x)\mathbb{Q}[x]$ are equal if and only if $r(x) = q(x)$.

(2) Fix $p \in \mathbb{P}$ and $\alpha \in \mathbb{Z}_p$. Observe that the map $\varphi\colon \mathrm{Int}(\mathbb{Z}) \to \mathbb{Z}_p/p\mathbb{Z}_p$ defined by $\varphi(f) = f(\alpha) + p\mathbb{Z}_p$ is a ring homomorphism whose kernel is $M_{p,\alpha}$. As $\mathbb{Z}_p$ is the disjoint

union of the balls $i+p\mathbb{Z}_p$ (for $i \in [\![0, p-1]\!]$), we see that $\varphi(X-j+1) = 1+p\mathbb{Z}_p$, where $j \in [\![1,k]\!]$ is chosen so that $\alpha + p\mathbb{Z}_p = j + p\mathbb{Z}_p$. Hence φ is surjective and, therefore, $\text{Int}(\mathbb{Z})/M_{p,\alpha} \cong \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$. Thus, $M_{p,\alpha}$ is a maximal ideal. Also, it is clear that $M_{p,\alpha}$ lies over (p).

Now let us argue that the $M_{p,\alpha}$ are the only prime ideals of $\text{Int}(\mathbb{Z})$ lying over (p). Suppose, by way of contradiction, that P is a prime ideal of $\text{Int}(\mathbb{Z})$ lying over (p) such that $P \neq M_{p,\alpha}$ for any $\alpha \in \mathbb{Z}_p$. Then for each $\alpha \in \mathbb{Z}_p$, we can take $f_\alpha \in M_{p,\alpha} \setminus P$. Now for each $\alpha \in \mathbb{Z}_p$, the continuity of f_α guarantees the existence of an open U_α containing α such that $v_p(f_\alpha(x)) \ge 1$ for all $x \in U_\alpha$. The compactness of $\mathbb{Z}_p$ ensures the existence of $\alpha_1, \dots, \alpha_k \in \mathbb{Z}_p$ such that $\mathbb{Z}_p = \bigcup_{i=1}^k U_{\alpha_i}$. Now set $f = f_{\alpha_1} \cdots f_{\alpha_k}$. Then $v_p(f(x)) = \sum_{i=1}^k v_p(f_{\alpha_i}(x)) \ge 1$ for all $x \in \mathbb{Z}_p$. As a result, we see that $f/p \in \text{Int}(\mathbb{Z})$, which implies that $f = p(f/p) \in P$. Now the fact that $f_{\alpha_i} \notin P$ for any $i \in [\![1,k]\!]$ contradicts that the ideal P is prime. Hence the only prime ideals of $\text{Int}(\mathbb{Z})$ over (p) in $\mathbb{Z}$ are the $M_{p,\alpha}$ with $\alpha \in \mathbb{Z}_p$.

Suppose now that $M_{p,\alpha} = M_{p,\beta}$ for some $p \in \mathbb{P}$ and $\alpha, \beta \in \mathbb{Z}_p$. Then $v_p(f(\alpha)) \ge 1$ if and only if $v_p(f(\beta)) \ge 1$ for every $f \in \text{Int}(\mathbb{Z})$. Now if $\alpha \neq \beta$, then we could take $k \in \mathbb{N}$ large enough so that the clopen balls $\alpha + p^k\mathbb{Z}_p$ and $\beta + p^k\mathbb{Z}_p$ are disjoint, and by virtue of Corollary 4, we could find a polynomial $f \in \text{Int}(\mathbb{Z})$ with $v_p(f(\alpha)) = 0$ and $v_p(f(\beta)) = 1$.

(3) It is clear that the ideal $P_{q(x)}$ is contained in $M_{p,\alpha}$ provided that $q(\alpha) = 0$. To argue the converse, assume that $P_{q(x)} \subseteq M_{p,\alpha}$ for some $p \in \mathbb{P}$ and $\alpha \in \mathbb{Z}_p$. Now suppose, by way of contradiction, that $q(\alpha) \neq 0$. After replacing $q(x)$ by a suitable integer multiple, we can assume that $q(x) \in \mathbb{Z}[x] \cap P_{q(x)}$. Set $n := v_p(q(\alpha)) \in \mathbb{N}_0$. As $q \in C(\mathbb{Z}_p, \mathbb{Z}_p)$, there is a clopen subset U of $\mathbb{Z}_p$ containing α such that $v_p(q(x)) = n$ for all $x \in U$. Then Corollary 4 guarantees the existence of $f \in \text{Int}(\mathbb{Z})$ such that $v_p(f(x)) = 0$ if $x \in U$ and $v_p(f(x)) = n$ if $x \in \mathbb{Z}_p \setminus U$. Set $g = f/p^n$. Since $gq \in \text{Int}(\mathbb{Z})$, it follows that $gq \in P_{q(x)}$. However, the fact that $v_p(g(\alpha)q(\alpha)) = 0$ implies that $gq \notin M_{p,\alpha}$. Therefore $P_{q(x)}$ is not contained in $M_{\alpha,p}$, which is a contradiction.

Finally, let $q(x)$ be an irreducible in $\mathbb{Q}[x]$, and let us argue that the prime ideal $P_{q(x)}$ is not maximal. After replacing $q(x)$ by an integer multiple we can actually assume that $q(x) \in \mathbb{Z}[x]$. We split the rest of the proof into two parts. First, we argue that the set

$$P := \{p \in \mathbb{P} : p \mid q(z) \text{ for some } z \in \mathbb{Z}\}$$

is infinite. It is clear that $P = \mathbb{P}$ when $q(x) \in x\mathbb{Z}[x]$, as in this case $q(x) = \pm x$. Suppose, therefore, that $q(x) = \sum_{i=0}^n c_i x^i$ for some $c_0, \dots, c_n \in \mathbb{Z}$ with $c_0 \neq 0$. Assume now, towards a contradiction, that P is finite, and let m be the product of all the primes in P (it is clear that P is nonempty). Since $q(x)$ is not constant, we can take $j \in \mathbb{N}$ such that $q(c_0 m^j) \neq \pm c_0$. Now observe that $q(c_0 m^j) = c_0(1 + m^j c)$ for some $c \in \mathbb{Z}$. As $q(c_0 m^j) \neq \pm c_0$, we see that $|1 + m^j c| \neq 1$, and so we can take $p \in \mathbb{P}$ dividing

$1 + m^j c$. As $p \nmid m$, it follows that $p \notin P$, which contradicts that $p \mid q(c_0 m^j)$. Hence $|P| = \infty$.

Since $q(x)$ is irreducible, $d := \gcd(q(x), q'(x)) \in \mathbb{Z}$. Take $a(x), b(x) \in \mathbb{Z}[x]$ such that $a(x)q(x) + b(x)q'(x) = d$. Let p be a prime in P that does not divide d (which exists because $|P| = \infty$), and let $\bar{q}(x)$ and $\bar{q}'(x)$ be the reductions of the polynomials $q(x)$ and $q'(x)$ modulo p, respectively. By definition of P, there exists $z_0 \in \mathbb{Z}$ such that $\bar{q}(z_0) = 0$. After reducing $a(x)q(x) + b(x)q'(x) = d$ module p, we see that $\bar{q}'(z_0) \neq 0$, whence z_0 is a simple root of $q(x)$ modulo p. Thus, by Hensel's Lemma, there exists $\alpha \in z_0 + p\mathbb{Z}_p$ such that $q(\alpha) = 0$. Therefore by the statement we have already proved, $P_{q(x)} \subseteq M_{p,\alpha}$. This containment is proper because $M_{p,\alpha}$ lies over (p). Hence the ideals described in part (2) are the only maximal ideals of $\mathrm{Int}(\mathbb{Z})$. □

Exercises

Exercise 1. *Let R be a Noetherian ring, and let I be a nonzero ideal of R. Prove that the addition and multiplication of R are continuous with respect to the I-adic topology. Deduce that R is a topological ring with respect to this topology.*

Exercise 2. *For $p \in \mathbb{P}$ and $n \in \mathbb{N}$, let f be a polynomial in $\mathrm{Int}(\mathbb{Z})$ with $\deg f < p^n$. Prove that $|f(b) - f(a)|_p \le p^{n-1}|b - a|_p$ for all $a, b \in \mathbb{Z}$.*

Exercise 3. *Show that the polynomial $x^2 + x - 6$ does not have any simple root in $\mathbb{Z}_5$ modulo $5\mathbb{Z}_5$ even though it has a root in $\mathbb{Z}_5$. Deduce that we cannot always use Hensel's Lemma to argue the existence of roots of certain polynomials.*

Exercise 4. *Let p be an odd prime, and consider the polynomial $q(x) = x^2 - x + p \in \mathbb{Z}[x]$, which is irreducible in $\mathbb{Q}[x]$. Prove that the prime ideal $P_{q(x)}$ of $\mathrm{Int}(\mathbb{Z})$ is contained in two different maximal ideals of $\mathrm{Int}(\mathbb{Z})$ lying over (p).*

References

[1] P. J. Cahen and J. L. Chabert: *Integer-Valued Polynomials*, Amer. Math. Soc. Surveys and Monographs, Vol. 48, Providence, 1997.

[2] P. J. Cahen and J. L. Chabert: *What you should know about integer-valued polynomials*, Amer. Math. Monthly **123** (2016) 311–337.

[3] J. Dieudonné: *Sur les fonctions continues p-adiques*, Bull. Sci. Math. **68** (1944) 79–95.

[4] K. Mahler: *An interpolation series for continuous functions of a p-adic variable*, J. Reine Angew. Math. **199** (1958) 23–34.

Department of Mathematics, MIT, Cambridge, MA 02139

Email address: `fgotti@mit.edu`