Appendix to: valuations, completions, and hyperbolic actions of metabelian groups

Carolyn R. Abbott Sahana Balasubramanya Sam Payne
Alexander J. Rasmussen

1 Appendix: classification of ideals and factorization of formal power series

Consider a monic polynomial $f(x) \in \mathbb{Z}[x]$ with constant term which does not lie in the set $\{-1, 0, 1\}$. We consider the ring $R = \mathbb{Z}[x]/(f)$ and the element $\gamma = x + (f)$. We consider the (γ)-adic completion $\widehat{R}$ of R. There is a pre-order on ideals of $\widehat{R}$ defined by $\mathfrak{a} \preccurlyeq \mathfrak{b}$ if $\gamma^n \mathfrak{a} \subset \mathfrak{b}$ for some $n \geq 0$. This defines an equivalence relation in the usual way: $\mathfrak{a} \sim \mathfrak{b}$ if $\mathfrak{a} \preccurlyeq \mathfrak{b}$ and $\mathfrak{b} \preccurlyeq \mathfrak{a}$. The pre-order $\preccurlyeq$ descends to a partial order $\preceq$ on equivalence classes of ideals. We will call the resulting poset the *poset of ideals of* $\widehat{R}$ *up to multiplication by* γ. Our goal is to describe this poset. By a Theorem of Bourbaki ([2, Ch. 2 Sec. 2 No. 4 Proposition 10]), this poset is isomorphic to the *poset of ideals* of the localization $\gamma^{-1}\widehat{R}$. So equivalently, we will describe the poset of ideals of $\gamma^{-1}\widehat{R}$.

First we give an alternative description of the (γ)-adic completion $\widehat{R}$ of R.

Lemma 1.1. *Consider the ring $R = \mathbb{Z}[x]/(f)$. Then the completion $\widehat{R}$ is isomorphic to $\mathbb{Z}[[x]]/(f)$.*

Proof. The sequence

$$0 \to (f) \to \mathbb{Z}[x] \to R \to 0$$

is an exact sequence of finitely-generated $\mathbb{Z}[x]$-modules. We consider the completions of these modules with respect to the ideals (x^i) of $\mathbb{Z}[x]$. Since $\mathbb{Z}[x]$ is Noetherian, the sequence of (x)–adic completions

$$0 \to \widehat{(f)} \to \widehat{\mathbb{Z}[x]} \to \widehat{R} \to 0$$

is exact by [1, Proposition 10.12]. Since x acts on R in the same way as γ, the (x)-adic completion $\widehat{R}$ is just the usual (γ)-adic completion. Of course $\widehat{\mathbb{Z}[x]}$ is just the formal power series ring $\mathbb{Z}[[x]]$. The $\mathbb{Z}[x]$-module homomorphism $(f) \to \widehat{(f)}$ defines a $\mathbb{Z}[[x]]$-module homomorphism $\mathbb{Z}[[x]] \otimes_{\mathbb{Z}[x]} (f) \to \widehat{(f)}$. By [1, Proposition 10.13] this homomorphism is an isomorphism. The image of the homomorphism is exactly the ideal of $\mathbb{Z}[[x]]$ generated by f. Hence $\widehat{(f)}$ coincides with the ideal of $\mathbb{Z}[[x]]$ generated by f. □

We will prove the following:

Theorem 1.2. *Let f be a monic polynomial in $\mathbb{Z}[x]$ with constant term not lying in $\{-1, 0, 1\}$. Then the poset of ideals of $\mathbb{Z}[[x]]/(f)$ up to multiplication by $\gamma = x + (f)$ is isomorphic to the poset of divisors of f in $\mathbb{Z}[[x]]$ considered up to associates. Equivalently, the poset of ideals of $\gamma^{-1}(\mathbb{Z}[[x]]/(f))$ is isomorphic to the poset of divisors of f in $\mathbb{Z}[[x]]$ considered up to associates.*

Denote by $\overline{g} = g + (f)$ the equivalence class of a power series g. We will switch between writing $\overline{g}$ and $g + (f)$ interchangeably. The localization $x^{-1}\mathbb{Z}[[x]]$ with respect to the powers of x is the ring of formal Laurent series with coefficients in $\mathbb{Z}$. In other words, there may be infinitely many terms but only finitely many with negative exponents on x. We first prove the following elementary lemma.

Lemma 1.3. *Let $g \in \mathbb{Z}[[x]]$ which is neither a unit nor divisible by x. Then the quotient $(x^{-1}\mathbb{Z}[[x]])/(g)$ (where (g) denotes the ideal generated by g in $x^{-1}\mathbb{Z}[[x]]$) is isomorphic to the localization $\overline{x}^{-1}(\mathbb{Z}[[x]]/(g))$ (where (g) denotes the ideal generated by g in $\mathbb{Z}[[x]]$).*

Proof. Note that since g is not divisible by x, $\overline{x}$ is not a zero divisor in $\mathbb{Z}[[x]]/(g)$. Thus an element $\overline{h}/\overline{x}^i$ in $\overline{x}^{-1}(\mathbb{Z}[[x]]/(g))$ is zero only if $\overline{h} = \overline{0}$ in $\mathbb{Z}[[x]]$.

Consider the natural homomorphism $\mathbb{Z}[[x]] \to \overline{x}^{-1}(\mathbb{Z}[[x]]/(g))$. As the image of x is a unit, there is an induced homomorphism $x^{-1}\mathbb{Z}[[x]] \to \overline{x}^{-1}(\mathbb{Z}[[x]]/(g))$ sending h/x^i to $\overline{h}/\overline{x}^i$ for $h \in \mathbb{Z}[[x]]$. We see immediately that this homomorphism is surjective. The kernel contains (g) (the ideal of $x^{-1}\mathbb{Z}[[x]]$). To see that the kernel is contained in (g), consider h/x^i in the kernel. Then $\overline{h} = \overline{0}$ so that h lies in the ideal generated by g in $\mathbb{Z}[[x]]$. That is, $h/x^i = fg/x^i$ for some $f \in \mathbb{Z}[[x]]$ and we see that the kernel is contained in (g), as desired. $\square$

We first consider quotients $\mathbb{Z}[[x]]/(g^i)$ where g is an irreducible power series which is not associate to a prime $p \in \mathbb{Z}$ or the monomial x. By [4, Proposition 3.1.3] (see also [3, Theorem 1.4]) there is an isomorphism $\mathbb{Z}[[x]]/(g) \to \mathbb{Z}_p[\alpha]$ where $p \in \mathbb{Z}$ is a prime and α is a root of an irreducible polynomial $w(x) \in \mathbb{Z}_p[x]$ satisfying the following condition:

$$w(x) = pu(x) + x^n \text{ where } u \in \mathbb{Z}[x] \text{ satisfies } \deg(u) \leq n - 1.$$

First we consider the case $i = 1$.

Lemma 1.4. *Let $g \in \mathbb{Z}[[x]]$ be an irreducible power series not associate to a prime $p \in \mathbb{Z}$ or to x. Then the localization $\overline{x}^{-1}(\mathbb{Z}[[x]]/(g))$ is a field.*

Proof. Consider the prime $p \in \mathbb{Z}$ and the polynomial $w \in \mathbb{Z}_p[x]$ as described in the last paragraph. Then the localization $\overline{x}^{-1}(\mathbb{Z}[[x]]/(g))$ is isomorphic to the localization $\alpha^{-1}\mathbb{Z}_p[\alpha]$. We have the equation $\alpha^n = -pu(\alpha)$ and therefore p is a unit in $\alpha^{-1}\mathbb{Z}_p[\alpha]$. There is a natural injection from $\alpha^{-1}\mathbb{Z}_p[\alpha]$ to the finite field extension $\mathbb{Q}_p(\alpha)$. Namely, $\mathbb{Q}_p(\alpha) = \mathbb{Q}_p[x]/(w)$ and $\mathbb{Z}_p[x]/(w)$ includes into $\mathbb{Q}_p[x]/(w)$ in such a way that $x + (w)$ is a unit. We claim that this homomorphism is also surjective and thus an isomorphism of fields. We may write an element of $\mathbb{Q}_p(\alpha)$ as $h(\alpha)$ with $h \in \mathbb{Q}_p[x]$. Multiplying by a high enough power of p to clear the denominators of the coefficients of h, we have $p^i h(x) \in \mathbb{Z}_p[x]$ for some i. Since p is a unit in $\alpha^{-1}\mathbb{Z}_p[\alpha]$ we have $p^{-i}(p^i h(\alpha)) \in \alpha^{-1}\mathbb{Z}_p[\alpha]$ and the image of this element is $h(\alpha)$. Thus, the natural map $\alpha^{-1}\mathbb{Z}_p[\alpha] \to \mathbb{Q}_p(\alpha)$ is surjective as desired. $\square$

Now we consider the case $i \geq 1$.

Lemma 1.5. *Let $g \in \mathbb{Z}[[x]]$ be an irreducible power series not associate to a prime $p \in \mathbb{Z}$ or to x. Let $i \geq 1$. Then the ideal $(\overline{g})$ is the unique non-zero prime ideal of $\overline{x}^{-1}(\mathbb{Z}[[x]]/(g^i))$.*

Proof. The quotient of the localization $\overline{x}^{-1}(\mathbb{Z}[[x]]/(g^i))$ by $(\overline{g})$ is a field by Lemma 1.4 and thus $(\overline{g})$ is prime. Moreover, we have $(\overline{g})^i = 0$. Let $\mathfrak{p}$ be a non-zero prime ideal of $\overline{x}^{-1}(\mathbb{Z}[[x]]/(g^i))$. Then $(\overline{g})^i \subset \mathfrak{p}$. Since $\mathfrak{p}$ is prime, we must have in fact $(\overline{g}) \subset \mathfrak{p}$. Since $(\overline{g})$ is maximal, it must be equal to $\mathfrak{p}$. $\square$

Lemma 1.6. *Let $g \in \mathbb{Z}[[x]]$ be an irreducible power series not associate to a prime $p \in \mathbb{Z}$ or to x. Let $i \geq 1$. Then the ideals of $\overline{x}^{-1}(\mathbb{Z}[[x]]/(g^i))$ are exactly the ideals $(\overline{g}^j)$ generated by powers $\overline{g}^j$ for $0 \leq j \leq i$.*

Proof. By Lemma 1.5, $(\overline{g})$ is the unique prime ideal of $\overline{x}^{-1}(\mathbb{Z}[[x]]/(g^i))$. By [1, Exercise 1.10], every element of $\overline{x}^{-1}(\mathbb{Z}[[x]]/(g^i))$ is either nilpotent or a unit. We may write an element of this ring as $\overline{h}/\overline{x}^k$ with $h \in \mathbb{Z}[[x]]$. If g divides h then $\overline{h}/\overline{x}^k$ is nilpotent. On the other hand, if g does not divide h then $\overline{h}/\overline{x}^k$ is a unit. To see this, suppose for contradiction that $\overline{h}/\overline{x}^k \in (\overline{g})$. Then $\overline{h}/\overline{x}^k = \overline{g}\overline{h'}/\overline{x}^l$ for some $h' \in \mathbb{Z}[[x]]$ and $\overline{h}\overline{x}^l = \overline{g}\overline{h'}\overline{x}^k$. In other words, $hx^l + (g^i) = gh'x^k + (g^i)$ so that $hx^l = gh'x^k + g^ih''$ for some $h'' \in \mathbb{Z}[[x]]$. However, g divides the right hand side of this equation while it does not divide the left. This is a contradiction. Thus, if g does not divide h then $\overline{h}/\overline{x}^k$ does not lie in $(\overline{g})$ and therefore it is a unit.

Now, given any $\overline{h}/\overline{x}^k \in \overline{x}^{-1}(\mathbb{Z}[[x]]/(g^i))$ we may write $h = h'g^j$ with h' not divisible by g. We have $\overline{h}/\overline{x}^k = (\overline{h'}/\overline{x}^k)(\overline{g}^j/1)$ and by the previous paragraph, $\overline{h'}/\overline{x}^k$ is a unit. In other words, $\overline{h}/\overline{x}^k$ is associate to $\overline{g}^j$. Consider an ideal $\mathfrak{a}$. Choose j to be the minimum such that there is an element of $\mathfrak{a}$ associate to $\overline{g}^j$. Then clearly $\mathfrak{a} \subset (\overline{g}^j)$ but also $\overline{g}^j \in \mathfrak{a}$. That is, $\mathfrak{a} = (\overline{g}^j) = (\overline{g})^j$. □

Now we consider the case of a monic polynomial $f \in \mathbb{Z}[x]$ with constant term not lying in $\{-1, 0, 1\}$. We consider its prime factorization $f = uf_1^{n_1} \cdots f_r^{n_r}$ in $\mathbb{Z}[[x]]$. Here $u \in \mathbb{Z}[[x]]$ is a unit and the f_i are prime. Moreover, since the constant term of f is not ± 1, f is not a unit in $\mathbb{Z}[[x]]$ and therefore there is at least one prime in its prime factorization. The prime power series of $\mathbb{Z}[[x]]$ are either:

- associate to x;
- associate to a prime integer $p \in \mathbb{Z}$;
- not associate to x or to any prime integer. Such a power series has constant term equal to a power of a prime in $\mathbb{Z}$ times ± 1.

Note that any prime of the first type has constant term 0. Any prime of the second type has all its coefficients divisible by p. Since f has non-zero constant term, the same holds for each f_i. That is, no f_i is associate to x. Since the coefficients of f are not all divisible by a common prime integer p, the same holds for each f_i. That is, no f_i is associate to a prime integer p.

Note that the localization of a unique factorization domain is a unique factorization domain. Thus $x^{-1}\mathbb{Z}[[x]]$ is a unique factorization domain and its prime and irreducible elements coincide.

Lemma 1.7. *Let $g \in \mathbb{Z}[[x]]$ be a prime power series which is neither associate to x nor to a prime $p \in \mathbb{Z}$. Then g is prime as an element of $x^{-1}\mathbb{Z}[[x]]$. Moreover, consider two prime powers $g_1, g_2 \in \mathbb{Z}[[x]]$ neither of which is associate to x nor to a prime $p \in \mathbb{Z}$. Suppose that g_1 and g_2 are not associate to each other in $\mathbb{Z}[[x]]$. Let $n_1, n_2 \geq 1$. Then the ideal $(g_1^{n_1}, g_2^{n_2})$ generated by $g_1^{n_1}$ and $g_2^{n_2}$ in $x^{-1}\mathbb{Z}[[x]]$ is all of $x^{-1}\mathbb{Z}[[x]]$.*

Proof. Let g be a prime power series with the desired properties. First we show that g is not a unit in $x^{-1}\mathbb{Z}[[x]]$. If g is a unit then there is an element $h/x^k \in x^{-1}\mathbb{Z}[[x]]$ with $gh/x^k = 1$ in $x^{-1}\mathbb{Z}[[x]]$. Hence $gh = x^k$. However, the prime g does not divide the prime power x^k so this is a contradiction.

Consider a product of elements of $x^{-1}\mathbb{Z}[[x]]$ which is equal to g. We may write this product as $g = (h_1/x^{k_1})(h_2/x^{k_2})$ where $h_1, h_2 \in \mathbb{Z}[[x]]$. This yields $gx^{k_1}x^{k_2} = h_1h_2$ in $\mathbb{Z}[[x]]$. Hence g divides one of the h_i. Say g divides h_1. Thus g and h_1/x^{k_1} divide each other in the domain $x^{-1}\mathbb{Z}[[x]]$ and therefore they are associates while h_2/x^{k_2} is a unit. This proves that g is irreducible in $x^{-1}\mathbb{Z}[[x]]$ and hence also prime.

For the last statement, consider two non-associate prime power series $g_1, g_2 \in \mathbb{Z}[[x]]$ with the desired properties. By the proof of Lemma 1.6, an element of $\overline{x}^{-1}(\mathbb{Z}[[x]]/(g_2^{n_2}))$ is either a unit or nilpotent. Moreover, an element $\overline{h}/\overline{x}^k$ with $h \in \mathbb{Z}[[x]]$ is nilpotent exactly if g_2 divides h in $\mathbb{Z}[[x]]$. Consider the element $\overline{g_1^{n_1}} \in \overline{x}^{-1}(\mathbb{Z}[[x]]/(g_2^{n_2}))$. Since g_2 does not divide $g_1^{n_1}$ in $\mathbb{Z}[[x]]$, $\overline{g_1}^{n_1}$ is a unit. Thus, $\overline{g_1}^{n_1}(\overline{h}/\overline{x}^k) = \overline{1}$ for some $h \in \mathbb{Z}[[x]]$. In other words,

$$g_1^{n_1}h + (g_2^{n_2}) = x^k + (g_2^{n_2}) \text{ and hence } g_1^{n_1}h = x^k + g_2^{n_2}h' \text{ for some } h' \in \mathbb{Z}[[x]].$$

So $1 = g_1^{n_1}(h/x^k) - g_2^{n_2}(h'/x^k) \in (g_1^{n_1}, g_2^{n_2})$. □

Proof of Theorem 1.2. Consider a monic polynomial $f \in \mathbb{Z}[x]$ with constant term not lying in $\{-1, 0, 1\}$. By the discussion above, there is a prime factorization $f = uf_1^{n_1} \cdots f_r^{n_r}$ in $\mathbb{Z}[[x]]$ with $r \geq 1$ and all the prime factors f_i are neither associate to x nor to a prime $p \in \mathbb{Z}$. By Lemma 1.3 we have $\overline{x}^{-1}(\mathbb{Z}[[x]]/(f)) \cong (x^{-1}\mathbb{Z}[[x]])/(f)$ where (f) denotes the ideal generated by f in the localization $x^{-1}\mathbb{Z}[[x]]$. We have $(f) = (f_1^{n_1}) \cdots (f_r^{n_r})$ in $x^{-1}\mathbb{Z}[[x]]$ and by Lemma 1.7, the ideals $(f_i^{n_i})$ are pairwise coprime. Thus by the Chinese Remainder Theorem we have

$$\overline{x}^{-1}(\mathbb{Z}[[x]]/(f)) \cong (x^{-1}\mathbb{Z}[[x]])/(f) \cong (x^{-1}\mathbb{Z}[[x]])/(f_1^{n_1}) \times \cdots \times (x^{-1}\mathbb{Z}[[x]])/(f_r^{n_r}).$$

Applying Lemma 1.3 again we have

$$\overline{x}^{-1}(\mathbb{Z}[[x]]/(f)) \cong \overline{x}^{-1}(\mathbb{Z}[[x]]/(f_1^{n_1})) \times \cdots \times \overline{x}^{-1}(\mathbb{Z}[[x]]/(f_r^{n_r})).$$

An ideal of this ring has the form $\mathfrak{a}_1 \times \cdots \times \mathfrak{a}_r$ where $\mathfrak{a}_i$ is an ideal of $\overline{x}^{-1}(\mathbb{Z}[[x]]/(f_i^{n_i}))$ for each i. By Lemma 1.6 we see that in fact an ideal has the form $(\overline{f_1}^{j_1}) \times \cdots \times (\overline{f_r}^{j_r})$ where $0 \leq j_i \leq n_i$ for each i.

The divisors of f in $\mathbb{Z}[[x]]$ up to associates are $f_1^{j_1} \cdots f_r^{j_r}$ and the function

$$f_1^{j_1} \cdots f_r^{j_r} \mapsto (\overline{f_1}^{j_1}) \times \cdots \times (\overline{f_r}^{j_r})$$

is a bijection from the poset of divisors of f with the order of divisibility to the poset of ideals of $\overline{x}^{-1}(\mathbb{Z}[[x]]/(f))$. This bijection is *order-reversing*. Thus the poset of ideals of $\overline{x}^{-1}(\mathbb{Z}[[x]]/(f))$ is isomorphic to the opposite of the poset of divisors of f in $\mathbb{Z}[[x]]$. However the poset of divisors of f in $\mathbb{Z}[[x]]$ is isomorphic to its own opposite, so $\overline{x}^{-1}(\mathbb{Z}[[x]]/(f))$ is also isomorphic to the poset of divisors of f. □

References

[1] M. Atiyah and I. MacDonald. *Introduction to Commutative Algebra*. Addison-Wesley Publishing Company, 1969.

[2] N. Bourbaki. *Commutative Algebra*. Elements of Mathematics. Addison-Wesley Publishing Company, 1972.

[3] J. Elliott. Factoring formal power series over principal ideal domains. *Trans. Amer. Math. Soc.*, 366(8):3997–4019, 2014.

[4] J. M. McDonough. Integral domains arising as quotient rings of $\mathbb{Z}[[x]]$. Master's thesis, California State University - Channel Islands, 2011.