What are Rings of Integer-Valued Polynomials?

Michael Steward, June 2015

These notes are largely drawn from Cahen and Chabert's *Integer-Valued Polynomials*.

1 Introduction

Every integer is either even or odd, so we know that the polynomial $f(x) = \dfrac{x(x-1)}{2}$ is integer-valued on the integers, even though its coefficients are not in $\mathbb{Z}$. Similarly, since every binomial coefficient $\dbinom{k}{n}$ is an integer, the polynomial $\dbinom{x}{n} = \dfrac{x(x-1)...(x-n+1)}{n!}$ must also be integer-valued. These polynomials were used for polynomial interpolation as far back as the 17^{th} century. Integer-valued polynomials did not become the subject of research on their own account until Pólya and Ostrowski considered the integer-valued polynomials on an algebraic number field K, that is the set $Int(\mathcal{O}) = \{f(x) \in K[x] \mid f(\mathcal{O}) \subseteq \mathcal{O}\}$, where $\mathcal{O}$ is the ring of algebraic integers of K. Then in 1936, Thoralf Skolem was the first author to consider $Int(\mathbb{Z})$ as a ring. Since then integer-valued polynomial rings have been the subject of much study in commutative algebra.

In this note we will consider various properties of integer-valued polynomial rings, focusing particularly on $Int(\mathbb{Z})$. We will see how integer-valued polynomial rings intersect with topics throughout algebra, and we will prove a few of the results along the way.

2 Notation

Throughout this note, unless otherwise speicifed, let D be an integral domain with quotient field K, and let $Int(D)$ be the set of integer-valued polynomials on D, that is $Int(D) = \{f(x) \in K[x] \mid f(D) \subseteq D\}$.

3 $Int(D)$ as a D-module

We can check without too much trouble that $Int(D)$ is a D-module. If we restrict our attention to $Int(\mathbb{Z})$, we can find a basis for it as a $\mathbb{Z}$-module.

Lemma 3.1 *The polynomials* $\dbinom{x}{n}$ *are integer-valued.*

Proof $f(x) = \dbinom{x}{n} = \dfrac{x(x-1)...(x-n+1)}{n!}$. Notice that $f(k) = 0$ for $0 \leq k < n$. If $k \geq n$, then $f(k) \in \mathbb{N}$. Finally, if $k < 0$, then

$$f(k) = \frac{k(k-1)...(k-n+1)}{n!} = (-1)^n \frac{(n-k-1)(n-k-2)...(-k)}{n!} = (-1)^n \binom{n-k-1}{n} \in \mathbb{Z}$$

The proof of the following proposition is due to Cahen and Chabert.

Proposition 3.2 *The polynomials* $\binom{x}{n}$ *form a basis of the* $\mathbb{Z}$*-module* $Int(\mathbb{Z})$*.*

Proof There is one polynomial of each degree, so they are a basis of the $\mathbb{Q}$-module $\mathbb{Q}[x]$. By Lemma 3.1, $\binom{x}{n}$ are integer-valued, so a $\mathbb{Z}$-linear combination of them is integer-valued. Now suppose that $f \in Int(\mathbb{Z})$ is of degree n. Write $f = \alpha_0 + \alpha_1 x + ... + \alpha_n \binom{x}{n}$. Then $\alpha_0 = f(0) \in \mathbb{Z}$. By induction, suppose that $\alpha_i \in \mathbb{Z}$ for all $i < k \leq n$. Let $g_k = f - \sum_{i=0}^{k-1} \alpha_i \binom{x}{i}$. We know that $g_k = \alpha_k \binom{x}{k} + ... + \alpha_n \binom{x}{n}$ is integer-valued and $\alpha_k = g_k(k) \in \mathbb{Z}$.

For a general D, we might then wonder if $Int(D)$ has a regular basis, that is a basis with exactly one polynomial of each degree. To begin to answer this question, let's make a new defintion.

Definition Let B be a domain such that $D[x] \subseteq B \subseteq Int(D)$. Define the characteristic ideals $J_n(B)$ of B to be $J_n(B) = \{0\} \bigcup \{\alpha \in K \mid \exists f \in B, f = \alpha x^n + \alpha_{n-1}x^{n-1} + ...\}$. That is, $J_n(B)$ is the collection of leading coefficients of polynomials of degree n in B.

We can see immediately that $D \subseteq J_n(B)$ for all n, since $D[x] \subseteq B$. Also, if f has degree $m < n$ is in B, then $x^{n-m}f \in B$. So we obtain the following containments.

$$D \subseteq J_0(B) \subseteq ... \subseteq J_{n-1}(B) \subseteq J_n(B) \subseteq ... \subseteq K$$

We called these objects ideals, but in what sense are they ideals? Recall that a fractional ideal of D is a D-submodule J of K such that there is an element $d \in D$ for which dJ is an integral ideal of D.

Proposition 3.3 *For each* $n \in \mathbb{N}$*,* $J_n(B)$ *is a fractional ideal of* D*.*

Now that we have defined characteristic ideals, we can state a couple of interesting results. Let $D[x] \subseteq B \subseteq Int(D)$.

Proposition 3.4 B *has a regular basis if and only if the* D*-modules* $J_n(B)$ *are principal fractional ideals of* D*.*

Corollary 3.5 *If* D *is a principal ideal domain, then* B *has a regular basis.*

Since we have already found a regular basis for $Int(\mathbb{Z})$, it is easy to observe that the characteristic ideals of $Int(Z)$ are $J_n(Int(\mathbb{Z})) = \frac{1}{n!}\mathbb{Z}$. It is interesting to consider what these characteristic ideals should be in a more general setting. It would be great if there were a generalization of the factorial function that made sense in more rings. In 1997, Bhargava discovered the appropriate generalization of factorials which answers the question for all Dedekind domains [1]. He defines:

Definition Let D be a Dedekind domain, let S be an arbitrary subset of D, and let $p \leq D$ be a prime ideal. A *p-ordering* of S is a sequence $\{a_i\}_{i=0}^{\infty}$ of elements of S that is formed as follows:
Choose any element $a_0 \in S$;
Choose an element $a_1 \in S$ that minimizes the ℓ such that $a_1 - a_0 \in p^{\ell}$.
and in general at the k^{th} step,
Chhose an element $a_k \in S$ that minimizes the ℓ such that $(a_k - a_0)(a_k - a_1)...(a_k - a_{k-1}) \in p^{\ell}$.

Definition We will also define $v_k(S, p) = p^{\ell}$ to be the minimal power ℓ of p used in the k^{th} step of the definition above. This makes $\{v_k(S, p)\}$ a monotone increasing sequence, which we will call the *associated p-sequence* of S.

It turns out that the associated p-sequence of S is independent of our choice of p-ordering, and this allows us to define a generalized factorial function!

Definition Let D be a Dedekind domain, and S be a subset of D. Then the factorial function of S is defined by:

$$k!_S = \prod_p v_k(S, p).$$

Notice that in general this gives us an ideal of D, not an element.

Theorem 3.6 *Let D be a Dedekind domain. $Int(D)$ has a regular basis if and only if $k!_D$ is a principal ideal for all $k \geq 0$. If this is the case, the regular basis is given by:*

$$\frac{(x - a_{0,k})(x - a_{1,k})...(x - a_{k-1,k})}{k!_D}$$

where $\{a_{i,k}\}_{i=0}^{\infty}$ is a sequence in D which is termwise congruent modulo $v_k(D, p)$ to some p-ordering of D.

4 $Int(D)$ as a Ring

$Int(D)$ has many interesting ring theoretic properties. Let's explore a few of them, paying particular attention to our concrete example, $Int(\mathbb{Z})$.
Recall for our first observation that a ring is Noetherian if each of its ideals is finitely generated, or equivalently, if it satisfies the Ascending Chain Condition. That is to say, any chain of ideals $I_1 \subseteq I_2 \subseteq ...$ of the ring eventually stabilizes.

Proposition 4.1 *$Int(\mathbb{Z})$ is non-Noetherian.*

Proof Let's consider the ideals generated by the basis elements of positive degree at most the i^{th} prime. $I_j = \left(\binom{x}{1}, ..., \binom{x}{p_j}\right)$, where p_j is the j^{th} prime. Then $I_1 \subset I_2 \subset ...$ is a nonterminating propoerly ascending chain of ideals.

Prime ideals play a central role in the study of commutative rings, and understanding of the prime and maximal ideals of a ring is important when studying the structure of a ring. For $Int(\mathbb{Z})$, we can give a complete description of its prime spectrum, though proving it requires a lengthy digression into ideal-adic topology.

Theorem 4.2 *(i) The prime ideals of $Int(\mathbb{Z})$ above a prime number p are in one-to-one correspondence with the elements of the p-adic completion $\widehat{\mathbb{Z}_p}$ of $\mathbb{Z}$. To each element $\alpha \in \widehat{\mathbb{Z}_p}$, corresponds the maximal ideal $M_{p,\alpha} = \{f \in Int(\mathbb{Z}) \mid f(\alpha) \in p\widehat{\mathbb{Z}_p}\}$*
(ii) The nonzero prime ideals of $Int(\mathbb{Z})$ above (0) are in one-to-one correspondence with the monic polynomials irreducible in $\mathbb{Q}[x]$. To the irreducible polynomial q corresponds the prime $B_q = q\mathbb{Q}[x] \cap Int(\mathbb{Z})$.

Remark What is $\widehat{\mathbb{Z}_p}$?

Every integer can be written in base p as $\pm \sum_{i=0}^{n} a_i p^i$. We could think of two numbers c and d being close together if their base p representations match at the beginning. This means $c - d$ is divisible by a high power of p. For example, if $p = 5$ a sequence beginning $\{1, 1 + 3 \times 5, 1 + 3 \times 5 + 2 \times 5^2, 1 + 3 \times 5 + 2 \times 5^2 + 2 \times 5^3, ...\}$ is a Cauchy sequence if it continues in this manner, since the elements differ by higher and higher multiples of 5. But if the sequence never stabilizes, it won't converge to an element of $\mathbb{Z}$. The collection of limit points of such sequences is $\widehat{\mathbb{Z}_p}$, and its elements can be viewed as power series in p.

We can make some weaker statements that apply to many more rings. First let's give a definition.

Definition The Krull dimension of a ring is the supremum of the lengths n of chains of prime ideals $p_0 \subset p_1 \subset ... \subset p_n$ in the ring .

Lemma 4.3 *Let p be a prime ideal of D, and let $d \in D$. Then $B_{p,d} = \{f \in Int(D) \mid f(d) \in p\}$ is a prime ideal of $Int(D)$ above p.*

Proof If $f, g \in B_{p,d}$, then $[f - g](d) = f(d) - g(d) \in p$, so $f - g \in B_{p,d}$. If $f \in B_{p,d}, g \in Int(D)$, then $[fg](d) = f(d)g(d) \in p$, and hence $fg \in B_{p,d}$. Clearly $B_{p,d} \cap D = p$.

Proposition 4.4 $dim(Int(D)) \geq dim(D) + 1$

Proof Let $(0) = p_0 \subset p_1 \subset ... \subset p_n$ be a chain of prime ideals of D and let $d \in D$. Then we will show that $(0) \subset B_{p_0,d} \subset B_{p_1,d} \subset ... \subset B_{p_n,d}$ is a chain of prime ideals in $Int(D)$ of length $n + 1$. We have shown in the lemma that $B_{p_i,d}$ lies over p_i, so these ideals are distinct. We then notice that $(x - d) \in B_{p_0,d}$, and so $B_{p_0,d} \neq (0)$.

4.1 The Skolem Property

One of the most interesting ideal theoretic properites of rings of integer-valued polynomials is the Skolem property. Since the elements of these rings are polynomials, we can evaluate them at various elements of the domain D.

Definition Let I be an ideal of $Int(D)$. For each $a \in D$, the set $I(a) = \{f(a) \mid f \in I\}$ is easily seen to be an ideal of D, which we will call the ideal of values of I at a.

Now that we have defined ideals of values, it's natural to ask whether any other polynomials take the same values as the polynomials in I.

Definition Let I be an ideal of $Int(D)$. Define $I^* = \{f \in Int(D) \mid f(a) \in I(a) foreacha \in D\}$, and call I^* the Skolem closure of I.

The Skolem closure is a true closure operation, and it is the smallest ideal of $Int(D)$ with the same ideals of values as I.

Definition i) We say that $Int(D)$ has the Skolem property if the Skolem closure of each proper finitely generated ideal of $Int(D)$ is also proper.
i') Equivalently, $Int(D)$ has the Skolem property if the only finitely generated ideal I of $Int(D)$ for which $I(a) = Int(D)$ for all $a \in D$ is the full ring $Int(D)$.
ii) We say that $Int(D)$ has the strong Skolem property if each finitely generated ideal of $Int(D)$ is Skolem closed.
ii') Equivalently, $Int(D)$ has the strong Skolem property if, for any two finitely generated ideals I, J of $Int(D)$, $I(a) = J(a)$ for all $a \in D$ implies $I = J$.

Remark We have defined the Skolem property for $Int(D)$, but we could have defined it in the same way for any subset of $Int(D)$.

Example The Skolem property is an unusual one for a ring to have. Let's demonstrate that $\mathbb{Z}[x]$ does not satisfy it. Consider the ideal $I = (2, x(x-1)+1)$. $I(a) = \mathbb{Z}$ for each $a \in \mathbb{Z}$ since $x(x-1)+1$ is always odd, but $I \neq \mathbb{Z}[x]$!

Proposition 4.5 *$Int(\mathbb{Z})$ has the strong Skolem property.*

More generally,

Theorem 4.6 *If D is the ring of integers of a number field, then $Int(D)$ has the strong Skolem property.*

The Skolem property is very closely related to a number of interesting topics, one of which is Hilbert's Nullstellensatz, which can be stated as follows to make the connection clear.

Theorem 4.7 (Hilbert's Nullstellensatz I) *Let K be an algebraically closed field, then each proper ideal I of $K[x]$ has a zero in K.*

This is exactly the Skolem property! The theorem can be stated equivalently as

Theorem 4.8 (Hilbert's Nullstellensatz II) *Let K be an algebraically closed field. For each ideal I of $K[x]$, if $f \in K[x]$ is such that for each $a \in K$, $f(a) \in I(a)$, then $f \in \sqrt{I}$.*

5 Applications and Extensions

Integer-valued polynomials are an interesting topic of study in their own right, but they also provide a useful tool in other areas of mathematics. In algebraic geometry, the Hilbert polynomial is integer-valued, and the basis we found for $Int(\mathbb{Z})$ is helpful in computations of the dimension and degree of algeraics varieties. The use of Hilbert polynomials also provides a simple proof of Bézout's Theorem, which states that the number of intersection points of two plane algebraic curves is equal to the product of their degrees. See for instance, [11].

Integer-valued polynomials also appear with some regularity in algebraic topology; they appear, for example, as the maps of certain categories in homotopy theory, [8].

There are many more interesting theorems and avenues of study surrounding integer-valued polynomials. We haven't mentioned polynomials that are integer-valued on subsets, the connection between $Int(D)$ and the I-adic topology, the Stone-Weierstrass Theorem for integer-valued polynomials, integer-valued polynomials in several indeterminates, and many more fascinating topics. Check out the references if you're intersted in seeing more!

References

[1] Manjul Bhargava. The factorial function and generalizations. *The American Math. Monthly*, 107:783–799, 2000.

[2] Demetrios Brizolis. Hilbert rings of integer-valued polynomials. *Communications in Algebra*, 3(12):1051–1081, 1975.

[3] Demetrios Brizolis. A theorem on ideals in Prüfer rings of integral-valued polynomials. *Communications in Algebra*, 7(10):1065–1077, 1979.

[4] Paul-Jean Cahen and Jean-Luc Chabert. *Integer-Valued Polynomials*, volume 48 of *Mathematical Surveys and Monographs*. American Mathematical Society, 1997.

[5] Paul-Jean Cahen and Jean-Luc Chabert. Old problems and new questions around integer-valued polynomials and factorial sequences. In James W. Brewer, Sarah Glaz, William J. Heinzer, and Bruce M. Olberding, editors, *Multiplicative ideal theory in commutative algebra*. Springer US, 2006.

[6] Paul-Jean Cahen, Jean-Luc Chabert, Evan Houston, and Thomas G. Lucas. Skolem properties, value-functions, and divisorial ideals. *Journal of Pure and Applied Algebra*, 135:207–223, 1999.

[7] Jean-Luc Chabert, Scott T. Chapman, and William W. Smith. The Skolem property in rings of integer-valued polynomials. *Proceeding of the American Mathematical Society*, 126(11):3151–3159, November 1998.

[8] Torsten Ekedahl. On minimal models in integral homotopy theory. *Homology, Homotopy and Applications*, 4(2):191–218, 2002.

[9] Hiroshi Gunji and Donald McQuillan. On rings with a certain divisibility property. *Michigan Math. J.*, 22:289–299, 1975.

[10] Hiroshi Gunji and Donald McQuillan. Polynomials with integral values. *Proc. Roy. Irish Acad. Sect. A*, 78:1–7, 1978.

[11] Robin Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer, 1977.

[12] Alan Loper. Sequence domains and integer-valued polynomials. *J. Pure Appl. Algebra*, 119(2):185–210, 1997.

[13] Alexander Ostrowski. Über ganzwertige polynome in algebraischen zahlkörpern. *J. reine angew. Math.*, 149:117–124, 1919.

[14] Alexander Ostrowski and Georg Pólya. Sur les polynômes à valeurs entières dans un corps algébrique. *L'enseignement matheématique*, 19:323–324, 1917.

[15] Georg Pólya. Über ganzwertige polynome in algebraischen zahlkörpern. *J. reine angew. Math.*, 149:97–116, 1919.

[16] Thoralf Skolem. Ein satz über ganzwetige polynome. *Det Kongelige Norske Videnskabers Selskab*, 9:111–113, 1936.

[17] Thoralf Skolem. Über die lösbarkeit der gleichung $f_1(x)\mathrm{F}_1(x) + ... + f_n(x)\mathrm{F}_n(x) = 1$, wo $f_1, ..., f_n$ gegebene ganzzahlige polynome sind, in agnzzahligen polynomen F_1,...,F_n,. *Det Kongelige Norske Videnskabers Selskab*, 12:1–4, 1939.

[18] Thoralf Skolem. Einige sätze über polynome. *Avhandlinger utgitt av Det Norske Videnskap. Akad. Oslo*, 4:1–16, 1940.