MATH 436 Notes: Examples of Rings.

Jonathan Pakianathan

November 20, 2003

1 Formal power series and polynomials

Let R be a ring. We will now define the ring of formal power series on a variable x with coefficients in R. We will denote this ring by $R[[x]]$.

As an Abelian group, $R[[x]] = \prod_{i\in\mathbb{N}} R = \{(a_0, a_1, a_2, \dots)|a_j \in R\}$ is a countable direct product of $(R, +)$ with itself. Thus the elements of $R[[x]]$ are arbitrary sequences with entries in R where addition is componentwise.

We define a multiplication $\star$ via $(a_0, a_1, \dots) \star (b_0, b_1, \dots) = (c_0, c_1, \dots)$ where $c_n = \sum_{k=0}^{n} a_k b_{n-k}$ for all $n \in \mathbb{N}$.

It is easy to check that the sequence $(1, 0, 0, \dots)$ is a two-sided identity for this multiplication.

It is also easy to check that the Mth term for the sequence given by $((a_0, a_1, \dots) \star (b_0, b_1, \dots) \star (c_0, c_1, \dots))$ is $\sum_{n=0}^{M}(\sum_{k=0}^{n} a_k b_{n-k})c_{M-n}$. Since R is a ring, this equals $\sum_{k,l,s\geq 0}^{k+l+s=M} a_k b_l c_s$. This final expression is also the Mth term of the sequence $(a_0, a_1, \dots) \star ((b_0, b_1, \dots) \star (c_0, c_1, \dots))$ and so we see that $\star$ makes $R[[x]]$ into a monoid.

Finally since R has distributivity, it is easy to check that $R[[x]]$ also does. Thus $(R[[x]], +, \star)$ is a ring. It is commutative if and only if R is.

We will now introduce a formal variable symbol x and adopt the more intuitive notation of $\sum_{n=0}^{\infty} a_n x^n$ for $(a_0, a_1, a_2, \dots)$. (Note: Changing the symbol of the index of summation does not change the element represented.) The addition and multiplication defined above now can be expressed as:

$$\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} (a_n + b_n) x^n$$

and

$$(\sum_{n=0}^{\infty} a_n x^n) \star (\sum_{m=0}^{\infty} b_m x^m) = \sum_{k=0}^{\infty} (\sum_{j=0}^{k} a_j b_{k-j}) x^k.$$

Note x is just a formal variable, and "commutes" with everything in this definition. As usual given $f, g \in R[[x]]$, we will write fg instead of $f \star g$ from now on.

We now define $R[x]$ the ring of polynomials in an indeterminate x. Additively $R[x] = \oplus_{n \in \mathbb{N}} R$. Thus $(R[x], +)$ is the subgroup of $(R[[x]], +)$ corresponding to sequences which are eventually zero.

It is easy to check that in fact $R[x]$ is closed under $\star$ also and so is a subring of $R[[x]]$. We refer to the elements in $R[x]$ as polynomials in x.

We will use some typical conventions when dealing with power series and polynomials in general. If $g = a_0 + a_1 x + a_2 x^2 + \dots$ is a power series, then we will write $1x^k$ as x^k in general and drop terms of the form $0x^k$ from the expression. We also write $a_1 x^1$ as $a_1 x$ and $a_0 x^0$ as just a_0.

If $f \in R[x]$ then $f = \sum_{k=0}^{\infty} a_k x^k$ where there exists N such that $a_k = 0$ for all $k > N$. Thus we may write $f = a_0 + a_1 x^1 + \cdots + a_N x^N$ to represent the polynomial.

Thus for example the polynomial $3 + 2x^2 + x^3$ is short hand for the formal element $(3, 0, 2, 1, 0, 0, 0, \dots)$ and so forth. We will denote the zero polynomial (power series) by 0.

We now define some important concepts in the rings $R[[x]]$ and $R[x]$.

Definition 1.1 (Codegree). *The codegree of a nonzero power series is defined as* $codeg(\sum_{n=0}^{\infty} a_n x^n) = min\{n \geq 0 | a_n \neq 0\}$.

Also if $f \in R[[x]]$ *is nonzero, we define* $L(f) = a_{codeg(f)}$ *to be this nonzero coeffiecient.*

Thus in general, $codeg(f) \in \mathbb{N}$ *and*

$$f = L(f)x^{codeg(f)} + \text{ terms in higher powers of } x.$$

By convention we formally set $codeg(0) = \infty$ *and agree* $n \leq \infty$ *for all* $n \in \mathbb{N}$.

Definition 1.2 (Degree). *The degree of a nonzero polynomial is defined as* $\deg(\sum_{n=0}^{\infty} a_n x^n) = max\{n \geq 0 | a_n \neq 0\}$.

Also if $f \in R[x]$ *is nonzero, we define* $H(f) = a_{deg(f)}$ *to be this nonzero coefficient.*

Thus in general, $deg(f) \in \mathbb{N}$ and

$$f = H(f)x^{deg(f)} + \text{ terms in lower powers of } x.$$

By convention we formally set $deg(0) = -\infty$ and $deg(g) = \infty$ if g is a power series which is not a polynomial. We agree to say $-\infty \leq n \leq \infty$ for all $n \in \mathbb{N}$.

Proposition 1.3. *For f, g nonzero power series then*

$$codeg(fg) \begin{cases} = codeg(f) + codeg(g) \text{ if } L(f)L(g) \neq 0 \\ > codeg(f) + codeg(g) \text{ if } L(f)L(g) = 0. \end{cases}$$

Furthermore if $L(f)L(g) \neq 0$ then $L(fg) = L(f)L(g)$.

Thus if R is an integral ring, so is $R[[x]]$. Furthermore in this case, the units of $R[[x]]$ are exactly the power series $\sum_{n=0}^{\infty} a_n x^n$ whose constant term a_0 is a unit in R.

Proof. If f and g are nonzero then we may write
$f = L(f)x^{codeg(f)} +$ terms in higher powers of x and similarly
$g = L(g)x^{codeg(g)} +$ terms in higher powers of x.

A simple calculation then shows that
$fg = L(f)L(g)x^{codeg(f)+codeg(g)} +$ terms in higher powers of x. The first part follows from this observation.

Now if R is an integral ring, it has no zero divisors. Given f, g nonzero, since $L(f)$ and $L(g)$ are nonzero, then $L(f)L(g) = L(fg)$ is not zero either. Thus we see that fg is nonzero and so $R[[x]]$ has no zero divisors.

Now if f is a unit of $R[[x]]$ then there is $g \in R[[x]]$ with $fg = 1 = gf$. Thus we see $codeg(f) + codeg(g) = codeg(1) = 0$ and $L(f)L(g) = L(1) = 1 = L(g)L(f)$. Thus we conclude $codeg(f) = codeg(g) = 0$ and that $L(f)$ and $L(g)$ are units in R.

Conversely suppose we have a power series $f = \sum_{n=0}^{\infty} a_n x^n \in R[[x]]$ with a_0 a unit in R. We seek a power series $g = \sum_{m=0}^{\infty} b_m x^m \in R[[x]]$ such that $fg = 1$. This translates to the equations

$$\sum_{k=0}^{N} a_k b_{N-k} = \delta_{N,0}$$

for $N \in \mathbb{N}$ where δ is the usual Kronecker symbol. Let us refer to the Nth equation as $P(N)$.

The equation $P(0)$ is $a_0 b_0 = 1$. This has a solution $b_0 \in R$ since a_0 is a unit. Suppose we have inductively solved for $b_0, b_1, \ldots, b_M \in R$ such that equations $P(0)$ thru $P(M)$ hold, then the equation $P(M+1)$ is $a_0 b_{M+1} + a_1 b_M + \cdots + a_M b_1 + a_{M+1} b_0 = 0$.

We may solve this for b_{M+1} via $b_{M+1} = a_0^{-1}(-a_1 b_M - \cdots - a_M b_1 - a_{M+1} b_0)$ and so we see that we can recursively solve for a power series g such that $fg = 1$. Similarly we may solve for a power series h such that $hf = 1$.

By basic monoid theory, since f has a left and a right inverse, they agree and f is a unit of $R[[x]]$. □

Proposition 1.4. *Let R be a ring and let f and g be nonzero polynomials in $R[x]$. Then*

$$deg(fg) \begin{cases} = deg(f) + deg(g) \text{ if } H(f)H(g) \neq 0 \\ < deg(f) + deg(g) \text{ if } H(f)H(g) = 0 \end{cases}$$

So if $H(f)H(g) \neq 0$, then $H(fg) = H(f)H(g)$.

Thus if R is an integral ring, so is $R[x]$. Thus in this case, the units of $R[x]$ are just the constant polynomials a_0 where a_0 is a unit of R.

Proof. The first part of the proof is similar to the previous proposition and is left to the reader.

Now if f is a unit of $R[x]$ then by definition, there is $g \in R[x]$ such that $fg = 1 = gf$. Thus we see $deg(f) + deg(g) = deg(fg) = deg(1) = 0$ and $L(f)L(g) = 1 = L(g)L(f)$. Thus $deg(f) = deg(g) = 0$ and $L(f), L(g)$ are units which proves the proposition.

□

Example 1.5. *Note that $f(x) = 1 + x$ is a polynomial in $\mathbb{Z}[x]$. Since $deg(f) > 0$, f is not a unit in $\mathbb{Z}[x]$. However since the constant term of f is a unit in $\mathbb{Z}$, we know that f is a unit in $\mathbb{Z}[[x]]$.*

In fact it is a simple check to see that $\sum_{n=0}^{\infty}(-1)^n x^n$ is its inverse in $\mathbb{Z}[[x]]$.

Example 1.6 (Bernoulli Series). *In $\mathbb{Q}[[x]]$ we may define the formal power series*

$$e^x = \sum_{n=0}^{\infty} \frac{1}{n!} x^n.$$

We may then write $e^x - 1 = xg(x)$ where $g(x) = \sum_{n=1}^{\infty} \frac{1}{n!} x^{n-1} = \sum_{n=0}^{\infty} \frac{1}{(n+1)!} x^n$.

We will write $g(x) = \frac{e^x - 1}{x}$ *by a slight abuse of notation.*

Since $g \in \mathbb{Q}[[x]]$ *has constant term* 1*, we know* $g^{-1} \in \mathbb{Q}[[x]]$ *exists. Thus* $g^{-1}(x) = \frac{x}{e^x - 1} = \sum_{n=0}^{\infty} B_n x^n$.

The B_n *are given recursively by* $\sum_{k=0}^{n} \frac{1}{(k+1)!} B_{n-k} = \delta_{n,0}$ *and are called the Bernoulli numbers.*

They are important in number theory and differential topology.

Example 1.7 (Generating functions). *Sometimes given a sequence* $\{a_n\}_{n \in \mathbb{N}}$ *in a ring* R*, it is useful to view the sequence as a formal power series* $f(x) = \sum_{n=0}^{\infty} a_n x^n \in R[[x]]$*.* f *is refered to as a generating function for the sequence* $(a_0, a_1, a_2, \dots)$.

For example we know that $(1 + x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k \in \mathbb{Z}[x] \subseteq \mathbb{Z}[[x]]$*. This can be used to obtain many identities involving the binomial coefficients.*

For example: $(1 + x)^n = (1 + x)^s (1 + x)^{n-s}$ *for any integer* $0 \leq s \leq n$ *yields the Van Der Monde identity* $\binom{n}{k} = \sum_{l=0}^{k} \binom{s}{l} \binom{n-s}{k-l}$*. (Here we use the convention* $\binom{b}{a} = 0$ *if* $a > b$ *or* $a < 0$*.)*

You will explore more generating functions in the exercises.

2 Group (Monoid) Rings

Definition 2.1. *Let* R *be a ring and* $(G, \star)$ *be a group (monoid). We define the group (monoid) ring* RG *as follows:*

Additively, i.e., as Abelian groups under $+$ *we set* $RG = \oplus_{g \in G} R$.

We will write $(r_g)_{g \in G}$ *as* $\sum_{g \in G} r_g g$ *and drop terms of the form* $0g$ *where* $0 \in R$ *is the additive identity of* R.

Thus the elements of RG *are finite formal sums of elements in* G *with coefficients in the ring* R.

We define the multiplication in this ring as follows:

$$(\sum_{g \in G} r_g g)(\sum_{h \in G} s_h h) = \sum_{w \in G} c_w w$$

where $c_w = \sum_{gh = w} r_g s_h$.

It is a routine check to show that this multiplication indeed makes RG *into a ring with multiplicative identity* $1e$ *where* $1 \in R$*,* $e \in G$ *are the respective identities.*

Example 2.2 (Polynomial rings). *Let* G *a free abelian monoid on a single element* x*. Thus* $G = \{e, x, x^2, x^3, \dots\}$ *is isomorphic to* $(\mathbb{N}, +)$.

It is easy to check that RG is just $R[x]$ the polynomial ring on the indeterminate x.

Now let H be a free abelian group on a single element x. We will write $H = \{\dots, x^{-2}, x^{-1}, e, x, x^2, \dots\}$ instead of in the usual way as it makes things easier to think about in the group ring. Note H is isomorphic to $(\mathbb{Z}, +)$.

It is easy to check that the group ring RH consists of elements of the form $a_{-n}x^{-n} + a_{-(n-1)}x^{-(n-1)} + \cdots + a_{-1}x^{-1} + a_0 + a_1x^1 + \cdots + a_nx^n$ for various $n \in \mathbb{N}$ and $a_j \in R$. This is called the ring of Laurent polynomials with coefficients in R and is often denoted $R[x, x^{-1}]$.

We do one more example to illustrate the computation of products in a group ring.

Example 2.3. *Let Σ_3 be the symmetric group on 3 letters and consider its integral group ring $\mathbb{Z}[\Sigma_3]$.*

Recall $\Sigma_3 = \{e, (12), (13), (23), (123), (132)\}$.

Now $2(12) + 5(13), 2(12) + 7(13) \in \mathbb{Z}[\Sigma_3]$. The product can be calculated as follows:

$$\begin{aligned}
&(2(12) + 5(13))(2(12) + 7(13)) \\
&= 4(12)(12) + 10(13)(12) + 14(12)(13) + 35(13)(13) \\
&= 4e + 10(123) + 14(132) + 35e \\
&= 39e + 10(123) + 14(132).
\end{aligned}$$

3 Direct Products

Let $\{R_\alpha\}_{\alpha \in I}$ be a collection of rings indexed by I. Then we may form the direct product ring, denoted $\prod_{\alpha \in I} R_\alpha$ as follows:

$\prod_{\alpha \in I} R_\alpha = \{(r_\alpha)_{\alpha \in I} | r_\alpha \in R_\alpha\}$, i.e., as a set, the direct product is just the Cartesian product.

The addition and multiplication are defined componentwise, i.e.,

$$(r_\alpha)_{\alpha \in I} \cdot (s_\alpha)_{\alpha \in I} = (r_\alpha s_\alpha)_{\alpha \in I}$$

and

$$(r_\alpha)_{\alpha \in I} + (s_\alpha)_{\alpha \in I} = (r_\alpha + s_\alpha)_{\alpha \in I}.$$

It is an easy check that this defines a ring structure as long as the individual R_α are rings.

The multiplicative identity is hence the tuple $(1_\alpha)_{\alpha \in I}$ where 1_α is the multiplicative identity in R_α for all $\alpha \in I$.

Note the direct sum $\oplus_{\alpha \in I} R_\alpha$ is a subring (without 1 if $|I| = \infty$) of the direct product.

Just as in the discussion for groups, it is easy to see that we have natural inclusion and projection maps $\lambda_\beta : R_\beta \to \prod_{\alpha \in I} R_\alpha$ and $\pi_\beta : \prod_{\alpha \in I} R_\alpha \to R_\beta$ for each $\beta \in I$ and that these maps are homomorphisms of rings.

Finally it is easy to check that with respect to these maps, the direct product of rings is a product for the category of rings and the direct sum of rings is a coproduct for the category of rings without 1 just as we did before for Abelian groups.