Polynomial Rings

1. Definitions and Basic Properties

For convenience, the ring will always be a commutative ring with identity.

Basic Properties
The polynomial ring $R[x]$ in the indeterminate x with coefficients from R is the set of all formal sums $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ with $n \geq 0$ and each $a_i \in R$.
Addition of polynomials is componentwise:

$$\sum_{i=0}^{n} a_ix^i + \sum_{i=0}^{n} b_ix^i = \sum_{i=0}^{n}(a_i + b_i)x^i.$$

Multiplication is performed by first defining $(ax^i)(bx^j) = abx^{i+j}$ and then extending to all polynomials by the distributive laws so that in general

$$\left(\sum_{i=0}^{n} a_ix^i\right) \times \left(\sum_{i=0}^{m} b_ix^i\right) = \sum_{k=0}^{n+m}\left(\sum_{i=0}^{k} a_ib_{k-i}\right)x^k.$$

In this way $R[x]$ is a commutative ring with identity (the identity 1 from R) in which we identify R with the subring of constant polynomials.

Proposition 1: Let R be an integral domain. Then

(1) degree $p(x)q(x)$ = degree $p(x)$ + degree $q(x)$ if $p(x)$, $q(x)$ are nonzero

(2) the units of $R[x]$ are just the units of R

(3) $R[x]$ is an integral domain.

Proof:

1. If R has no zero divisors then neither does $R[x]$; if $p(x)$ and $q(x)$ are polynomials with leading terms a_nx^n and b_mx^m, respectively, then the leading term of $p(x)q(x)$ is $a_nb_mx^{n+m}$, and $a_nb_m \neq 0$. (*This also proves* (3)).
2. If $p(x)$ is a unit, say $p(x)q(x) = 1$ in $R[x]$, then degree $p(x)$ + degree $q(x) = 0$, so both $p(x)$ and $q(x)$ are elements of R, hence are units in R since their product is 1.
3. Since R is an integral domain, it is in particular a commutative ring with identity. From the definition of multiplication in $R[x]$, it follows very easily that $R[x]$ is also a commutative with identity $1_{R[x]} = 1_R$. By proof of induction on degree n you can show that the product of nonzero polynomials in $R[x]$ is nonzero. Therefore, $R[x]$ is an integral domain.

Proposition 2: Let I be an ideal of ring R and let $(I) = I[x]$ denote the ideal of $R[x]$ generated by I. Then

$$R[x]/(I) \cong (R/I)[x].$$

In particular, if I is a prime ideal of R then (I) is a prime ideal of $R[x]$.

Proof: There is a natural map $\varphi : R[x] \to (R/I)[x]$ given be reducing each of the coefficients of a polynomial modulo I. Show that φ is a ring homomorphism, and ker $\varphi = I[x] = (I)$. By Proposition 1, I is a prime ideal in $R \to R/I$ and $(R/I)[X]$ are integral domains.

The next definition, is one we looked at in class last week, which is the description of the natural extension to polynomial rings in several variables.

Definition 3: The polynomial ring in the variables $x_1, x_2, ..., x_n$ with coefficients in R, denoted

$$R[x_1, x_2, ..., x_n] = R[x_1, x_2, ..., x_{n-1}][x_n]$$

Example 4:

Let $p(x, y, z) = 2x^2y - 3xy^3z + 4y^2z^5$ and $q(x, y, z) = 7x^2 + 5x^2y^3z^4 - 3x^2z^3$ be polynomials in $\mathbb{Z}[x, y, z]$.

Note: The polynomial ring $\mathbb{Z}[x, y, z]$ in three variables x, y and z with integers coefficients consists of all finite sums of monomial terms of the form $ax^iy^jz^k$ (of degree $i + j + k$).

```
sage: R1 = QQ['x,y,z']
sage: (x,y,z) = R1.gens()
sage: px = 2*x^2*y-3*x*y^3*z+4*y^2*z^5;
sage: qx = 7*x^2+5*x^2*y^3*z^4-3*x^2*z^3;
```

(a) Write each of p and q as a polynomial in x with coefficients in $\mathbb{Z}[y, z]$.

```
sage: R2 = QQ['y,z']['x']
sage: R2(px)
(2*y)*x^2 - (3*y^3*z)*x + 4*y^2*z^5
sage: R2(qx)
(5*y^3*z^4 - 3*z^3 + 7)*x^2
```

(b) Find the degree of p and q.

```
sage: px.degree()
7
sage: qx.degree()
9
```

(c) Find the degree of p and q in each of the three variables x, y and z.

```
sage: px.exponents()
[(0, 2, 5), (1, 3, 1), (2, 1, 0)]
sage: qx.exponents()
[(2, 3, 4), (2, 0, 3), (2, 0, 0)]
```

(d) Compute pq and find the degree of pq in each of the three variables x, y and z.

```
sage: rx = px*qx; rx
20*x^2*y^5*z^9 - 15*x^3*y^6*z^5 + 10*x^4*y^4*z^4 - 12*x^2*y^2*z^8 +
9*x^3*y^3*z^4 + 28*x^2*y^2*z^5 - 6*x^4*y*z^3 - 21*x^3*y^3*z + 14*x^4*y
sage: rx.degree()
16
sage: rx.exponents()
[(2, 5, 9), (3, 6, 5), (4, 4, 4), (2, 2, 8), (3, 3, 4), (2, 2, 5),
(4, 1, 3), (3, 3, 1), (4, 1, 0)]
```

(e) Write pq as a polynomial in the variable z with coefficients in $\mathbb{Z}[x, y]$.

```
sage: R3 = QQ['x,y']['z']
sage: R3(rx)
20*x^2*y^5*z^9 - 12*x^2*y^2*z^8 + (-15*x^3*y^6 + 28*x^2*y^2)*z^5 +
(10*x^4*y^4 + 9*x^3*y^3)*z^4 - 6*x^4*y*z^3 - 21*x^3*y^3*z + 14*x^4*y
```

2. Polynomial Rings over Fields I

Theorem 5: (*Division Algorithm*) Let F be a field. The polynomial $F[x]$ is a Euclidean Domain. Specifically, if $a(x)$ and $b(x)$ are two polynomials in $F[x]$ with $b(x)$ nonzero, then there are *unique* $q(x)$ and $r(x)$ in $F[x]$ such that

$$a(x) = q(x)b(x) + r(x) \qquad \text{with } r(x) = 0 \text{ or degree } r(x) < \text{degree } b(x).$$

Proof: If $a(x)$ is the zero polynomial then take $q(x) = r(x) = 0$. We may therefore assume $a(x) \neq 0$ and prove the existence of $q(x)$ and $r(x)$ by induction on $n =$ degree $a(x)$.
As for the uniqueness, suppose $q_1(x)$ and $r_1(x)$ also satisfied the conditions of the theorem.

$$a(x) - q(x)b(x) < m \text{ and } a(x) - q_1(x)b(x) < m \rightarrow b(q(x) - q_1(x)) < m$$

hence $q(x) - q_1(x)$ must be 0, that is, $q(x) = q_1(x) \Rightarrow r(x) = r_1(x)$.

Example 6:

Determine the greatest common divisor of $a(x) = x^3 + 1$ and $b(x) = x^2 + 2x + 1$ in $\mathbb{Q}[x]$.

$$\boxed{\begin{aligned} x^3 + 1 &= (x^2 + 2x + 1)(Ax + B) + Cx + D \\ &= Ax^3 + (2A + B)x^2 + (A + 2B + C)x + (B + D) \\ A = 1, &\qquad B = -2, \qquad C = 3, \qquad D = 3 \end{aligned}}$$

$$\begin{aligned} x^3 + 1 =& (x^2 + 2x + 1)(x - 2) + 3(x + 1) \\ x^2 + 2x + 1 =& (x + 1)(x + 1) + 0 \end{aligned}$$

Thus, $\gcd(x^3 + 1, x^2 + 2x + 1) = x + 1$.

Definition 7: *Principal Ideal Domain* (PID)
A *principal ideal domain* is an integral domain R in which every ideal has the form

$$(a) = \{ra | r \in R\}$$

for some a in R.

Definition 8: *Unique Factorization Domain* (UFD)
An integral domain D is a *unique factorization domain* if

(1) every nonzero element of D that is not a unit can be written as a product of irreducibles of D; and

(2) the factorization into irreducibles is unique up to associates and the order in which the factors appear.

Exercise 9: Show that if F is a field, then $F[x]$ is a Principal Ideal Domain and a Unique Factorization Domain.

Corollary 10: If R is any commutative ring such that the polynomial ring $R[x]$ is a Principal Ideal Domain, then R is necessarily a field.

Proof: Assume $R[x]$ is a Principal Ideal Domain. Since R is a subring of $R[x]$ then R must be an integral domain (recall that $R[x]$ has an identity if and only if R does). The ideal (x) is a nonzero prime ideal in $R[x]$ because $R[x]/(x)$ is isomorphic to the integral domain R. (x) is a maximal ideal, (*since every nonzero prime ideal in a Principal Ideal Domain is a* *maximal ideal*), hence the quotient R is a field (*since the ideal* (x) *is a maximal ideal if and only if the quotient ring* R *is a field*).

Example 11:

The ring $\mathbb{Z}$ of integers is a Principal Ideal Domain, but the ring $\mathbb{Z}[x]$ is not a Principal Ideal Domain, since $(2, x)$ is not principal in this ring.

Proof: The ideal (p, x), where $p \in \mathbb{Z}$ is any prime, is a non-principal ideal (the only divisor of both p and x is 1). Suppose $(x, 2)(p(x))$, where $p(x) \in \mathbb{Z}[x]$.
If $2 \in (x, 2)$, then $p(x) = c$, where $c \in \{-2, 2\}$. Thus, $(x, 2) = (p(x)) = (c)$, $c \in \{-2, 2\}$.
Now for $x \in (x, 2)$, there exists $h(x) \in \mathbb{Z}[x]$ such that $x = h(x)c$, where $h(x) = ax$, $a \in \mathbb{Z}$.
Therefore, $x = h(x)c = axc$, where $a \neq 0$ and $c \neq 0$. Then $1 = ac$, $c \in \{-2, 2\}$. So $c = 2$ and $a = \frac{1}{2}$ or $c = -2$ and $a = -\frac{1}{2}$ but $a = \pm\frac{1}{2} \notin \mathbb{Z}$ then $h(x) \notin \mathbb{Z}$, contradiction.
Thus, $(x, 2)$ cannot be generated by a single polynomial $p(x)$, and $\mathbb{Z}[x]$ is not a principal ideal domain.

3. Polynomial Rings that are Unique Factorization Domains

Proposition 12: Let R be a Unique Factorization Domain. Suppose that g and h are elements of $R[x]$ and let $f(x) = g(x)h(x)$. Then the content of f is equal to the content of g times the content of h.

Proof: It is clear that the content of g divides the content of f. Therefore we may assume that the content of g and h is one, and we only have to prove that the same is true for f. However, let's assume this not true. Since R is a Unique Factorization Domain, it follows that there is a prime p that divides the content of f. We may write

$$g(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \quad \textit{and} \quad h(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0.$$

As the content of g is one, at least one coefficient of g is not divisible by p. Let i be the first such, so that p divides a_k, for $k < i$ whilst p does not divide a_i. Similarly pick j so that p divides b_k, for $k < j$, whilst p does not divide b_j.
Consider the coefficient of x^{i+j} in f. This is equal to

$$a_0 b_{i+j} + a_1 b_{i+j-1} + \cdots + a_{i-1} bj + 1 + a_i b_j + a_{i+1} b_{j+1} + \cdots + a_{i+j} b_0.$$

Note that p divides every term of this sum, except the middle one $a_i b_j$. Thus p does not divide the coefficient of x^{i+j} . But this contradicts the definition of the content.

Proposition 13: (*Gauss' Lemma*) Let R be a Unique Factorization Domain with field of fractions F and let $p(x) \in R[x]$. If $p(x)$ is reducible in $F[x]$ then $p(x)$ is reducible in $R[x]$. More precisely, if $p(x) = A(x)B(x)$ for some non-constant polynomials $A(x), B(x) \in F[x]$, then there are nonzero elements $r, s \in F$ such that $rA(x) = a(x)$ and $sB(x) = b(x)$ both lie in $R[x]$ and $p(x) = a(x)b(x)$ is a factorization in $R[x]$.

Proof: The coefficients of the polynomials on the right hand side of the equation $p(x) = A(x)B(x)$ are elements in the field F, hence are quotients of elements from the Unique Factorization Domains R. Multiplying through by a common denominator for all these coefficients, we obtain

$$dp(x) = a'(x)b'(x),$$

where now $a'(x)$ and $b'(x)$ are elements of $R[x]$ and d in a nonzero element of R. Now write

$$a'(x) = ra(x) \qquad \textit{and} \qquad b'(x) = sb(x).$$

We get

$$dp(x) = rsa(x)b(x).$$

By the proposition above, d divides rs, $rs = d\gamma$, where $\gamma \in R$. Thus, replacing $a(x)$ with $\gamma a(x)$, we have

$$p(x) = a(x)b(x).$$

Example 14:

Prove that if $f(x)$ and $g(x)$ are polynomials with rational coefficients whose product $f(x)g(x)$ has integer coefficients, then the product of any coefficient of $g(x)$ with any coefficient of $f(x)$ is an integer.

Note that $f(x)g(x)$ has integer coefficients, $\mathbb{Z}[x]$, and factors with rational coefficients, $\mathbb{Q}[x]$. By Gauss' Lemma, there exists $r, s \in \mathbb{Q}$ such that $rf, sg \in \mathbb{Z}[x]$ and $(rf)(sg) = fg$. Since $\mathbb{Q}$ is an integral domain, in fact $rs = 1$. Let f_i and g_i denote the coefficients of f and g, respectively; we have $rf_i \in \mathbb{Z}$ and $r^{-1}g_i \in \mathbb{Z}$, so that $f_i g_j \in \mathbb{Z}$ for all i and j.

Exercise 15: Prove that R is a Unique Factorization Domain if and only if $R[x]$ is a Unique Factorization Domain.

Corollary 16: If R is a Unique Factorization Domain, then a polynomial ring in any number of variables with coefficients in R is also a Unique Factorization Domain.

Proof: For finitely many variables, this follows by induction from the theorem (exercise 14) above, since a polynomial ring in n variables can be consdered as a polynomial ring gin one variable with coefficients in a polynomial ring in $n-1$ variables. The general case follows from the definition of a polynomial ring in an arbitrary number of variables as the union of polynomial rings in finitely many variables.

Example 17:

- $\mathbb{Z}[x]$, $\mathbb{Z}[x, y]$, etc. are Unique Factorization Domains. The ring $\mathbb{Z}[x]$ gives an example of a Unique Factorization Domain that is not a Principal Ideal Domain.
- $\mathbb{Q}[x]$, $\mathbb{Q}[x, y]$, etc. are Unique Factorization Domains.

4. Irreducibility Criteria

Proposition 18:

(a) Let F be a field and let $p(x) \in F[x]$. Then $p(x)$ has a factor of degree one if and only if $p(x)$ has a root in F, that is, there is an $\alpha \in F$ with $p(\alpha) = 0$.

Proof: If $p(x)$ has a factor of degree one, then since F is a field, we may assume the factor is monic, i.e., is of the form $(x - \alpha)$ for some $\alpha \in F$. But then $p(\alpha) = 0$. Conversely, suppose $p(\alpha) = 0$. By the Division Algorithm in $F[x]$ we amy write

$$p(x) = q(x)(x - \alpha) + r$$

where r is a constant. Since $p(\alpha) = 0$, r must be 0, hence $p(x)$ has $(x - \alpha)$ as a factor.

(b) A polynomial of degree two or three over a field F is reducible if and only if it has a root in F.

Proof: This follows immediately from the previous proposition, since a polynomial of degree two or three is reducible if and only if it has at least one linear factor.

(c) Let $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial of degree n with integer coefficients. If $r/s \in \mathbb{Q}$ is in lowest terms (i.e., r and s are relatively prime integers) and r/s is a root of $p(x)$, then r divides the constant term and s divides the leading coefficient of $p(x)$: $r|a_0$ and $s|a_n$. In particular, if $p(x)$ is a *monic* polynomial with integer coefficients and $p(d) \neq 0$ for all integers d dividing the constant term of $p(x)$, then $p(x)$ has no roots in $\mathbb{Q}$.

Proof: By hypothesis, $p(r/s) = 0 = a_n(r/s)^n + a_{n-1}(r/s)^{n-1} + \cdots + 0$. Multiplying through by s^n gives

$$0 = a_n r^n + a_{n-1}r^{n-1}s + \cdots + a_0 s^n.$$

Thus $a_n r^n = s(-a_{n-1}r^{n-1} - \cdots - a_0 s^{n-1})$, so s divides $a_n r^n$. By assumption, s is relatively prime to r and it follows that $s \mid a_n$. Similarly, solving the equation for $a_0 s^n$ shows that $r \mid a_0$. The last assertion of the proposition follows from the previous ones.

Example 19:

The polynomial $p(x) = x^2 + x + 1$ is irreducible in $\mathbb{Z}/2\mathbb{Z}[x]$ since it does not have a root in $\mathbb{Z}/2\mathbb{Z}[x]$: $0^2 + 0 + 1 = 1$ and $1^2 + 1 + 1 = 1$.

Proposition 20: Let I be a proper ideal in the integral domain R and let $p(x)$ be a non-constant monic polynomial in $R[x]$. If the image of $p(x)$ in $(R/I)[x]$ can't be factored in $(R/I)[x]$ into two polynomials of smaller degree, then $p(x)$ is irreducible in $R[x]$.

Proof: Suppose $p(x)$ cannot be factored in $(R/I)[x]$ but that $p(x)$ is reducible in $R[x]$. This means there are monic, non-constant polynomials $a(x)$ and $b(x)$ in $R[x]$ such that $p(x) = a(x)b(x)$. By Proposition 2, reducing the coefficients modulo I gives a factorization in $(R/I)[x]$ with non-constant factors, a contradiction.

Example 21:

Consider the polynomial $p(x) = x^2+x+1$ in $\mathbb{Z}[x]$. Reducing modulo 2, we see from Example 19 above that $p(x)$ is irreducible in $\mathbb{Z}[x]$. Similarly, $x^3 + x + 1$ is irreducible in $\mathbb{Z}[x]$ because it is irreducible in $\mathbb{Z}[x]/2\mathbb{Z}[x]$.

Exercise 22: Let $f(x) \in \mathbb{Z}[x]$. Prove that if $f(x)$ is reducible over $\mathbb{Q}$, then it is reducible over $\mathbb{Z}$.

Corollary 23: (*Eisenstein's Criterion for* $\mathbb{Z}[x]$) Let p be a prime in $\mathbb{Z}$ and let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, $n \geq 1$. Suppose p divides a_i for all $i \in \{0, 1, \cdots n-1\}$ but that p^2 does not divide a_0. Then $f(x)$ is irreducible in both $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$.

Proof: Suppose $f(x)$ is reducible over $\mathbb{Z}$, then there exist elements $g(x)$ and $h(x)$ in $\mathbb{Z}[x]$ such that $f(x) = g(x)h(x)$, $1 \leq \deg\, g(x)$, and $1 \leq \deg\, h(x) < n$. Say $g(x) = b_r x^r + \cdots + b_0$ and $h(x) = c_s x^s + \cdots + c_0$. Then, since $p \mid a_0$, $p^2 \nmid a0$, and $a_0 = b_0 c_0$, it follows that p divides one of b_0 and c_0 but not the other. Let us say $p \mid b_0$ and $p \nmid c_0$. Also, since $p \mid a_n = b_r c_s$, we know that $p \mid b_r$. So, there is a least integer t such that $p \nmid b_t$. Now, consider $a_t = b_t c_0 + b_{t-1}c_1 + \cdots + b_0 c_t$. By assumption, p divides a_t and, by choice of t, every summand on the right after the first one is divisible by p. Clearly, this forces p to divide $b_t c_0$ as well. This is impossible, however, since p is prime and p divides neither b_t nor c_0.

Example 24:

Prove that the polynomial $x^4 - 4x^3 + 6$ is irreducible in $\mathbb{Z}[x]$.

The polynomial $x^4 - 4x^3 + 6$ is irreducible in $\mathbb{Z}[x]$ because $2 \nmid 1$ and $4 \nmid 6$ but 2 does divide -4, 0, and 6.

Example 25:

Let p be a prime, the p^{th} cyclotomic polynomial

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

is irreducible over $\mathbb{Z}$.

Let $f(x) = \Phi_p(x+1) = \frac{(x+1)^p - 1}{(x+1)-1} = x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \cdots + \binom{p}{1}$. Then, since every coefficient except that of x^{p-1} is divisible by p and the constant term is not divisible by p^2, by Eisenstein's Criterion, $f(x)$ is irreducible over $\mathbb{Z}$. So, if $\Phi_p(x) = g(x)h(x)$ were a nontrivial factorization of $\Phi_p(x)$ over $\mathbb{Z}$, then $f(x) = \Phi_p(x+1) = g(x+1) \cdot h(x+1)$ would be a nontrivial factorization of $f(x)$ over $\mathbb{Z}$. Since this is impossible, we conclude that $\Phi_p(x)$ is irreducible over $\mathbb{Z}$.

Definition:

(1) A commutative ring with identity $1 \neq 0$ is called an *integral domain* if it has no zero divisors.

(2) An ideal M in an arbitrary ring S is called a *maximal ideal* if $M \neq S$ and the only ideals containing M are M and S.

(3) Assume R is commutative. An ideal P is called a *prime ideal* if $P \neq R$ and whenever the product ab of two elements $a, b \in R$ is an element of P, then at least one of a and b is an element of P.

(4) A *principal ideal* is an ideal I in a ring R that is generated by a single element a of R through multiplication by every element of R, $(a) = \{ra | r \in R\}$.

Propsition:

(1) Every nonzero prime ideal in a Principal Ideal Domain is a maximal ideal.

Proof: Let (p) be a nonzero prime ideal in the Principal Ideal Domain R and let $I = (m)$ be any ideal containing (p). We must show that $I = (p)$ or $I = R$. Now $p \in (m)$ so $p = rm$ for some $r \in R$. Since (p) is a prime ideal and $rm \in (p)$, either r or m must lie in (p). If $m \in (p)$ then $(p) = (m) = I$. If, on the other hand, $r \in (p)$ write $r = ps$. In this case $p = rm = psm$, so $sm = 1$ (recall that R is an integral domain) and m is a unit so $I = R$.

(2) Assume R is commutative. The ideal M is a maximal ideal if and only if the quotient ring R/M is a field.

Proof: There are two things to be shown here.
$\Rightarrow$ If M is a maximal ideal of R, then every non-zero element of R/M is a unit. A strategy for doing this is as follows: if $a \in R$ does not belong to M (so $a + M$ is not the zero element in R/M), then the fact that M is maximal as an ideal of R means that the only ideal of R that contains both M and the element a is R itself. In particular the only ideal of R that contains both M and the element a contains the identity element of R.
$\Leftarrow$ If R/M is a field (i.e. if every non-zero element of R/M is a unit), then M is a maximal ideal of R. A useful strategy for doing this is to suppose that I is an ideal of R properly containing M, and try to show that I must be equal to R.