1. Polynomial Rings and UFDs

We have seen that if A is an integral domain, then $A[x]$ is also an integral domain. If Q is the field of fractions of A, then $A[x] \subseteq Q[x]$, and $Q[x]$ is an Euclidean Domain, a PID, and a UFD. Then all polynomials in $A[x]$ can be uniquely factored over $Q[x]$.

Therefore, we want to know how a factorization in $Q[x]$ can help us to factor over $A[x]$ although $A[x]$ is not always a UFD. For this, we shall need the famous Gauss's Lemma.

Proposition 1.1 (10.6)**.** *Let I be an ideal of the ring A and let $I[x]$ denote the ideal of $A[x]$ generated by I, i.e., the set of polynomials with coefficients in I. Then,*

$$\frac{A[x]}{I[x]} \cong \left(\frac{A}{I}\right)[x].$$

Proof. Let's define the surjective ring homomorphism

$$\theta : A[x] \to \left(\frac{A}{I}\right)[x]$$

by reducing each of the coefficients of a polynomial modulo I. It is clear that the kernel of θ is the set of polynomials each of whose coefficients is an element of I, i.e.,

$$\text{Ker}(\theta) = I[x].$$

Then, by the first theorem of isomorphism, we have that

$$\frac{A[x]}{I[x]} \cong \left(\frac{A}{I}\right)[x].$$

□

Remark 1.1.1 (10.3)**.** Proposition 10.6 implies that if I is a prime ideal of A, then $I[x]$ is a prime ideal of $A[x]$.

Theorem 1.2 (10.2 (Gauss's Lemma))**.** *Let A be a UFD and Q the field of fractions of A. If $p(x)$ is reducible in $Q[x]$, then $p(x)$ is reducible in $A[x]$. Moreover, if $p(x) = r(x)s(x)$ for some non-constant polynomials $r(x), s(x) \in Q[x]$, then there are nonzero elements $A, B \in Q$ such that $Ar(x) = a(x)$ and $Bs(x) = b(x)$ and*

$$a(x) \in A[x], \quad b(x) \in A[x], \quad p(x) = a(x)b(x).$$

Therefore, $a(x)b(x)$ is a factorization of $p(x)$ in $A[x]$.

Proof. In the equality $p(x) = r(x)s(x)$, the coefficients of the term $r(x)s(x)$ are elements of Q by hypothesis. Then, it is possible to obtain the equality

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

where d represents the common denominator of all the coefficients of $r(x)s(x)$ and $a'(x), b'(x) \in A[x]$.

(i) If d is invertible, then take $a(x) = d^{-1}a'(x)$ and $b(x) = d^{-1}b'(x)$ and the proof is complete.

(ii) If d is not invertible, since A is a UFD and $d = p_1 \cdots p_n$, it follows that p_1 is irreducible and $\langle p_1 \rangle$ is a prime ideal. Therefore, by Proposition 10.6, the ring $(A/p_1A)[x]$ is an integral domain and $p_1A[x]$ is prime in $A[x]$. Reducing modulo p_1 over the quotient ring $(A/p_1A)[x]$, the equality $dp(x) = a'(x)b'(x)$ becomes

$$0 = a'(x)b'(x),$$

where the bars denote the equivalence class in this quotient ring. Since this ring is an integral domain, one of the factors must be 0. Say, $a'(x) = 0$. Therefore, all the coefficients of $a'(x)$ are divided by p_1, so $\frac{1}{p_1}a'(x) \in A[x]$. Thus we can simplify the factor p_1 from the factorization of d in the equality $dp(x) = a'(x)b'(x)$. Proceeding in the same way with each of the remaining factors of d, we can cancel d in the equation $dp(x) = a'(x)b'(x)$ and obtain a factorization

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

where $a(x), b(x) \in A[x]$ are multiples of $r(x)$ and $s(x)$ by elements of Q, respectively.

□

Corollary 1.3 (10.2)**.** *Let A be a UFD and Q be its field of fractions, and let $p(x) \in A[x]$. If the greatest common divisor of $p(x)$ is 1, then $p(x)$ is irreducible in $A[x]$ if and only if it is irreducible in $Q[x]$. In particular, every monic polynomial that is irreducible in $A[x]$ is also irreducible in $Q[x]$.*

Proof. (i) By Gauss' Lemma, if $p(x)$ is irreducible in $A[x]$, then $p(x)$ is irreducible in $Q[x]$.

(ii) Conversely, if $p(x) = a(x)b(x)$ is reducible in $A[x]$, the assumption on the greatest common divisor of the coefficients of $p(x)$ implies that neither $a(x)$ nor $b(x)$ are constant polynomials in $A[x]$. Therefore, the same factorizations show that $p(x)$ is reducible in $Q[x]$.

□

The following theorem will be stated without proof. For a demonstration, see [1].

Theorem 1.4 (10.3)**.** *A is a UFD if and only if $A[x]$ is a UFD.*

2. Irreducibility Criteria

We have seen in Section 10.4 that A is a UFD (for example, $\mathbb{Z}$) if and only if $A[x]$ is also a UFD. In this section, we want to determine the irreducible elements in such a polynomial ring.

In this ring, a non-constant monic polynomial is irreducible if it cannot be factored as the product of two other polynomials of small degree. The purpose of the irreducibility criteria presented in this section is to introduce tools that allow one to easily determine when a polynomial is irreducible. For a given integral domain A, by Gauss's Lemma it suffices to consider factorizations over $F[x]$, where F is the ring of fractions of A.

Proposition 2.1 (10.7)**.** *Let F be a field and let $p(x) \in F[x]$. Then $p(x)$ has a root in F if and only if $p(x)$ has a factor of degree one.*

Proof. (i) Since F is a field, if $p(x)$ has a factor of degree one, we can assume that this factor is monic, i.e., is of the form $(x - a)$ for some $a \in F$. Then $p(a) = 0$.

(ii) Suppose that $p(a) = 0$ for some $a \in F$. By the Division Algorithm in $F[x]$,

$$p(x) = q(x)(x - a) + r,$$

where $r \in F$ is a constant. Since

$$0 = p(a) = q(a)(a - a) + r = r,$$

we have that $r = 0$, hence $p(x)$ has $(x - a)$ as a factor.

□

Proposition 2.2 (10.8 (First Irreducibility Criterion: Polynomials of Degree Two or Three))**.** *A polynomial of degree two or three over a field F is reducible if and only if it has a root in F.*

Proof. Since a polynomial of degree two or three is reducible if it has at least one linear factor, Proposition 10.7 concludes the proof. □

Proposition 2.3 (10.9)**.** *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. Let $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ be a monic polynomial in $\mathbb{Z}[x]$. If $x = r/s \in \mathbb{Q}$ is a root of $p(x)$, where r and s are relative primes, then

$$0 = p(r/s) = (r/s)^n + a_{n-1}(r/s)^{n-1} + \cdots + a_1(r/s) + a_0,$$

and

$$0 = r^n + a_{n-1}r^{n-1}s + \cdots + a_1rs^{n-1} + a_0s^n,$$

where $r^n = s(-a_{n-1}r^{n-1} - \cdots - a_0s^{n-1})$.

Since r and s are relatively prime, s divides 1. Then, r is a root of $p(x)$ and solving the equations for a_0s^n, r divides a_0. A contradiction since $p(d) \neq 0$ for all integers d dividing a_0. □

Example 1 (10.10)**.** By Proposition 10.9, the only candidates for rational roots of the polynomial $p(x) = x^3 - 4x - 1$ are integers which divide the constant term 1, i.e., ± 1. Note that $p(1) \neq 0$ and $p(-1) \neq 0$. Then $p(x)$ has no rational roots, thus by 10.7, $p(x)$ is irreducible in $\mathbb{Q}[x]$ and by Gauss's Lemma, is irreducible in $\mathbb{Z}[x]$.

Example 2 (10.11)**.** The polynomial $q(x) = x^2 + 1 \in \mathbb{Z}_2[x]$ factors as $(x+1)^2$ since 1 is a root of $q(x)$.

The first irreducibility criterion works for a polynomial of small degree. For polynomials of higher degree, by applying several times the following criterion allows us to identify when is irreducible.

Proposition 2.4 (10.10 (Second Irreducibility Criterion: Reducing the Coefficient of a Polynomial Modulo an Ideal))**.** *Let I be a proper ideal in the integral domain A and let $p(x)$ be a non-constant monic polynomial in $A[x]$. Then $p(x)$ is irreducible in $A[x]$ if the class $p(x)$ in $(A/I)[x]$ cannot be factored in $(A/I)[x]$ into two polynomials of smaller degree.*

Proof. Assume that $p(x)$ cannot be factored in $(A/I)[x]$ but it does in $A[x]$. Then there exist two non-constant polynomials $a(x)$ and $b(x)$ in $A[x]$ such that

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

Reducing the coefficients of $a(x)$ and $b(x)$ modulo I, this is a factorization in $(A/I)[x]$ with non-constant factors by Proposition 10.6. A contradiction. □

Example 3 (10.12)**.** Reducing modulo 2 the polynomials $p(x) = x^2 + x + 1$ and $q(x) = x^3 + x + 1$, we see that $p(x)$ and $q(x)$ are irreducibles in $\mathbb{Z}[x]$ since these polynomials have no roots in $\mathbb{Z}_2$.

Example 4 (10.13)**.** The converse of Proposition 10.10 does not hold. For this, observe that the polynomial $x^2 + 1$ is irreducible in $\mathbb{Z}[x]$ since it has no roots in $\mathbb{Z}_3[x]$, therefore is irreducible in $\mathbb{Z}_3[x]$, but is reducible in $\mathbb{Z}_2[x]$.

From this second criterion, a new criterion known as Eisenstein's Criterion can be proved. This criterion is raised only on the ring of polynomials $\mathbb{Z}[x]$, while a general case is left as an exercise at the end of the section.

Proposition 2.5 (10.11 (Third Irreducibility Criterion—Eisenstein's Criterion))**.** *Let p be a prime in $\mathbb{Z}$ and let $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ for $n \geq 1$. If p divides a_i for all $i \in \{0, \ldots, n-1\}$ but p^2 does not divide a_0, then $p(x)$ is irreducible in both $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$.*

Proof. Consider $P = \langle p \rangle$, then P is a prime ideal of $\mathbb{Z}$. Suppose that $f(x)$ is reducible in $\mathbb{Z}[x]$ (therefore $f(x)$ is reducible in $\mathbb{Q}[x]$ by Corollary 10.2). Thus $f(x) = a(x)b(x)$ where $a(x), b(x) \in \mathbb{Z}[x]$ are non-constant polynomials. Reducing the coefficient of $f(x)$ modulo P, we obtain the equation

$$x^n = a(x)b(x),$$

since p divides a_i for all $i \in \{0, \ldots, n-1\}$, where the bar denotes the equivalence class of $a(x)b(x)$ in the ring $(\mathbb{Z}/P)[x]$. Since P is prime, the ring $(\mathbb{Z}/P)[x]$ is an integral domain and

therefore, the constant terms of $a(x)$ and $b(x)$ are elements of P. But then the constant term $a_0 \in \mathbb{Z}$ is the product of two terms divisible by p, therefore is divisible by p^2. A contradiction. $\square$

This lecture needs to be reviewed