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.

[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.,

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

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

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

□

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

[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 $a'(x), b'(x) \in A[x]$.

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

2. 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.

$\square$

[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 $Q[x]$.