The Gauss Lemma and The Eisenstein Criterion

**Theorem 1** \( R \) a UFD implies \( R[X] \) a UFD.

**Proof** First, suppose \( f(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n \), for \( a_j \in R \). Then define the content of \( f(X) \) to be \( \text{cont}(f(X)) = \gcd(a_0, \ldots, a_n) = d \) in \( R \). (So \( \text{cont}(f(X)) \) is well-defined up to a unit factor in \( R \).)

(Existence) If \( p \in R \) is irreducible then \( p \) is also irreducible in \( R[X] \). If \( f(X) \in R[X] \), write \( f(X) = dF(X) \), where \( d = \text{cont}(f(X)) \). Then \( \text{cont}(F(X)) = 1 \). We can certainly factor \( d \) into a product of irreducibles in \( R \). Either \( F(X) \) is irreducible in \( R[X] \) or it factors properly as a product of lower degree polynomials (since \( \text{cont}(F(X)) = 1 \)). All the factors will also have content 1 (since a divisor of any factor would divide \( F \)). We can only lower degree of factors finitely often, so we get a factorization of \( F(X) \), and hence \( f(X) \), as a product of irreducibles in \( R[X] \).

(Uniqueness) It suffices to prove each irreducible element of \( R[X] \) generates a prime ideal in \( R[X] \). For irreducibles \( p \in R \) this is clear, since \( R[X]/pR[X] = (R/p)[X] \), which is an integral domain. The general case will follow two lemmas.

**Lemma 1** If \( \text{cont}(F(X)) = \text{cont}(G(X)) = 1 \), \( F(X), G(X) \in R[X] \), then \( \text{cont}(F(X)G(X)) = 1 \). More generally, for \( f(X), g(X) \in R[X] \), \( \text{cont}(f(X)g(X)) = \text{cont}(f(X)) \cdot \text{cont}(g(X)) \).

**Proof** Suppose irreducible \( p \in R \) divides all coefficients of \( F(X)G(X) \). Then \( F(X)G(X) = 0 \) in \( (R/p)[X] \), which is an integral domain. Thus \( p \) either divides all coefficients of \( F(X) \) or \( p \) divides all coefficients of \( G(X) \), since one of \( F(X), G(X) \) must be 0 in \( (R/p)[X] \). But this contradicts the assumption \( \text{cont}(F) = \text{cont}(G) = 1 \).

In the general case, write \( f = dF, g = d'G \), where \( \text{cont}(F) = \text{cont}(G) = 1 \). Then \( fg = dd'FG \), so, by the first part of the Lemma, \( \text{cont}(fg) = dd' = \text{cont}(f) \cdot \text{cont}(g) \).

**Lemma 2** (Gauss) Let \( K \) be the field of fractions of \( R \). If \( P(X) \in R[X] \) factors in \( K[X] \) then \( P(X) \) factors in \( R[X] \) with factors of the same degrees as the \( K[X] \) factors. In particular, if \( P(X) \in R[X] \) is irreducible then \( P(X) \) is also irreducible in \( K[X] \).

**Proof** Every element of \( K[X] \) can be written \( A(X)/a \), where \( A(X) \in R[X] \) and \( a \in R \). Suppose in \( K[X] \) we have \( P(X) = (A(X)/a)(B(X)/b) \), with \( a, b \in R \) and \( A(X), B(X) \in R[X] \). Then \( abP(X) = A(X)B(X) \in R[X] \). Consider an irreducible factor \( p \) of \( ab \) in \( R \). Then \( A(X)B(X) = 0 \) in \( (R/p)[X] \). Thus \( p \) either divides all coefficients of \( A(X) \) or \( p \) divides all coefficients of \( B(X) \). We can then cancel a factor \( p \) in the \( R[X] \) equation \( abP(X) = A(X)B(X) \), without leaving \( R[X] \). By induction on the number of prime factors of \( ab \) in \( R \), conclude \( P(X) = A'(X)B'(X) \in R[X] \), where \( \deg A' = \deg A \) and \( \deg B = \deg B' \).

Now we finish the proof of Theorem 1 by showing \( (P(X)) \subset R[X] \) is a prime ideal if \( P(X) \) is irreducible in \( R[X] \). Certainly \( \text{cont}(P(X)) = 1 \), and by the Gauss Lemma \( P(X) \) is irreducible in \( K[X] \). Suppose \( P(X)Q(X) = F(X)G(X) \in R[X] \subset K[X] \). Since \( K[X] \) is a PID, we know \( P(X) \) divides \( F(X) \) or \( G(X) \) in \( K[X] \). Say in \( K[X] \) we have \( F(X) = P(X)(S(X)/s) \), with \( S(X) \in R[X] \), \( s \in R \). Then in \( R[X] \) we have \( P(X)S(X) = sF(X) \). Then \( s \) divides \( \text{cont}(P(X)S(X)) = \text{cont}(S(X)) \) by the first Lemma. So \( S(X)/s \) is in \( R[X] \) and \( F(X) \) is in the ideal \( (P(X)) \subset R[X] \).

It is often useful to combine the Gauss Lemma with Eisenstein’s criterion.

**Theorem 2** (Eisenstein) Suppose \( A \) is an integral domain and \( Q \subset A \) is a prime ideal. Suppose \( f(X) = q_0 X^n + q_1 X^{n-1} + \cdots + q_n \in A[X] \) is a polynomial, with \( q_0 \notin Q, q_j \in Q, 0 < j \leq n, \) and \( q_n \notin Q^2 \). Then in \( A[X] \), the polynomial \( f(X) \) cannot be written as a product of polynomials of lower degree.
If \( f(X) = g(X)h(X) \) could be factored in \( A[X] \), certainly the leading coefficients of \( g \) and \( h \) are not in \( Q \), since \( q_0 \notin Q \). Reducing mod \( Q \) would give \( \bar{f}(X) = \bar{g}_0X^n = \bar{g}(X)\bar{h}(X) \in \bar{A}X \), where \( \bar{A} = A/Q \). But over the integral domain \( \bar{A} \), the only factorizations of \( \bar{q}_0X^n \) are \( \bar{q}_0X^n = (\bar{a}X^i)(\bar{b}X^j) \), with \( i + j = n \). It follows that all coefficients of \( g(X) \) and \( h(X) \), except the leading coefficients, belong to the ideal \( Q \subset A \), contradicting \( q_0 \notin Q^2 \).

Example 1  \( f(X) = 2X^6 + 25X^4 - 15X^3 + 20X - 5 \in \mathbb{Z}[X] \) has content 1, and is irreducible in \( \mathbb{Z}[X] \) by the Eisenstein criterion for the prime 5. By the Gauss Lemma, \( f(X) \) is irreducible in \( \mathbb{Q}[X] \).