4.6 Appendix: Gauss’ Theorem

Let $A$ be a ring. Recall $x \in A$ is **irreducible** if $x$ is not a unit and, for all $y, z \in A$,

$$x = yz \implies y \text{ or } z \text{ is a unit},$$

and **prime** if $x \neq 0$, $x$ is not a unit and, for all $y, z \in A$,

$$x \mid yz \implies x \mid y \text{ or } x \mid z.$$
Call \( a, b \in A \) associates if there exists a unit \( c \in A \) such that \( a = bc \).

Suppose throughout that \( A \) is a unique factorization domain (UFD), by which we mean

(i) \( A \) is an integral domain;

(ii) every nonzero nonunit of \( A \) can be expressed as a product of irreducibles;

(iii) the factorization of (ii) is unique up to order and associates.
We will develop a sequence of lemmas leading to the proof of

**Gauss’ Theorem:** $A[x]$ is a UFD.

That $A[x]$ is an integral domain is a straightforward exercise.

Observe that everything divides 0 in $A$.

If $x_1, \ldots, x_n \in A$ are not all zero, then
by inspecting irreducible divisors, unique up to associates, one can write down a product of (powers of) irreducibles

\[ g = \gcd \{ x_1, \ldots, x_n \}, \]

having the property that

\[ g \mid x_1, \ldots, g \mid x_n \]

and

\[ h \mid x_1, \ldots, h \mid x_n \implies h \mid g. \]
It follows quickly that g.c.d.’s are unique up to associates.

Further

If \( g = \text{g.c.d.} \{ x_1, \ldots, x_n \} \) and

\[ x_1 = gy_1, \quad \ldots, \quad x_n = gy_n \]

then

\[ 1 = \text{g.c.d.} \{ y_1, \ldots, y_n \} . \]
Call $p(x) \in A[x]$ **primitive** if

$$1 = \gcd\left\{ \text{coefficients of } p(x) \right\}.$$

Certainly then,

all irreducible polynomials in $A[x]$ of degree $> 0$ are primitive.

(The irreducible polynomials of degree 0 are just the irreducible elements of $A$.)
Observation: Suppose

\[ 0 \neq f(x) \in A[x] \quad \text{and} \quad \lambda \in A . \]

Then

\[ f(x) = \lambda g(x) \]

for some primitive \( g(x) \) iff

\[ \lambda = \text{g.c.d.} \{ \text{coefficients of } f(x) \} . \]

Proof: Write \( f(x) = a_0 + \ldots + a_n x^n \quad (a_n \neq 0) . \)
(⇐⇒) Suppose $\lambda = \text{g.c.d.} \{ a_0, \ldots, a_n \}$. Write

$$a_0 = \lambda b_0, \ldots, a_n = \lambda b_n,$$

and put $g(x) = b_0 + \ldots + b_n x^n$. Then

$$f(x) = \lambda g(x) \quad \text{and} \quad 1 = \text{g.c.d.} \{ b_0, \ldots, b_n \},$$

so $g$ is primitive.

(⇒⇒) Suppose $f(x) = \lambda g(x)$ for some primitive $g(x) = b_0 + \ldots + b_n x^n$. Then
\[ a_0 = \lambda b_0, \ldots, a_n = \lambda b_n, \]
so certainly \( \lambda \) divides each of \( a_0, \ldots, a_n \).

If also \( \mu \) divides each of \( a_0, \ldots, a_n \) then \( \mu \) must divide \( \lambda \),

for otherwise, since \( A \) is a UFD, some irreducible divisor of \( \mu \) would divide each of \( b_0, \ldots, b_n \), contradicting that \( 1 = \gcd\{b_0, \ldots, b_n\} \).

Hence \( \mu | \lambda \), proving \( \lambda = \gcd\{a_0, \ldots, a_n\} \).
Lemma 1: Let $f(x)$ be a nonzero polynomial over $A$ such that

$$f(x) = \lambda g(x) = \mu h(x),$$

where $\lambda, \mu \in A$ and $g(x)$ and $h(x)$ are primitive.

Then $g(x)$ and $h(x)$ are associates.

Proof: By the previous Observation, both $\lambda$ and $\mu$ are g.c.d.’s of the coefficients of $f(x)$, so divide
each other, so

\[ \lambda = \mu \sigma \quad \exists \text{ unit } \sigma . \]

Hence

\[ \mu \sigma g(x) = \lambda g(x) = \mu h(x) , \]

so

\[ \sigma g(x) = h(x) \]

since \( A[x] \) is an integral domain and \( \mu \neq 0 \), which proves \( g(x) \) and \( h(x) \) are associates.
Since $A$ is an integral domain, let $F$ be its

field of fractions,


Lemma 2: Let $f(x), g(x) \in A[x]$ be primitive polynomials which are associates in $F[x]$. Then $f(x)$ and $g(x)$ are associates in $A[x]$. 
Proof: The units of $F[x]$ are nonzero elements of $F$, so

$$f(x) = \frac{a}{b}g(x) \quad \exists a, b \in A\{0\},$$

so

$$bf(x) = ag(x).$$

By Lemma 1, $f(x)$ and $g(x)$ are associates in $A[x]$. 
Lemma 3: Products of primitive polynomials are primitive.

Proof: Let $f(x), g(x)$ be primitive and write

$$f(x) = a_0 + \ldots + a_n x^n$$

$$g(x) = b_0 + \ldots + b_n x^n$$

for some $a_0, \ldots, a_n, b_0, \ldots, b_n \in A$

(using zero coefficients if necessary).
Suppose

\[ f(x)g(x) = c_0 + \ldots + c_{2n}x^{2n} \]

is not primitive. Then \( 1 \neq \gcd \{ c_0, \ldots, c_{2n} \} \), so, for some irreducible \( p \in \mathbb{A} \), \( p \mid c_i \) for all \( i \).

But \( f(x) \) and \( g(x) \) are primitive, so

\[ (\exists j \leq n) \quad p \nmid a_j \quad \text{and} \quad p \mid a_{j+1}, \ldots, a_n \]

\[ (\exists k \leq n) \quad p \nmid b_k \quad \text{and} \quad p \mid b_{k+1}, \ldots, b_n. \]
But

\[ c_{j+k} = a_0b_{j+k} + \ldots + a_{j-1}b_{k+1} + a_jb_k + a_{j+1}b_{k-1} + \ldots + a_{j+k}b_0 \]

all divisible by \( p \)
(where \( b_\ell = a_\ell = 0 \) for \( \ell > n \)),
so that \( p \mid a_j b_k \), yielding
\[
p \mid a_j \quad \text{or} \quad p \mid b_k \quad (\text{since } p \text{ is prime}),
\]
which contradicts the choice of \( j \) and \( k \).
Hence \( f(x)g(x) \) is primitive.
Lemma 4: Suppose $f(x) \in A[x]$ is irreducible of degree $> 0$.

Then $f(x)$ is irreducible in $F[x]$.

Proof: Suppose that $f(x)$ is not irreducible in $F[x]$, so

$$f(x) = g_1(x)g_2(x)$$

for some nonunits $g_1(x), g_2(x)$ in $F[x]$, so

$$\deg (g_1(x)) , \deg (g_2(x)) > 0.$$
By taking common denominators,

\[ g_1(x) = \frac{h_1(x)}{b_1} , \quad g_2(x) = \frac{h_2(x)}{b_2} \]

for some

\[ h_1(x) , h_2(x) \in A[x] , \quad b_1 , b_2 \in A\backslash\{0\} . \]

Then

\[ b_1 b_2 f(x) = h_1(x) h_2(x) . \]

Certainly \( f(x) \) is primitive (being irreducible).
Write

\[ h_1(x) = c_1 k_1(x), \quad h_2(x) = c_2 k_2(x) \]

where \( k_1(x), \ k_2(x) \) are primitive and \( c_1, c_2 \in A \), so

\[ b_1 b_2 f(x) = c_1 c_2 k_1(x) k_2(x). \]

By Lemma 3, \( k_1(x)k_2(x) \) is primitive,

so, by Lemma 1,

\[ f(x) \text{ and } k_1(x)k_2(x) \text{ are associates.} \]
But
\[ \deg (k_1(x)), \deg (k_2(x)) > 0, \]
so neither \( k_1(x) \) nor \( k_2(x) \) is a unit,
contradicting that \( f(x) \) is irreducible in \( A[x] \).
Hence \( f(x) \) is irreducible in \( F[x] \) and the lemma proved.

| Lemma 5: | \( F[x] \) is a UFD. |
Proof: This follows because $F[x]$ is a principal ideal domain (being a Euclidean domain) and details are left as an exercise or further reading.

Now we can prove

**Gauss’ Theorem:** $A[x]$ is a UFD.

Proof: Let $0 \neq f(x) \in A[x]$ where $f(x)$ is
not a unit. Then

\[ f(x) = \lambda g(x) \]

for some primitive \( g(x) \in A[x] \), where

\[ \lambda = \text{g.c.d.} \{ \text{coefficients of } f(x) \} . \]

If \( \deg (g(x)) = 0 \) then \( g(x) \) is a unit (since it is primitive).

Suppose \( \deg (g(x)) > 0 \).
If \( g(x) \) is not irreducible then

\[
g(x) = g_1(x)g_2(x)
\]

for some nonunits \( g_1(x), g_2(x) \),

both of degree \( > 0 \) (for otherwise \( \lambda \) would not be the g.c.d. of the coefficients of \( f(x) \)),

and continuing, if necessary, we get a factorization

\[
g(x) = g_1(x) \ldots g_n(x)
\]
where each $g_i(x)$ is irreducible of degree $> 0$

(this point being reached because there is no infinite strictly descending sequence of degrees).

Also (using the fact that $A$ is a UFD) we can factorize

$$\lambda = \lambda_1 \ldots \lambda_n$$

where $\lambda_1, \ldots, \lambda_n$ are irreducible in $A$ and hence in $A[x]$. 
Thus we get at least one factorization

\[ f(x) = \lambda_1 \ldots \lambda_n \, g_1(x) \ldots g_m(x) \]

into a product of irreducibles (possibly \( m = 0 \)).

Suppose also

\[ f(x) = \mu_1 \ldots \mu_s \, h_1(x) \ldots h_t(x) \]

is a product of irreducibles, where each \( \mu_i \in A \) and each \( h_j(x) \in A[x] \) has degree \( > 0 \).
Certainly \( g_1(x), \ldots, g_m(x), h_1(x), \ldots, h_t(x) \) are primitive so, by Lemma 3,

\[
g_1(x) \ldots g_m(x) \quad \text{and} \quad h_1(x) \ldots h_t(x)
\]

are primitive, so, by Lemma 1, are associates. Hence WLOG

\[
g_1(x) \ldots g_m(x) = h_1(x) \ldots h_t(x)
\]

\[
\lambda_1 \ldots \lambda_n = \mu_1 \ldots \mu_s.
\]
Since $A$ is a UFD, $n = s$ and $\lambda_1, \ldots, \lambda_n$ and $\mu_1, \ldots, \mu_s$ can be paired off into associates.

By Lemma 4,

$$g_1(x), \ldots, g_m(x), h_1(x), \ldots, h_t(x)$$

are irreducible in $F[x]$,

so, by Lemma 5, these can be paired off into associates with respect to $F[x]$. 

951
But by Lemma 2, these are then associates with respect to $A[x]$, and Gauss’ Theorem is proved.

If $K$ is a field then $K$ is trivially a UFD, so by iterating Gauss’ Theorem we get that

$$K[x_1, \ldots, x_n] \text{ is a UFD.}$$