GCDs and Gauss’ Lemma

R. C. Daileda

1 GCD Domains

Let $R$ be a domain and $S \subseteq R$. We say $c \in R$ is a common divisor of $S$ if $c | s$ for every $s \in S$. Equivalently, $S \subseteq (c)$ or $(S) \subseteq (c)$. We say a common divisor $d$ is a greatest common divisor (GCD) of $S$ if every common divisor $c$ of $S$ satisfies $c | d$. That is, $d$ is a GCD of $S$ if and only if $(d)$ is the least element of the set

$$\{(c) \mid c \in R, (S) \subseteq (c)\},$$

provided the least element exists. When it exists, the GCD of $S$ is only defined up to association: the GCDs of $S$ are the generators of the least element of (1). We will write $a \approx b$ to indicate that $a, b \in R$ are associates. In this case their common equivalence class is $aR^\times$. The association classes form a commutative multiplicative monoid under the operation $(aR^\times)(bR^\times) = abR^\times$ (see the appendix). Let $\gcd S$ denote the association class consisting of the GCDs of $S$. Thus, the statement “$d$ is a GCD of $S$” is equivalent to $d \in \gcd S$. A domain $R$ is called a GCD domain if every finite subset of $R$ has a GCD.

Suppose that $R$ is a GCD domain and $d$ is a GCD for $a_1, a_2, \ldots, a_m \in R$. Write $a_i = db_i$ for each $i$, with $b_i \in R$. If $c \in R$ and $c | b_i$ for all $i$, then $cd | a_i$ for all $i$. This means $cd | d$ and hence $c | 1$, so that $c$ is a unit. It follows that 1 is a GCD for the $a_i$ and hence $\gcd\{a_i\} = R^\times$.

Example 1.

a. In $\mathbb{Z}$, $\gcd(49, 21) = \{\pm 7\}$. In $\mathbb{Z}[X]$, $\gcd(2, X) = \{\pm 1\}$. Notice that in the first case we have $(49, 21) = (7)$, while in the second $(2, X) \neq (1) = \mathbb{Z}[X]$.

b. Every PID $R$ is a GCD domain. Given any $S \subseteq R$, $(S) = (d)$ for some $d \in R$, and hence $\gcd S = dR^\times$.

c. Every Bézout domain $R$ is a GCD domain for similar reasons.

d. Every UFD is a GCD domain. See section 3.

e. Let $F$ be a field. The monoid ring $F[X; \mathbb{Q}^*_0]$ is an GCD domain but is not a UFD.

f. Every GCD domain is an AP domain. See Theorem 1.

Remark 1.

a. There are now two different notions of the GCD of $S$: (i) the the smallest ideal containing $S$; (ii) (the generators of) the smallest principal ideal containing $S$. These need not be the same! Take $R = \mathbb{Z}[X]$ and $S = \{2, X\}$. The ideal-theoretic GCD is the proper ideal $(2, X) = \{f \in \mathbb{Z}[X] \mid f(0) \text{ even}\}$, while the element-wise GCDs are $\{\pm 1\}$. The reason for the distinction here (and in general) is that $S$ does not generate a principal ideal.

b. Consider $R$ as a subring of its quotient field. If $a, b \in R$, $b \neq 0$ and $b | a$, then there is a unique $c \in R$ so that $bc = a$. We call $c$ the factor or divisor complementary to $b$. We can use fractions to help us represent it. If we embed $R$ in its quotient field, $bc = a$ becomes $\frac{bc}{b} = \frac{a}{b}$, which is equivalent to $\frac{c}{1} = \frac{a}{b}$. When $b | a$ in $R$ we will therefore write $\frac{a}{b}$ to denote the divisor complementary to $b$.

Lemma 1. Let $R$ be a domain and $S, T \subseteq R$. 1
1. If $c \in R$ is nonzero, $S \subset (c)$ and \gcd $S$ exists, then \gcd $(S/c) = \frac{\gcd S}{c}$.

2. For any $c \in R$, \gcd $(cS) = c \cdot \gcd S$, provided \gcd $(cS)$ exists.

3. \gcd $(S \cup T) = \gcd (S \cup \gcd T)$, provided the \GCD$s exist.

**Proof.**

1. Let $d \in \gcd S$. Then $c \mid d$ by definition. So $S \subset (d)$ implies $S/c \subset \left(\frac{d}{c}\right)$. If $S/c \subset (e)$, then $S \subset (ce)$ so that $(d) \subset (ce)$ and hence $\left(\frac{d}{c}\right) \subset (e)$. This proves that \gcd $(S/c) = \frac{\gcd S}{c}$.

2. If $c = 0$ there is nothing to prove. Otherwise, if \gcd $(cS)$ exists, then since $cS \subset (c)$, the first part implies

\[
\gcd S = \gcd \left(\frac{cS}{c}\right) = \frac{\gcd(cS)}{c} \Rightarrow c \cdot \gcd S = \gcd(cS).
\]

3. For any $d \in R$, $T \subset (d)$ if and only if $\gcd T \subset (d)$. So

\[
S \cup T \subset (d) \iff S \subset (d) \text{ and } T \subset (d)
\]

\[
\iff S \subset (d) \text{ and } \gcd T \subset (d)
\]

\[
\iff S \cup \gcd T \subset (d).
\]

The result follows.

**Lemma 2.** Let $R$ be a \GCD domain, let $c \in R$ and let $S, T \subset R$ be finite. Then

\[
\gcd (S \cup cT) = \gcd (S \cup c \cdot \gcd (S \cup T)).
\]

**Proof.** Repeatedly apply parts 2 and 3 of Lemma 1:

\[
\gcd (S \cup cT) = \gcd (\gcd (S) \cup cT)
\]

\[
= \gcd (\gcd (S \cup cS) \cup cT)
\]

\[
= \gcd (S \cup cS \cup \gcd (cT))
\]

\[
= \gcd (S \cup c \cdot \gcd (S \cup c \cdot \gcd (T)))
\]

\[
= \gcd (S \cup c \cdot \gcd (S \cup \gcd (T)))
\]

\[
= \gcd (S \cup c \cdot \gcd (S \cup T)).
\]

**Corollary 1.** Let $R$ be a \GCD domain, $a, b, c \in R$. If $\gcd(a, b) = R^\times$, then $\gcd(a, bc) = \gcd(a, c)$.

**Proof.** Apply Lemma 2 with $S = \{a\}$ and $T = \{b\}$.

**Corollary 2.** Let $R$ be a \GCD domain, $a, b, c \in R$. If $\gcd(a, b) = \gcd(a, c) = R^\times$, then $\gcd(a, bc) = R^\times$.

Under the stronger hypothesis that $R$ is a Bézout domain, Corollaries 1 and 2 have dramatically simpler proofs. The examples of \GCD domains that we have seen so far are all \AP domains. Corollary 2 can be used to show that there’s a reason for this.

**Theorem 1.** Every \GCD domain is an \AP domain.

**Proof.** Let $R$ be a \GCD domain and suppose $a \in R$ is irreducible. Suppose $b, c \in R$ and $a \mid bc$. Then $\gcd(a, bc) = aR^\times \neq R^\times$. By Corollary 2, $\gcd(a, b) \neq R^\times$ or $\gcd(a, c) \neq R^\times$. Without loss of generality assume that $\gcd(a, b) \neq R^\times$. Since the only divisors of $a$ are its associates and units, it must be the case that $\gcd(a, b) = aR^\times$. In particular, $a \mid b$, and $a$ is prime.
2 Gauss’ Lemma

Let $R$ be a GCD domain. Given a polynomial $f(X) = \sum_i a_i X^i \in R[X]$, we define the content of $f$ to be

$$c(f) = \gcd(a_0, a_1, a_2, \ldots).$$

The GCD exists because only finitely many of the $a_i$ are nonzero. When $c(f) = R^\times$ say that $f$ is primitive.

As we will see, in terms of factorization, the primitive polynomials over a domain play the same role the monic polynomials over a field play. If $0 \neq d \in c(f)$, then

$$f = d \sum_i \left(\frac{a_i}{d}\right) X^i = d\tilde{f},$$

where $\tilde{f}$ is primitive by part 1 of Lemma 1. Furthermore, by part 2 of Lemma 1 we have

$$c(ef) = e \cdot c(f)$$

for any $r \in R$. In particular, if $a \in R$, then $c(a) = a \cdot c(1) = aR^\times$. This means that $a \in R$ is primitive if and only if $a \in R^\times$. These are the only observations we need to prove Gauss’ lemma.

**Lemma 3 (Gauss).** Let $R$ be a GCD domain and let $f, g \in R[X]$. If $f$ and $g$ are primitive, then $fg$ is primitive.

**Proof.** We prove the contrapositive by induction on $n = \deg fg$. When $n = 0$, $f, g \in R$ and $c(fg) = \deg fg = (\deg f)(\deg g) = c(f)c(g)$. Since $c(fg) \neq R^\times$, this implies $c(f) \neq R^\times$ or $c(g) \neq R^\times$. Now let $n \geq 1$ and assume we have proven the result for all pairs of polynomials whose product has degree less than $n$.

Suppose $\deg fg = n$. Write $c(fg) = dR^\times \neq R^\times$. Let $f = aX^\ell + O(X^{\ell-1})$ and $g = bX^m + O(X^{m-1})$. Then $fg = abX^n + O(X^{n-1})$ and $ab \in (d)$. Thus $(ab, d) = (d) \neq R$ and either $\gcd(a, d) \neq R^\times$ or $\gcd(b, d) \neq R^\times$, by Lemma 2. Assume, without loss of generality, that $\gcd(a, d) = eR^\times \neq R^\times$. Then $e$ divides every coefficient of $fg = aX^m g = (f - aX^\ell)g$. This implies that $c((f-aX^\ell)g) \subseteq (e) \neq R$ and hence $(f-aX^\ell)g$ is imprimitive. Since $\deg(f-aX^\ell) < \deg f$, $\deg(f-aX^\ell)g < \deg fg = n$. The inductive hypothesis therefore implies that either $f_1 = f - aX^\ell$ or $g$ is imprimitive.

If $g$ is imprimitive, we’re finished. If $g$ is primitive, write $f_1 = e_1 \tilde{f}_1$ where $c(f_1) = e_1 R^\times$ and $\tilde{f}_1 \in R[X]$ is primitive. Because $\deg \tilde{f}_1 = \deg f_1$, we can again apply the (contrapositive of the) inductive hypothesis to conclude that $\tilde{f}_1 g$ is primitive. Then

$$c(f_1g) = c(e_1\tilde{f}_1g) = e_1c(\tilde{f}_1g) = e_1R^\times = c(f_1).$$

It follows that $c(f_1) \subseteq (e)$. So $e$ divides all the coefficients of $f_1$ as well as the coefficients of $aX^\ell$. Thus $e$ divides all the coefficients of $f_1 + aX^m = f$. That is, $c(f) \subseteq (e)$. Since $(e) \neq R$, $c(f) \neq R^\times$ so that $f$ is imprimitive. This completes the induction. \qed

**Corollary 3.** Let $R$ be a GCD domain and let $f, g \in R[X]$. Then $c(fg) = c(f)c(g)$.

**Proof.** If $f = 0$ or $g = 0$ there is nothing to prove, so we may assume $f, g \neq 0$. Then $f = d\tilde{f}$ and $g = e\tilde{g}$, where $d \in c(f)$, $e \in c(g)$ and $\tilde{f}, \tilde{g} \in R[X]$ are primitive. Then $\tilde{f}\tilde{g}$ is primitive by Gauss’ lemma so that

$$c(fg) = c(de\tilde{f}\tilde{g}) = de \cdot c(\tilde{f}\tilde{g}) = deR^\times = c(f)c(g).$$

There is a somewhat simpler and more intuitive proof of Gauss’ lemma when $R$ is a a UFD. See Appendix 2.

**Remark 2.** Some authors define the content of a polynomial $f$ to be the ideal $c'(f)$ generated by coefficients. Others define the content to be a specific greatest common divisor $c''(f)$ of the coefficients. Our definition of $c(f)$ lies somewhere in the middle. For any $f \in R[X],

$$c''(f) \in c(f) = \gcd(c'(f)).$$


3 Consequences

We now apply Gauss’ lemma and its corollary to study irreducibility and factorization in \( R[X] \).

**Theorem 2.** Let \( R \) be a GCD domain and let \( f \in R[X] \). If \( f \) is primitive, then \( f \) is irreducible in \( R[X] \) if and only if \( f \) is irreducible in \( R[\bar{X}] \).

**Proof.** We prove the contrapositive. Suppose \( f \) is reducible in \( R[X] \). Then \( f = gh \) for some \( g, h \in R[X] \). If \( g \in R \), then \( g \in c(f) = R^{\times} \), which is impossible. So \( g \not\in R \). By symmetry, \( h \not\in R \). This means that \( \deg g, \deg h \geq 1 \). In particular, \( g, h \in Q(R)[\bar{X}] \) cannot be units. Thus the factorization \( f = gh \) is nontrivial and \( f \) is reducible in \( Q(R)[\bar{X}] \).

Now suppose \( f \) is reducible in \( Q(R)[\bar{X}] \). Write \( f = gh \) with \( g, h \in Q(R)[\bar{X}] \) of positive degree. Choose \( a, b \in R \) so that \( ag, bh \in R[\bar{X}] \). Let \( d \in c(\bar{a}g) \), \( e \in c(\bar{b}h) \) and write \( ag = d\bar{g}, bh = ch \) with \( \bar{g}, \bar{h} \in R[\bar{X}] \). Then
\[
ab R^{\times} = ab \cdot c(f) = c(abf) = c((af)(bh)) = c(bf) = de R^{\times}.
\]

Thus \( abf = \deg \bar{g}h = u ab\bar{g}\bar{h} \) for some \( u \in R^{\times} \), so that \( f = (u\bar{g}\bar{h})h \). This is a nontrivial factorization of \( f \) in \( R[\bar{X}] \), because \( \deg \bar{g} = \deg g \geq 1 \) and \( \deg \bar{h} = \deg h \geq 1 \). Hence \( f \) is reducible in \( R[\bar{X}] \) if it is reducible in \( Q(R)[\bar{X}] \).

**Remark 3.** In the second paragraph, the final factorization of \( f \) over \( R \) can differ from the initial factorization over \( Q(R) \). For instance, consider \( X^2 \) over \( \mathbb{Z} \). It is certainly primitive, and \( X^2 = (2X)(X/2) \) over \( \mathbb{Q} \). In the notation of the proof, \( a = 1, b = 2, d = 2, e = 1, \) and \( \bar{g} = \bar{h} \). Since \( ab = de, u = 1 \), so our final factorization over \( \mathbb{Z} \) is just \( X^2 = \bar{g}h = X \cdot X \).

**Example 2.** Let \( F \) be a field and \( X, T \) independent variables. We claim that for any \( n \in \mathbb{N} \), \( T^n - X \) is irreducible over \( F(X) \). As a polynomial in \( T \) over \( F[X] \), the nonzero coefficients of \( T^n - X \) are 1 and \( -X \), so \( T^n - X \) is primitive. So it suffices to prove that \( T^n - X \) is irreducible in \( F[X, T] \), by Theorem 2. But as polynomial in \( X \) over \( F[T] \), \( T^n - X \) is also primitive, so that we need only check irreducibility in \( F(T)[X] \). But here \( T^n - X \) is a linear polynomial over a field, so it is automatically irreducible. This prove the claim.

The proof of Theorem 2 can be modified to yield the following somewhat more precise statement.

**Corollary 4.** Let \( R \) be a GCD domain. If \( f \in R[X] \) is primitive and \( f = g_1 \cdots g_r \) over \( Q(R) \), then \( f = \bar{g}_1 \cdots \bar{g}_r \) over \( R \) with \( \bar{g}_i \) a primitive \( Q(R)^{\times} \)-multiple of \( g_i \). In particular, \( \deg \bar{g}_i = \deg g_i \) for all \( i \).

**Proof.** Choose \( a_i \in R \) so that \( a_i g_i \in R[X] \) for all \( i \) and write \( a_i g_i = b_i \bar{g}_i \), with \( b_i \in c(a_i g_i) \) and \( \bar{g}_i \in R[\bar{X}] \) primitive. By the corollary to Gauss’ lemma
\[
a_1 \cdots a_r R^{\times} = c(a_1 \cdots a_r f) = c((a_1 g_1) \cdots (a_r g_r)) = b_1 \cdots b_r R^{\times}.
\]

Therefore
\[
a_1 \cdots a_r f = b_1 \cdots b_r \bar{g}_1 \cdots \bar{g}_r = u a_1 \cdots a_r \bar{g}_1 \cdots \bar{g}_r
\]
for some \( u \in R^{\times} \). The result now follows upon replacing \( u \bar{g}_1 \) with \( \bar{g}_1 \).

**Corollary 5.** Let \( R \) be a GCD domain and let \( f \in R[X] \) be monic. If \( a \in Q(R) \) is a root of \( f \), then \( a \in R \). That is, \( R \) is integrally closed in its quotient field.

**Proof.** Write \( f = (X - a)g \) over \( Q(R) \). Since \( f \) is monic, it is primitive. Since \( X - a \) is also monic, \( g \) is monic. By Corollary 4, there exist \( r, s \in Q(R) \) so that \( r(X - a), sg \in R[X] \) are primitive and \( rs = 1 \). Since the leading coefficients of \( r(X - a) \) and \( rg \) are \( r, s \), we must have \( r, s \in R \). But then the equation \( rs = 1 \) implies that \( r, s \in R^{\times} \). Hence \( g, X - a \in R[X] \) and so \( a \in R \).
Now let $R$ be a UFD. If $a_1, a_2, \ldots, a_n \in R$, then there are primes/irreducibles $\pi_j$, exponents $e_{ij} \in \mathbb{N}_0$ and units $u_i \in R^\times$ so that
\[ a_i = u_i \prod_{j=1}^r \pi_j^{ij} \]
for $i = 1, 2, \ldots, n$. We can assume every factorization involves the same set of primes because we have allowed zero exponents. In this setting, the $e_{ij}$ are unique. Let $n_j = \min_i \{n_{ij}\}$ and set
\[ d = \prod_{j=1}^r \pi_j^{nj} \].
Then $d$ is a common divisor of the $a_i$. If $e|a_i$ and $\pi$ is a prime dividing $e$, then $\pi|a_i$. Uniqueness of prime factorizations implies that $\pi$ is associate to $\pi_j$ for some $j$. Thus
\[ e = u \prod_{j=1}^r \pi_j^{\ell_j}, \quad \ell_j \in \mathbb{N}_0, \quad u \in R^\times. \]
Since the hypotheses apply to $\frac{a_i}{e}$ as well,
\[ \frac{a_i}{e} = v \prod_{j=1}^r \pi_j^{m_j}, \quad m_j \in \mathbb{N}_0, \quad v \in R^\times. \]
Thus
\[ a_i = e \frac{a_i}{e} = uv \prod_{j=1}^r \pi_j^{\ell_j+m_j}. \]
Uniqueness of prime factorizations now implies that $\ell_j + m_j = n_{ij}$, which means $\ell_j \leq n_{ij}$. If $e|a_i$ for all $i$, then $\ell_j \leq n_{ij}$ for all $i$, so that $\ell_j \leq n_j$. This implies that $e|d$. Hence $d \in \gcd(a_1, \ldots, a_n)$. This proves that $R$ is a GCD domain. We will use this fact in the proof of our final result.

**Theorem 3.** If $R$ is a UFD, then $R[X]$ is a UFD.

**Proof.** Let $f \in R[X] \setminus R^\times$. Write $f = d \bar{f}$ with $d \in R$ and $\bar{f} \in R[X]$ primitive. Because $Q(R)$ is a field, $Q(R)[X]$ is a UFD. We can therefore write $\bar{f} = p_1 \cdots p_s$ with $p_i \in Q(R)[X]$ irreducible. By Lemma 4, $\bar{f} = \bar{p}_1 \cdots \bar{p}_s$ with $\bar{p}_i \in R[X]$ a primitive $Q(R)^\times$-multiple of $p_i$. Because $\bar{p}_i$ is a unit multiple of $p_i$, it is irreducible over $Q(R)$. By Theorem 2, $\bar{p}_i$ is irreducible over $R$. If $d = \pi_1 \cdots \pi_r$ is the prime/irreducible factorization of $d$ in $R$, we then have the factorization
\[ f = d \bar{f} = \pi_1 \cdots \pi_r \bar{p}_1 \cdots \bar{p}_s. \] (2)
in $R[X]$. Since an irreducible in $R$ remains irreducible in $R[X]$ (exercise), (2) is an irreducible factorization of $f$ over $R$.

We now need to show that every irreducible in $R[X]$ is prime. Let $p \in R[X]$ be irreducible and suppose $p|fg$ for some $f, g \in R[X]$. If $d \in \gcd(p)$ and we write $p = dp\bar{p}$ with $\bar{p} \in R[X]$ primitive, then irreducibility implies that $d \in R[X]^\times = R^\times$. Hence $p$ is already primitive. Theorem 2 tells us that $p$ is irreducible over $Q(R)$. Since $Q(R)[X]$ is a UFD, $p$ is prime in that ring. So, without loss of generality, $p|f$ in $Q(R)[X]$. Set $f = pq$ with $q \in Q(R)[X]$. Choose $a \in R$ so that $aq \in R[X]$ and set $aq = e\bar{q}$ with $c(aq) = eR^\times$ and $\bar{q} \in R[X]$ primitive. Then
\[ ac(f) = c(af) = c(p(aq)) = c(p)c(aq) = eR^\times \Rightarrow a|e \Rightarrow q = \frac{e}{a} \bar{q} \in R[X]. \]
Thus $p$ divides $f$ over $R$, and we’re finished. \[\square\]

**Remark 4.** It is also true that if $R$ is a GCD domain, then $R[X]$ is a GCD domain.
Example 3. a. Since \( \mathbb{Z} \) is a UFD, so is \( \mathbb{Z}[X] \). But then \( \mathbb{Z}[X,Y] = \mathbb{Z}[X][Y] \) is a UFD. And this implies \( \mathbb{Z}[X,Y,Z] = \mathbb{Z}[X,Y][Z] \) is a UFD. We can clearly continue this on indefinitely to conclude that \( \mathbb{Z}[X_1,X_2,\ldots,X_n] \) is a UFD for all \( n \geq 1 \) (\( \mathbb{Z} \) can be replaced by any UFD).

b. In \( \mathbb{Z}[X,Y] \) we have \( 60XY + 30Y + 40X + 20 = 10(6XY + 3Y + X + 2) = 2 \cdot 5 \cdot (2X + 1)(3Y + 2) \). By Theorem 2, any primitive linear polynomial over \( \mathbb{Z} \) is irreducible. So \( 2X + 1 \in \mathbb{Z}[X] \) is irreducible. It remains irreducible in \( \mathbb{Z}[X,Y] \). Likewise, \( 3Y + 2 \) is irreducible in \( \mathbb{Z}[X,Y] \). So we have the irreducible factorization
\[
60XY + 30Y + 40X + 20 = 2 \cdot 5 \cdot (2X + 1)(3Y + 2).
\]

4 Appendix 1: Quotients of Monoids

Let \( M \) be a (multiplicative) commutative monoid and let \( G \) be a subgroup of \( M \). For \( a,b \in M \), define \( a \cong b \) (mod \( G \)) if and only if \( a = bg \) for some \( g \in G \). Because \( G \) contains the identity of \( M \) and the inverse of each of its elements, \( \cong \) is an equivalence relation. The equivalence class of \( a \in M \) is clearly \( aG \). Moreover, if \( a,b \in M \), then \( (aG)(bG) = abG \), since \( G \) contains the identity and \( M \) is commutative. This binary operation makes \( M/\cong \) into a commutative monoid. Associativity is immediate and if \( e \in M \) is the identity, then \( eG \) is the identity in \( M/\cong \).

This seems to mimic the situation with quotient groups quite well, with one exception. While the “cosets” \( aG \) still partition \( M \), they need not all have the same cardinality. This is because the map \( \lambda_a : G \to aG \) given by \( g \mapsto ag \) need not be one-to-one. So there’s no analogue of Lagrange’s theorem, in general. If we assume \( M \) is cancellative, however, the map \( \lambda_a \) is a bijection for all \( a \in M \), and Lagrange’s theorem holds with the same proof.

The group \( G \) acts on \( M \) by left translation. The orbit of \( a \in M \) is \( Ga = aG \). If \( H = \text{Stab}(a) \), then according to the orbit-stabilizer theorem, \( |aG| = [G:H] \). Hence, although it need not be the case that \( |aG| = |G| \), we always at least have \( |aG||G| \).

Example 4. Let \( R \) be a ring. Then \( R \) is a monoid under multiplication and \( R^\times \) is a subgroup. The congruence modulo \( R^\times \) is simply the associate relation, and its equivalence classes are the sets \( aR^\times, a \in R \). The element 0 prevents \( R \) from being cancellative and its class \( 0R^\times = \{0\} \) is usually exceptionally small.

If \( R \) is a domain, then \( \lambda_a \) is a bijection for all nonzero \( a \in R \), so that every nonzero association class has cardinality \( |R^\times| \). Moreover, the association classes are in one-to-one correspondence with the principal ideals in \( R \), via \( aR^\times \mapsto (a) \).

5 Appendix 2: Gauss’ Lemma over Other Domains

For certain subclasses of the GCD domains, Gauss’ lemma can be proved by simpler, more ideal theoretic means.

Theorem 4. Let \( R \) be a UFD and let \( f,g \in R[X] \). If \( f \) and \( g \) are primitive, then \( fg \) is primitive.

Proof. We prove the contrapositive. If \( c(fg) = dR^\times \neq R^\times \), then \( d \notin R^\times \). Because \( R \) is UFD, it follows that \( d \) must have a prime factor \( p \in R \). Consider the natural map \( R \to R/(p) \). It lifts to a homomorphism \( \varphi : R[X] \to (R/(p))[X] \) by acting on coefficients. Since \( p|d \in c(fc) \), \( p \) divides the coefficients of \( fg \). That is, \( \varphi(fg) = 0 \). But \( \varphi(fg) = \varphi(f)\varphi(g) \) and \( R/(p) \) is a domain, so (WLOG) \( \varphi(f) = 0 \). This means that every coefficient of \( f \) is divisible by \( p \) so that \( c(f) \neq R^\times \).

Theorem 5. Let \( R \) be a B’ezout domain and let \( f,g \in R[X] \). If \( f \) and \( g \) are primitive, then \( fg \) is primitive.

Proof. We prove the contrapositive. If \( c(fg) = dR^\times \neq R^\times \), then \( d \notin R^\times \). Choose a maximal ideal \( m \) of \( R \) containing \( (d) \). As above the natural map \( R \to R/m \) lifts to a homomorphism \( \varphi : R[X] \to (R/m)[X] \). Since
$R$ is a Bézout domain, $(d)$ is the ideal generated by the coefficients of $fg$. This means every coefficient of $fg$ lies in $\mathfrak{m}$. That is, $\varphi(fg) = 0$. But $\varphi(fg) = \varphi(f)\varphi(g)$ and $R/\mathfrak{m}$ is a field, so (WLOG) $\varphi(f) = 0$. This means that every coefficient of $f$ lies in $\mathfrak{m}$. Hence so that $c(f) \neq R^\times$. 

Although the proof of Theorem 5 seems general enough to handle the GCD case, it is in the last step that it breaks down. In general, even if the elements in a GCD are contained in a maximal ideal, the GCD itself need not be. For example, $(2, X)$ is maximal in $\mathbb{Z}[X]$ but the GCD of its generators is $\{\pm 1\}$. 

\[ \boxed{} \]