Recall that we introduced the *greatest common divisor* (gcd) in our discussion of PIDs (Definition 2.13). Now we will reconsider this concept in the more general situation of UFDs. Of course, since every PID is a UFD, our discussion here will apply to PIDs as well.

The key to our discussion is the following lemma, which is very useful in its own right.

Lemma 2.58. *Let R be a UFD and let α and β be nonzero elements of R. Then α divides β if and only if*

(1) every prime p that divides α also divides β, and

(2) for every such prime p, if p^e is the highest power of p dividing α, and if p^f is the highest power of p dividing β, then $f \geq e$.

Proof: First, let us suppose that conditions (1) and (2) are satisfied. Then, for some primes $p_1, \ldots, p_k, q_1, \ldots, q_\ell$ and some exponents, and some units u and v, we have

$$\begin{aligned}\alpha &= up_1^{e_1}p_2^{e_2}\cdots p_k^{e_k},\\ \beta &= vp_1^{f_1}p_2^{f_2}\cdots p_k^{f_k}q_1^{g_1}q_2^{g_2}\cdots q_\ell^{g_\ell}.\end{aligned}$$

Then, setting

$$\gamma = wp_1^{f_1-e_1}p_2^{f_2-e_2}\cdots p_k^{f_k-e_k}q_1^{g_1}q_2^{g_2}\cdots q_\ell^{g_\ell}$$

with $w = uv^{-1}$, we have

$$\beta = \alpha\gamma,$$

so in this situation α divides β.

On the other hand, suppose α divides β, so $\beta = \alpha\gamma$.

Factor α and γ into primes, where we allow the exponents $d_1, \ldots, d_k$ to be zero:

$$\begin{aligned}\alpha &= up_1^{e_1}\cdots p_k^{e_k},\\ \gamma &= wp_1^{d_1}\cdots p_k^{d_k}q_1^{g_1}\cdots q_\ell^{g_\ell}.\end{aligned}$$

Then, setting $v = uw$,

$$\beta = vp_1^{f_1}\cdots p_k^{f_k}q_1^{g_1}\cdots q_\ell^{g_\ell}$$

with $f_i = e_i + d_i \geq e_i$ for each $i = 1, \cdots, k$, and so we see that conditions (1) and (2) are satisfied. □

Proposition 2.59. *Let R be a UFD and let α and β be nonzero elements of R with prime factorizations*

$$\alpha = up_1^{e_1} \cdots p_k^{e_k} q_1^{g_1} \cdots q_\ell^{g_\ell},$$
$$\beta = vp_1^{f_1} \cdots p_k^{f_k} r_1^{h_1} \cdots r_m^{h_m}.$$

Then α and β have a $\gcd \delta$*, and, moreover,*

$$\delta = p_1^{d_1} \cdots p_k^{d_k}$$

where $d_i = min(e_i, f_i)$ for each $i = 1, \ldots, k$. In case α and β have no common prime factors, $\delta = 1$.

Proof: By Lemma 2.58, δ divides both α and β. Furthermore, also by Lemma 2.58, any ζ dividing both α and β must be of the form

$$\zeta = wp_1^{c_1} \cdots p_k^{c_k}$$

with $c_i \leq e_i$ and $c_i \leq f_i$, i.e., $c_i \leq \min(e_i, f_i) = d_i$ for each i, so, once again by Lemma 2.58, ζ divides δ. Thus, δ satisfies the properties of $\gcd(\alpha, \beta)$ (Definition 2.13). □

Remark 2.60. Recall that the gcd is only defined up to multiplication by a unit, so for any unit w,

$$\delta' = w\delta = wp_1^{d_1} \cdots p_k^{d_k}$$

is also a gcd of α and β.

Recall that we defined two elements α and β of a PID to be *relatively prime* if their gcd is 1. We use the same language in the more general situation of a UFD here.

Note that Lemma 2.61 is the direct (word-for-word) generalization of Euclid's Lemma (Lemma 2.41) to the case of a UFD. But in this more general situation we need a new proof.

Lemma 2.61. *Let R be a UFD and let α be a nonzero element of R. Let β_1 and β_2 be elements of R and suppose that α divides $\beta_1\beta_2$. If α and β_1 are relatively prime, then α divides β_2.*

Proof: Since α and β_1 are relatively prime, they have no common prime factors. Thus, we have prime factorizations

$$\alpha = p_1^{e_1} \cdots p_k^{e_k},$$
$$\beta_1 = q_1^{g_1} \cdots q_\ell^{g_\ell}.$$

Now we are assuming that α divides $\beta_1\beta_2$, so by Lemma 2.58 we see that the prime factorization of $\beta_1\beta_2$ must include $p_1^{f_1}\cdots p_k^{f_k}$ with $f_i \geq e_i$, for each i. But the prime factorization of $\beta_1\beta_2$ is the product of the prime factorization of β_1 and the prime factorization of β_2. Since $p_1^{f_1}\cdots p_k^{f_k}$ does not appear in the prime factorization of β_1, it must appear in the prime factorization of β_2, and hence α divides β_2. □

The following corollaries are word-for-word generalizations of Corollary 2.42 and Corollary 2.43 to the case of a UFD.

Corollary 2.62. *Let R be a UFD and let α and β be relatively prime nonzero elements of R. Let γ be an element of R and suppose that α divides γ and β divides γ. Then $\alpha\beta$ divides γ.*

Proof: Once we have the generalization of Euclid's Lemma 2.41 to UFDs in Lemma 2.61, the *identical* proof of Corollary 2.42 works for UFDs, so we may just quote that proof.

But we will give a second (albeit longer) proof that uses prime factorization directly: Again, since α and β are relatively prime, they have no common prime factors, so we have prime factorizations

$$\alpha = p_1^{e_1}\cdots p_k^{e_k},$$
$$\beta = q_1^{g_1}\cdots q_\ell^{g_\ell}.$$

Then, by Lemma 2.58, applied first to α and γ and then to β and γ, we see that the prime factorizations of γ must contain every $p_i^{e_i}$ and every $q_j^{g_j}$, so it contains $p_i^{e_1}\cdots p_k^{e_k}q_1^{g_1}\cdots q_\ell^{g_\ell}$ and hence $\alpha\beta$ divides γ. □

Corollary 2.63. *Let R be a UFD and let α, β, and γ be elements of R. Suppose that α and β are relatively prime, and also that α and γ are relatively prime. Then α and $\beta\gamma$ are relatively prime.*

Proof: Once we have the generalization of Euclid's Lemma 2.41 to UFDs in Lemma 2.61, the *identical* proof of Corollary 2.43 works for UFDs, so we may just quote that proof.

But again we will give a proof that uses prime factorization directly: Let α have prime factorization

$$\alpha = p_1^{e_1}\cdots p_k^{e_k}.$$

Since α and β are relatively prime, no p_i appears in the prime factorization of β, and since α and γ are relatively prime, no p_i appears in the prime factorization of γ. Hence no p_i appears in the prime factorization of $\beta\gamma$, from which we conclude that α and $\beta\gamma$ are relatively prime. □