where $p_i, q_j \in A$ are irreducible, and the product of the common factors of a and b is a gcd of a and b (it is 1 is there are no common factors).

We conclude this section on UFD's by proving a proposition characterizing when a UFD is a PID. The proof is nontrivial and makes use of Zorn's lemma (several times).

Proposition 32.13. *Let A be a ring that is a UFD, and not a field. Then, A is a PID iff every nonzero prime ideal is maximal.*

Proof. Assume that A is a PID that is not a field. Consider any nonzero prime ideal, (p), and pick any proper ideal $\mathfrak{A}$ in A such that

$$(p) \subseteq \mathfrak{A}.$$

Since A is a PID, the ideal $\mathfrak{A}$ is a principal ideal, so $\mathfrak{A} = (q)$, and since $\mathfrak{A}$ is a proper nonzero ideal, $q \neq 0$ and q is not a unit. Since

$$(p) \subseteq (q),$$

q divides p, and we have $p = qp_1$ for some $p_1 \in A$. Now, by Proposition 32.1, since $p \neq 0$ and (p) is a prime ideal, p is irreducible. But then, since $p = qp_1$ and p is irreducible, p_1 must be a unit (since q is not a unit), which implies that

$$(p) = (q);$$

that is, (p) is a maximal ideal.

Conversely, let us assume that every nonzero prime ideal is maximal. First, we prove that every prime ideal is principal. This is obvious for (0). If $\mathfrak{A}$ is a nonzero prime ideal, then, by hypothesis, it is maximal. Since $\mathfrak{A} \neq (0)$, there is some nonzero element $a \in \mathfrak{A}$. Since $\mathfrak{A}$ is maximal, a is not a unit, and since A is a UFD, there is a factorization $a = a_1 \cdots a_n$ of a into irreducible elements. Since $\mathfrak{A}$ is prime, we have $a_i \in \mathfrak{A}$ for some i. Now, by Proposition 32.3, since a_i is irreducible, the ideal (a_i) is prime, and so, by hypothesis, (a_i) is maximal. Since $(a_i) \subseteq \mathfrak{A}$ and (a_i) is maximal, we get $\mathfrak{A} = (a_i)$.

Next, assume that A is not a PID. Define the set, $\mathcal{F}$, by

$$\mathcal{F} = \{\mathfrak{A} \mid \mathfrak{A} \subseteq A, \quad \mathfrak{A} \text{ is not a principal ideal}\}.$$

Since A is not a PID, the set $\mathcal{F}$ is nonempty. Also, the reader will easily check that every chain in $\mathcal{F}$ is bounded in $\mathcal{F}$. Indeed, for any chain $(\mathfrak{A}_i)_{i\in I}$ of ideals in $\mathcal{F}$ it is not hard to verify that $\bigcup_{i\in I} \mathfrak{A}_i$ is an ideal which is not principal, so $\bigcup_{i\in I} \mathfrak{A}_i \in \mathcal{F}$. Then, by Zorn's lemma (Lemma C.1), the set $\mathcal{F}$ has some maximal element, $\mathfrak{A}$. Clearly, $\mathfrak{A} \neq (0)$ is a proper ideal (since $A = (1)$), and $\mathfrak{A}$ is not prime, since we just showed that prime ideals are principal. Then, by Theorem C.3, there is some maximal ideal, $\mathfrak{M}$, so that $\mathfrak{A} \subset \mathfrak{M}$. However, a maximal ideal is prime, and we have shown that a prime ideal is principal. Thus,

$$\mathfrak{A} \subseteq (p),$$