### Vocabulary: irreducible element, prime element, Unique Factorization Domain, UFD.

**Definition.** A ring $R$ is called a domain provided that $R$ is nonzero and for all $a, b \in R$ we have $ab = 0$ implies $a = 0$ or $b = 0$. A commutative domain is called an integral domain.

**Definition.** Let $R$ be an integral domain and let $r$ be an element of $R$. We say that $r$ is composite if $r$ is nonzero and $r$ can be written as a product of two non-units. We say that $r$ is irreducible if it is neither composite, nor 0, nor a unit.

Thus every element of $R$ is described by precisely one of the adjectives “zero”, “unit”, “composite”, “irreducible”.

**Definition.** Let $R$ be an integral domain and let $r$ be an element of $R$. We say that $r$ is prime if $(r)$ is a prime ideal and $r \neq 0$.

(50) Show that prime elements are irreducible.

(51) Let $k$ be a field and let $k[t^2, t^3]$ be the subring of $k[t]$ generated by $t^2$ and $t^3$.

(a) Check that $t^2$ is irreducible in $k[t^2, t^3]$.
(b) Show that $t^2$ is not prime in $k[t^2, t^3]$.

(52) Consider the subring $\mathbb{Z}[\sqrt{-13}]$ of $\mathbb{C}$.

(a) Show that 7 is irreducible in $\mathbb{Z}[\sqrt{-13}]$. (Hint: Complex absolute value.)
(b) Show that 7 is not prime in $\mathbb{Z}[\sqrt{-13}]$.

**Definition.** A Unique Factorization Domain or UFD is an integral domain $R$ is which every nonzero, nonunity $r \in R$ has the following properties:

- (factorization) $r$ can be written as a finite product of (not necessarily distinct) irreducibles $p_i$ of $R$: $r = p_1p_2\cdots p_n$.
- (uniqueness of factorization) if $r = q_1q_2\cdots q_m$ is another factorization of $r$ into irreducibles then $m = n$ and there exists $\sigma \in S_n$ so that $p_j = q_{\sigma(j)}R^\times$ for $1 \leq j \leq n$.

In plain language, in a UFD every non-zero non-unit can be written uniquely (up to reordering and unit multiple) as a product of irreducible elements.

(53) Show that $\mathbb{Z}[\sqrt{-13}]$ and the ring $k[t^2, t^3]$ are not UFDs, by giving elements with two factorizations.

(54) Show that, in a UFD, irreducible elements are prime.

**Definition.** If $R$ is a commutative domain and $X$ is a subset of $R$, we define an element $g$ of $R$ to be a greatest common divisor or GCD of $X$

- if $g$ divides every element of $X$ and
- if $h$ divides every element of $X$, then $h$ divides $g$.

(55) Let $X$ be a subset of $R$. Show that, if $g$ and $g'$ are both GCD’s of $X$, then there is a unit $u$ such that $g' = gu$.

(56) Show that, if $R$ is a UFD, then every subset of $R$ has a GCD.

(57) Let $R$ be a ring where $\{x, y\}$ has a GCD for any $x$ and $y \in R$. Show that irreducible elements of $R$ are prime. Hint: Suppose that $p$ is irreducible and $p|ab$. Consider $\text{GCD}(pb, ab)$.

(58) Let $R$ be a domain. Show that any element of $R$ can be written in at most one way as a product of prime elements. (Uniqueness is up to reordering and multiplication by units, as in the definition of a UFD.)

Combining Problems 57 and 58, we see that, in a ring where any two elements have a GCD, every element has at most one irreducible factorization. We now have to address the question of when irreducible factorizations exist. It turns out that this holds in every Noetherian integral domain.

(59) Let $R$ be a Noetherian integral domain. Show that there does not exist a sequence $q_1, q_2, q_3, \ldots$ of elements of $R$ such that $q_j+1$ divides $q_j$ and $q_j$ does not divide $q_j+1$.

(60) Let $R$ be a Noetherian integral domain. Show that elements of $R$ have at least one irreducible factorization.

Putting together everything we have seen:

**Theorem:** Noetherian integral domain is a UFD, if and only if every two elements have a GCD, if and only if every subset has a GCD.

---

1The very careful student will notice a use of the Axiom of Choice here.