1. *Demonstrate an example of a subring D of ring D' such that: D' is a unique factorization domain but not a field, and D is an integral domain but not a unique factorization domain.*

   An easy example is that $\mathbb{C}[x]$ is a UFD (easily shown since $\mathbb{C}$ is a field, so $\mathbb{C}[x]$ is a principal ideal domain, so $\mathbb{C}[x]$ is a unique factorization domain; alternatively, note that every element of $\mathbb{C}[x]$ factors into linear polynomials) but not a field, since in a polynomial ring, nonconstants are uninvertable. Now $\mathbb{Z}[\sqrt{3}i]$ is, as seen in class, an integral domain which is not a unique factorization domain because $(1+\sqrt{3}i)(1-\sqrt{3}i) = 4 = 2\cdot 2$ and $1 \pm \sqrt{3}i$ and 2 are irreducible. Note that $\mathbb{Z}[\sqrt{3}i] \subseteq \mathbb{C} \subseteq \mathbb{C}[x]$.

2. *Let an integral domain D be called* reverse-Noetherian *if every sequence of ideals $D \supseteq I_1 \supsetneq I_2 \supsetneq I_3 \supsetneq \cdots$ is finite. Prove that D is reverse-Noetherian if and only if D is a field.*

   One direction of the implication is easy: if D is a field, then it contains exactly two distinct ideals, D and $\{0\}$, so every descending chain of ideals is not only finite, but has only two elements at the most.

   In the other direction, suppose D is reverse-Noetherian. We may note that, in general, for ring elements a and b, $\langle ab\rangle \subseteq \langle a\rangle$; this will be the case since for any $r \in D$, the element $(ab)r$ of $\langle ab\rangle$, written as $a(br)$, is clearly also an element of $\langle a\rangle$. In particular, for any ring element a and natural number n, $\langle a^{n+1}\rangle \subseteq \langle a^n\rangle$, so that for any nonzero a we can create the **nonstrictly** decreasing infinite chain of ideals:

   $$\langle a\rangle \supseteq \langle a^2\rangle \supseteq \langle a^3\rangle \supseteq \langle a^4\rangle \supseteq \cdots$$

   Since D is reverse-Noetherian, this infinite chain cannot be **strictly** decreasing; thus, there must be a value of n such that $\langle a^n\rangle = \langle a^{n+1}\rangle$; which is to say, $a^n = a^{n+1}x$ for some $x \in D$. Canceling the nonzero quantity a^n from both sides (as is permissible in an integral domain), we find that $1 = ax$, so a has an inverse; since a was an arbitrarily chosen nonzero element of D, every nonzero element of D has an inverse and so D is a field.

   Note: "reverse-Noetherian" is not a terribly popular concept for exactly this reason; it doesn't add anything to the set of concepts we already have.

3. *Prove that if D is a principal ideal domain, then for every pair of nonzero $a, b \in D$, there is a value d such that:*

   - *d divides both a and b.*
   - *If $e \in D$ is such that e divides both a and b, then e divides d.*
   - *$d = ar + bs$ for some $r, s \in D$.*

   Prove furthermore that d is unique up to multiplication by a unit.

   (Note that these three properties are those which, in $\mathbb{N}$, describe the greatest common divisor).

   We know an intersection of ideals is an ideal, and in a principal ideal domain, it must be specifically a principal ideal. Let $I = \{ar + bs : r, s \in D\}$; this is easily shown to be an ideal, so we may define d as an element of D such that $\langle d\rangle = I$; we shall show that this value d satisfies the given three properties, making use of the fact that the relation $x \mid y$ is equivalent to the ideal-membership $y \in \langle x\rangle$.

   Specifically: $a = a1 + b0 \in I = \langle d\rangle$ and $b = a0 + b1 \in I = \langle d\rangle$, so d divides a and b. Since $d \in \langle d\rangle$, it is clear that $d = ar + bs$ for some $r, s \in D$. Finally, suppose e divides both a and b. Then $a = ek$ and $b = e\ell$ for some $k, \ell \in D$, and so $d = ar + bs = (ek)r + (e\ell)s = e(kr + \ell s)$, so e divides d.

   To prove uniqueness up to multiplication b a unit, suppose we have elements d_1 and d_2 satisfying the above properties. Then, in particular, both d_1 and d_2 satisfy the first two properties; since d_1 divides both a and b, it must divide d_2, and conversely, since d_2 divides both a and b, it must divide

d_1. Thus $d_1 = kd_2$ and $d_2 = \ell d_1$ for some $k, \ell \in D$. But then $d_1 = (k\ell)d_1$, so $k\ell = 1$, and k is a unit, so d_1 is simply d_2 multiplied by the unit k.

4. *For a linear transformation T from a vector space V to a vector space W, the* image *of T is the set of all $w \in W$ such that $w = T(v)$ for some T, and the* kernel *of T is the set of all $v \in V$ such that $T(v) = 0$. Prove that the kernel and image of T are* subspaces *of V and W respectively.*

   Definitionally these two objects are subsets of V and W; it will thus suffice to show that they are closed under vector addition and scalar multiplication to prove that they are subspaced. Let us use the name F to denote the field over which V and W are vector fields.

   Let us start by showing closure of the kernel $\ker T$. If $v_1, v_2 \in \ker T$ and $k \in F$, then we may note that by the linear-transformation properties (which are "homomorphism-like"), $T(v_1 + v_2) = T(v_1) + T(v_2) = 0_W + 0_W = 0_W$; since $T(v_1 + v_2) = 0$, $v_1 + v_2 \in \ker T$. Likewise, $T(kv_1) = kT(v_1) = k0_W = 0_W$ so $kv_1 \in \ker T$. Thus $\ker T$ is a subset of V which is closed under vector addition and scalar multiplication, so it is a subspace of V.

   Similarly, we shall show closure of the image $T(V)$ by considering $w_1, w_2 \in T(V)$ and $k \in F$. By definition, there must be v_1 and v_2 in V such that $T(v_1) = w_1$ and $T(v_2) = w_2$. Then, $T(v_1 + v_2) = T(v_1) + T(v_2) = w_1 + w_2$, so $w_1 + w_2 \in T(V)$, and likewise $T(kv_1) = kT(v_1) = kw_1$ so $kw_1 \in T(V)$.

5. *Let W be a vector space of finite dimension. Prove that there are not subspaces U and V of W such that $U \cap V = \{0\}$ and $\dim U + \dim V > \dim W$.*

   Suppose, contrariwise, that such U and V exist, and let B_U and B_V be bases of U and V respectively. If B_U and B_V are not disjoint, then the element on which they intersect is a nonzero vector in both U and V, violating the condition that $U \cap V = \{0\}$; thus we may assume they are disjoint and so taking $B = B_U \cup B_V$, we have that $|B| > \dim W$. If B was linearly independent, then B or some expansion thereof would be a basis for W whose size exceeds the dimension of W, which is impossible (since the cardinality of a basis must be exactly the dimension of a finite-dimensional vector-space). Thus B is not linearly independent, so denoting $B_U = \{e_1, e_2, \ldots, e_m\}$ and $B_V = \{f_1, f_2, \ldots, f_n\}$, there are coefficients a_i and b_j such that $\sum_{i=1}^{m} a_i e_i + \sum_{j=1}^{n} b_j f_j = 0$ and not all the coefficients are zero. In fact, since B_U and B_V are themselves bases, we know that $\{e_1, \ldots, e_m\}$ and $\{f_1, \ldots, f_n\}$ are themselves linearly independent, so at least one a_i term and at least one b_j term must be nonzero and specifically $\sum_{i=1}^{m} a_i e_i \neq 0$. Then we might note that $\sum_{i=1}^{m} a_i e_i = -\sum_{j=1}^{n} b_j f_j \neq 0$, and by closure under addition and scalar multiplication, $\sum_{i=1}^{m} a_i e_i \in U$ and $-\sum_{j=1}^{n} b_j f_j \in V$, so the above-named sum is a nonzero element of the intersection of U and V, violating the condition that $U \cap V = \{0\}$.