Math 831 Homework 2 : Due February 20.

Throughout \( R \) will denote a commutative ring with identity. You may discuss these problems with your classmates or me and you may also freely use results established or assumed in class. Please do not consult with other students, professors, texts or online material. Note: we write UFD as an abbreviation for unique factorization domain.

1. Let \( R \) be a UFD.
   (a) Prove that \( R \) is also a GCD domain and an LCM domain, i.e., every pair of non-zero, non-unit elements in \( R \) has a greatest common divisor and a least common multiple.
   (b) Let \( A := \mathbb{Z} + \mathbb{Q}[X] \). Prove that \( A \) is a GCD domain, but not a UFD.

2. Let \( R \) be an integral domain, \( P := \{p_i\}_{i \in I} \) be a collection of prime elements, and let \( S \) the multiplicatively closed set generated by the \( p_i \).
   (a) Prove that if \( R \) is a UFD, then \( R[S] \) is a UFD.
   (b) Assume that no element in \( R \) is divisible by infinitely many \( p \in P \) (e.g., \( R \) satisfies ACC on principal ideals) and \( R[S] \) is a UFD. Prove that \( R \) is a UFD.

3. Use the theorem from class characterizing UFDs or the previous problem to give quick proofs of the following facts : 
   (a) Every PID is a UFD.
   (b) \( R \) is a UFD if and only if \( R[X] \) is a UFD.

4. Prove that the ring \( G \) of Gaussian integers \( \mathbb{Z} + \mathbb{Z}i \) is a principal ideal domain. (Hint : Prove that there is a division algorithm for \( G \) where the size of a remainder \( a + bi \) is given by \( a^2 + b^2 \).)

5. Let \( X_1, Y_1, \ldots, X_n, Y_n \) be indeterminates over \( R \). Prove that if \( R \) is a UFD and \( n \geq 3 \), then
   \[ R[X_1, Y_1, \ldots, X_n, Y_n]/(X_1Y_1 + \cdots + X_nY_n) \]
   is also a UFD.

6. Let \( X, Y \) be indeterminates over \( \mathbb{C} \) and set \( A_2 := \mathbb{C}[X, Y]/(X^2 + Y^2 - 1) \). Prove that \( A_2 \) is a UFD.

7. Let \( X, Y \) be indeterminates over \( \mathbb{R} \) and set \( B_2 := \mathbb{R}[X, Y]/(X^2 + Y^2 - 1) \). Prove that \( B_2 \) is not a UFD.

8. For \( B := B_2 \) in the previous problem, it is known that \( B_M \) is a PID for every maximal ideal, and thus a UFD for every maximal ideal. Take a step in this direction by showing the following :
   (a) For \( (\alpha, \beta) \in \mathbb{R}^2 \) such that \( \alpha^2 + \beta^2 = 1 \) and \( M := (X - \alpha, Y - \beta)B \), show that \( M \) is a maximal ideal of \( B \).
   (b) Prove that \( MB_M \) is a principal ideal.
9. Let $R$ be a commutative ring and $X$ an infinite set of prime ideals. Suppose that $J \subseteq R$ is an ideal maximal with respect to the property that $J$ is contained in infinitely many elements of $X$. Prove that $J$ is a prime ideal. Conclude that if $R$ is a Noetherian ring, then every ideal has only finitely many primes minimal over it.

10. Let $M$ be a Noetherian $R$ module and $\phi : M \to M$ a surjective module homomorphism. Prove that $\phi$ is an isomorphism. Formulate and prove a version of this for a module $A$ satisfying the descending chain condition.

Remarks. (i) Problems 5, 6 and 7 should suggest that the UFD property is a subtle one. If you are not convinced, consider that if $X, Y, Z$ are indeterminates over $\mathbb{C}$, then for

$$A_3 := \mathbb{C}[X, Y, Z]/(X^2 + Y^2 + Z^2 - 1) \text{ and } B_3 := \mathbb{R}[X, Y, Z]/(X^2 + Y^2 + Z^2 - 1),$$

$A_3$ is not a UFD and $B_3$ is a UFD.

(ii) In a similar vein, for the rings

$$C := \mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^5) \text{ and } D := \mathbb{C}[X, Y, Z]/(X^2 + Y^3 + Z^6),$$

$C$ is a UFD and $D$ is not a UFD.

(iii) Here is a special case of an important result. Let $K$ be a field and $X, Y, Z$ indeterminates over $K$. Let $M := (X, Y, Z)S$, where $S$ is the polynomial ring in $X, Y, Z$ over $K$. Let $f \in S$ and set $R := S_M/fS_M$. Then $R$ is a UFD if and only if $f$, as an element of $S_M$, is not the determinant of some square matrix over $S_M$. The same applies if we replace the ring $S_M$ by the formal power series ring in $X, Y, Z$ over $K$. 

2