Homework IV (due November 18), Math 602, Fall 2002. (GJSZ)

B I(a). Let $P(X_1, \ldots, X_n) = X_1^2 + \cdots + X_n^2$. First, we prove that $P(X_1, \ldots, X_n) \in \mathbb{C}[X_1, \ldots, X_n]$ is irreducible for all $n \geq 3$. The intuition is geometric: The hypersurface defined by $P(X_1, \ldots, X_n) = 0$ is nonsingular, except at the origin, which means that the normal vector $N = (P_{X_1}, \ldots, P_{X_n})$ is nonzero except at the origin, where P_{X_i} denotes the partial derivative $\partial P/\partial X_i$. Indeed, we have $N = (2X_1, \ldots, 2X_n)$.

If P factors, it can be written as the product $P = l_1 l_2$ of two linear forms, l_1, l_2. But, we have

$$N_{X_i} = (l_1 l_2)_{X_i} = (l_1)_{X_1} l_2 + l_1 (l_2)_{X_i}.$$

Furthermore, the equations $l_1 = 0$ and $l_2 = 0$ define two hyperplanes through the origin; if ≥ 3, the intersection of these hyperplanes has dimension at least $n - 2$, and so, for all $i = 1, \ldots, n$, we would have $N_{X_i} = (l_1 l_2)_{X_i} = 0$ on a subspace of dimension at least $n-2 \geq 1$, contradicting the fact that N is zero only at the origin. Therefore, P is irreducible.

We can now apply theorem 1.1 from B I(f), and this shows that $\mathbb{C}[X_1, \ldots, X_n]/(X_1^2 + \cdots + X_n^2)$ is a UFD whenever $n \geq 5$.

B I(b) Let $Q(X_1, \ldots, X_n) = X_1^3 + \cdots + X_n^3$. As in B I(a) we prove that $Q(X_1, \ldots, X_n) \in \mathbb{C}[X_1, \ldots, X_n]$ is irreducible for all $n \geq 3$. Again, the hypersurface, $Q(X_1, \ldots, X_n) = 0$, is nonsingular, except at the origin, which means that the normal vector $N = (Q_{X_1}, \ldots, Q_{X_n})$ is nonzero, except at the origin, where Q_{X_i} denotes the partial derivative $\partial Q/\partial X_i$. Indeed, we have $N = (3X_1^2, \ldots, 3X_n^2)$.

If Q factors, then $Q = LR$, where L is a linear form and R is (homogeneous) of degree 2. We claim that the intersection of the hyperplane, $L = 0$, with the quadric, $R = 0$, in $\mathbb{C}^n$, is infinite, provided that $n \geq 3$. (Actually, this is also true for any hypersurface $R = 0$ in $\mathbb{C}^n$).

A hyperplane, H, in $\mathbb{C}^n$ is determined by n affinely independent points, $p^1, \ldots, p^n$, and any point, $X = (X_1, \ldots, X_n)$ in H can be written as an affine combination,

$$X = \lambda_1 p^1 + \cdots + \lambda_n p^n, \quad \text{where} \quad \lambda_1 + \cdots + \lambda_n = 1.$$

If we write $p^i = (p_1^i, \ldots, p_n^i)$, we see that

$$X_i = \lambda_1 p_i^1 + \cdots + \lambda_n p_i^n,$$

for $i = 1, \ldots, n$. We find the intersection of $L = 0$ and $R = 0$ by plugging the X_i's in R, and we find a polynomial of degree 2 in $\lambda_1, \ldots, \lambda_n$. Further, we can eliminate λ_n, and we find a polynomial, T, of degree 2, in $\lambda_1, \ldots, \lambda_{n-1}$. Since $n \geq 3$, we have $n - 1 \geq 2$. If any of the λ_i is missing from T, then $T = 0$ has infinitely many solutions over $\mathbb{C}^{n-1}$. If not, give arbitrary values to $\lambda_2, \ldots, \lambda_{n-1}$, which is possible, since $n - 1 \geq 2$. The resulting polynomial $T(\lambda_1)$ is a polynomial of degree 2, and over $\mathbb{C}$, its has some zero. Therefore, $T = 0$ has infinitely many solutions.

As in B I(a), we have

$$N_{X_i} = (LR)_{X_i} = L_{X_1}R + LR_{X_i},$$

and by the above fact, for all $i = 1, \ldots, n$, we would have $N_{X_i} = (LR)_{X_i} = 0$ on an infinite set, a contradiction. Therefore, Q is irreducible.

Again, we apply theorem 1.1 from B I(f), and this shows that $\mathbb{C}[X_1, \ldots, X_n]/(X_1^2 + X_2^2 + X_3^3 + \cdots + X_n^3)$ is a UFD whenever $n \geq 5$.

B I(c). We have $X_1^2 + X_2^2 = (X_1 + iX_2)(X_1 - iX_2)$. Thus, $B = \mathbb{C}[X_1, X_2]/(X_1^2 + X_2^2)$ is not a domain, since $(X_1 + iX_2)(X_1 - iX_2) = 0$ in B.

Since $X_1^2 + X_2^2 + X_3^2 = (X_1 + iX_2)(X_1 - iX_2) - (iX_3)^2$, the ring $B = \mathbb{C}[X_1, X_2, X_3]/(X_1^2 + X_2^2 + X_3^2)$ is not a UFD, since

$$(X_1 + iX_2)(X_1 - iX_2) = (iX_3)^2$$

in B (but it is a domain).

Since $X_1^2 + X_2^2 + X_3^2 = (X_1 + iX_2)(X_1 - iX_2) - (iX_3 + X_4)(iX_3 - X_4)$, the ring $B = \mathbb{C}[X_1, X_2, X_3, X_4]/(X_1^2 + X_2^2 + X_3^2 + X_4^2)$ is not a UFD, since

$$(X_1 + iX_2)(X_1 - iX_2) = (iX_3 + X_4)(iX_3 - X_4)$$

in B (but it is a domain).

We have $X_1^3 + X_2^3 = (X_1 + X_2)(X_1^2 - X_1X_2 + X^2)$. Thus, $B = \mathbb{C}[X_1, X_2]/(X_1^3 + X_2^3)$ is not a domain, since

$$(X_1 + X_2)(X_1^2 - X_1X_2 + X^2) = 0$$

in B.

Since $X_1^3 + X_2^3 + X_3^3 = (X_1 + X_2)(X_1^2 - X_1X_2 + X^2) - (-X_3)^3$, the ring $B = \mathbb{C}[X_1, X_2, X_3]/(X_1^3 + X_2^3 + X_3^3)$ is not a UFD, since

$$(X_1 + X_2)(X_1^2 - X_1X_2 + X^2) = (-X_3)^3$$

in B (but it is a domain).

Since $X_1^3 + X_2^3 + X_3^3 + X_4^3 = (X_1 + X_2)(X_1^2 - X_1X_2 + X^2) - (-X_1 - X_2)(X_1^2 - X_1X_2 + X^2)$ the ring
$B = \mathbb{C}[X_1, X_2, X_3, X_4]/(X_1^3 + X_2^3 + X_3^3 + X_4^3)$ is not a UFD, since

$$(X_1 + X_2)(X_1^2 - X_1X_2 + X^2) = (-X_1 - X_2)(X_1^2 - X_1X_2 + X^2)$$

in B (but it is a domain).

B I(d).

B I(e). We will prove the following main theorem:

Theorem 1.1 *If A is a noetherian UFD, for any irreducible $f_0 \in A$ and any polynomial $g(X) \in A[X]$, if we let $f(X,Y) = XY + f_0 + Xg(X)$, then $B = A[X,Y]/(f(X,Y))$ is a UFD.*

We can apply Theorem 1.1 to B I(a) and B I (b) using the following simple fact:

Lemma 1.2 *For any polynomial $h(X_3, \ldots, X_n) \in \mathbb{C}[X_3, \ldots, X_n]$, we have the isomorphism*

$$\mathbb{C}[X_1, X_2, X_3, \ldots, X_n]/(X_1^2 + X_2^2 + h) \cong \mathbb{C}[U, V, X_3, \ldots, X_n]/(UV + h).$$

Proof. We have $X_1^2 + X_2^2 = (X_1 + iX_2)(X_1 - iX_2)$. Use the isomorphisms induced by $U \mapsto (X_1 + iX_2)$, $V \mapsto (X_1 - iX_2)$, and $X_1 \mapsto (U+V)/2$, $X_2 \mapsto (U-V)/2i$. $\square$

We can apply Theorem 1.1 to B I(a) by letting:
$A = \mathbb{C}[X_3, \ldots, X_n]$, $g(X) = 0$, and $f_0 = (X_3^2 + \cdots + X_n^2)$, for $n \geq 5$, because in this case, f_0 is irreducible.

We can apply Theorem 1.1 to B I(b) by letting:
$A = \mathbb{C}[X_3, \ldots, X_n]$, $g(X) = 0$, and $f_0 = (X_3^3 + \cdots + X_n^3)$, for $n \geq 5$, because in this case, f_0 is also irreducible.

The proof of Theorem 1.1 proceeds in several steps. We denote the image of a polynomial $f(X,Y) \in A[X,Y]$ by $\overline{f}$.

Unfortunately, we could not figure out how to use the criterion of $AI(b)$, but we could manage by using the following lemma apparently due to Nagata, from Matsumura (*Commutative Ring Theory*, Chapter 7, Section 20, Theorem 20.2. (see also, Bourbaki (Commutative Algebra, Chapter VII, Section 4, Proposition 3 (b)):

Lemma 1.3 *(Nagata) Let A be a noetherian domain and let $S \subseteq A$ be a multiplicative subset of A with $1 \in S$; if S is generated by elements $p \in S$ (which means that every $x \neq 1$ in S is the product of some of these elements) so that the principal ideal, (p), is prime, and $S^{-1}A$ is a UFD, then A itself is a UFD.*

The proof of the above lemma uses the a characterization of noetherian UFD's given below and a version of Krull's "principal ideal theorem."

Recall the notion of height of a prime ideal in a noetherian ring. Given a prime ideal, $\mathfrak{p} \subseteq A$, the *height* of $\mathfrak{p}$ is the supremum of the lengths, r, of all strictly decreasing chains of prime ideals

$$\mathfrak{p} = \mathfrak{p}_0 > \mathfrak{p}_1 > \cdots > \mathfrak{p}_r.$$

Note: If A is a domain, then $\mathfrak{p}_r = (0)$.

Theorem 1.4 *Let A be a noetherian domain. Then A is a UFD iff every height 1 prime is a principal ideal.*

The proof of Theorem 1.4 requires a version of Krull's "principal ideal theorem" stating:

Theorem 1.5 *(Krull) Let A be a noetherian ring. For any nonunit, $x \in A$, every minimal prime ideal, $\mathfrak{p}$, containing x has height at most 1.*

Lemma 1.6 *If A is a UFD and $f(X, Y)$ is a polynomial as in Theorem 1.1, then the image, $\overline{X}$, of X in $B = A[X, Y]/(f(X, Y))$, is prime.*

Proof. In the factor ring $B/(\overline{X})$, we have $\overline{X} = 0$, and so, we have the isomorphism

$$B/(\overline{X}) \cong A[X, Y](f_0).$$

However, since A is a UFD, so is $A[X, Y]$, and since $f_0 \in A$ is irreducible, it is also irreducible in $A[X, Y]$. As in a UFD, every irreducible element is prime, the ideal (f_0) is prime, and thus, $A[X, Y](f_0)$ is an integral domain. This shows that $B/(\overline{X})$ is an integral domain, which implies that $(\overline{X})$ is a prime ideal. □

Lemma 1.7 *If A is a UFD and $f(X, Y)$ is a polynomial as in Theorem 1.1, then $B = A[X, Y]/(f(X, Y))$ is an integral domain.*

Proof. Since A is a UFD, the ring $A[X, Y]$ is also a UFD. Since every irreducible element in a UFD is prime, and since the quotient of a ring by a prime ideal is an integral domain, it is enough to prove that $f(X, Y) = XY + f_0 + Xg(X)$ is irreducible in $A[X, Y]$. If $f(X, Y)$ factored in $A[X, Y]$, it would also factor viewed as a polynomial in $A[X][Y]$. But over $A[X][Y]$, the polynomial $XY + f_0 + Xg(X)$ is of the form $aY + b$, with $a, b \in A[X]$, and such a polynomial is clearly irreducible. Thus, $f(X, Y) = XY + f_0 + Xg(X)$ is irreducible. □

Lemma 1.8 *If A is a UFD and $f(X, Y)$ is a polynomial as in Theorem 1.1, if we let S be the multiplicative subset of $B = A[X, Y]/(f(X, Y))$ generated by $\overline{X}$, then $S^{-1}B$ is a UFD.*

Proof. Since $\overline{X}$ is invertible in $S^{-1}B$ and

$$\overline{X}\,\overline{Y} + \overline{f_0} + \overline{X}\,\overline{g(X)} = 0,$$

we can express $\overline{Y}$ in terms of $\overline{X}$, and we see that

$$S^{-1}B \cong (A[X])_X,$$

the localization of $A[X]$ at X. However, since A is a UFD, so is $A[X]$, and the localization of a UFD is a UFD. □

Finally, we prove Theorem 1.1.

Proof of Theorem 1.1. By Lemma 1.7, the ring $A[X, Y]/(f(X, Y))$ is an integral domain. Since A is noetherian, by Hilbert's basis theorem, the ring $A[X, Y]$ is noetherian. Now, a factor of a noetherian ring is noetherian. Therefore, $B = A[X, Y]/(f(X, Y))$ is a noetherian domain. By Lemma 1.6, the element $\overline{X}$ is prime in B. If we let S be the multiplicative subset of B generated by $\overline{X}$, by Lemma 1.8, $S^{-1}B$ is a UFD. Thus, the hypotheses of Lemma 1.3 are fulfilled, and B is a UFD. $\square$

BIV (a). Let A be any commutative ring (with unity), and let $f(X) = a_0X^m + a_1X^{m-1} + \cdots + a_m$ and $g(X) = b_0X^n + b_1X^{n-1} + \cdots + b_n$ be two polynomials in $A[X]$. We wish to prove that if $g(X) \neq 0$ and $g(X)f(X) = 0$, then there is some $\alpha \in A$ with $\alpha \neq 0$, so that $\alpha f(X) = 0$.

This is trivial if $n = \deg(g) = 0$; just let $\alpha = g$. Now, assume $n \geq 1$. There must be some polynomial $g(X) \neq 0$ of minimal degree, so that $g(X)f(X) = 0$; let $g(X)$ be such a minimal polynomial, and so, we may assume that $b_0 \neq 0$. The term of highest degree in $g(X)f(X)$ is $a_0b_0X^{m+n}$, and since $n \geq 1$ and $f(X)g(X) = 0$, we have

$$a_0b_0 = 0.$$

We claim that

$$a_0g(X) = 0.$$

Indeed, if $a_0g(X) \neq 0$, since $a_0b_0 = 0$, we have $\deg(a_0g(X)) < \deg(g(X))$, and yet, $(a_0g(X))f(X) = a_0g(X)f(X) = 0$, contradicting the minimality of $g(X)$. Now, we prove by induction on i that

$$a_ig(X) = 0, \quad \text{for } i = 0, \ldots, m.$$

The base case, $i = 0$, has already been established. Assume that $a_jg(X) = 0$, for $j = 0, \ldots, i$, with $0 \leq i \leq m-1$. Consider $f(X) - (a_0X^m + a_1X^{m-1} + \cdots + a_iX^{m-i})$. The hypothesis $g(X)f(X) = 0$ and the induction hypothesis implies that

$$g(X)(f(X) - (a_0X^m + a_1X^{m-1} + \cdots + a_iX^{m-i})) = 0.$$

Now, the term of highest degree in the above product is $a_{i+1}b_0X^{m+n-i-1}$, and since $i \leq m-1$ and $n \geq 1$, we have $a_{i+1}b_0 = 0$. Then, the same reasoning as above shows that $a_{i+1}g(X) = 0$ (otherwise, $a_{i+1}g(X)$ would be a polynomial of strictly smaller degree that $g(X)$ so that $g(X)f(X) = 0$). This concludes the induction step, and therefore,

$$a_ig(X) = 0, \quad \text{for } i = 0, \ldots, m.$$

As a consequence, $b_0a_i = 0$, for $i = 0, \ldots, m$. Since $b_0 \neq 0$, letting $\alpha = b_0$, we have found $\alpha \neq 0$ in A so that $\alpha f(X) = 0$

(b) Assume that K is a field (actually, it is enough for our proof to assume that K is an integral domain), and consider $A = K[X_{ij},\ 1 \leq i, j \leq n]$ and the $n \times n$ matrix $M = (X_{ij})$. We want to prove that $D = \det(M)$ is an irreducible polynomial of A. We proceed by induction on n. The base case $n = 1$ is trivial, since $X_{1,1}$ is irreducible in $A = K[X_{11}]$. If $n \geq 2$, we can expand the determinant, D, with respect to its first row, and we have

$$D = X_{11}D_1 + \cdots + X_{1k}D_k + \cdots + X_{1n}D_n,$$

where D_k, the cofactor of X_{1k}, is an $(n-1)\times(n-1)$ determinant, a polynomial in $K[X_{ij},\ 2\leq i,j\leq n,\ j\neq k]$. Thus, we can view D as a polynomial in the variables $X_{11},\ldots,X_{1n}$, with coefficients in the ring $B=K[X_{ij},\ 2\leq i\leq n, 1\leq j\leq n]$, which is an integral domain, since K is. If D can be factored as $D=PQ$, then, over the ring, B, we can write

$$P=P_0+P_1 \quad \text{and} \quad Q=Q_0+Q_1,$$

where $P_0,Q_0\in B$, and $P_1,Q_1\in B[X_{11},\ldots,X_{1,n}]$ are polynomials consisting only of monomials $cX_{11}^{k_1}\cdots X_{1n}^{k_n}$, with $k_1+\cdots+k_n\geq 1$. Since each cofactor D_k is an $(n-1)\times(n-1)$ determinant over $\{X_{ij},\ 2\leq i,j\leq n,\ j\neq k\}$, by the induction hypothesis, each D_k is irreducible in $K[X_{ij},\ 2\leq i,j\leq n,\ j\neq k]$, and a fortiori, in B. Now, since $D=PQ$, i.e.,

$$X_{11}D_1+\cdots+X_{1n}D_n=(P_0+P_1)(Q_0+Q_1)=P_0Q_0+P_0Q_1+P_1Q_0+P_1Q_1$$

and B is an integral domain, the assumptions on $P_0,P_1,\ Q_0,Q_1$ imply that either $P_1=0$ and $Q_0=0$ or $Q_1=0$ and $P_0=0$. Assume that $P_1=0$ and $Q_0=0$, the other case being similar. From

$$X_{11}D_1+\cdots+X_{1n}D_n=P_0Q_1$$

and the fact that $D_1,\ldots,D_n,P_0\in B$, we must have

$$Q_1=X_{11}R_1+\cdots+X_{1n}R_n,$$

where $R_i\in B$, for $i=1,\ldots,n$; thus $D_k=P_0R_k$ for $k=1,\ldots,n$, and since each D_k is irreducible in B, we see that P_0 belongs to K, which shows that D is irreducible.

BV. Let A be a commutative noetherian ring and let B be a finitely generated A-algebra. If $G\subseteq \mathrm{Aut}_{\mathrm{CR}^A}(B)$ is a finite subgroup of automorphisms of B, we write

$$B^G=\{b\in B\mid \sigma(b)=b,\ \text{for all}\ \sigma\in G\}.$$

It is trivial that B^G is an A-algebra. First, we prove the following lemma:

Lemma 1.9 *The A-algebra, B, is integral over B^G.*

Proof. Pick any $b\in B$. We need to show that b is a zero of some monic polynomial with coefficients in B^G. Since G is finite, the orbit of b is finite, say $\{b_1,\ldots,b_m\}$. Obviously, b is a zero of the monic polynomial $P_b(X)=\prod_{i=1}^m(X-b_i)$. We just have to show that the coefficients of $P_b(X)$ are in B^G. But the coefficient of X^{m-k} in $P_b(X)$ is $(-1)^k\sigma_k$, where σ_k is the kth elementary symmetric function,

$$\sigma_k=\sum_{\substack{I\subseteq\{1,\ldots,m\}\\ |I|=k}}\prod_{i\in I}b_i.$$

Since every $\sigma\in G$ induces a permutation on $\{b_1,\ldots,b_m\}$ and σ_k is invariant under permutations, the coefficients of $P_b(X)$ are invariant under G, and so, they belong to B^G.

We will need the following fact:

Lemma 1.10 *If B is an A-algebra and $b_1, \ldots, b_n \in B$ are integral over A, then the A-subalgebra, $A[b_1, \ldots, b_n]$, of B generated by $b_1, \ldots, b_n$, is a finitely generated A-module.*

Proof. We proceed by induction on n. Let $\varphi \colon A \to B$ be the ring homomorphism that makes B into an A-algebra. For $n = 1$, since b_1 is integral over A, this means that there is some monic polynomial $P(X) = X^m + a_1 X^{m-1} + \cdots + a_{m-1}X + a_m$ in $A[X]$, so that

$$b_1^m + \varphi(a_1)b_1^{m-1} + \cdots + \varphi(a_{m-1})b_1 + \varphi(a_m) = 0.$$

(From now on, we will omit the homomorphism φ, for simplicity of notation). As a consequence, we see that $1, b_1, b_1^2, \ldots, b_1^{m-1}$ generate $A[b_1]$, as A-module. Now, assume by induction that $C = A[b_1, \ldots, b_{n-1}]$ is a finitely generated A-module. Since b_n is integral over A, it is integral over C, and so, by the above argument, $B = C[b_n]$ is a finitely generated C-module. Thus, B is a finitely generated C-module and C is a finitely generated A-module. However, this immediately implies that B is a finitely generated A-module. $\square$

Next, we prove

Lemma 1.11 *If A is a (commutative) noetherian ring, B is a finitely generated A-algebra, and C is an A-subalgebra of B so that B in integral over C, then C is finitely generated as A-algebra.*

Proof. Let $b_1, \ldots, b_n$ be a set of generators for B. Since B is integral over C, for every b_i, there is some monic polynomial, $P_i(X) \in C[X]$, so that $P_i(b_i) = 0$. Let C' be the A-subalgebra of C generated by the coefficients of $P_1(X), \ldots, P_n(X)$. Obviously, C is a C'-module, and each b_i is integral over C' (since C' contains the coefficients of $P_i(X)$ and $P_i(b_i) = 0$). Moreover, the A-algebra, $C'[b_1, \ldots, b_n]$, generated by C' and the b_i's, is just B, because B is already finitely generated over A (which means that every $b \in B$ is of the form $Q(b_1, \ldots, b_n)$, where $Q(X_1, \ldots, X_n)$ is some polynomial in $A[X_1, \ldots, X_n]$.) Now, since $B = C'[b_1, \ldots, b_n]$, we see that B is a C'-algebra, and by Lemma 1.10, the C'-algebra, B, is a finitely generated C'-module. Also, since A is noetherian and C' is a finitely generated A-algebra, by a corollary of the Hilbert basis theorem proved in class, C' is a noetherian ring. By another proposition proved in class, since B is a finitely generated C'-module and C' is noetherian, B is a noetherian C'-module. However, it has also been proved in class that the noetherian property is inherited by submodules; so, we see that $C \subseteq B$ is a finitely generated C'-submodule. As C' is a finitely generated A-algebra, this implies that C is a finitely generated A-algebra. $\square$

Applying Lemma 1.9 and Lemma 1.11 to $C = B^G$, we conclude that B^G is a finitely generated A-algebra.