Comments on HW Set 4

Problem 1.

The most interesting part of this problem was to prove that, for $d \geq 1$ and any positive integer $n \geq 2$, the polynomial

$$P_{n,d}(X_1, \ldots, X_n) = X_1^d + X_2^d + \cdots + X_n^d - 1$$

is irreducible. This is done by induction on n. When $n = 2$, the polynomial in question is

$$P_{2,d} = X_2^d + (X_1^d - 1)$$

which we view as a polynomial in $\mathbb{Q}[X_1][X_2]$. The polynomial $X_1^d - 1 = (X_1 - 1)(q(X_1))$ where $q(1) \neq 0$ ($q(X_1) = 1 + X_1 + \cdots + X_1^{d-1}$). Therefore $X_1 - 1$ generates a prime ideal $\mathbf{p}$ in $\mathbb{Q}[X_1]$ and so $P_{2,d}$ is an Eisenstein polynomial in $\mathbb{Q}[X_1][X_2]$ for this prime $\mathbf{p}$ and therefore irreducible.

Now suppose we know that $P_{n,d}$ is irreducible in $\mathbb{Q}[X_1, \ldots, X_n]$. Since this multivariable polynomial ring is a UFD, $P_{n,d}$ generates a prime ideal. Therefore $X_{n+1}^d + P_{n,d}$ is an Eisenstein polynomial for that prime, and is therefore irreducible.

Problem 3.

Let

$$R = F[x, y_1, y_2, \ldots]/I$$

where I is the ideal generated by $(x - y_1^2, y_1 - y_2^2, \ldots)$.

The element

$$\overline{y}_m = y_m + I \in R$$

satisfies

$$\overline{y}_m^{2^m} = \overline{x}$$

and more generally

$$\overline{y}_m^2 = \overline{y_{m-1}}$$

. We let R_n be the subring of R generated by

$$\overline{y}_n$$

. To simplify matters, we write

$$\overline{y}_0 = \overline{x}$$

.

a. $R = \bigcup_{i=m}^{\infty} R_m$.

Proof: Any element f of R is a polynomial in finitely many of the variables

$$\overline{y}_i$$

. Let N be the largest integer such that $\overline{y}_N$ appears in a monomial with nonzero coefficient in f. Since

$$\overline{y}_m = \overline{y}_N^{2^{N-m}}$$

for $m \leq N$, we may rewrite f as a polynomial in

$$\overline{y}_N$$

. Therefore f belongs to

$$R_N$$

.

b. R_n is isomorphic to a polynomial ring in one variable over F.

Proof: Let $S_n = F[x, y_1, \ldots, y_n]$. We have a ring homomorphism $\phi_n : S_n \to R$ coming from the inclusion of the polynomial ring S_n into the big ring $F[x, y_1, \ldots]$. If $f \in S_n$, then $\phi(f) \in R_n$ because, as we've seen in the argument in part (a), any polynomial in the variables $\overline{y_i}$ for $i \leq n$ is equivalent mod I to a polynomial in

$$\overline{y}_n$$

and thus lies in

$$R_n$$

. In fact,

$$\phi_n$$

is a map *onto*

$$R_n$$

since

$$R_n$$

is generated by

$$\overline{y}_n$$

and

$$\overline{y}_n$$

lies in the image of

$$\phi_n$$

.

The ideal $J_n = (x - y_1^2, y_1 - y_2^2, \ldots, y_{n-1} - y_n^2) \subset S_n$ lies in the kernel of ϕ. The quotient S_n/J_n is isomorphic to $F[y_n]$. To see this, note that

$$S_n = F[y_1, \ldots, y_n][x]$$

so that any polynomial in f can be written *uniquely*

$$f = f_1 + a_1(x - y_1^2)$$

where f_1 belongs to $F[y_1, \ldots, y_n]$. Iterating this process, we can write f uniquely as

$$f = f_n + a_n(y_{n-1} - y_n^2) + a_{n-1}(y_{n-2} - y_{n-1}^2) + \cdots + a_1(x - y_1^2)$$

where f_n is in $F[y_n]$.

We would like to show that the kernel of the map $\phi_n : S_n \to R_n$ is J_n, since that would prove that R_n isomorphic to $S_n/J_n = F[y_n]$. But if $\phi_n(f) = 0$ in R it means that, viewed as an element of the big polynomial ring $F[x, y_1, \ldots]$, the polynomial $f \in S_n$ belongs to I. In other words, we can write

$$f = \sum_{j=1}^{N} b_j(y_{j-1} - y_j^2).$$

This equation holds in S_N for some finite N so it says that f lies in J_N. Since we already know that $f = a_0 + a_1 y_n + \cdots + a_k y_n^k + J_n$ can be written uniquely as a polynomial in y_n modulo J_n, in the ring S_N we know that f must be $a_0 + a_1 y_N^{2^{N-n}} + \cdots + a_k y_N^{2^{N-n}}$ modulo J_N and since f lies in J_N all of the coefficients a_i must be zero. In other words, f was already zero modulo J_n and therefore ϕ_n is injective.

Remark: I think this is what is meant by the comment in DF about algebraic relations holding in S_N for some $N \geq n$. Essentially we have proved that if we view S_n as a subring of $F[x, y_1, \ldots,]$ then $I \cap S_n = J_n$; but to prove this we had to deal with the possibility that if f involves the variables only up to y_n, it couldn't still somehow be an element of I involving higher numbered variables.

b'. R is a Bezout domain.

Proof: Suppose that a and b are two elements of R. Then they lie in R_n for some finite n. Since R_n is a polynomial ring in one variable, there is a polynomial $h, x, y \in R_n$ such that $ax + by = h$ and such that $a = uh$ and $b = vh$. Then if $z = ra + sb$ for $r, s \in R$, we have $z = (ru + sv)h$ so z belongs to hR; and conversely hR belongs to (a, b) since $h = ax + by$. Thus any ideal generated by two elements (or, more generally, any finitely generated ideal) is principal.

c. The ideal generated by $x, y_1, y_2, \ldots$ in R is not finitely generated.

Proof: If it were, it would be principal and generated by some h belonging to R_n for some finite n. This would mean that for each $m \geq n$ there would be an $N \geq m$ for which we would have an equation

$$\overline{y}_m = hr_N$$

for

$$r_N \in R_N$$

. Since

$$h \in R_n$$

, it can be written as a polynomial in

$$\overline{y}_n$$

and, in

$$R_N$$

, as a polynomial in

$$\overline{y}_N^{2^{N-n}}$$

. Similarly

$$\overline{y}_m = \overline{y}^{2^{N-m}}$$

. Since

$$2^{N-m}$$

is smaller than

$$2^{N-n}$$

, such a relation can only hold in

$$R_N = F[y_N]$$

if h is a constant polynomial, which would mean that the ideal generated by $x, y_1, \ldots$ would contain a unit and hence be all of $F[x, y_1, \ldots]$. But this is not true; the quotient of the big polynomial ring by this ideal is F.

Problem 5

Let V be a vector space of dimension n over a field F. A *complete flag* in V is a sequence of subspaces

$$Z : W_0 = (0) \subset W_1 \subset W_2 \subset \cdots \subset W_{n-1} \subset W_n = V$$

where W_i has dimension i. The group $\mathrm{GL}(V)$ acts on the flags by permuting the subspaces.

Given a subspace $W_i \subset W_{i+1}$ where W_{i+1} is of one higher dimension, then, given a basis of W_i, you can find a vector in W_{i+1} to add to this basis to get a basis of W_{i+1}. Using this inductively, given a flag, you can construct an ordered basis of V. Conversely, given an ordered basis $v_1, \ldots, v_n$ you get a flag by taking the span of v_1, then the span of v_1, v_2, and so on.

Now suppose you have two flags. Using the above process you get two ordered bases for V. Choose an element of $GL(V)$ carrying one basis to the other; it will carry one flag to the other. This proves the action on flags is transitive.

Now fix a flag and choose a compatible ordered basis $v_1, \ldots, v_n$. Suppose g is an element of $\mathrm{GL}(V)$ that fixes this flag. This means that $gW_i \subset W_i$ for each i, and since W_i is spanned by $v_1, \ldots, v_i$ we must have

$$gv_i = \sum_{j=1}^{i} b_{ji} v_j$$

with $b_{ji} = 0$ if $j > i$. This means the matrix of g is upper triangular. Since it's invertible, the diagonal entries can't be zero.

Finally, over a finite field, we know that $\mathrm{GL}(V)$ has $\prod_{i=0}^{n-1}(q^n - q^i)$ elements. An upper triangular matrix can have arbitrary entries in the off diagonal upper spots, and must have nonzero entries on the diagonal. So the there are $\prod_{i=1}^{n}(q-1)q^{n-1}$ elements of this type. The quotient gives the number of flags:

$$(1+q)(1+q+q^2)\cdots(1+q+\cdots+q^{n-1})$$

If $q = 2$ and $n = 3$ this gives $3 \cdot 7 = 21$ flags.