Math 505 HW2

Anonymous

January 28, 2024

> **Definition 1** (Lang IV.6)**.** Define the weight of a monomial $X_1^{v_1}\cdots X_n^{v_n}$ to be $v_1 + 2v_2 + \cdots + nv_n$, and the weight of a polynomial $g(X_1, \cdots, X_n)$ to be the max of the weights of each of it's monomials.

1. (a) Clearly the theorem is true for $n = 1$, since in that case we only have one symmetric polynomial being x_1, and every symmetric polynomial is of course of the form $f(x_1)$ (since every polynomial is of that form). Suppose the claim is true for $n - 1$, with the added condition that if f is symmetric of degree d, then we can find a weight $\leq d$ polynomial $g \in R[y_1, \cdots, y_n]$ such that $f = g(e_1, \cdots, e_n)$. Now, for the symmetric polynomials on n variables, suppose that the theorem is true for all polynomials of degree $\leq d$ for some $d \geq 1$ (the case $d = 0$ is clear, because given a constant polynomial $f(x_1, \ldots, x_n) = c$, we can just take $F(y_1, \ldots, y_n) = c$–this is induction on d).

   If we write,

   $$P(t, x_1, \ldots, x_n) = (t - x_1)\cdots(t - x_n)$$

   We can see that,

   $$\begin{aligned} P(t, x_1, \ldots, x_{n-1}, 0) &= (t - x_1)\cdots(t - x_{n-1})t \\ &= t^n - e_1(x_n = 0)t^{n-1} + e_2(x_n = 0)t^{n-2} + \cdots + (-1)^n e_n(x_n = 0)t \end{aligned}$$

   Where $f(x_n = 0) := f(x_1, \ldots, x_{n-1}, 0)$. Dividing out by t shows that the $e_k(x_n = 0)$ for $1 \leq k \leq n - 1$ are the elementary symmetric polynomials on $n - 1$ variables.

   Now, let $f(x) \in R[x_1, \ldots, x_n]$ be a degree d symmetric polynomial, and let $g(x_1, \ldots, x_{n-1}) := f(x_n = 0)$. Notice first that g is symmetric on $x_1, \ldots, x_{n-1}$, and has degree $\leq d$, so by induction on n we can find a polynomial $F \in R[y_1, \ldots, y_{n-1}]$ with weight $\leq d$ such that $g(x_1, \ldots, x_{n-1}) = F(e_1(x_n = 0), \ldots, e_{n-1}(x_n = 0))$. We consider the "lift" of this polynomial $h(x_1, \ldots, x_n) = F(e_1, \ldots, e_{n-1})$ (we are taking away the evaluation at 0).

Notice that if $e_1^{\alpha_1} \cdots e_n^{\alpha_n}$ is a monomial of F, it's degree is $\alpha_1 + 2\alpha_2 + \cdots + n\alpha_n$ since $\deg e_i = i$ (explicit calculation). The max of all these is just the weight, which is $\leq d$ by hypothesis, so $\deg h \leq d$.

Now, the idea is that we have f "up to" addition by a power of e_n. Thus, we consider $l(x_1, \ldots, x_n) \coloneqq f(x_1, \ldots, x_n) - h(x_1, \ldots, x_n)$, and notice that $l(x_n = 0) = f(x_n = 0) - g(x_1, \ldots, x_n) = f(x_n = 0) - f(x_n = 0) = 0$, and, since $\deg h \leq d$, $\deg l \leq d$ (This is where the weight portion of the claim comes in). Since l is symmetric, $l(x_n = 0) = l(x_k = 0) = 0$ for every other k, so by the factor theorem $x_k \mid l$ for each $1 \leq k \leq n$, which shows that $(x_1 \cdots x_n) \mid l$. Notice then that $l/(x_1 \cdots x_n)$ has degree $\leq d - n < d$, so we may apply the inductive hypothesis (on d) to find a polynomial $T \in R[y_1, \ldots, y_n]$ of weight $\leq d - n$ such that $l/(x_1 \ldots x_n) = T(e_1, \ldots, e_n)$. Taking

$$T' = y_n T(y_1, \ldots, y_n) + F(y_1, \ldots y_{n-1}, y_n)$$

will yield $f = T'(e_1, \ldots, e_n)$ (Notice that the last y_n of F is technically unnecessary). The $y_n T(y_1, \cdots, y_n)$ term has weight $n + \text{weight}(T(y_1, \cdots, y_n)) \leq n + d - n = d$, and the latter term has weight $\leq d$, so the sum has weight $\leq d$, completing the proof.

(b) Again we prove the claim by induction on n. e_1 is clearly algebraically independent, so suppose the claim is true for some $n \geq 1$. Suppose instead that there was a polynomial $F \in R[y_1, \cdots, y_{n+1}]$ so that $F(e_1, \ldots, e_{n+1}) = 0$. If $y_{n+1} \mid F$, we can see that $F'(y_1, \cdots, y_{n+1}) = \frac{1}{y_{n+1}} F(y_1, \cdots, y_{n+1})$ will also have $F'(e_1, \cdots, e_{n+1}) = 0$ everywhere, since otherwise F would be a product of two non-zero polynomials and hence itself nonzero. Letting α be the highest power of y_{n+1} appear in every monomial of F and replacing F with F/y_{n+1}^{α} will yield a (non-zero) polynomial relation on $e_1, \cdots, e_{n+1}$ where at least one monomial of F is not divisible by y_{n+1}.

Now, $F(e_1, \ldots, e_{n+1})$ is a function of $X_1, \ldots, X_{n+1}$ which is equal to 0 everywhere, so in particular we can plug in $X_{n+1} = 0$ and the new F will still be 0 everywhere. In symbols, $F(e_1(x_{n+1} = 0), \ldots, e_{n+1}(x_{n+1} = 0)) = 0$. Since $e_{n+1}(x_{n+1} = 0) = 0$ (since $e_{n+1} = x_1 \cdots x_{n+1}$), $F(e_1(x_{n+1} = 0), \ldots, e_{n+1}(x_{n+1} = 0)) = F(e_1(x_{n+1} = 0), \ldots, e_n(x_{n+1} = 0), 0)$, so $T(y_1, \cdots, y_n) = F(x_1, \cdots, x_n, 0)$ is so that $T(e_1, \cdots, e_n) = 0$. If T were equivalently 0, then every monomial of F would be divisible by y_{n+1}, which we constructed above to not happen. Thus T is a relation on the elementary symmetric polynomials on $n - 1$ variables, a contradiction.

2. (a) This theorem follows from these two simple claims:

Claim. $S_n = \langle (\alpha_1\ \alpha_2), (\alpha_1\ \alpha_2\ \cdots\ \alpha_n) \rangle$.

Proof. Let σ be the permutation sending α_i to i, and let $\varphi(\tau) = \sigma^{-1}\tau\sigma$. Then $\varphi(\langle (\alpha_1\ \alpha_2), (\alpha_1\ \alpha_2\ \cdots\ \alpha_n) \rangle) = \langle (1\ 2), (1\ 2\ \cdots\ n) \rangle = S_n$, so by order considerations and since φ is an automorphism $\langle (\alpha_1\ \alpha_2), (\alpha_1\ \alpha_2\ \cdots\ \alpha_n) \rangle = S_n$. □

Claim. If $\tau = (\alpha_1\ \alpha_2)$ is any transposition and σ is any p-cycle, then some power of σ, which is another p-cycle, sends α_1 to α_2.

Proof. Since p is prime, σ^n has order p. It can be factored into the product of disjoint cycles, each of which has order dividing p. Thus precisely one has order p and the rest have order 1, which shows that σ^n is just a p-cycle. Let $\mathcal{F} = \left\{ \sigma(\alpha_1), \cdots, \sigma^{-(p-1)}(\alpha_1) \right\}$, and $1 \leq m < n \leq p-1$. If somehow $\sigma^m(\alpha_1) = \sigma^n(\alpha_1)$, then $\sigma^{n-m}(\alpha_1) = \alpha_1$, a contradiction since σ^{n-m} is a p-cycle. Thus $|\mathcal{F}| = p-1$, not containing α_1, so $\mathcal{F} = \{ \alpha_2, \ldots, \alpha_n \}$. In particular, there is an n so that $\sigma^n(\alpha_1) = \alpha_2$. □

Minimality is obvious as removing either generator would reduce the group to size p or 2 respectively, which is (strictly) less than $p!$ for odd p.

(b) Notice that $(13)(1234)(13) = (4321)$, so if we let $x = (13)$ and $a = (1234)$, we have the following properties:

$$a^4 = x^2 = e,\ xax^{-1} = a$$

We also recall that $D_8 = \left\langle r, s \mid r^4 = s^2 = e, xax^{-1} = a \right\rangle$. Thus we have a surjective homomorphism

$$\begin{aligned} \varphi : \langle (13), (1234) \rangle &\to D_8 \\ (13) &\mapsto s \\ (1234) &\mapsto r \end{aligned}$$

Since every element of D_8 is of the form $s^a r^b$, we only have to check injectivity on those elements. Indeed, if $\varphi(x^c a^b) = \varphi(x^d a^w)$, then $s^{d-c} = \varphi(x^{d-c}) = \varphi(a^{b-w}) = r^{b-w}$. Since $\langle s \rangle \cap \langle r \rangle = \langle 1 \rangle$, we must have $\varphi(x^{d-c}) = \varphi(a^{b-w}) = e$. The only power of a mapping to e is e, and similarly the only power of x mapping to e is e, which shows injectivity. Thus $\langle (13), (1234) \rangle \cong D_8$, and in particular $8 = |\langle (13), (1234) \rangle| < |S_4| = 4! = 24$. For the curious reader, the second claim from part (a) fails since $(1234)^2 = (13)(24)$, so no power of (1234) is a 4-cycle sending 1 to 3.

(c) This proof has multiple parts. First,

Claim. $S_n = \langle (12), (23), (34), \ldots, (n-1\ n) \rangle$.

Proof. Clearly $(12) = (12)$. Assume that $(12)(34)\cdots(n-1\ n) = (1234\cdots n)$ (where multiplication is taken from right to left) for some $n \geq 2$. Then $(12)(34)\cdots(n-1\ n)(n\ n+1) = (1234\cdots n)(n\ n+1) = (n\ n+1\ 123\cdots)$, which completes this subclaim. Since $S_n = \langle (12), (123\cdots n) \rangle$, this completes the proof of the claim. $\square$

Claim. $\{\, (12), (34), \cdots, (n-1\ n) \,\}$ is a minimal system of generators.

Proof. We need only show it is minimal. If you throw away (12) or $(n-1\ n)$, the remaining elements cannot generate the whole group since they either fix 1 or n respectively (since 1 and n don't show up in any transposition). The more important and more general case follows now. Suppose we drop $(l\ l+1)$ for some $2 \leq l < n-1$. Clearly this transposition is not a product of the transpositions

$$\{\, (l+1\ l+2), \cdots, (n-1\ n) \,\}$$

Since each of those fix l (so any product fixes l). Similarly $(l\ l+1)$ is not a product of the transpositions

$$\{\, (12), \cdots, (l-1\ l) \,\}$$

Notice at last that if $(l\ l+1)$ were a product of transpositions of the above form, we could group transpositions with values $\leq l$ on the left and values $\geq l+1$ on the right since disjoint cycles commute. To be a transposition, precisely one of these groups would have to be a transposition, otherwise you would get a product of two disjoint cycles. We have shown above that these products cannot be $(l\ l+1)$, which completes the proof. $\square$

The above two claims shows that S_n has a minimal system of generators for the extreme cases of $k = 2, n-1$.

The idea behind getting the remaining k is the following: If a transposition and an n-cycle is minimal, and only transpositions is minimal, maybe some transpositions and a k-cycle is minimal.

Indeed, we have our final claim.

Claim. $\{\, (12\cdots k), (k\ k+1), \cdots, (n-1\ n) \,\}$ is a minimal system of generators for S_n.

Proof. First, notice that it is in fact a system of generators–$(12\cdots k)(k\ k{+}1)\cdots(n{-}1\ n) = (123\cdots n)$, so we can use the first claim of part (a). The proof of minimality is almost the same as last time. Indeed, if we drop the k-cycle or the last transposition, the rest of the generators fix 1 or n respectively, hence cannot generate the whole group. If we instead dropped $(l\ l+1)$ for some $k \leq l < n-1$, we again have 3 cases. The above transposition is not a product of $(123\cdots k), (k\ k+1), \ldots, (l-1\ l)$, since each of those fix $l+1$ so any product does. Similarly, $(l\ l+1)$ is not a product of $(l+1\ l+2), \cdots, (n-1\ n)$ since each of those fix l. For a general product, commute the disjoint transpositions on the left/right resp. depending on if they have values $\leq l$ or $\geq l+1$ only. For powers of the k-cycle, similarly commute it to the left. Once again since we have a product of disjoint cycles, to get a transposition we would need precisely one of the groups to be a transposition (and the other to be the identity). The above cases show this is not possible, which completes the proof. $\square$

Finally notice that this system of generators has $n-1-k+1 = n-k$ elements for each $2 \leq k \leq n-1$.