Solutions to Homework 3 **Math 5590H**

5pt **1.3.14.** *Let p be a prime. Show that a permutation $\sigma \in S_n$ has order p iff σ is a product of disjoint p-cycles. Show by example that this doesn't need to be so if p is not prime.*

Solution. Every permutation is uniquely representable as a product of disjoint cycles, and the order of the permutation is the lcm of the lengths of these cycles. So, the order $p = |\sigma|$ of $\sigma \in S_n$ is prime iff cycles in the cyclic decomposition of σ have length p (excluding, as usual, 1-cycles).

For the permutation $\sigma = (1,2)(3,4,5)$ we have $|\sigma| = 6$.

10pt **3.5.4,5.** (a) *For any $n \in \mathbb{N}$, prove that S_n is generated by any n-cycle $\rho = (i_1, i_2, \ldots, i_n)$ and the transposition $\tau = (i_1, i_2)$.*

Solution. W.l.o.g., let $\rho = (1, 2, \ldots, n)$ and $\tau = (1, 2)$. For any $i < n$, we have $(i, i+1) = \rho^{i-1}\tau\rho^{-(i-1)}$. (We know how a conjugation changes a permutation. If not, notice that $\rho^{i-1}\tau\rho^{-(i-1)}$: $i \mapsto 1 \mapsto 2 \mapsto i+1$, $i+1 \mapsto 2 \mapsto 1 \mapsto i$, and for every $j \neq i, i+1$, $\tau(\rho^{-(i-1)}(j)) = \rho^{-(i-1)}(j)$, so $\rho^{i-1}\tau\rho^{-(i-1)}(j) = j$.) Since transpositions of the form $(i, i+1)$ generate S_n, we see that τ and ρ generate S_n too.

10pt (b) *If p is prime, show that $S_p = \langle \tau, \rho \rangle$ where ρ is any p-cycle and τ is any transposition.*

Solution. Let $\rho = (i_1, i_2, \ldots, i_p)$. Then for any $k < p$, $\rho^k = (i_1, i_{1+k}, i_{1+2k}, \ldots, i_{1+(p-1)k})$, where the products ik are computed modulo p. This is still a p-cycle, since for any $l < p$, $lk \neq 0 \bmod p$. W.l.o.g., let $\tau = (i_1, i_k)$, then $\rho^{k-1} = (i_1, i_k, i_{1+2(k-1)}, \ldots)$. By (a), τ and ρ^{k-1} generate S_p, so τ and ρ also do.

5pt **2.4.7.** *Prove that the subgroup of S_4 generated by $\tau = (1,2)$ and $\rho = (1,3)(2,4)$ is isomorphic to D_8.*

Solution. Let's draw a square S with vertices $1, 3, 2, 4$:

$$\begin{array}{ccc} 2 & — & 3 \\ | & & | \\ 4 & — & 1 \end{array}$$

Then the permutations τ and ρ act as two distinct reflections of S, their product $\tau\rho = (1,2)(1,3)(2,4) = (1,3,2,4)$ is the $\pi/2$-angle rotation of S, so these permutations generate a group isomorphic to D_8.

Another solution. Let H be the subgroup. The permutation $\lambda = \tau\rho = (1,3,2,4)$ is a 4-cycle; thus, H has at least 8 elements: $1, \lambda, \lambda^2, \lambda^3, \tau, \rho, \tau\lambda, \rho\lambda$. We have $\tau^2 = \rho^2 = 1$ and $(\tau\rho)^4 = \lambda^4 = 1$. These are just the relations defining (by exercise 1.2.7) the group D_8, which has 8 elements. Hence, H has at most 8 elements, so has exactly 8 elements, and is isomorphic to D_8. (We will have a rigorous justification of this approach later.)

10pt **2.2.7.** *For all $n \geq 3$, prove that $Z(D_{2n}) = \{1, r^{n/2}\}$ if n is even and $Z(D_{2n}) = 1$ if n is odd.*

Solution. We have $r^k s = sr^{-k}$ for all k, so r^k and s don't commute unless $k = -k \bmod n$, that is, n is even and $k = n/2$. For any k, $(sr^k)r = r^{-1}(sr^k)$, so sr^k and r don't commute for all k. Hence, the only non-identity element of D_{2n} that commutes with all other elements is $r^{n/2}$, in the case n is even.

10pt **A1.** *Prove that for any $n \in \mathbb{N}$ and field F, $Z(\mathrm{GL}_n(F))$ is the set of scalar matrices cI, $c \in F^*$.*

Solution. Scalar matrices do commute with all other matrices, $(cI)A = cA = A(cI)$ for all $c \in F$.

If $A = (a_{i,j}) \in \mathrm{GL}_n(F)$ is not diagonal, let $k \neq l$ be such that its (k,l)-th entry $a_{k,l} \neq 0$. Define matrix $B = (b_{i,j}) \in \mathrm{GL}_n(F)$ by $b_{i,i} = 1$ for all i and $b_{i,j} = 0$ for all $i \neq j$ unless $b_{l,k} = 1$. Then the (k,k)-th entry of AB is $a_{k,k} + a_{k,l}$ and the (k,k)-th entry of BA is $a_{k,k}$, so $AB \neq BA$, so $A \notin Z(\mathrm{GL}_n(F))$.

If A is diagonal but not scalar, let $k \neq l$ be such that $a_{k,k} \neq a_{l,l}$ then for B as above, the (k,l)-th entry of AB is $a_{k,k}$ and of BA is $a_{l,l}$, so, again, $AB \neq BA$.

5pt **3.2.8.** *Prove that if H and K are finite subgroups of G whose orders are relatively prime, then $H \cap K = 1$.*

Solution. $H \cap K$ is a subgroup of both H and K, so its order $|H \cap K|$ divides both $|H|$ and $|K|$. Since $|H|$ and $|K|$ are relatively prime, we must have $|H \cap K| = 1$, so $H \cap K = 1$.

5pt **3.2.22.** *Determine the last two digits of* $3^{3^{100}}$.

Solution. Interested in the last two digits of an integer, we may deal with the residues modulo 100, that is, with the elements of $\mathbb{Z}_{100}$ instead of integers. The order of $\mathbb{Z}_{100}^*$ is $\varphi(100) = 40$. (We will learn that if $n = \prod_{i=1}^{k} p_i^{r_i}$ where p_i are distinct primes, then $\varphi(n) = \prod_{i=1}^{k} p_i^{r_i-1}(p_i - 1)$.) So, $a^{40} = 1$ for all $a \in \mathbb{Z}_{100}^*$. Now, modulo 40, 3 has order 4, since $3^4 = 81 = 1 \bmod 40$. Hence, $3^{100} = 1 \bmod 40$. So, $a^{3^{100}} = a^1 = a$ for all $a \in \mathbb{Z}_{100}^*$, and in particular, $3^{3^{100}} = 3 \bmod 100$.