Math 430
Dr. Songhao Li
Spring 2016

HOMEWORK 4 SOLUTIONS
Due 2/22/16

1. Let G be a group. A minimal generating set of G is a generating set $M_G \subseteq G$ of G such that if $S \subseteq G$ is another generating set of G, then $|M_G| \leq |S|$. Give an example of a finite group G and a proper subgroup $H \lneq G$ such that there is some M_G such that $|M_G| \lneq |M_H|$ for any minimal gernerating set M_H of H.

Solution: Consider the finite group S_6. By Homework 3 Problem 39, $S_6 = \langle (1\,2), (1\,2\,3\,4\,5\,6)\rangle$, and since S_6 is not cyclic, $\{(1\,2), (1\,2\,3\,4\,5\,6)\}$ is a minimal generating set of S_6. We claim that the subgroup $H = \langle (1\,2), (3\,4), (5\,6)\rangle$ is not generated by any two of its elements. We first note that since these transpositions are disjoint, they commute. Thus, since transpositions have order 2, we have $H = \{(1\,2)^a(3\,4)^b(5\,6)^c \ : \ a, b, c \in \{0, 1\}\}$. Note that all eight elements of H are of order two since these transpositions are disjoint. We will now show that H is not generated by any of its two element subsets, and thus any minimal generating subset of H must have at least three elements. We will do this by exhaustive case analysis (alternatively, you might just believe that since $H \equiv (\mathbb{Z}/2\mathbb{Z})^3$ via the map $\phi\Big((1\,2)^a(3\,4)^b(5\,6)^c\Big) = \big([a], [b], [c]\big)$ and $(\mathbb{Z}/2\mathbb{Z})^3$ is not generated by any two of its elements, neither is H). Suppose $S \subseteq H$ such that $|S| = 2$. There are then 5 possible cases.

Case 1: Suppose $\iota \in S$. Then $\langle S\rangle = \langle S \setminus \{\iota\}\rangle$ is of order 2, and hence is not H.

Case 2: Suppose $S = \{\tau, \sigma\}$ for two distinct transpositions $\tau, \sigma \in H$. Then these transpositions are disjoint, and hence commute. Then $\langle S\rangle = \{\iota, \tau, \sigma, \tau\sigma\} \lneq H$.

Case 3: Suppose $S = \{\tau, \tau \circ \sigma\}$ for two distinct transpositions $\tau, \sigma \in H$. Then, as before, $\langle S\rangle = \{\iota, \tau, \sigma, \tau\sigma\} \lneq H$ since $(\tau\sigma)\tau = (\tau^2)\sigma = \sigma$ and $(\tau\sigma)^2 = \iota$.

Case 4: Suppose $S = \{\tau\sigma, \tau\lambda\}$, where $\tau, \sigma, \lambda \in H$ are the three distinct transpositions in H. Then, again by commuting these disjoint transpositions, we have $\langle S\rangle = \{\iota, \tau\sigma, \tau\lambda, \sigma\lambda\} \lneq H$.

Case 5: Suppose $S = \{\tau, \tau\sigma\lambda\}$. Then $\langle S\rangle = \{\iota, \tau, \tau\sigma\lambda, \sigma\lambda\} \lneq H$.

Case 6: Suppose $S = \{\tau\sigma, \tau\sigma\lambda\}$. Then $\langle S\rangle = \{\iota, \tau\sigma, \tau\sigma\lambda, \lambda\} \lneq H$.

Thus, $M_H = \{(1\,2), (3\,4), (5\,6)\}$ is a minimal generating set of H, and $|M_G| = 2 \lneq 3 = |M_H|$ as desired.

■

Part II Section 10 Exercises

16. Let $\mu = (1\,2\,4\,5)(3\,6) \in S_6$. Compute $(S_6 : \langle\mu\rangle)$.

Solution: Since $\mu = (1\,2\,4\,5)(3\,6)$, $|\langle\mu\rangle| = \text{lcm}(4, 2) = 4$. Since S_6 is finite with order $6!$, by Lagrange's Theorem, $(S_6 : \langle\mu\rangle) = \dfrac{|S_6|}{|\langle\mu\rangle|} = \dfrac{6!}{4} = 180$.

■

For Problems 30, 31, and 32, let G be a group, $H \leq G$, and $a, b \in G$. Give a proof or a counterexample to each claim.
30. If $aH = bH$, then $Ha = Hb$.

Solution: Let $G = D_4$, $H = \langle(2\,4)\rangle$, $a = (1\,2\,3\,4)$, and $b = (1\,2)(3\,4)$. Then

$aH = \{a \circ \iota, a \circ (2\,4)\} = \{(1\,2\,3\,4), (1\,2)(3\,4)\} = \{b \circ (2\,4), b \circ \iota\} = bH$ but

$Ha = \{\iota \circ a, (2\,4) \circ a\} = \{(1\,2\,3\,4), (1\,4)(2\,3)\} \neq \{(1\,2)(3\,4), (1\,4\,3\,2)\} = \{\iota \circ b, (2\,4) \circ b\} = Hb$.

■

31. If $Ha = Hb$, then $b \in Ha$.

Proof. Since $e \in H$, $b = eb \in Hb = Ha$. ■

32. If $aH = bH$, then $Ha^{-1} = Hb^{-1}$.

Proof. Let $ha^{-1} \in Ha^{-1}$. Since $h \in H$ and H is a group, $h^{-1} \in H$. Them, since $aH = bH$, $ah^{-1} = bh'$ for some $h' \in H$. Then $ha^{-1} = (ah^{-1})^{-1} = (bh')^{-1} = (h')^{-1}b^{-1} \in Hb^{-1}$, and so $Ha^{-1} \subseteq Hb^{-1}$. The same argument with a and b interchanged gives the reverse inclusion, and hence equality. In fact, this argument in reverse shows that $aH = bH$ if and only if $Ha^{-1} = Hb^{-1}$, a result we will use in the next problem. ■

35. Given a group G and a subgroup $H \leq G$, exhibit a bijection from the set of left cosets of H in G to the set of right cosets of H in G.

Proof. Let $L = \{gH \; : \; g \in G\}$ be the set of (distinct) left cosets of H in G and $R = \{Hg \; : \; g \in G\}$ be the set of (distinct) right cosets of H in G. Define the function $\Sigma : L \to R$ by $\Sigma(gH) = Hg^{-1}$. We claim that Σ is a well-defined bijection. Suppose $aH = bH$. Then, by Problem 32, $\Sigma(aH) = Ha^{-1} = Hb^{-1} = \Sigma(bH)$, and so Σ is well-defined. Now, suppose $\Sigma(xH) = \Sigma(yH)$. Then $Hx^{-1} = Hy^{-1}$ and so $xH = yH$ by Problem 32 (the reverse implication). Thus, Σ is injective. Let $Hg \in R$. Then $g \in G$, and hence $g^{-1} \in G$ since G is a group. Then $g^{-1}H \in L$, and $\Sigma(g^{-1}H) = H(g^{-1})^{-1} = Hg$, i.e. Σ is surjective. Then Σ is in fact a bijection from the left cosets of H to the right cosets of H. ■

39. Show that if H is a subgroup of index 2 in G, then every left coset of G is also a right coset of G.

Proof. Since H is of index 2 and the left cosets of H in G partition G as a set, the left cosets of H in G must be H itself (since $H = eH$) and $G \setminus H$. Similarly, the right cosets of H in G are H itself ($H = He$) and $G \setminus H$. Note that we do not require that G be a finite group. ■

44 a. Let A be a set, $c \in A$, and S_A be the symmetric group on A. Prove that $S_c = \{\sigma \in S_A \ : \ \sigma(c) = c\}$ is a subgroup of S_A.

Proof. Since $\iota(c) = c$, $\iota \in S_c$. In particular, S_c is non-empty. Suppose $\sigma, \lambda \in S_c$. Then $\sigma \circ \lambda(c) = \sigma\big(\lambda(c)\big) = \sigma(c) = c$, and so $\sigma \circ \lambda \in S_c$. Since $\iota(a) = a$ for all $a \in A$, $\iota(c) = c$, and so $\iota \in S_c$. Suppose $\rho \in S_c$. Then $\rho \in S_A$, and so $\rho^{-1} \in S_A$ such that $\rho^{-1} \circ \rho = \iota$. Then $\rho^{-1}(c) = \rho^{-1}\big(\rho(c)\big) = \rho \circ \rho^{-1}(c) = \iota(c) = c$, and so $\rho^{-1} \in S_c$. Therefore, $S_c \leq S_A$. ■

Part II Section 11 Exercises

50. Let H and K be groups, and let $G = H \times K$. Show that the subgroups $H \times \{e_K\}$ and $\{e_H\} \times K$ have the following properties: every $g \in G$ can be written $g = hk$ for some $h \in H \times \{e_K\}$ and some $k \in \{e_H\} \times K$, $hk = kh$ for all $h \in H \times \{e_K\}$ and $k \in \{e_H\} \times K$, and $(H \times \{e_K\}) \cap (\{e_H\} \times K) = \{e_G\}$.

Proof. Let $g \in G$. Then $g = (h, k)$ for some $h \in H$ and $k \in K$. Then $(h, e_K) \in H \times \{e_K\}$, $(e_H, k) \in \{e_H\} \times K$, and $g = (h, k) = (h, e_K)(e_H, k)$. Directly, since $he_H = h = e_H h$ and $ke_K = k = e_K k$ for all $h \in H$ and $k \in K$, we have $(h, e_K)(e_H, k) = (h, k) = (e_H, k)(h, e_K)$ for all $(h, e_K) \in H \times \{e_K\}$ and all $(e_H, k) \in \{e_H\} \times K$. Since the second coordinate of every $(h, e_K) \in H \times \{e_K\}$ is $e_K \in K$ and the first coordinate of every $(e_H, k) \in \{e_H\} \times K$ is $e_H \in H$, the only element in the intersection of these two subgroups must have e_H in the first coordinate and e_K in the second coordinate, i.e. $(H \times \{e_K\}) \cap (\{e_H\} \times K) = \{(e_H, e_K)\} = \{e_G\}$. ■

51. Let $H, K \leq G$ satisfy the three properties given in Problem 50. Show that $G \equiv H \times K$.

Proof. We first show that the decomposition $g = hk$ is unique. Suppose that $h'k' = g = hk$. Then $h'k' = hk$, and thus $h^{-1}h' = k(k')^{-1}$. Since $h^{-1}h' \in H$ and $k(k')^{-1} \in K$, $h^{-1}h' = k(k')^{-1} \in H, K$, and hence $h^{-1}h' = k(k')^{-1} = e$ since $H \cap K = \{e\}$. Then $h' = h$ and $k' = k$.

Define the function $\phi : G \to H \times K$ by $\phi(g) = (h, k)$, where $g = hk$ is the unique factorization of g in H and K. We will show that ϕ is a group isomorphism. Let $hk, h'k' \in G$. Then, since $kh' = h'k$, we have $\phi\big((hk)(h'k')\big) = \phi(hkh'k') = \phi(hh'kk') = \phi\big((hh')(kk')\big) = (hh', kk') = (h, k)(h', k') = \phi(hk)\phi(h'k')$, and so ϕ is a homomorphism. Suppose $hk, h'k' \in G$ such that $\phi(hk) = \phi(h'k')$. Then $(h, k) = (h', k')$, and so $h = h'$ and $k = k'$. In particular, $hk = h'k'$, and so ϕ is injective. Let $(h, k) \in H \times K$. Then $hk \in G$ and $\phi(hk) = (h, k)$, so ϕ is surjective.

Therefore, ϕ is an isomorphism, and $G \equiv H \times K$. ∎

53. Prove that if a group G has order p^k for some prime p and some natural number k, then $|g|$ is a power of p for all $g \in G$.

Proof. By Lagrange's Theorem, $|g|$ divides $|G| = p^k$ for every $g \in G$. Since p is prime, the only divisors of p^k are $1, p, \ldots, p^{k-1}$, and p^k. Thus, $|g|$ must be a power of p. Note that this argument does not require G to be abelian. ∎