Math 120 Homework 3 Solutions

April 24, 2008

p. 85

22.) a. Suppose $x, y \in H \cap K$. Then $x, y \in H$ implies $x^{-1}y \in H$ since H is a subgroup. Similarly $x^{-1}y \in K$ so $x^{-1}y \in H \cap K$ so that $H \cap K$ is a subgroup by the subgroup criterion. Take $g \in G$. Then $H \cap K \subset H$ implies $g(H \cap K)g^{-1} \subset H$ since H is normal. Similarly, $g(H \cap K)g^{-1} \subset K$ so $g(H \cap K)g^{-1} \subset H \cap K$ and thus $H \cap K$ is normal.

33.) The subgroups $\langle s, r^2 \rangle$, $\langle r \rangle$ and $\langle rs, r^2 \rangle$ are all normal by virtue of being index 2. Their quotient groups all have order 2, hence are isomorphic to Z_2 (the cyclic group of order 2). The subgroups of order 2 in D_8 are normal if and only if their non-identity elements are in the center (since conjugating the non-identity element cannot move it to the identity, but must move it within the subgroup, hence maps it to itself). The only non-identity element in the center of D_8 is r^2. Thus $\langle r^2 \rangle$ is the only normal subgroup of index 4. Its quotient group has order 4, hence is either Z_4 or $Z_2 \times Z_2$. In passing to the quotient, we have $\overline{r} = \overline{r^3}$ so $|\overline{r}| = 2$. All other elements of D_8 had order 1 or 2 and so their images in $D_8/\langle r^2 \rangle$ have order 1 or 2. Hence $D_8/\langle r^2 \rangle$ has no elements of order 4, hence must be isomorphic to $Z_2 \times Z_2$.

p. 95

4.) As suggested in the hint, we'll first check that if $G/Z(G)$ is cyclic, then G is abelian. Suppose $G/Z(G)$ is cyclic. Then for $w, y \in G$ we may write $w = x^a z_1$, $y = x^b z_2$ with $z_1, z_2 \in Z(G)$. Then $wy = x^a z_1 x^b z_2 = x^{a+b} z_1 z_2 = x^{a+b} z_2 z_1 = x^b z_2 x^a z_1 = yw$, where we have used, repeatedly, that the elements z_1, z_2 commute with all elements in G. Hence $wy = yw$ and G is abelian.

Applying this to the problem at hand, we may not have $|Z(G)| = p$ since this would force $|G/Z(G)| = q$ so $|G/Z(G)|$ cyclic implies $|Z(G)| = pq$, contradiction. Similarly $|Z(G)| \neq q$. Thus, as $|Z(G)|$ divides $|G| = pq$, $|Z(G)| = pq$ or $|Z(G)| = 1$. In the first case, $G = Z(G)$ and G is abelian. In the second, $Z(G) = 1$.

8.) Take $x \in H \cap K$. Then $|x|$ divides both $|H|$ and $|K|$ so $|x|$ divides $(|H|, |K|)$ so $|x| = 1$ and $x = 1$. Thus $H \cap K = 1$.

11.) Let $\{x_i\}_{i \in I}$ be a list of coset representatives for K in G such that $x_i K \cap x_j K = \varnothing$ if $i \neq j$ and $G = \bigcup_{i \in I} x_i K$. Let $\{y_j\}_{j \in J}$ be a corresponding list of coset representatives of H in K. I claim that $\{x_i y_j\}_{i \in I, j \in J}$ is a list of coset representatives of H in G. Indeed, $G = \bigcup_{i \in I} x_i K = \bigcup_{i \in I} x_i \left(\bigcup_{j \in J} y_j H \right) = \bigcup_{i \in I} \bigcup_{j \in J} x_i y_j H$. Here, moving x_i inside the union

is justified because $x_i \bigcup_{j\in J} y_j H = \{x_i y_j H : j \in J\} = \bigcup_{j\in J} x_i y_j H$.

Now suppose $z \in x_i y_j H \cap x'_i y'_j H$, $z = x_i y_j h = x'_i y'_j h'$. Since $y_j H, y'_j H \subset K$ and $x_k K \cap x'_k K = \varnothing$ for $k \neq k'$ we must have $x_i = x'_i$. Thus $x_i^{-1} z = y_j h = y_j h' \in y_j H \cap y'_j H$, and now the condition $y_k H \neq y'_k H$ for $k \neq k'$ implies $j = j'$. Thus $x_i y_j H \cap x'_i y'_j H \neq \varnothing$ implies $x_i = x'_i$ and $y_j = y'_j$, so indeed, the list $\{x_i y_j\}_{i\in I, j\in J}$ is a list of coset representatives of H in G. This shows that $|G : H| = |I \times J| = |I| \cdot |J| = |G : K| \cdot |K : H|$ where the equality is an equality of cardinality.

14.) If N is normal and $x \in N$ then all conjugates of x also lie in N. An order 8 normal subgroup of S_4 could contain only elements of order 1, 2, or 4 (since there are no permutations in S_4 of order 8). Order 4 elements are 4 cycles while order 2 elements are either 2-cycles, or products of disjoint 2-cycles. The only order 1 element is the identity. Now any two permutations of the same cycle type are conjugate in S_n (i.e. because $\pi(1, \sigma(1), ..., \sigma^k(1))\pi^{-1} = (\pi(1), \sigma(\pi(1)), ..., \sigma^k(\pi(1))))$ so a normal subgroup of order eight would have to contain some combination of all six 4-cycles, all six 2-cycles, all three products of distinct 2-cycles, and the identity. There is no combination of 6, 6, 3, and 1 that adds to 8, so it is not possible to have a normal subgroup of order 8.

A normal subgroup of order three is also impossible, since it would contain an element of order 3, that is, a three cycle, hence would have to contain all eight 3-cycles.

p. 101

3.) Suppose K is not contained in H. Since H is normal, HK is a subgroup of G properly containing H. Thus $p = |G : H| = |G : HK| \cdot |HK : H|$. Now $|HK : H| > 1$ implies $|HK : H| = p$ since it divides p, hence $|G : HK| = 1$ and $HK = G$. By the second isomorphism theorem, $HK/H \cong K/(K \cap H)$ and so $|HK : H| = |K : K \cap H|$, that is $p = |G : H| = |K : K \cap H|$.

Shuffling problem

i.) Two cards: (1 2)
Four cards: (1 2 4 3)
Six cards: (1 2 4)(3 6 5)
Eight cards: (1 2 4 8 7 5)(3 6)

ii.) Answer: $n = 2^{k-1} - 1$.
Proof: On shuffle s, card j moves to position $2^s j \mod 2n + 1$. The condition that the deck returns to its original configuration after k perfect shuffles is equivalent to $2^k \equiv 1$

mod $2n+1$. Indeed, if this holds then j is mapped to $j2^k \equiv j \mod 2n+1$, while if $2^k \not\equiv 1 \mod 2n+1$ then 1 is mapped to $2^k \equiv r \mod 2n+1$ with $r \not\equiv 1$ and hence 1 is not mapped to its original position.

Suppose $n = 2^{k-1}-1$ so that $2n+1 = 2^k-1$. Certainly $2^k \equiv 1 \mod 2^k-1$ so $n = 2^{k-1}-1$ is a choice for which the deck returns to its original position after k shuffles. (Incidently, for such choice of n, the deck does not return to its original configuration in fewer than k shuffles because $2^j \equiv 1 \mod 2^k-1$ implies 2^k-1 divides 2^j-1 so $j \geq k$.) Now suppose we have a deck of $m > 2^{k-1}-1$ cards. Then after k shuffles, if the first card is in its original position we must have $2^k \equiv 1 \mod 2m+1$, that is, $2m+1$ divides 2^k-1. But this is impossible, because $m > 2^{k-1}-1$ implies $2m+1 > 2^k-1$. Thus the choice $n = 2^{k-1}-1$ is maximal.