MATH 594, WINTER 2006, PROBLEM SET 2

DUE: 1/30/2006

Warm-up (not to be handed in)

[DF], §4.4, Exercises 1, 3, 5, 6 (done in class), 13, 19 (after you have done 18, see below), §4.5, Exercise 1, 3, 4, 7, 13.

Exercises to be handed in

Exercise 1. Do [DF], §4.4, exercise 8.

Solution.
(a) Suppose that \( g \in G \). The map \( c_g : K \to K \) given by \( h \mapsto ghg^{-1} \) is well defined because \( K \) is normal. We have \( gHg^{-1} = c_g(H) = H \) because \( c_g \) is an automorphism of \( K \) and \( H \) is characteristic in \( K \). This shows that \( H \) is normal in \( G \).

(b) Suppose that \( \sigma \) is an automorphism of \( G \). Then \( \sigma(K) = K \) because \( K \) is characteristic, and \( \sigma \) induces an automorphism of \( K \) by restriction. This automorphism will be denoted by \( \sigma |_K \). Since \( H \) is characteristic in \( K \), we have \( \sigma(H) = \sigma |_K (H) = H \). This shows that \( H \) is characteristic in \( G \).

The group \( V_4 \) is the unique 2-Sylow subgroup of \( A_4 \). In other words, \( V_4 \) is the unique subgroup of \( A_4 \) with 4 elements, so it must be characteristic in \( A_4 \). (Indeed, if \( \sigma \) is an automorphism of \( A_4 \) then \( \sigma(V_4) \leq A_4 \) has 4 elements, so \( \sigma(V_4) = V_4 \).) The group \( A_4 \) is characteristic in \( S_4 \), because \( A_4 \) is the subgroup of \( S_4 \) generated by all elements of order 3. This shows that \( A_4 \) is characteristic in \( S_4 \). (More generally \( A_n \) is characteristic in \( S_n \) because it is the unique normal subgroup of index 2: Suppose that \( N \) is any normal subgroup of \( S_n \) with index 2. Suppose that \( \sigma \) is a transposition. If \( \sigma \in N \) then \( N \) contains all transpositions because \( N \) is normal. Since \( S_n \) is generated by transpositions, \( N = S_n \).) We conclude that \( V_4 \) is characteristic in \( S_4 \).

(c) Let \( G \cong D_8 \) generated by \( r \) and \( s \) as usual, where \( r \) is rotation about \( 90^\circ \) and \( s \) is a reflection in a line. The group \( K \cong V_4 \) generated by \( r^2 \) and \( s \) is characteristic in \( D_8 \), because it is the subgroup generated by all elements of order 2. The subgroup \( H \) generated by \( s \) is normal in \( K \).
because $K$ is abelian. However, $H = \{1, s\}$ is not normal in $G$. Indeed, 
$r^2s = r^{-1}r^2s = r^{-1}s \not\in \{1, s\} = H$.

**Exercise 2.** Do [DF], §4.4, exercise 18.

**Solution.**

(a) Suppose that $\sigma$ is an automorphism of the group $G$ and $h_1, h_2 \in G$. Suppose that $h_1, h_2$ lie in the same conjugacy class, say $h_2 = gh_1g^{-1}$. We get $\sigma(h_2) = \sigma(g)\sigma(h_1)\sigma(g)^{-1}$, so $\sigma(h_1)$ and $\sigma(h_2)$ are conjugate. Similarly, if $\sigma(h_1)$ and $\sigma(h_2)$ are conjugate, then the same argument, using $\sigma^{-1}$ instead of $\sigma$, shows that $h_1 = \sigma^{-1}(\sigma(h_1))$ and $h_2 = \sigma_2^{-1}(\sigma(h_2))$ are conjugate. Conclusion: $h_1$ and $h_2$ are conjugate if and only if $\sigma(h_1)$ and $\sigma(h_2)$ are conjugate. So $\sigma$ permutes the conjugacy classes.

(b) We have

$$|K| = \binom{n}{2}.$$ 

Let $K'$ be another conjugacy class that corresponds to the partition 

$$(2^r, 1^{n-2r}) = \underbrace{(2, 2, \ldots, 2)}_r \underbrace{(1, 1, \ldots, 1)}_{n-2r}$$

with $r \geq 2$. The cardinality of $K'$ is 

$$\frac{n!}{(n-2r)!r!2^r}$$

(See §4.3, exercise 33, which was a warm-up question on the last problem set.) So we get 

$$\frac{|K'|}{|K|} = \frac{(n-2)!}{(n-2r)!r!2^{r-1}} = \left(\frac{n-2}{r} \cdot \frac{n-3}{r-1} \cdot \frac{n-r}{2} \cdot \frac{n-r-1}{2} \cdots \frac{n-2r+1}{2}\right).$$

If $n > 2r$ and $r \geq 2$ then all factors above are $> 1$, except the last one which is still $\geq 1$. So we get $|K'| > |K|$. Suppose that $n = 2r$. Then 

$$\frac{|K'|}{|K|} = \left(\frac{2r-2}{r} \cdot \frac{2r-3}{r-1} \cdot \frac{r}{2} \cdot \frac{r-1}{2} \cdots \frac{1}{2}\right).$$

If $r \geq 5$ then all factors except for the last are $\geq 1$ and 

$$\frac{r-1}{2} \cdot \frac{r-2}{2} \cdots \frac{1}{2} \geq 2 \cdot \frac{3}{2} \cdot 1 \cdot \frac{1}{2} > 1$$

so $|K'| > |K|$. One easily checks that $|K'| \neq |K|$ for $r = 2$ ($n = 4$) and $r = 4$ ($n = 8$).

If $\sigma$ is any automorphism and $n \neq 6$, then $\sigma(K)$ is the conjugacy class of some element of order 2. Since $|\sigma(K)| = |K|$ we must have $\sigma(K) = K$. 


(c) Suppose that \( \sigma((1\,2)) = (a\,b) \) and \( \sigma((1\,3)) = (c\,d) \) with \( a \neq b \) and \( c \neq d \). Since \((1\,2)\) and \((1\,3)\) do not commute, \((a\,b)\) and \((c\,d)\) do not commute. This shows that \( \{a, b\} \cap \{c, d\} \neq \emptyset \) and \( \{a, b\} \neq \{c, d\} \). So \( \{a, b\} \cap \{c, d\} \) has exactly one element. Without loss of generality we may assume that \( a = c \). We define \( b_2 := b \) and \( b_3 := d \) to get \( \sigma((1\,2)) = (a\,b) \) and \( \sigma(a\,b) \) where \( a, b, b_2 \) are distinct. Suppose that \( \sigma((1\,4)) = (e\,f) \). We know that \( \{e, f\} \cap \{a, b_2\} \) and \( \{e, f\} \cap \{a, b_3\} \) have exactly 1 element. If \( a \not\in \{e, f\} \) then we must have \( \{e, f\} = \{b_2, b_3\} \). Since \((1\,4)\) and \((2\,3)\) commute,

\[
\sigma((2\,3)) = \sigma((1\,2)(1\,3)(1\,2)) = (a\,b_1)(a\,b_2)(a\,b_3) = (b_1\,b_2)
\]

and \( \sigma((1\,4)) = (b_2\,b_3) \) commute. Contradiction. So we have \( a \in \{e, f\} \), say \( e = a \). We write \( b_4 := f \). We have \( b_4 \neq b_2, b_3 \). Using induction and the reasoning above for \((1\,i−1)\), \((1\,i)\) and \((1\,i+1)\) we see that \( \sigma(1\,i) = (a\,b_i) \) for \( i = 1, 2, \ldots, n \). Since no pair among \((1\,2), (1\,3), \ldots, (1\,n)\) commutes, we see that \( a, b_2, b_3, \ldots, b_n \) are all distinct.

(d) Note that \((1\,i)(1\,j)(1\,i) = (i\,j)\) and \( S_n \) is generated by all transpositions. Another way: Identify \( S_i \) with the subgroup of \( S_n \) which stabilizes each of the elements \( i + 1, i + 2, \ldots, n \). \( S_2 \) is generated by \((1\,2)\). We prove by induction that \( S_n \) is generated by \((1\,2), \ldots, (1\,n)\). Assume that \( S_{n−1} \) is generated by \((1\,2), (1\,3), \ldots, (1\,n−1)\). We have seen that \( S_n \) is the disjoint union of \( S_{n−1} \) and \( S_{n−1}(1\,n)S_{n−1} \) (see Problem set 1). This proves that \( S_n \) is generated by \((1\,2), \ldots, (1\,n)\). (In fact, this procedure gives a unique representation of any permutation as the product of transpositions from \((1\,2), \ldots, (1\,n)\).)

**Exercise 3.** Prove Cauchy’s Theorem using the Sylow theorems. Cauchy’s theorem states: *If \( G \) is a finite group and \( p \) is a prime number dividing the group order \( |G| \) then \( G \) has an element of order \( p \).*

**Solution.** Let \( P \) be a \( p \)-Sylow subgroup of \(|G|\). Since \( p \) divides \(|G|\), the group \( P \) is nontrivial. Let \( g \in P \) be a nontrivial element. Then the order of \( g \) is \( p^\alpha \) where \( \alpha \geq 1 \). Then the order of \( g^\alpha \) is exactly \( p \).

**Exercise 4.** Let \( q = p^\alpha \) where \( \alpha \) is a positive integer and \( p \) is a prime number. Let \( \mathbb{F}_q \) be a field with \( q \)-elements. (We will prove later that such a field always exists and that it is unique up to isomorphism. If \( q = p \), then \( \mathbb{F}_p \) is just \( \mathbb{Z}/p\mathbb{Z} \).)

(a) Let \( \text{GL}_n(\mathbb{F}_q) \) be the set of invertible \( n \times n \) matrices with entries in \( \mathbb{F}_q \). What is the group order \(|\text{GL}_n(\mathbb{F}_q)|\)? (This is a standard problem, you may have seen it before. *Hint:* Let \( v_1, v_2, \ldots, v_n \) be the columns of a matrix in \( \text{GL}_n(\mathbb{F}_q) \). What are the possibilities for \( v_1 \)? Given \( v_1 \) what are the possibilities for \( v_2 \), and so forth.)

**Solution.** The vector \( v_1 \) should be a nonzero vector. There are \( q^n - 1 \) possibilities for this. The vector \( v_2 \) should not lie in the span of \( v_1 \). The
The number of elements of order \( n \) is

\[
(q^n - 1)(q^{n-1} - q)(q^{n-2} - q) \cdots (q^2 - q) = q^{0+1+2+\cdots+(n-1)}(-1)(q^n-1)(q^{n-1}-1)\cdots(q-1) = \]

\[
q^2(q^n-1)(q^{n-1}-1)\cdots(q-1).
\]

(b) Let \( B \leq \text{GL}_n(\mathbb{F}_q) \) be the subgroup of all upper triangular matrices with 1’s on the diagonal. Prove that \( B \) is a \( p \)-Sylow subgroup.

Solution. All the \( \binom{n}{2} \) entries above the diagonal can be chosen arbitrarily for elements of \( B \). This shows that \(|B| = q^\binom{n}{2}\). From the previous part it is clear that the largest power of \( p \) dividing \(|G|\) is \( q^2 \). This shows that \( B \) is a \( p \)-Sylow subgroup.

Exercise 5. Do [DF], §4.5, Exercise 18.

Solution. 200 = 2^3 \cdot 5^2. Now \( n_5 \) divides 2^3 = 8 so \( n_5 = 1, 2, 4, 8 \). On the other hand \( n_5 \equiv 1 \mod 5 \). We conclude that \( n_5 = 1 \) and the 5-Sylow subgroup must be normal.

Hard Exercises (optional, for extra credit)

Exercise 6. [DF], §4.5, 16.

Solution. Suppose not, i.e., suppose that \( n_p > 1, n_q > 1, n_r > 1 \). Since \( n_r \) divides \( pq \) we must have \( n_r = p, q, pq \). But \( n_r \equiv 1 \mod r \) so we conclude that \( n_r = pq \) (because \( p, q < r \)). Similarly, \( n_q \) divides \( pr \), so \( n_q = p, r, pr \). Since \( n_q \equiv 1 \mod q \) and \( p < q \), we see that \( n_q \neq p \). We conclude that \( n_q \geq r \). Finally \( n_p \) divides \( qr \) so \( n_r = q, r, qr \). So \( n_p \geq q \). The number of elements of order \( r \) is \( n_r(r-1) = pq(r-1) \). The number of elements of order \( q \) is \( n_q(q-1) = r(q-1) \). The number of elements of order \( p \) is \( n_p(p-1) = q(p-1) \). There is of course also 1 element of order 1. So the total number of elements in the group is

\[
\geq pq(r-1)+r(q-1)+q(p-1)+1 = pqr-pq+rq-r+qp+q-1 = pqr+rq-r-q+1 = pqr+r-1(q-1) > pqr.
\]

Contradiction.

Exercise 7. [DF], §4.5, 29.

Solution. There are no simple groups of order

61, 64, 67, 71, 73, 79, 81, 83, 89, 91, 97

because these are prime powers. There are no simple groups of order

62, 65, 69, 74, 77, 82, 85, 86, 87, 91, 93, 94, 95
because these are of the form $pq$ with $p, q$ distinct primes. There are no simple
groups of order 63, 68, 76, 92, 98, 99 because these are of the form $p^2q$ with $p$ and
$q$ distinct primes. There are no simple groups of order 66, 70, 78 because these
are of the form $pqr$ with $p, q, r$ distinct primes. The other orders we deal with
case by case:

72. We have $n_3 | 2^3 = 8$, so $n_3 = 1, 2, 4, 8$. We also have $n_3 \equiv 1 \bmod 3$ so
$n_3 = 4$. Let $P$ be the 3-Sylow subgroup. Consider the transitive action of $G$
on the set of 3-Sylow subgroups. If $G$ is simple then this action must be faithful. So
$G$ can be seen as a subgroup of $S_4$. But $|G| = 72 > 24 = |S_4|$. Contradiction.

75. A group of order 75 has a 5-Sylow subgroup of index 3. This implies that
there exists a normal subgroup whose index is $\geq 3$ and $\leq 6$.

80. The 2-Sylow subgroup of a group of order 80 has index 5. This gives a
permutation representation on 5 elements which has to be faithful if the group
is simple. So the group is a subgroup of $S_5$, but this contradicts the fact that 80
does not divide 120 = $|S_5|$.

84. $n_7 | 12$ so $n_7 = 1, 2, 3, 4, 6, 12$. Also $n_7 \equiv 1 \bmod 7$ which implies $n_7 = 1$
and a group of order 84 cannot be simple.

88. $n_{11} = 1, 2, 4, 8$ and $n_{11} \equiv 1 \bmod 11$ implies that $n_{11} = 1$ and a group of
order 88 cannot be simple.

90. Suppose that $n_2 > 1$, $n_3 > 1$ and $n_5 > 1$. Then $n_2 \geq 3$, $n_3 = 10$ and
$n_5 = 6$. The action of $G$ on the set of 5-Sylow subgroups allows us to view $G$ as
a subgroup of $S_6$. The 3-Sylow of $G$ is isomorphic to the 3-Sylow subgroup of $S_6$,
so it is isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Each 3-Sylow subgroup of $G$ has therefore
8 elements of order 3. Every two 3-Sylow subgroups in $S_6$ intersect trivially, so
the same is true for $G$. This shows that there are exactly $8n_3 = 80$ elements of
order 3. There are also $4n_5 = 24$ elements of order 5. So the group has at least
$80 + 24 = 104$ elements. Contradiction!

96. A group of order 96 has a 2-Sylow subgroup of index 3. But then there
must be a normal subgroup of index $\geq 3$ and $\leq 3! = 6$. So a group of order 96 is
not simple.

HARM DERKSEN, 3067EH, 763 2309
Office hours: MWF 3-4pm (changed).
http://www.math.lsa.umich.edu/~hderksen/math594.w06/index.html