Math 3560 **Fall 2011**

Solutions to the Second Prelim

Problem 1: (10 points for each theorem) Select two of the the following theorems and state each carefully: (a) Cayley's Theorem; (b) Fermat's Little Theorem; (c) Lagrange's Theorem; (d) Cauchy's Theorem.

Make sure in each case that you indicate which theorem you are stating.

Each of these theorems appears in the text book.

Problem 2: (a) (10 points) Prove that the center $Z(G)$ of a group G is a normal subgroup of G.

Solution: $Z(G)$ is the subgroup of G consisting of all elements that commute with every element of G. Let z be any element of the center, and let g be any element of G, Then, $gz = zg$. Since z is chosen arbitrarily, this shows that $gZ(G) \subseteq Z(G)g$, for every g. It also demonstrates the reverse inclusion, so that $gZ(G) = Z(G)g$. Since this holds for every $g \in G$, $Z(G)$ is normal in G.

(b) (10 points) Let H be the subgroup of S_3 generated by the transposition (12). That is, $H =< (12) >$. Prove that H is not a normal subgroup of S_3.

Solution: Denote $< (12) >$ by H. There are many ways to show that H is not normal. Most are equivalent to the following. Choose some $\sigma \in S_3$ different from ε and different from the transposition (12). In this case, almost any such choice will do. Say $\sigma = (13)$. Compute (13)(12) and (12)(13) and see that they are not equal. Since the first permutation take 1 to 2 and the second takes 1 to 3, they are clearly not equal. Now argue that this shows that the left coset $(13)H$ is not equal to the right coset $H(13)$, showing that H is not normal.

Problem 3: Consider the cycles $(123), (45), (542), (31)$.

(a) (10 points) Find an *odd* permutation $\sigma \in S_5$ such that

$$\sigma(123)(45)\sigma^{-1} = (542)(31).$$

Verify this equality.

Solution: As shown in the textbook, we may let σ equal the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 3 & 1 \end{pmatrix}.$$

Now it was shown in the textbook and in the homework solution sets that if α is a permutation and β is a cycle, say, $(b_1b_2 \ldots b_k)$, then $\alpha\beta\alpha^{-1}$ is the cycle $(\alpha(b_1)\alpha(b_2)\ldots\alpha(b_k))$. Furthermore, we have seen that conjugation in any group preserves group multiplication. Therefore, we can compute as follows:

$$\sigma(123)(45)\sigma^{-1} = \sigma(123)\sigma^{-1} \cdot \sigma(45)\sigma^{-1} = (\sigma(1)\sigma(2)\sigma(3))(\sigma(4)\sigma(5)) = (542)(31),$$

as desired. Finally, it is easy to check that, in cycle notation, $\sigma = (15)(243)$, a product of two cycles, one of which is odd and the other even. Therefore, σ is odd.

(b) (10 points) With σ as in part (a), define $\tau = (13)\sigma$. Of course, τ is even since σ is odd. Verify that

$$\tau(123)(45)\tau^{-1} = (542)(31).$$

Solution: One way to do this is compute τ directly from the definitions, and then follow the method of part (a). The reader can easily do this. Another approach is to use the equation above proved in (a), and then conjugate the right-hand side by (13). Conjugation by (13) is an isomorphism, as shown in class, so it respects multiplication; this means we can conjugate separately on the two factors on the right-hand side, and then multiply them (in order, of course). Since (542) doesn't involve the numbers 1 and 3, conjugation by (13) doesn't change it. But (13) = (31), so conjugation by (13) fixes that too. In short, conjugation by (13) fixes the entire right-hand side of the equation in part (a). Showing that we get the same right-hand side in part (b) when we conjugate the given permutation by τ.

Problem 4: You are given a finite group G and some arbitrary, fixed $g \in G$. Define the set H by $H = \{x \in G |\ xgx^{-1} = g\}$.

(a) (10 points) Prove that H is a subgroup of G.

Solution: The element e belongs to H because $ege^{-1} = ege = g$. Suppose that x and y belong to H. Then, since $xgx^{-1} = g$ and $ygy^{-1} = g$, we can compute: $x^{-1}g(x^{-1})^{-1} = x^{-1}(xgx^{-1})(x^{-1})^{-1} = ege = g$, so $x^{-1} \in H$. Further, $(xy)g(xy)^{-1} = x(ygy^{-1})x^{-1} = xgx^{-1} = g$. So, $xy \in H$. Thus, the three basic conditions for verifying that H is a subgroup are satisfied.

For the remaining parts of this problem, H will denote this subgroup and g will denote the fixed element above. You are now also given r distinct elements $y_1, y_2, \dots y_r$ in G such that

(1) $\bigcup_{i=1}^{r} y_i H = G$.

(2) $y_i H \cap y_j H = \emptyset$, for all subscripts i and j such that $i \neq j$.

(b) (10 points) Using (1), prove that for each $y \in G$, there exists an $i \in \{1, 2, \dots, r\}$ such that $ygy^{-1} = y_i g y_i^{-1}$.

Solution: By (1), any $y \in G$ must belong to some $y_i H$. Therefore, the given y equals $y_i h$, for some $h \in H$. We now compute:

$$ygy^{-1} = (y_i h)g(y_i h)^{-1} = y_i(hgh^{-1})y_i^{-1}.$$

Since $hgh^{-1} = g$, by the definition of H and h, the above chain of equalities reduces to $ygy^{-1} = y_i g y_i^{-1}$, as required.

(c) (10 points) Using (2), prove that whenever $i \neq j$, $y_i g y_i^{-1} \neq y_j g y_j^{-1}$.

Solution: Suppose the contrary of what we are supposed to verify is true: that is, suppose $y_i g y_i^{-1} = y_j g y_j^{-1}$. By conjugating both sides by y_j^{-1}, the equation becomes, $y_j^{-1} y_i g y_i^{-1} y_j = g$, which, in turn, can be written as $(y_j^{-1} y_i) g (y_j^{-1} y_i)^{-1} = g$, implying that $y_j^{-1} y_i \in H$, hence $y_i H = y_j H$. But this last is forbidden by (2) when $i \neq j$, so our original assumption that $y_i g y_i^{-1} = y_j g y_j^{-1}$ must have been false, yielding the desired result.

For your convenience, the following statements summarize what has been proved so far. You need not prove these. Part (b) shows that the conjugacy class of g, $C(g)$ satisfies

$$C(g) = \{y_1 g y_1^{-1}, y_2 g y_2^{-1}, \dots, y_r g y_r^{-1}\}.$$

Hence, the order of $C(g)$, namely $|C(g)|$ satisfies $|C(g)| \leq r$. Part (c) shows that

$$|C(g)| = r.$$

(d) (10 points) Use (a)–(c) to prove that $|C(g)|$ divides $|G|$. (Hint: Recall how Lagrange's Theorem was proved.)

Solution: By the foregoing comments, it is required to show that r divides —G—. But (1) and (2) state that the left cosets $y_i H$ partition G, just as in the proof of Lagrange's Theorem. Further, there it is also shown that each of the cosets $y_i H$ has the same number of elements as H. (This is because the rule $x \mapsto y_i x$ defines a bijection between H

and y_iH.) Therefore, as in the proof of Lagrange's Theorem, $r|H| = |G|$. In Lagrange's proof, one then draws the conclusion that $|H|$ divides $|G|$. But one could equally well conclude from the equation that r divides $|G|$, which is what we want. This concludes the proof.

A couple of comments on Problem 4. Some students mistakenly thought that the conjugacy class $C(g)$ is the same as the subgroup H. If you think about the definition of both, you will see that they are far from the same. H consist of all x that commute with g, i.e., $xgx^{-1} = g$. The conjugacy class of g consist of all the elements of the form $ygy^{-1}s$, y ranging over G.

Another, more fundamental problem occurred in a few of the exam papers. The element g in Problem 4 is given and fixed throughout the duration of the exercise. It is not something that can be modified or selected by you. It is *given*. Similarly, in 4 (b), the element $y \in G$ is given, fixed, immutable. You may not modify it in Problem 4 b). *What this means in both cases* is that the proof(s) that you devise cannot use or assume any special features of the given elements, other than that they are elements in G. Your proof(s) must be general enough to work no matter what that element happens to be.