INTRO TO GROUP THEORY - MAR. 28, 2012
PROBLEM SET 8 - GT11/12. MORE AUTOMORPHISMS/ FERMAT'S LITTLE THEOREM

1. Let X be any set, and let G be the power set $P(X)$ of X. That is, the elements of $P(X)$ consist of all subsets of X. Recall that the symmetric difference of two subsets A, B in X (denoted by $A \oplus B$) is equal to $(A \cup B) \backslash (A \cap B)$ (which is the same as $(A \backslash B) \cup (B \backslash A)$).

(a) Show that G forms a group under $\oplus$

(b) Let $X = \{1, 2\}$. Find $Aut(G)$, and describe explicitly.

2. (a) Find generators for A_4. Use this to find an upper bound for $|Aut(A_4)|$.

(b) Find generators of S_4. Use this to find $|Aut(S_4)|$, and show that

$$Aut(S_4) = Inn(S_4) \cong S_4.$$

3. Let $N \triangleleft G$. Define $\pi : G \to Aut(N)$ by $\pi_g(n) = gng^{-1}$.

(a) Show that π is a homomorphism.

(b) What is $Ker(\pi)$?

(c) Let H_4 be the 4 element subgroup of A_4. Calculate $Im(\pi)$ and $Ker(\pi)$ for (G, N) equal to (S_4, A_4), (A_4, H_4), (S_4, H_4), and (D_{2n}, R_n).

(d) Is π onto? (Hint: A_4)

4. A subgroup H in G is called characteristic if H is preserved under each element of $Aut(G)$.

(a) Show that each characteristic subgroup is normal in G. Is the converse true?

(b) Find all characteristic subgroups of $\mathbb{Z}/n$, A_4, S_4, D_8, S_3, and $\mathbb{Z}/2 \times \mathbb{Z}/2$.

(c) Show that $Z(G)$ is characteristic. If G is abelian, is every subgroup characteristic?

(d) If H is characteristic, show that each element π in $Aut(G)$ induces an automorphism of G/H by $\pi'(gH) = \pi(g)H$. Does this hold in general if H is normal?

Date: March 28, 2012.

5. A subgroup H in G is called maximal if whenever $H \subseteq H' \subseteq G$, either $H' = H$ or $H' = G$. If G is non-trivial, the Frattini subgroup $\Phi(G)$ is defined as the intersection of all maximal subgroups of G.

(a) Show that $\Phi(G)$ is a characteristic subgroup of G.

(b) If G is finite, show that $\Phi(G)$ is the set of non-generators of G; that is, if S is a generating set of G and f is in $\Phi(G)$, then $S' = S\backslash\{f\}$ is also a generating set. (This is true in general, but requires Hausdorff's Maximal Principle to show.)

(c) Calculate $\Phi(G)$ for $G = \mathbb{Z}/n, S_3, A_4, D_{2n}$, and Q.

6. Assume unique factorization for integers into powers of primes. For positive integers j and k, define the greatest common divisor $d = gcd(j,k)$ of j and k by the following conditions: (1) $d|j$ and $d|k$, and (2) for any positive integer d' that satisfies (1), $d'|d$.

Likewise, define the least common multiple $m = lcm(j,k)$ of j and k by the conditions: (1') $j|m$ and $k|m$, and (2') for any positive integer m' that satisfies (1'), $m|m'$.

(a) If j divides kl and $gcd(j,k) = 1$, then j divides l.

(b) Show that $jk = lcm(j,k)gcd(j,k)$.

(c) Prove Bezout's identity: if $gcd(j,k) = d$ then there exists x, y in $\mathbb{Z}$ such that $xj+yk = d$.

(d) Look up the Euclidean algorithm and use it to find $gcd(560, 10000)$. Then find x and y from part (c) in this case.

7. If R is a ring, the group of units R^* is the subset of all x in R such that there exists a y in R with $xy = yx = 1$.

(a) Show that $(R \times S)^* = R^* \times S^*$ as groups.

(b) Find the isomorphism class of $(\mathbb{Z}/30)^*$. Verify directly and using part (a).

8. Prove Wilson's Theorem: if p is a prime, then $(p-1)! = -1 \pmod p$. Verify for $p = 3, 5, 7, 11$.

9. Let $\phi(n)$ be the Euler totient function.

(a) Show that, if $gcd(m,n) = 1$, then $\phi(mn) = \pi(m)\phi(n)$.

(b) Calculate $\phi(p^k)$ for all primes p.

(c) Suppose $n = p_1^{i_1} \dots p_k^{i_k}$. Calculate $\phi(n)$, and use this to show that there are infinitely many primes.

(d) Find all n such that $\phi(n) = 2, 3, 4, 6$.

(e) Calculate $|Aut(\mathbb{Z}/n)|$ for $n = 10000, 24300, 36000$.

10. (a) Find 4 prime divisors of $6^p - 6$ for any prime $p \neq 2, 3$. Factor completely for $p = 2, 3, 5$.

(b) Find 3 prime divisors of $7^4 - 1$ using only Euler's Rule. Verify.

11. Describe the isomorphism classes of $Inn(G)$, $Aut(G)$, and $Out(G)$ for $G = D_{30}$ and D_{60}.