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

1. (a) Closure: Since G is the power set of X, the symmetric difference of any two subsets of X is in G. Associative: using a Venn diagram, we see that $(A \oplus B) \oplus C$ and $A \oplus (B \oplus C)$ both equal

$$(A \cup B \cup C) \backslash ((A \cap B) \cup (B \cap C) \cup (A \cap C)).$$

Identity: $e = \emptyset : A \oplus \emptyset = \emptyset \oplus A = A$. Inverse: $A^{-1} = A$ since $A \oplus A = \emptyset$.

(b) $P(X) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$. Since $A \oplus A = \emptyset$, each element has order 2, and $G \cong \mathbb{Z}/2 \times \mathbb{Z}/2$, which means $Aut(G)$ is isomorphic to S_3. That is, any permutation of the non-identity elements is an automorphism. For example, consider the automorphism

$$\pi(\emptyset) = \emptyset, \quad \pi(\{1\}) = \{1,2\}, \quad \pi(\{2\}) = \{1\}, \quad \pi(\{1,2\}) = \{2\}.$$

Then

$$\pi(\{1\} \oplus \{1,2\}) = \pi(\{2\}) = \{1\},$$

and

$$\pi(\{1\}) \oplus \pi(\{1,2\}) = \{1,2\} \oplus \{2\} = \{1\}.$$

2. (a) Since A_4 has no subgroup of order 6, A_4 is generated by (12)(34) and (123). Since automorphisms carry generating sets to generating sets, this means there are at most $3 \times 8 = 24$ automorphisms for A_4.

(b) First $Inn(S_4) \cong S_4$ since $Z(S_4) = \{e\}$.

One can show using brute force that S_4 is generated by (12) and (1234). We have six choices for where to send (1234). The centralizer of (12) has 4 elements; the centralizer of, say, (12)(34) has 8 elements as a copy of D_8. Thus two cycles are carried to two cycles. Since (12) does not commute with $(1234)^2 = (13)(24)$, there are 6-2=4 choices for (12). Thus there are at most 24 automorphisms of S_4, and every automorphism is thus inner and implemented by the Conjugation/Relabeling Rule.

If we use (12), (23), and (34), the above centralizer argument shows two cycles must go to two cycles. There are six choices for (12). Once chosen, the choice of (23) will share a single label, and the choice for (34) will not (so fixed). Thus there are four choices for (23), and at most 24 automorphisms.

3. (a) First π_g is in $Aut(N)$ since

$$\pi_g(nn') = gnn'g^{-1} = (gng^{-1})(gn'g^{-1}) = \pi_g(n)\pi_g(n').$$

Date: April 4, 2012.

The bijective property is straightforward. For all n in N,

$$\pi_g\pi_h(n) = \pi_g(hnh^{-1}) = ghnh^{-1}g^{-1} = \pi_{gh}(n).$$

So π is a homomorphism.

(b) If $\pi_g(n) = n$ for all n in N, then $gng^{-1} = n$ for all n in N and g is in $Z_G(N)$, the centralizer of N in G. Conversely, every element of this centralizer is in $Ker(\pi)$.

(c)

(1) (S_4, A_4): Ker$(\pi) = \{e\}$, so $Im(\pi) \cong Aut(A_4)$ by 2(a).
(2) (A_4, H_4): Ker$(\pi) = H_4$ since the centralizer of H_4 in A_4 is H_4. Thus Im$(\pi) \cong \mathbb{Z}/3$. Note that $Aut(H_4)$ has 6 elements as $H_4 \cong \mathbb{Z}/2 \times \mathbb{Z}/2$. The automorphisms from π fix no non-identity elements.
(3) (S_4, H_4): Ker$(\pi) = H_4$ since the centralizer of H_4 in S_4 is H_4. Thus Im$(\pi) = Aut(H_4) \cong S_3$.
(4) (D_{2n}, R_n): Ker$(\pi) = R_n$ since the centralizer of R_n is D_{2n} is R_n. Thus Im(π) has 2 elements corresponding to the identity and inverse automorphisms.

(d) No. See the (A_4, H_4) example. It is also not true for the (D_{2n}, R_n).

4. (a) If H is characteristic, then H is preserved by inner automorphisms of G. Thus normal. The converse is not true. Each subgroup of $G = \mathbb{Z}/2 \times \mathbb{Z}/2$ is normal, but only the trivial subgroup and G are characteristic

(b)

(1) $\mathbb{Z}/n$,: Since there is only one subgroup of given order in $\mathbb{Z}/n$ (and thus mapped to itself by automorphisms), all subgroups are characteristic, and there is one for each divisor of n.
(2) A_4, S_4 : the only interesting normal subgroup of A_4 is H_4, so characteristic. Similarly S_4 only has interesting normal subgroups H_4 and A_4, both of unique order, so both are characteristic.
(3) D_8: the only normal 2 element subgroup is $Z(D_8) = \{e, (13)(24)\}$, which is characteristic by part (c). There are three subgroups of order 4, all normal. Only the rotation subgroup has elements of order 4, so characteristic. An automorphism interchanges the other two (see video GT12.1), so both are not characteristic.
(4) S_3: the three element subgroup has unique order, so characteristic. Since the automorphisms permute the elements of order 2, no two element subgroup is characteristic.
(5) $\mathbb{Z}/2 \times \mathbb{Z}/2$: we can find an automorphism that carries any two element subgroup to any other two element subgroup. So no interesting characteristic subgroups.

(c) It is straightforward to show that z in $Z(G)$ implies $\pi(z)$ is in $Z(G)$. So characteristic. No, see $\mathbb{Z}/2 \times \mathbb{Z}/2$ in part (b).

(d) Since H is normal, G/H is a group. Since $\pi(H) = H$, π is defines a map π' from G/H to itself. The homomorphism and bijection properties are straightforward. No, consider $\mathbb{Z}/2 \times \mathbb{Z}/2$.

5. (a) Automorphisms carry maximal subgroups to maximal subgroups (verify), so the intersection of all maximal subgroups is preserved under automorphisms.

(b) Suppose S is a generating set, but $S\backslash\{f\}$ is not. Then $S\backslash\{f\}$ generates a subgroup H not containing f. Partially order all subgroups H' containing H but not f. Since G is finite, there exists a finite, maximal chain of inclusions of subgroups H_i not containing $\{f\}$, and $\cup H_i$ is a maximal subgroup of G that does not contain $\{f\}$, a contradiction. Thus $\Phi(G)$ is contained in the subset of non-generators.

On the other hand, if f is a non-generator and H is a maximal subgroup, then $H \cup \{f\}$ is not a generating set of G, so $H \cup \{f\} = H$. Since H is an arbitrary maximal subgroup, f is in $\Phi(G)$.

(c)

(1) $\mathbb{Z}/n$: If n is prime, then $\Phi = \{0\}$. Otherwise there is a unique subgroup for each divisor on n, and the maximal subgroups have order n/p where p is a prime divisor of n. The maximal subgroup of order n/p is the multiples of p in $\mathbb{Z}/n$. Thus the intersection of the maximal subgroups is $\Phi = \{0\}$ if each prime divisor of n occurs with degree 1, and $\Phi = \langle p_1 \dots p_k \rangle$ if some exponent > 1.
(2) S_3: $\Phi = \{e\}$. The proper characteristic subgroups are $\{e\}$ and the three element subgroup, but the two element subgroups are maximal.
(3) A_4: Since there is no subgroup of order 6, the three element subgroups are maximal and $\Phi = \{e\}$.
(4) D_{2n}: If n is prime, then $\langle c \rangle$ and $\langle r \rangle$ are maximal, and $\Phi = \{e\}$. Suppose n is not prime. Noting the $\mathbb{Z}/n$ result or the fact that a subgroup of order $|G|/p$ with p prime is maximal, $\langle r \rangle$ and $\langle c, r^{n/p} \rangle$ are maximal for each prime divisor p of n. Intersecting these shows that $\Phi \subseteq \langle r^{p_1 \cdots p_k} \rangle$. Conversely the computation of the automorphism group (GT12.1) shows that these elements are non-generators. So $\Phi = \langle r^{p_1 \cdots p_k} \rangle$.
(5) Q : the three subgroups with four elements are maximal. So $\Phi = Z(Q) = \{\pm 1\}$.

6. (a) Apply unique factorization to j, k, l, and $gcd(j, k)$.

(b) We assume that $gcd(j, k) = d$ and show that $lcm(j, k) = (j/d)(k/d)d$. Suppose j and k divide m. Then $m = sj = tk$, and $m/d = s(j/d) = t(k/d)$ with $gcd(j/d, k/d) = 1$. Now (j/d) divides $t(k/d)$, so j/d divides t, and m is a multiple of $(j/d)k$. This means jk/d satisfies (1') and (2').

(c) It suffices to consider j and k with $gcd(j, k) = 1$. Consider the homomorphism $\pi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ given by $\pi(x, y) = jx + ky$. We show that π is onto. Since $Im(\pi)$ is a subgroup of $\mathbb{Z}$, it is equal to some $n\mathbb{Z}$. Now $j\mathbb{Z}$ and $k\mathbb{Z}$ are subgroups of $Im(\pi)$, so n divides j and k, and $n = 1$.

If you used Bezout's identity to show every subgroup of $\mathbb{Z}$ is cyclic as suggested, we offer a more elementary proof of this fact. Let H be a subgroup of G. Let n be the smallest positive integer in H. If $H \neq \langle n \rangle$, then there exists an m not in H, and thus not a multiple of n. We can add or subtract multiples of n to m to obtain an integer between 1 and $n-1$ (the remainder upon division by n) that lies in H by closure under multiplication, contradicting the minimal property of n.

(d)

$$\begin{aligned} 1000 &= (1)(560) + 440 \\ 560 &= (1)(440) + 120 \\ 440 &= (3)(120) + 80 \\ 120 &= (1)(80) + 40 \\ 80 &= 2(40) + 0 \end{aligned}$$

It follows that $gcd(560, 1000) = 40$. Now it suffices to find x and y such that $14x + 25y = 1$. Experimenting shows that $x = 9$ and $y = -5$ works; that is,

$$560(9) + 1000(-5) = 5040 - 5000 = 40.$$

7. (a) If $x = (a, b)$ is a unit, then there exists $y = (c, d)$ such that

$$xy = (a, b)(c, d) = (ac, bd) = (1, 1) = e.$$

Thus $ac = 1$ and $bd = 1$, so a is in R^*, b is in S^*, and (a, b) is in $R^* \times S^*$. Conversely if a in R and b in S are units, then (a, b) is a unit in $R \times S$, or (a, b) is in $(R \times S)^*$.

(b) As a set, $(\mathbb{Z}/30)^* = \{1, 7, 11, 13, 17, 19, 23, 29\}$. We have the following inverse pairs with orders:

(1) 7, 13: 4
(2) 11: 2
(3) 17, 23 : 4
(4) 19: 2
(5) 29: 2

An abelian group with these orders is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/4$. Alternatively, using part (a),

$$\begin{aligned} (\mathbb{Z}/30)^* &\cong (\mathbb{Z}/2 \times \mathbb{Z}/3 \times \mathbb{Z}/5)^* \\ &= (\mathbb{Z}/2)^* \times (\mathbb{Z}/3)^* \times (\mathbb{Z}/5)^* \\ &\cong \{1\} \times \mathbb{Z}/2 \times \mathbb{Z}/4 \cong \mathbb{Z}/2 \times \mathbb{Z}/4 \end{aligned}$$

8. Since $(\mathbb{Z}/p)^*$ is a cyclic group of even order when $p > 2$, $p - 1$ is the unique element of order 2. That is, the remaining elements are the identity or occur in inverse pairs. Thus $(p-1)! = (p-1) = -1$.

(1) $(3-1)! + 1 = 3$.

(2) $(5-1)!+1 = 25$.
(3) $(7-1)!+1 = 721 = 7 \times 103$.

9. (a) Note that $\phi(k) = |(\mathbb{Z}/k)^*|$. If $gcd(m,n) = 1$, then by 7(a),

$$(\mathbb{Z}/mn)^* \cong (\mathbb{Z}/m)^* \times (\mathbb{Z}/n)^*,$$

and the assertion follows.

(b) Now $\mathbb{Z}/p^k$ has p^k elements. To be in $(\mathbb{Z}/p^k)^*$, k must be relatively prime to p. There are p^{k-1} multiples of p in $\mathbb{Z}/p^k$ $\quad(= \{0, p, 2p, 3p, \ldots, p^k - p\})$, so

$$\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1).$$

(c) Suppose $n = p_1^{i_1} \ldots p_k^{i_k}$. Then

$$\begin{aligned}\phi(n) &= \phi(p_1^{i_1} \ldots p_k^{i_k}) \\ &= \phi(p_1^{i_1}) \ldots \phi(p_k^{i_k}) \\ &= p_1^{i_1-1}(p_1-1) \ldots p_k^{i_k-1}(p_k-1) \\ &= n[(p_1-1)\ldots(p_k-1)]/(p_1 \ldots p_k).\end{aligned}$$

If there were finitely many primes, say $\{p_1, \ldots p_k\}$, then $n/\phi(n)$ is bounded as a function of n. Since

$$p/(p-1) = 1/(1-1/p) = 1 + 1/p + 1/p^2 + \ldots,$$

we have informally

$$\begin{aligned}(p_1 \ldots p_k)/((p_1-1)\ldots(p_k-1)) &= (1 + 1/p_1 + 1/p_1^2 + \ldots)\ldots(1 + 1/p_k + 1/p_k^2 + \ldots) \\ &= 1 + 1/2 + 1/3 + 1/4 + \ldots.\end{aligned}$$

By the finiteness assumption, each positive integer factorization occurs exactly once in the denominators. Now the series on the right-hand side is the harmonic series, which diverges, a contradiction to boundedness. Of course, one wants a rigorous proof with convergence results from real analysis.

(d) $\phi(n) = 2$: the only prime with $\phi(n) = 2$ is 3 and power of a prime is 4. We also have that $\phi(2) = 1$ and equals 1 only for $n = 2$, so multiplying an odd k by 2 preserves $\phi(k)$. So $n = 3, 4, 6$. Verify these directly using $\mathbb{Z}/n$.

$\phi(n) = 3$: $p^k - p^{k-1}$ is always even unless $p = 2$ and $k = 1$. So $\phi(n)$ is never equal to 3. Note $\phi(n)$ is never odd unless $n = 2$.

$\phi(n) = 4$: first consider prime powers. If $p = 2$, then $n = 8$. If $p = 5$, then $k = 1$. If $p = 7$ or larger, $p-1$ is greater than 4. For composites, we look for relatively prime factors of n with $\phi(n)$ equal to 1, 2 or 4. Only 10 and 12 work. Thus $n = 5, 8, 10, 12$.

$\phi(n) = 6$: first consider prime powers. No power of 2 or 5 works. For $p = 3$, $n = 9$ works, as does $n = 7$. Since $p - 1$ is greater than 6 for larger primes, no other cases. For

composites, $\phi(n) = 3$ never occurs, so we can multiply the previous cases by 2 if odd. This gives $n = 14, 18$. All together, we have $n = 7, 9, 14, 18$.

(e) $\phi(10000) = \phi(2^4 5^4) = \phi(2^4)\phi(5^4) = 8 \times 500 = 4000$
$\phi(243000) = \phi(2^3 3^5 5^3) = \phi(2^3)\phi(3^5)\phi(5^3) = 4 \times 162 \times 100 = 64800$
$\phi(36000) = \phi(2^5 3^2 5^3) = \phi(2^5)\phi(3^2)\phi(5^3) = 16 \times 6 \times 100 = 9600$.

10. (a) 2, 3, p, and 5. 6^p always ends in a 6, so $6^p - 6$ is divisible by 10. $6^2 - 6 = 30 = 2 \times 3 \times 5$. $6^3 - 6 = 210 = 2 \times 3 \times 5 \times 7$. $6^5 - 6 = 7770 = 2 \times 3 \times 5 \times 7 \times 37$.

(b) We seek integers n with $\phi(n) = 4$ and $(n, 7) = 1$. Since Euler's Rule also applies to 49, we can also use $\phi(n) = 2$. So possible $n = 3, 4, 5, 6, 8, 10, 12$. $7^4 - 1 = 2400 = 2^5 \times 3 \times 5^2$.

11. Since $Inn(D_{30}) \cong D_{30}/Z(D_{30})$, $Inn(D_{30}) \cong D_{30}$. Since $n = 15$ is odd, $Out(D_{30}) \cong (\mathbb{Z}/15)^*/\{\pm 1\}$. Now $(\mathbb{Z}/15)^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$ is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/4$ by 7(b) (since $(\mathbb{Z}/2)^* \cong \{1\}$). Since $-1 = 14$ is not a square (check), $Out(D_{30}) \cong \mathbb{Z}/4$.

Since $Inn(D_{60}) \cong D_{60}/Z(D_{60})$, $Inn(D_{60}) \cong D_{30}$. Since $n = 30$ is even, $Out(D_{60}) \cong \mathbb{Z}/2 \times [(\mathbb{Z}/30)^*/\{\pm 1\}] \cong \mathbb{Z}/2 \times \mathbb{Z}/4$ as before.

Eventually, we identify $Aut(D_{2n})$ as a semidirect product of $(\mathbb{Z}/n)^*$ and $\mathbb{Z}/n$, which verifies the order calculation of $n\phi(n)$. For now, we describe $Aut(D_{2n})$ as matrices of the form $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$, where a is in $(\mathbb{Z}/n)^*$ and b is in $\mathbb{Z}/n$.