MATH 113: ABSTRACT ALGEBRA (AUTUMN 2007)
MIDTERM # 2
SOLUTIONS

1. (10 points) Compute $5^{8,238,390,323}$ in $\mathbb{Z}_{33}$.

Solution: $33 = 3 \times 11$. Hence, $\mathbb{Z}_{33} \cong \mathbb{Z}_2 \times \mathbb{Z}_{11}$ so that $\mathbb{Z}_{33}^\times \cong \mathbb{Z}_3^\times \times \mathbb{Z}_{11}^\times$ which has $(3-1) \times (11-1) = 20$ elements. Dividing, we see that the remainder of $8,238,390,323$ upon division by 20 is 3. Hence, $5^{8,238,390,323} = 5^3$ in $\mathbb{Z}_{33}$. Of course, $5^3 = 125 = 3 \times 33 + 26$. Hence, $5^{8,238,390,323} = 26$ in $\mathbb{Z}_{33}$.

2. (15 points) Let G be a finite group and $\phi : G \to H$ a homomorphism of groups. Prove or disprove: $\#\phi[G]$ divides $\#G$.

Solution: The statement is true. Indeed, if $K := \ker \phi$ is the kernel of ϕ, then $\phi[G] \cong G/K$ which has order dividing $\#(G)$ by Lagrange's Theorem.

3. (15 points) Consider the factor group $G := (\mathbb{Z}_{24} \times \mathbb{Z}_4)/\langle(6,2)\rangle$.

a. What is the order of G? (Prove that your answer is correct.)
b. Is G cyclic? (Again, prove that your answer is correct.)

Solution: G is a quotient of a group of order $24 \times 4 = 96$ by a normal subgroup of order $\#\{(6,2),(12,0),(18,2),(0,0)\} = 4$. Hence, by Lagrange's Theorem, $\#(G) = 24$, answering part a. If G were cyclic, then as it would be isomorphic to $\mathbb{Z}_{24}$, there would be exactly one element of order 2, namely the element corresponding to 12. However, in G, the elements $(3,1) + \langle(6,2)\rangle$ and $(6,0) + \langle(6,2)\rangle$ are distinct as $(6,0) - (3,1) = (3,3) \notin \langle(6,2)\rangle$ but each has order 2. Hence, G is not cyclic.

4. (10 points) Show that if G is a nontrivial group having the property that for all subgroups $H \leq G$ either $H = G$ or H is trivial, then G is finite and has a prime number of elements.

Solution: Let $a \in G$ be any element other than the identity. Such must exist as G is nontrivial. Let $H := \langle a \rangle$ be the group generated by a. By hypothesis, as $a \in H$ so that H is nontrivial, $H = G$. That is, G is a cyclic group. If G were infinite, then $G \cong \mathbb{Z}$, but $2\mathbb{Z} < \mathbb{Z}$ is a proper nontrivial subgroup of $\mathbb{Z}$ contrary to our hypothesis on G. Thus, $G \cong \mathbb{Z}_n$ for some $n > 1$. If n were composite, say d is a proper divisor of n, then $0 < d\mathbb{Z}_n < \mathbb{Z}_n$ would be a proper nontrivial subgroup of $\mathbb{Z}_n$, again contradicting our hypothesis on G. Therefore, n is prime as claimed.

5. (10 points) Suppose that G is a group of order 203. Show that if $H < G$ is a proper subgroup, then H is cyclic.

Solution: Let $H < G$ be a proper subgroup of G. By Lagrange's Theorem, $\#H$ divides $\#G = 203 = 7 \times 29$. As H is a proper subgroup, we must has $\#H = 1$, 7,

Date: 8 November 2007.

or 29. Of course, the trivial group is cyclic and we know that any group of prime order is cyclic. Hence, H is cyclic.

6. (15 points) How many solutions are there to the equation $x^2 + 5x + 4 = 0$ in the ring $\mathbb{Z}_{30}$? [Hint: How many solutions are there in $\mathbb{Z}_2$? in $\mathbb{Z}_3$? and in $\mathbb{Z}_5$? Answering these questions correctly is worth seven points of partial credit.]

Solution: By the Chinese Remainder Theorem, $\mathbb{Z}_{30} \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$. Thus, the number of solutions to the equation $x^2 + 5x + 4 = 0$ in $\mathbb{Z}_{30}$ is the product of the number of such solutions in $\mathbb{Z}_2$, in $\mathbb{Z}_3$ and in $\mathbb{Z}_5$. Evaluating in each of these rings, we find the solutions in $\mathbb{Z}_2$ are 0 and 1, in $\mathbb{Z}_3$ we have just 2, and in $\mathbb{Z}_5$ we have 1 and 4. Hence, there are exactly four solutions in $\mathbb{Z}_{30}$, namely 11, 14, 26 and 29.

7. (10 points) Suppose that the group G acts on a set X of size n. Show that there is a normal subgroup $N \trianglelefteq G$ for which $\#(G/N)$ divides $n!$.

Solution: From the action we obtain a homomorphism $\rho : G \to S_X$ defined by $g \mapsto [x \mapsto g \cdot x]$. Let $N := \ker \rho$ be the kernel of ρ, which is necessarily a normal subgroup of G. Then, $G/N \cong \rho[G] \leq S_X$. By Lagrange's Theorem, $\#\rho[G]$ divides $\#S_X = n!$. Hence, $\#G/N$ divides $n!$.

8. (15 points) Let R be a commutative ring for which $\mathbb{Z}_2$ is a subring. Show that the function $F : R \to R$ defined by $F(x) := x^2$ is a ring homomorphism.

Solution: We check:

$F(1) = 1$	$F(1) = 1^2 = 1 \cdot 1 = 1$
$F(xy) = F(x)F(y)$	Let x and y be elements of R. Then $F(xy) = (xy)^2 = xyxy =^{\text{by commutativity}} xxyy = x^2y^2 = F(x)F(y)$.
$F(x+y) = F(x) + F(y)$	Let x and y be elements of R. Then $F(x+y) = (x+y)^2 = (x+y)(x+y) = (x+y)x + (x+y)y = x^2 + yx + xy + y^2 =^{\text{by commutativity}} x^2 + (xy + xy) + y^2 = x^2 + xy(1+1) + y^2 =^{\text{as } \mathbb{Z}_2 \text{ is a subring}} x^2 + xy \cdot 0 + y^2 = x^2 + y^2 = F(x) + F(y)$.

Hence, F is a ring endomorphism.