MATH 251: ABSTRACT ALGEBRA I
EXAM #1

Problem 1(a). Apply the Euclidean algorithm to find $c \equiv 65 \pmod{109}$.

Problem 1(b). The set of integers n is just the set of primes.

If $n = p$ is prime, then $ab \equiv 0 \pmod{p}$ if and only if $p \mid ab$ if and only if ($p \mid a$ or $p \mid b$) if and only if ($a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$). Conversely, if n is composite, and $n = ab$ for integers $1 < a, b < n$, then $ab = n \equiv 0 \pmod{n}$ but $a, b \not\equiv 0 \pmod{n}$.

Problem 2(a). False: we have

$$a \star (b \star c) = \frac{a + (b+c)/5}{5} = \frac{5a+b+c}{25} \quad \text{but} \quad (a \star b) \star c = \frac{(a+b)/5 + c}{5} = \frac{a+b+5c}{25}.$$

Problem 2(b). False: $1/2$ is in the set but $1/2 + 1/2 = 1$ is not in the set, so addition is not a binary operation on the set (it is not closed).

Problem 2(c). We have $x = r^2 s r^{-1} s^2 r^6 = r^2 s r^{-1} r = r^2 s = s r^{-2} = s r^3$.

Problem 2(d). True: $\det \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} = 1 - 2 \not\equiv 0 \pmod{3}$, so the matrix is invertible and hence belongs to $\mathrm{GL}_2(\mathbb{F}_3)$.

Problem 2(e). True: if $ax = 1$ and $ay = 1$ then $ax = ay$ and by cancellation $x = y$.

Problem 3(a). For all $x, y \in G$, we have

$$\phi(x)\phi(y) = (g^{-1}xg)(g^{-1}yg) = g^{-1}(xy)g = \phi(xy)$$

so ϕ is a homomorphism. The inverse of ϕ is the map $\psi : G \to G$ by $x \mapsto gxg^{-1}$, since $(\phi \circ \psi)(x) = g^{-1}(gxg^{-1})g = x$ and similarly $(\psi \circ \phi)(x) = g(g^{-1}xg)g^{-1} = x$.

Problem 3(b). The map ϕ is the identity map if and only if $\phi(x) = g^{-1}xg = x$ for all $x \in G$, which holds (multiplying on the left by g) if and only if $xg = gx$ for all $x \in G$, which is to say g commutes with all $x \in G$. This does not (necessarily) mean that G is abelian: that would require that *all* elements commute.

Problem 4(a). We have $\sigma = (1\ 6\ 4)(2\ 9\ 7)(3\ 10)$ and $\tau = (2\ 5\ 3\ 9\ 7\ 8)$. Thus $\sigma^2 = (1\ 4\ 6)(2\ 7\ 9)$ and

$$\sigma\tau = (1\ 6\ 4)(2\ 9\ 7)(3\ 10)(2\ 5\ 3\ 9\ 7\ 8) = (1\ 6\ 4)(2\ 5\ 10\ 3\ 7\ 8\ 9).$$

Problem 4(b). The order is the least common multiple of the lengths of the cycles: $|\sigma| = 6$ and $|\tau| = 6$.

Problem 4(c). No, there is no such element of order 8 in S_7. If there was, we could write a product of disjoint cycles with the least common multiple of their lengths being 8. But the least common multiple is a prime power if and only if that prime power actually occurs, so this must be an 8-cycle in S_7, and this is impossible since the longest cycle in S_7 is a 7-cycle.

Problem 5. S_8 is not isomorphic to any of the other groups because $\#S_8 = 8!$ whereas the other groups have order 8: isomorphic groups have the same order.

$\mathbb{Z}/8\mathbb{Z}$ is not isomorphic to any of the other groups because it is abelian and the others are nonabelian.

It remains to show that $D_8 \not\cong Q_8$. But Q_8 has 6 elements of order 4 ($\pm i, \pm j, \pm k$) but D_8 only has 2 elements of order 4 (r, r^3, all other elements have order ≤ 2). Isomorphic groups have the same number of elements of each given order, so $D_8 \not\cong Q_8$.

Date: 30 September 2011.