February 15, 2011

Math 320 — Exam I

Make sure your reasoning is clear, in most cases in English sentences, with symbols used only for abbreviation and then used correctly. (Possible total points 75.)

1. *(16 points)* Which of the following are groups? For each of those that are not groups, cite a property of groups that it doesn't have.
   (a) $(\mathbb{Z}^+, +)$
   (b) $(\mathcal{P}(X), \cap)$, where X is a nonempty set
   (c) $(GL(2,\mathbb{R}), *)$, where $A * B = AB^{-1}$
   (d) $(\mathbb{Q} - \{0\}$,multiplication$)$

2. *(10 points)* (a) Draw the subgroup lattice of $\mathbb{Z}_{50}$ (under $\oplus$). (In Section 5 we proved that, because this group is cyclic, all its subgroups are cyclic, and you may use that fact here.)
   (b) Where in your diagram do $\langle 12 \rangle$ and $\langle 13 \rangle$ lie?

3. *(14 points)* Let S be a set with an associative operation $*$.
   (a) Prove that, if elements e, f of S satisfy $e * x = x$ and $x * f = x$ for every x in S (i.e., e is a "left identity" and f is a "right identity"), then $e = f$.
   (b) Show that, under matrix multiplication, the set
   $$S = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in \mathbb{R} \right\}$$
   has infinitely many left identities but no right identity. (You do not need to show that S is closed under multiplication.)

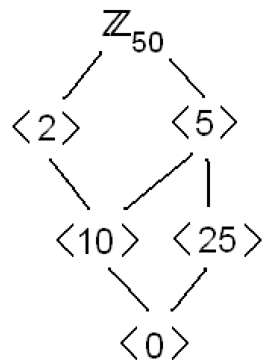
4. *(15 points)* Let x be an element of a group for which $o(x) = n$, and let r, s be factors (i.e., divisors) of n. Prove that $\langle x^r \rangle \subseteq \langle x^s \rangle$ if and only if s divides r. (Warning: $x^r = (x^s)^d$ does not imply $r = sd$.)

5. *(20 points)* Let f, g be elements of a group, neither equal to the identity e, for which $o(g) = 2$ and $o(f) = 4$ and gfg^{-1} is a power of f but not equal to f itself.
   (a) What power f^k of f must gfg^{-1} be (out of the possible powers e, f^2, f^3)? (Note this gives $gf = f^k g$. This fact is used below.)
   (b) We can rewrite any gf^n (for n a positive integer) in the form $f^m g$. Use (a) to express m in terms of n.
   (c) We can list the products of f and g as
   $$e,\ f,\ f^2,\ f^3,\ g,\ fg,\ f^2g,\ f^3g\ .$$
   Find the orders of the last three of these.
   (d) The 8 elements in (c) form a group D. The groups $\mathbb{Z}_8$ and Q_8 also have 8 elements. Does either of these groups "look just like" D? (As usual, if your answer is "no", give a reason why not, i.e., give a property that one has and the other doesn't. For example, $\mathbb{Z}_8$ and Q_8 don't "look just like" each other because $\mathbb{Z}_8$ is cyclic and Q_8 is not.)

Solutions to Exam I

1. (a) No identity: 0 isn't in the set.
(b) No inverses (except that the identity, X, is its own inverse).
(c) Not associative: $(A * B) * C = AB^{-1}C^{-1}$ but $A * (B * C) = A(BC^{-1})^{-1} = ACB^{-1}$ — and it would rarely be the case that $B^{-1}C^{-1} = CB^{-1}$.
(d) A group.

2. (a)



(b) $\langle 12 \rangle = \langle 2 \rangle$, because $\gcd(12, 50) = 2$, and $\langle 13 \rangle = \mathbb{Z}_{50}$ because $\gcd(13, 50) = 1$.

3. (a) Because e is a left identity, $e * f = f$; and because f is a right identity, $e * f = e$. Thus, $f = e * f = e$.
(b) In order to get
$$\begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$$
we must have $ca = a$ and $cb = b$, so we must have $c = 1$. But there is no condition on d; so all matrices $\begin{pmatrix} 1 & d \\ 0 & 0 \end{pmatrix}$, for any d in $\mathbb{R}$, are left identities. If there were a right identity, by (a) it would have to equal all the left identities; but they are not equal to each other; so there is no right identity.

4. Suppose s divides r, say $r = sd$ where $d \in \mathbb{Z}$; then $x^r = (x^s)^d$, so every integral power of x^r is also an integral power of x^s, i.e., $\langle x^r \rangle \subseteq \langle x^s \rangle$. Conversely, suppose $\langle x^r \rangle \subseteq \langle x^s \rangle$. Then $x^r = (x^s)^d$ for some $d \in \mathbb{Z}$. Thus $x^{r-sd} = e$, so $r - sd = nk$ for some k in $\mathbb{Z}$. Because s divides both terms on the left side of $r = nk + sd$, it also divides the right side, r, and the proof is complete.

5. (a) By one of the homework problems, the conjugate gfg^{-1} of f has the same order as f. The distinct powers of f are e, f, f^2, f^3, but e, f^2 have smaller order, and we are told $gfg^{-1} \neq f$, so we must have $gfg^{-1} = f^3$. (And hence $gf = f^3g$.)
(b) $gf^n = f^3gf^{n-1} = f^6gf^{n-2} = \cdots = f^{3n}g$, so $m = 3n$ (or we can replace $3n$ with its remainder on division by 4, the order of f).
(c) [I didn't expect you to verify that these three elements are distinct from the ones that came before and from each other; but I will put an argument here for completeness: None of the three is a power of f, because if we had, say, $f^kg = f^\ell$, then $g = f^{\ell-k}$, which is impossible because g does not commute with f. And if $f^kg = f^\ell g$, then $f^{k-\ell} = e$, so $k \equiv \ell \mod 4$. Now

to the part I <u>did</u> expect you to do:] We have

$$(fg)^2 = fgfg = ff^3gg = e\ , \qquad (f^2g)^2 = f^2gf^2g = f^2f^6gg = e$$
$$\text{and} \qquad (f^3g)^2 = f^3gf^3g = f^3f^9gg = e\ ,$$

so fg, f^2g, f^3g all have order 2.
(d) D is not abelian (because $fg \neq gf$), so it does not "look just like" $\mathbb{Z}_8$. It has 5 elements of order 2, so it does not "look just like" Q_8, which has only 1 such, $-I$.