# Selected Solutions to Homework 3, Math 4107

October 25, 2005

**Page 70.**

**1.**

a. Yes, $x \to -x$ is an automorphism.

b. Yes, $x \to x^2$ is an automorphism of the positive reals. Let's see: Clearly, it is a bijection from $\mathbb{R}^+ \to \mathbb{R}^+$. Also, $T(ab) = (ab)^2 = a^2b^2 = T(a)T(b)$. What saved us here was that multiplication of reals is commutative; otherwise, the squareing map would not be a homomorphism.

c. No, $x \to x^3$ is not an automorphism if $G$ is cyclic of order 12, because it fails to be injective (the image has order 4).

d. No, $x \to x^{-1}$ is not an automorphism on $S_3$, because it doesn't preserve structure, so is not even a homomorpism.

**5.** Let $A$ denote the set of automorphisms of $G$, and let $I$ denote the set of all inner automorphisms. Now let $\varphi \in A$, $\alpha \in I$, be arbitrary. We have then that $\alpha(g) = a^{-1}ga$ for some $a \in G$. Now, since $\varphi$ is an automorphism, so is $\varphi^{-1}$ (remember the problem on the exam?). So, for an arbitrary $g \in G$ we have

$$\begin{aligned}
(\varphi^{-1}\alpha\varphi)(g) &= (\varphi^{-1}\alpha)(\varphi(g)) \\
&= \varphi^{-1}(a^{-1}\varphi(g)a) \\
&= [\varphi^{-1}(a^{-1})][\varphi^{-1}\varphi)(g)][\varphi^{-1}(a)] \text{ (Here we used } \varphi^{-1} \text{ is automorphism.)} \\
&= [\varphi^{-1}(a)]^{-1}g\varphi^{-1}(a).
\end{aligned}$$

If let let $b = \varphi^{-1}(a)$, then we observe that this last expression is just $b^{-1}gb$, meaning that $\varphi^{-1}\alpha\varphi$ is an inner automorphism, menaing that $\varphi^{-1}I\varphi = I$, meaning that $I \lhd A$.

**12.** This was a problem I mentioned in class earlier in the semester, that was part of the qualifying exams at U. C. Berkeley (By the way, as good practice for the Putnam exam, there is a book with past qualifying exams for UCB math called something like Berkeley Problems).

First, suppose that $T(x) = x^{-1}$ for more than $3|G|/4$ of the elements $x$ of $G$, where $T$ is an automorphism. Let $a \in G$ be one of these elements where $T(a) = a^{-1}$.

Now, as we run through the values $b \in G$, at least $3|G|/4$ of them will satisfy $T(ab) = (ab)^{-1}$; and, among these values $b$, fewer than $|G|/4$ of them fail to satisfy $T(b) = b^{-1}$. So, there are more than $3|G|/4 - |G|/4$ elements $b \in G$ satisfying both

$$T(ab) = (ab)^{-1} \text{ and } T(b) = b^{-1}.$$

Thus, for each of these elements $b$ we will have

$$a^{-1}b^{-1} \ = \ T(a)T(b) \ = \ T(ab) \ = \ (ab)^{-1} \ = \ b^{-1}a^{-1};$$

or, put another way,

$$ab \ = \ ba.$$

This tells us that the centralizer of $a$, denoted by $C(a)$, contains more that $|G|/2$ values $b \in G$; and so, since $|C(a)|||G|$, we conclude that $C(a) = G$, and therefore $a \in Z$, the center of the group. Since $Z$ contains more than $3|G|/4$ elements $a$ (that satisfy $T(a) = a^{-1}$), and since $|Z|||G|$, we conclude that $|Z| = |G|$, and therefore $Z = G$, and therefore $G$ is abelian.

## Page 74

**6.** This is an immediate consequence of the fact that groups of order $p^2$ are abelian.

Another way to prove the claim is as follows: Let $H$ be the subgroup of $G$ having order $p$. Since $H$ is normal, we know that it is closed under conjugation: That is, for every $g \in G$ we have $g^{-1}Hg = H$. This allows us to decompose $H$ into orbits under conjugation by elements of $G$ in a nice way, since all the conjugates belong to $H$. That is

$$H \ = \ \bigcup_{i=1}^{k} O_i,$$

where the $O_i$ are the distinct orbits for conjugation. One of these orbits has only one element, namly the identity. The remaining orbits must have either 1 or $p$ elements. Clearly, they cannot have $p$ elements, because then the identity together with this $p$ orbit give $p+1$ elements, which is more than $|H|$. So, all the orbits have size 1, and we conclude that for every $g \in G, h \in H$, $g^{-1}hg = h$, which implies $H < Z$.

**7.** Pick an arbitrary element $g \in G$, $g \neq e$. Then, $g$ has order $p$ or $p^2$. If $g$ has order $p^2$, then $G$ is cyclic, and therefore abelian, and we are done. If $g$ has order $p$, then $(g)$ lies in $Z$ from problem 6. Thus, every element of $G$ lies in $Z$ (since $g$ was arbitrary), and we conclude $G$ is abelian.

**Page 80.**

**11.** One way (perhaps not the simplest) to solve this problem is to start by taking conjugates of (1 2): First, note that I do my cycle multiplications from right-to-left, not left-to-right like Herstein. Now, then, we have that for $j = 1, ..., n-2$,

$$(1\ 2\ \cdots\ n)^j (1\ 2)(1\ 2\ \cdots\ n)^{-j} \ = \ (j+1\ j+2),$$

and for $j = n-1$, this conjugation gives $(n\ 1)$. Note that $(1\ 2\ \cdots\ n)^{-j} = (1\ 2\ \cdots\ n)^{n-j}$.

So, we have the transpositions $(1\ 2), (2\ 3),\ (3\ 4), ...(n-1\ n), (n\ 1)$ in our subgroup. From these we can get all other transpositions: First, we can get all transpositions $(1\ j)$ by doing the following. We have

$$(1\ 3) \ = \ (2\ 3)(1\ 2)(2\ 3),$$

then

$$(1\ 4) \ = \ (3\ 4)(1\ 3)(3\ 4),$$

then

$$(1\ 5) \ = \ (4\ 5)(1\ 4)(4\ 5),$$

and so on (requires an induction proof). Once we have that we can get all other transpositions as follows: For $a \neq b$, and $a, b \neq 1$ we have

$$(a\ b) \ = \ (1\ a)(1\ b)(1\ a).$$

So, our subgroup contains all transpositions, and therefore equals $S_n$.