UNIVERSITY OF PENNSYLVANIA DEPARTMENT OF MATHEMATICS
Math 370 Algebra Fall Semester 2006
Prof. Gerstenhaber, T.A. Asher Auel

Homework #2 Solutions (due 9/19/06)
Chapter 2 Groups

2.1 Let $M = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$, then

$$M^2 = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \quad M^3 = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

So we already see that $M^3 = -I$ where I is the identity matrix, so we know $M^6 = (M^3)^2 = (-I)^2 = I$. So we know M has order dividing 6. Let's compute some more

$$M^4 = M^3M = (-I)M = -M = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \quad M^5 = M^3M^2 = -M^2 = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}.$$

So in fact, M has order 6 and the cyclic subgroup of $\mathrm{GL}_2(\mathbb{R})$ generated by M is

$$\begin{aligned} < M > &= \{I, M, M^2, M^3, M^4, M^5\} \\ &= \left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}\right\}. \end{aligned}$$

2.2 Let G be a group and $a, b \in G$ such that a has order 5. Then

$$\begin{aligned} a^3b = ba^3 \quad &\Rightarrow \quad a^3(a^3b) = a^3(ba^3) \Rightarrow (a^3a^3)b = (a^3b)a^3 \\ &\Rightarrow \quad ab = (ba^3)a^3 = ba, \end{aligned}$$

noting that we've used our hypotheses $a^6 = a^5a = a$ and $a^3b = ba^3$ in the final implication.

2.3 Which are subgroups?

a) Note that the product of real matrices is again real since it only involves multiplications and additions of real numbers (i.e. $\mathrm{GL}_m(\mathbb{R})$ is closed), and the identity matrix of $\mathrm{GL}_n(\mathbb{C})$ is the same as for $\mathrm{GL}_n(\mathbb{R})$. Thus $\mathrm{GL}_n(\mathbb{R}) \subset \mathrm{GL}_n(\mathbb{C})$ is a subgroup.
b) Note that $1 \in \mathbb{R}^\times$ is the identity, and $(-1)^2 = 1$ so $\{\pm 1\} \subset \mathbb{R}^\times$ is a subgroup.
c) The set of positive integers under addition contains neither an identity not inverses, so is not a subgroup of $\mathbb{Z}$.
d) The set $\mathbb{R}^\times_{>0}$ of positive reals contains the identity $1 \in \mathbb{R}^\times$, and is closed since the product of positive numbers is again positive. Thus $\mathbb{R}^\times_{>0} \subset \mathbb{R}^\times$ is a subgroup.
e) The set

$$R = \left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{R}^\times\right\}$$

is not even a subset of $\mathrm{GL}_2(\mathbb{R})$ since all matrices of R have zero determinant, so are not invertible, so in particular, it cannot be a subgroup of $\mathrm{GL}_2(\mathbb{R})$. Note however that under matrix multiplication the set R forms a group isomorphic to $\mathbb{R}^\times$.

3.7 Let $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$. We'll show they are conjugate in $GL_2(\mathbb{R})$ but not in $\mathrm{SL}_2(\mathbb{R})$. To this, note that $P = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$ satisfies $A = PBP^{-1}$ iff $AP = PB$ iff

$$\begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} a+b & b \\ c+d & d \end{pmatrix}.$$

Equating the entries of these two matrices, we have in particular

$$a + c = a + b \Rightarrow c = b, \quad b + d = b \Rightarrow d = 0.$$

Thus any such matrix P must be of the form $P = \begin{pmatrix} a & b \\ b & 0 \end{pmatrix}$ for $a, b \in \mathbb{R}$ such that $\det P = -b^2 \neq 0$, i.e. such that $b \neq 0$. Taking for example, $a = 0$ and $b = 1$, we have that $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ conjugates B to A in $\mathrm{GL}_2(\mathbb{R})$. As already noted, any such conjugating matrix P has $\det P = -b^2 < 0$ so can never be an element of $\mathrm{SL}_2(\mathbb{R})$.

4.16 Claim: Let $\varphi : G \to G'$ be a homomorphism of groups and $x \in G$ have finite order. Then $\varphi(x) \in G'$ has finite order and

$$\mathrm{ord}(\varphi(x)) \mid \mathrm{ord}(x).$$

Recall that for $n, m \in \mathbb{Z}$ we write $n|m$ to to mean that n divides m, i.e. that there exists $\ell \in \mathbb{Z}$ such that $m = \ell n$.

Proof. First, I'd like to clearly state an important fact.

Lemma: Let G be a group and $x \in G$ have finite order. Then if $x^m = e_G$ for some $m \in \mathbb{Z}$ then $\mathrm{ord}(x) \mid m$.

Proof. Let $r = \mathrm{ord}(x)$. Then r is the order of the finite cyclic subgroup $< x >= \{e_G, x, x^2, \ldots, x^{r-1}\}$ of G generated by x, i.e. (and this is how your should remember it) either $x = e_G$ in which case $\mathrm{ord}(x) = 1$ or

$$\boxed{\mathrm{ord}(x) = r > 1 \text{ iff } x^r = e_G \textbf{ and } x^k \neq e_G \text{ for all } 1 \leq k < r}.$$

Now suppose $x^m = e_G$ and write $m = r \cdot \ell + k$ for some $\ell \in \mathbb{Z}$ and where $0 \leq k < r$ is the remainder when dividing m by r (note that this is an important trick.) Then we have

$$e_G = x^m = x^{rl+k} = (x^r)^l x^k = e_G^l x^k = x^k,$$

which is impossible by the above boxed definition of order, unless $k = 0$. But now $k = 0$ means that $m = r\ell$, i.e. that $r = \mathrm{ord}(x) \mid m$. □

Now back to the proof. Note that for $x \in G$, by the homomorphism criterion and by induction on n, that

$$\varphi(x^n) = \varphi(x)^n,$$

so that if $\mathrm{ord}(x) = r$, in particular, $x^r = e_G$, then

$$\varphi(x)^r = \varphi(x^r) = \varphi(e_G) = e_{G'},$$

since homomorphisms always carry the identity to the identity. Thus $\varphi(x) \in G'$ has finite order and by the lemma $\mathrm{ord}(\varphi(x)) \mid r$. □