Math 301 **Sketch of Solutions to Homework 3** **03/13/04**

Part A.

1. (a) Recall that in $\mathbb{Z}_2$ we have $1+1=0$, i.e. $-1=1$. The elements of $SL(2,\mathbb{Z}_2)$ are as follows:

$$\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, \quad \begin{bmatrix}1 & 1\\ 1 & 0\end{bmatrix}, \quad \begin{bmatrix}0 & 1\\ 1 & 1\end{bmatrix}, \quad \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}, \quad \begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}, \quad \begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}.$$

   Note that determinants here are also elements of $\mathbb{Z}_2$.

   (b) The Cayley table for D_4 is given in the textbook, and the one for D_3 is similar.

2. (a) Pick any two elements $x, y \in G$. Then $x^2 = y^2 = (xy)^2 = e$, hence, $x^2y^2 = (xy)^2$ (we don't even need the fact that all squares are equal to the identity, only that $x^2y^2 = (xy)^2$ for any $x, y \in G$). In other words, $xxyy = xyxy$, so cancelling x on the left and y on the right, we get $xy = yx$. This holds for any two elements of G, thus G is abelian.

   (b) Consider the first two equations (for n and $n+1$). Since $(xy)^{n+1} = (xy)^n(xy)$, we have $x^ny^nxy = (xy)^n(xy) = (xy)^{n+1} = x^{n+1}y^{n+1} = x^nxy^ny$. In $x^ny^nxy = x^nxy^ny$, cancel x^n on the left and y on the right to get $y^nx = xy^n$. Consider the last two equations (for $n+1$ and $n+2$). We can similarly obtain $y^{n+1}x = xy^{n+1}$. Now we have $y^nx = xy^n$ and $y^{n+1}x = xy^{n+1}$ for *any* two elements $x, y \in G$ (hence, we can substitute any elements of G for x and y in our equations), so $xyy^n = xy^{n+1} = y^{n+1}x = yy^nx = yxy^n$. Therefore, $xyy^n = yxy^n$. Cancel y^n on the right to get $yx = xy$. This holds for any two elements $x, y \in G$, thus G is abelian.

Part B.

1. Consider the product $l(l(x)) * l(x) * x * l(x)$. Since $*$ is associative we will get the same result no matter how we parenthesize it (i.e. regardless of order in which we perform multiplication). Note that $l(x) * x = e$ for any $x \in G$, hence $l(l(x)) * l(x) = e$ for any $x \in G$. Therefore,

$$(l(l(x)) * l(x)) * (x * l(x)) = e * (x * l(x)) = x * l(x).$$

   On the other hand,

$$l(l(x)) * ((l(x) * x) * l(x)) = l(l(x)) * (e * l(x)) = l(l(x)) * l(x) = e.$$

   Thus, $x * l(x) = e$, so $l(x)$ the right inverse as well as the left inverse of x.

   Now consider the product $x * l(x) * x$. Again, any parenthesization will yield the same result. But $(x * l(x)) * x = e * x = x$ and $x * (l(x) * x) = x * e$, so $x * e = x$ for any $x \in G$. Hence, e is the right identity as well as the left identity.

   Thus, it follows immediately that G satisfies all group axioms, so G is a group.

   Remark: A similar proof (actually, a mirror image of ours) holds in the case where we have the right identity and the right inverse. However, if we have the left identity and the right inverse, or the right identity and the left inverse, then we can no longer conclude that G is a group.

2. (a) Clearly, associativity holds in both $SL(2,\mathbb{Z})$ and $GL(2,\mathbb{Z})$, and both sets have the identity matrix I_2 as the identity element. Thus, the only issue here is closure under taking inverses. An inverse of a matrix $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is $M^{-1} = \dfrac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$. In $SL(2,\mathbb{Z})$, $a, b, c, d \in \mathbb{Z}$ and $ad - bc = 1$, so if $M \in SL(2,\mathbb{Z})$, then $M^{-1} \in SL(2,\mathbb{Z})$. Thus, $SL(2,\mathbb{Z})$ is a group. But $GL(2,\mathbb{Z})$, we only know that $a, b, c, d \in \mathbb{Z}$ and and $ad - bc \neq 0$, so $\det(M^{-1}) = 1/\det(M)$ and hence M^{-1} has non-integer entries when $\det(M) \neq \pm 1$. Thus, $GL(2,\mathbb{Z})$ is only a monoid, but not a group.

   (b) Let $x = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, $y = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}$, then it is easy to check that $x, y \in SL(2,\mathbb{Z})$ and $x^2 = y^3 = -I$, so $x^4 = y^6 = (-I)^2 = I$. We also have $xy = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. A simple induction argument shows that $(xy)^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$ for any integer $n \geq 0$. Also, $(xy)^{-1} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$ (check!), so the same induction argument shows that $(xy)^{-n} = \begin{bmatrix} 1 & -n \\ 0 & 1 \end{bmatrix}$ for any integer $n \geq 0$. Thus, $(xy)^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$ for any $n \in \mathbb{Z}$, so $(xy)^n \neq I$ for $n \neq 0$.

Part C.

1. Here, we can only obtain $y^n x = xy^n$ for any $x, y \in G$. Now this part requires only an example, so we can look for the easiest one. For example, if we had $y^n = e$ for any $y \in G$, then our equation would reduce to the trivial identity $x = x$. So, we only need to find some nonabelian group G and some integer n such that $y^n = e$ for any $y \in G$. Then the two equations in the problem reduce to the trivial identities $ee = e$ and $xy = xy$. For example, let $G = S_3$. Recall that elements of S_3 (or D_3) have orders 1, 2 or 3, hence $y^6 = 1$ for any element $y \in S_3$ ($6 = lcm(1,2,3)$), so we can choose $n = 6$. (Similarly, we can choose $n = 4$ for D_4.) There are infinitely many other examples like this as well. In fact, we will see later that we can always choose $n = |G|$, so *any* group, abelian or nonabelian, satisfies both of our equations for $n = |G|$.

2. It is not difficult to see that the Euclidean algorithm, which finds the greatest common divisor $\gcd(a,b)$ for any two integers a and b, can be split into basic steps of two kinds for $a, b \geq 0$: $(a,b) \to (b,a)$ if $a > b$, and $(a,b) \to (a, b-a)$ if $a \leq b$. In other words, if $a \leq b$, we keep subtracting a from b until we get the remainder $r = b \mod a$, then interchange a and r, and keep going. Our algorithm will terminate when we reach the pair $(0, \gcd(a,b))$ (check that we should reach it at some point). If $a < 0$ or $b < 0$, we change a to $-a$ or b to $-b$, respectively, so that both a and b are nonnegative, and then apply our algorithm.

   Now let $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL(2,\mathbb{Z})$, then $a, b, c, d \in \mathbb{Z}$ and $\det(M) = ad - bc = 1$. Since $\gcd(a,b)$ is the least positive integer which can be written in the form $an - bm$ for some $n, m \in \mathbb{Z}$, it follows that $\gcd(a,b) = 1$. Thus, if $a, b \geq 0$, then applying our algorithm to (a,b), we should reach $(0,1)$. If both $a < 0$ and $b < 0$, let $(a,b) \to (-a,-b)$; if $a \geq 0 > b$, let $(a,b) \to (b,a)$; if $a < 0 \leq b$, let $(a,b) \to (b, b-a)$.

   Thus, the steps we use are $(a,b) \to (b,a)$, $(a,b) \to (a, b-a)$, $(a,b) \to (-a,-b)$, and $(a,b) \to$

$(b, b-a)$. Now look at the top rows of the following products:

$$Mx^{-1} = Mx^3 = M(-x) = -Mx = \begin{bmatrix} b & a \\ -c & -d \end{bmatrix},$$

$$M(xy)^{-1} = My^{-1}x^{-1} = My^5x^3 = M(-y^2)(-x) = My^2x = \begin{bmatrix} a & b-a \\ c & d-c \end{bmatrix},$$

$$Mx^2 = M(-I) = -M = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix},$$

$$My = \begin{bmatrix} b & b-a \\ d & d-c \end{bmatrix}.$$

Thus, any step in our algorithm for any pair of integers (a, b) can be accomplished by multiplication by an appropriate product of x's and y's. When our algorithm terminates, we will have $Mz = \begin{bmatrix} 0 & 1 \\ r & s \end{bmatrix}$, for some integers r, s and some product z of x's and y's. Now $Mz \in SL(2, \mathbb{Z})$, so $1 = \det(Mz) = 0s - 1r = -r$, so $r = -1$ and $Mz = \begin{bmatrix} 0 & 1 \\ -1 & s \end{bmatrix}$.

Note that $M(xy)^{-1} = My^2x = \begin{bmatrix} a & b-a \\ c & d-c \end{bmatrix}$ and $Mxy = \begin{bmatrix} a & b+a \\ c & d+c \end{bmatrix}$ for any M, thus $Mz(xy)^s = \begin{bmatrix} 0 & 1 \\ -1 & s-s \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = x$. Therefore, $M = x(xy)^{-s}z^{-1} = x(y^2x)^sz^{-1}$, so M can be written as a product of a string of matrices each of which is x, y, $x^{-1} = x^3$ and $y^{-1} = y^5$. Since M is any matrix in $SL(2, \mathbb{Z})$, it follows that $SL(2, \mathbb{Z})$ is generated by x and y.