Part A.

1. (a) Pick any two elements $x, y \in G$. Then $x^2 = y^2 = (xy)^2 = 1$, hence, $x^2y^2 = (xy)^2$ (we do not even need the fact that both sides are equal to the identity). 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 $y^nyx = y^{n+1}x = xy^{n+1} = (xy)y^n = y^n(xy)$. Therefore, $y^nyx = y^nxy$. Cancel y^n on the left to get $yx = xy$. This holds for any two elements $x, y \in G$, thus G is abelian.

   (c) Here, we can only obtain $y^nx = xy^n$ 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 $y^n = 1$ 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 $y^n = 1$ for any $y \in G$. Then the two equations in the problem reduce to the trivial identities $1 \cdot 1 = 1$ and $xy = xy$. For example, let $G = S_3$. Recall that elements of S_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 $n = 6$. There are infinitely many other examples like this as well. In fact, we will see later that we can always choose $n = o(G)$.

2. (a) Let $y_1, y_2 \in x^{-1}Hx$. Then $y_1 = x^{-1}h_1x$ and $y_2 = x^{-1}h_2x$ for some $h_1, h_2 \in H$. Then $y_1y_2 = x^{-1}h_1xx^{-1}h_2x = x^{-1}h_1h_2x$. Since $h_1h_2 \in H$, we have $y_1y_2 \in x^{-1}Hx$. Also, if $y \in x^{-1}Hx$, then $y = x^{-1}hx$ for some $h \in H$, so $y^{-1} = x^{-1}h^{-1}(x^{-1})^{-1} = x^{-1}h^{-1}x \in x^{-1}Hx$ since $h^{-1} \in H$. The above holds for any $y, y_1, y_2 \in x^{-1}Hx$, so $x^{-1}Hx$ is a subgroup of G.

   (b) $N = \bigcap_{x \in G} x^{-1}Hx$, hence, $n \in N$ if and only if $n \in x^{-1}Hx$ for any $x \in G$. Let $n \in N$, then $n \in x^{-1}Hx$ for any $x \in G$, hence, by part (a), $n^{-1} \in x^{-1}Hx$ for any $x \in G$, i.e. $n^{-1} \in N$. Let $n_1, n_2 \in N$, then $n_1, n_2 \in x^{-1}Hx$ for any $x \in G$, so, by part (a), $n_1n_2 \in x^{-1}Hx$ for any $x \in G$, i.e. $n_1n_2 \in N$. Therefore, N is a subgroup of G.

   In order to prove $y^{-1}Ny = N$ for any $y \in G$, we must show both $y^{-1}Ny \subseteq N$ and $y^{-1}Ny \supseteq N$ for any $y \in G$. We will first show that $y^{-1}Ny \subseteq N$ for any $y \in G$. Let $g \in y^{-1}Ny$, then $g = y^{-1}ny$ for some $n \in N$. But $n \in x^{-1}Hx$ for any $x \in G$, so $g = y^{-1}ny \in y^{-1}x^{-1}Hxy = (xy)^{-1}H(xy)$ for any $x \in G$. Now the key word here is "*any*". Notice that if y is fixed and x ranges over all elements of G, then xy ranges over all elements of G as well! In other words, any element $z \in G$ may be represented as $z = xy$ for some $x \in G$ (in fact, $x = zy^{-1}$). Thus, we actually have $g \in z^{-1}Hz$ for any $z \in G$, i.e. $z \in N$. This proves that $y^{-1}Ny \subseteq N$ for any $y \in G$.

   Now we need to prove $y^{-1}Ny \supseteq N$ for any $y \in G$. We could do the same proof as above, but notice how we can cut a little corner here. We proved that $y^{-1}Ny \subseteq N$ for *any* $y \in G$. Therefore, the statement is true for y^{-1} as well! (Oh, the miracle of substitution.) Thus, $(y^{-1})^{-1}Ny^{-1} \subseteq N$, i.e. $yNy^{-1} \subseteq N$ for any $y \in G$. Multiply both sides by y^{-1} on the left and y on the right to get $N \subseteq y^{-1}Ny$ for any $y \in G$. Thus, we finally get $y^{-1}Ny = N$ for any $y \in G$.

Part B.

1. Consider the product $inv(inv(x)) * inv(x) * x * inv(x)$. 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 $inv(x)*x = e$ for any $x \in G$, hence $inv(inv(x))*inv(x) = e$ for any $x \in G$. Therefore, $[inv(inv(x))*inv(x)]*[x*inv(x)] = e*[x*inv(x)] = x*inv(x)$. On the other hand, $inv(inv(x))*[[inv(x)*x]*inv(x)] = inv(inv(x))*[e*inv(x)] = inv(inv(x))*inv(x) = e$. Thus, $x * inv(x) = e$, so $inv(x)$ the right inverse as well as the left inverse of x.

   Now consider the product $x*inv(x)*x$. Again, any parenthesization will yield the same result. But $[x * inv(x)] * x = e * x = x$ and $x * [inv(x) * x] = x * e$, 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 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) Let $x = \alpha = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $y = \gamma = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$, $z = \alpha\gamma = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, then it is easy to check that x, y, z satisfy the properties listed in the problem. Since H is a subgroup, H must contain the identity matrix I as well α, γ and $\alpha\gamma$, i.e. I, x, y, z. Now $x^2 = y^2 = z^2 = -I$, so $-I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in H$, so $-x = -Ix, -y = -Iy, -z = -Iz$ are also in H. Therefore, $\{\pm I, \pm x, \pm y, \pm z\} \subseteq H$. However, it is easy to check that $\{\pm I, \pm x, \pm y, \pm z\}$ is closed under multiplication and that $(\pm I)^{-1} = \pm I$, $(\pm x)^{-1} = \mp x$, $(\pm y)^{-1} = \mp y$, $(\pm z)^{-1} = \mp z$, so $\{\pm I, \pm x, \pm y, \pm z\}$ is closed under taking inverses as well. Thus, $\{\pm I, \pm x, \pm y, \pm z\}$ is a subgroup containing α and γ. But H is the *smallest* subgroup containing α and γ, so $H \subseteq \{\pm I, \pm x, \pm y, \pm z\}$. Thus, $H = \{\pm I, \pm x, \pm y, \pm z\}$.

   (b) Similarly, let $a = \alpha = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $b = \beta = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $c = \alpha\beta = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Then $a^2 = -I$, $b^2 = c^2 = I$, $ab = c$, $ac = -b$, $cb = a$, $ba = -c$, $ca = b$, $bc = -a$. Thus, $\{\pm I, \pm a, \pm b, \pm c\} \subseteq D$. However, it is easy to check that $\{\pm I, \pm a, \pm b, \pm c\}$ is closed under multiplication and that $(\pm I)^{-1} = \pm I$, $(\pm a)^{-1} = \mp a$, $(\pm b)^{-1} = \pm b$, $(\pm c)^{-1} = \pm c$, so $\{\pm I, \pm a, \pm b, \pm c\}$ is closed under taking inverses as well. Using the same argument as in part (a), we can now conclude that $D = \{\pm I, \pm a, \pm b, \pm c\}$. In particular D is finite and has 8 elements just like D_4.

   However, more is true. Label vertices of a square clockwise from 1 to 4. Consider a map $f : D \to D_4$ defined by $f(I) = e$, $f(a) = (1234)$, $f(b) = (12)(34)$, $f(c) = (13)$, $f(-I) = (13)(24)$, $f(-a) = (1432)$, $f(-b) = (14)(23)$, $f(-c) = (24)$. Then f is a bijection such that $f(gh) = f(g)f(h)$ for any $g, h \in D$, in other words, f is an isomorphism (see the definition in the homework).

   (c) Suppose there exists an isomorphism $\phi : D \to H$. What is $\phi(I)$? We know that $\phi(g)\phi(h) = \phi(gh)$ for any $g, h \in D$, so in particular, $\phi(g)\phi(I) = \phi(gI) = \phi(g) = \phi(Ig)\phi(I)\phi(g)$ for any $g \in D$. Since ϕ is a bijection, it is onto, so any element of H may be represented as $\phi(g)$ for some $g \in D$. Thus, $h\phi(I) = h = \phi(I)h$ for any $h \in H$, so $\phi(I) = I$. Also, since ϕ is a bijection, it follows that $\phi(g) \neq I$ if $g \neq I$.

   Now let $g \in D$, then $\phi(g^2) = \phi(gg) = \phi(g)\phi(g) = \phi(g)^2$, so if $g^2 = I$, then $\phi(g)^2 = I$, and if $g^2 \neq I$, then $\phi(g)^2 \neq I$. Thus, any isomorphism $\phi : D \to H$ must preserve the number of elements whose square is the identity element. But D has 6 such elements ($\pm I$, $\pm b$ and $\pm c$) while H has only 2 ($\pm I$). Thus, there is no isomorphism from D to H, i.e. D and H are not isomorphic.

3. (a) Let $x = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $y = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$, 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 $xy = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. A simple induction argument shows that $(xy)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ for any integer $n \geq 0$. Also, $(xy)^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ (check!), so the same induction argument shows that $(xy)^{-n} = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$ for any integer $n \geq 0$. Thus, $(xy)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ for any $n \in \mathbb{Z}$, so $(xy)^n \neq I$ for $n \neq 0$.

(b) It is not hard 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 from division of b by 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 $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z})$, 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:

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

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

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

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

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 $Mz = \begin{pmatrix} 0 & 1 \\ r & s \end{pmatrix}$, 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 $Mz = \begin{pmatrix} 0 & 1 \\ -1 & s \end{pmatrix}$.

Note that $M(xy)^{-1} = My^2x = \begin{pmatrix} a & b-a \\ c & d-c \end{pmatrix}$ and $Mxy = \begin{pmatrix} a & b+a \\ c & d+c \end{pmatrix}$ for any M, thus $Mz(xy)^s = \begin{pmatrix} 0 & 1 \\ -1 & s-s \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = x$. Therefore, $M = x(xy)^{-s}z^{-1}$, 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.