Part A.

1. Recall that the elements of $SL(2,\mathbb{Z}_2)$ are as follows:

$$e=\begin{bmatrix}1&0\\0&1\end{bmatrix},\quad \rho=\begin{bmatrix}1&1\\1&0\end{bmatrix},\quad \rho^2=\begin{bmatrix}0&1\\1&1\end{bmatrix},\quad \phi=\begin{bmatrix}0&1\\1&0\end{bmatrix},\quad \phi\rho=\begin{bmatrix}1&0\\1&1\end{bmatrix},\quad \phi\rho^2=\begin{bmatrix}1&1\\0&1\end{bmatrix}.$$

   It is easy to check that $\rho^3=e$, $\phi^2=e$, and $\rho\phi=\phi\rho^2$, exactly as in D_3 (or S_3). Therefore, $SL(2,\mathbb{Z}_2)\cong D_3$.

2. Let $a,b\in H\cap K$ and consider ab^{-1}. Since $a,b\in H\cap K$, it follows that $a,b\in H$ and $a,b\in K$. Both H and K are subgroups of G, so by the 1-step subgroup test, $ab^{-1}\in H$ and $ab^{-1}\in K$, so $ab^{-1}\in H\cap K$. Therefore, by the 1-step subgroup test, $H\cap K$ is also a subgroup of G.

   Remark: Note that the same proof shows that the intersection of any collection of subgroups of G is also a subgroup of G. However, unions of subgroups are not necessarily subgroups, in fact, unions of subgroups are usually not subgroups.

3. (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 $h_1,h_2\in H$, so $y_1y_2=x^{-1}h_1xx^{-1}h_2x=x^{-1}h_1h_2x$. 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. (Alternatively, we can use the generalization of the result of Problem 2: the intersection of subgroups of the same group is also a subgroup of that group.)

   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. (a) Let $x=\alpha=\begin{bmatrix}0&1\\-1&0\end{bmatrix}$, $y=\gamma=\begin{bmatrix}0&i\\i&0\end{bmatrix}$, $z=\alpha\gamma=\begin{bmatrix}i&0\\0&-i\end{bmatrix}$, 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 $-I = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \in H$, 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 $a = \alpha = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, $b = \beta = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $c = \alpha\beta = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$. 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 $f(I) = e$, $f(a) = (1234)$, $f(b) = (12)(34)$, $f(c) = (13)$, $f(-I) = (13)(24)$, $f(-a) = (1432)$, $f(-b) = (14)(23)$, $f(-c) = (24)$ (in the cycle notation with fixed points omitted). 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, so $D \cong D_4$.

(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.

2. ($\Leftarrow$) Suppose that H and K are subgroups of G such that $HK = KH$. Let us prove that HK is also a subgroup of G.

Let $g_1, g_2 \in HK$, then $g_1 = h_1k_1$ and $g_2 = h_2k_2$ for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Then $g_1g_2 = (h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2$. But $k_1h_2 \in KH = HK$, so $k_1h_2 = h_3k_3$ for some $h_3 \in H$ and $k_3 \in K$. Hence, $g_1g_2 = h_1(h_3k_3)k_2 = (h_1h_3)(k_3k_2) \in HK$ since $h_1h_3 \in H$ and $k_3k_2 \in K$.

Similarly, let $g \in HK$, then $g = hk$ for some $h \in H$ and $k \in K$. Then $g^{-1} = (hk)^{-1} = k^{-1}h^{-1} \in KH = HK$, so $g^{-1} \in HK$.

Thus, $HK = KH$ is a subgroup of G by the 2-step subgroup test.

($\Rightarrow$) Suppose that H and K are subgroups of G such that HK is also a subgroup of G. Let us prove that $HK = KH$.

Let $h \in H$, $k \in K$, then $h^{-1} \in H$ and $k^{-1} \in K$, so $h^{-1}k^{-1} \in HK$. Since HK is a subgroup of G, we must have $kh = (h^{-1}k^{-1})^{-1} \in HK$. Note that this is true for any $h \in H$ and any $k \in K$, hence $KH \subseteq HK$.

On the other hand, if $g \in HK$, then $g^{-1} \in HK$, so $g^{-1} = hk$ for some $h \in H$ and $k \in K$, and hence $g = (g^{-1})^{-1} = (hk)^{-1} = k^{-1}h^{-1} \in KH$ since $k^{-1} \in K$ and $h^{-1} \in H$. Therefore, $g \in KH$ for any $g \in HK$, so $HK \subseteq KH$.

Thus, $HK = KH$.