Solutions to HW2

1. Since $uw = w$, the identity element must be u. The Cayley table uniquely completes as:

	u	v	w	x	y
u	u	v	w	x	y
v	v	x	y	w	u
w	w	y	v	u	x
x	x	w	u	y	v
y	y	u	x	v	w

   Note that G is cyclic: any one of the four elements other than u generates G. For example, the powers $1, v, v^2, v^3, v^4$ give u, v, x, w, y respectively.

2. G has one element of order 1, and 26 elements of order 3. Every nonidentity element $g \in G$ satisfies

$$g = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \text{ for some } a, b, c \in \mathbb{F}_3; \qquad g^3 = \begin{bmatrix} 1 & 3a & 3ac+3b \\ 0 & 1 & 3c \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

   Note that the group $C_3 \times C_3 \times C_3$ (where C_3 is cyclic of order 3) also has one element of order 1, and 26 elements of order 3. This is the smallest example of two nonisomorphic groups, having the same number of elements of each order. Strangely, I don't see this fact mentioned on pp.69–70 of the textbook, where Heisenberg groups are defined.

3. G has
   - 1 element of order 1: the identity element $I = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$
   - 1 element of order 2: $-I = \left[\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right]$
   - 8 elements of order 3: $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 2 & 1 \\ 2 & 0 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 2 & 2 \\ 1 & 0 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 0 & 1 \\ 2 & 2 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 0 & 2 \\ 1 & 2 \end{smallmatrix}\right]$. Other than I, these are all the elements of trace 2.
   - 6 elements of order 4: $\pm\left[\begin{smallmatrix} 0 & 1 \\ 2 & 0 \end{smallmatrix}\right]$, $\pm\left[\begin{smallmatrix} 1 & 1 \\ 1 & 2 \end{smallmatrix}\right]$, $\pm\left[\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right]$. These are all the elements of trace 0. Together with $\pm I$, these elements form the unique quaternionic subgroup (isomorphic to Q_8).
   - 8 elements of order 6: $\left[\begin{smallmatrix} 2 & 2 \\ 0 & 2 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 2 & 1 \\ 0 & 2 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 2 & 0 \\ 2 & 2 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 2 & 0 \\ 1 & 2 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 1 & 2 \\ 1 & 0 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 1 & 1 \\ 2 & 0 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 0 & 2 \\ 1 & 1 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 0 & 1 \\ 2 & 1 \end{smallmatrix}\right]$. These are the negatives of the elements of order 3. Other than $-I$, these are all the elements of trace 1.

4. If G is a finite nonabelian group of order n, we may list its elements as $g_1, g_2, g_3, \ldots, g_n$ where g_1 and g_2 do not commute. Then the products $g_1 g_2 g_3 \cdots g_n$ and $g_2 g_1 g_3 \ldots g_n$ are not the same.

5. (a) If $G = \{g_1, g_2, \ldots, g_n\}$, then $\pi = g_1 g_2 \cdots g_n = g_1^{-1} g_2^{-1} \cdots g_n^{-1}$ and so
$$\pi^2 = (g_1 g_2 \cdots g_n)(g_1^{-1} g_2^{-1} \cdots g_n^{-1}) = e$$
after cancelling each $g_i g_i^{-1} = e$. (I am writing e for the identity element of G.)

In preparation for (d), let's re-examine the product π by considering the set of involutions $\mathcal{I} = \{g \in G \ : \ |g| = 2\}$. In $\pi = \prod_{g \in G} g$, every element of order > 2 cancels with its inverse; and the identity does not contribute anything to the product. So $\pi = \prod_{g \in \mathcal{I}} g$ is the product of the involutions. Once again, we have $\pi^2 = \prod_{g \in \mathcal{I}} g^2 = \prod_{g \in \mathcal{I}} e = e$.

(b) In a Klein four-group, the product of all elements is the identity.

(c) For cyclic groups of even order (including order $2, 4, 6, 8$), π is the unique element of order 2.

(d) As explained in class, it is clear that $\langle \mathcal{I} \rangle = \{e\} \cup \mathcal{I}$ is a subgroup. Let $\mathcal{K}$ be the collection of all Klein four-subgroups of G. Fix an involution $\tau \in \mathcal{I}$. Every Klein four-subgroup containing τ has the form $\langle \tau, x \rangle = \{e, \tau, x, \tau x\}$ for some $x \in \mathcal{I}$ different from τ. The product of the involutions in $\langle \tau, x \rangle$ different from τ, is $x \cdot \tau x = \tau$. Now let $\mathcal{K}_\tau$ be the collection of all Klein-four subgroups containing τ; let's say the number of such subgroups is $N = |\mathcal{K}_\tau|$. Considering the product of all the involutions in the subgroups $K \in \mathcal{K}_\tau$, we get $\tau^N \in \langle \tau \rangle$. However, this is actually the product of all involutions except for τ itself. Including τ itself in this product, we get $\pi = \tau^{N+1} \in \langle \tau \rangle$.

If G has more than one involution, then $\tau = e$ as explained before. If G has a unique involution τ, then $\pi = \tau$ has order 2, also as we have explained already. But if G has at least two involutions $\tau_1 \neq \tau_2$, our argument shows that $\pi \in \langle \tau_1 \rangle \cap \langle \tau_2 \rangle = \{e\}$.

In class I showed that if the number of involutions is $k = |\mathcal{I}|$; and if $k > 0$, then the number of Klein four-groups containing each involution is $N = \frac{k-1}{2}$, so k must be odd. Also, the number of Klein four-subgroups is $|\mathcal{K}| = \frac{k(k-1)}{6}$, so $k \equiv 1$ or $3 \mod 6$. Much more can be said. In fact, $|\langle \mathcal{I} \rangle| = k+1 \in \{1, 2, 4, 8, 16, \ldots\}$ (a power of 2). Let us explain.

If we write $\langle \mathcal{I} \rangle$ as an additive group rather than multiplicative, its identity should be written as 0. In this case it is obvious (think about it) that $\langle \mathcal{I} \rangle$ is nothing other than a vector space over $\mathbb{F}_2 = \{0, 1\}$. Let $\{g_1, g_2, \ldots, g_d\}$ be a basis for $\langle \mathcal{I} \rangle$; then

$\langle \mathcal{I} \rangle = \{a_1 g_1 + a_2 g_2 + \cdots + a_d g_d : a_1, a_1, \ldots, a_d \in \mathbb{F}_2\}$ and $|\langle \mathcal{I} \rangle| = 2^d$. Of course $\langle \mathcal{I} \rangle \cong \mathbb{F}_2^d = \mathbb{F}_2 \times \mathbb{F}_2 \times \cdots \times \mathbb{F}_2$; the element $g = a_1 g_1 + a_2 g_2 + \cdots + a_d g_d$ is expressed as a vector $(a_1, a_2, \ldots, a_d)$ using coordinatewise addition with coordinates in $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Assuming $d > 1$, the sum of all the vectors in $\langle \mathcal{I} \rangle$ is $\sum_{g \in \langle \mathcal{I} \rangle} g = 0 = (0, 0, \ldots, 0)$ since in each of the d coordinates, there are 2^{d-1} zeroes and 2^{d-1} ones in the sum, giving an even number of ones, and the sum is the zero vector. This gives another proof of #5(d).

We have discussed groups like this before, very early in the semester. Recall that if G is a finite group in which every element has order $\leqslant 2$, we proved that G is abelian. Groups of this description are called *elementary abelian 2-groups* (see p.276).