There seems to be some confusion in the way I presented the subgroups of $C_2 \times C_2$, so I’d like to run through it again.

We had

$\{e_G, a\} \times \{e_H, b\}$

where $a \ast_G a = e_G$ and $b \ast_H b = e_H$. So there are four elements

$\{(e_G, e_H), (a, e_H), (e_G, b), (a, b)\}$.

Each group has two subgroups. I’ll call them

$G_1 = \{e_G\}, G_2(=G) = \{e_G, a\},$

$H_1 = \{e_H\}, H_2(=H) = \{e_H, b\}$.

This gives four subgroups of $G \times H$:

$G_1 \times H_1 = \{(e_G, e_H)\}$

$G_2 \times H_1 = \{(e_G, e_H), (a, e_H)\}$

$G_1 \times H_2 = \{(e_G, e_H), (e_G, b)\}$,

$G_2 \times H_2 = G \times H$. 

Bruce Reznick  University of Illinois at Urbana-Champaign  Math 417 – Twelfth Day – Class
My point was only that $G \times H$ has one more subgroup which is not of that form: $\{(e_G, e_H), (a, b)\}$.

Under the familiar isomorphism to $V$ which takes

$$(e_G, e_H) \mapsto I, (a, e_H) \mapsto X, (e_G, b) \mapsto Y, (a, b) \mapsto Z.$$ 

these five subgroups are $\{I\}, \{I, X\}, \{I, Y\}, \{I, X, Y, Z\}, \{I, Z\}$.

There is nothing special about $Z$! It is just the image of $(a, b)$ under the isomorphism. Remember that $X, Y, Z$ are somehow equivalent to each other, and

$$(e_G, e_H) \mapsto I, (a, e_H) \mapsto Y, (e_G, b) \mapsto Z, (a, b) \mapsto X.$$ 

is also an isomorphism.
This leads to another important piece of terminology. Suppose $G$ is a group. An isomorphism of $G$ to itself is called an \textit{automorphism}. To distinguish these, I’ll use the letter $\Psi$, rather than $\Phi$. (Personal choice, not in the book. Automorphisms aren’t in the book this early, except as a homework problem. )

Every group has an automorphism! Define $\Psi_0$ on $G$ by: $\Psi_0(g) = g$ for all $g$. Then $\Psi_0$ is a bijection and $\Psi_0(g) \ast \Psi_0(h) = \Psi_0(g \ast h)$.

Remember that automorphisms are isomorphisms, so we can specialize our early results, which I’ll quickly review;

$$\Psi(e) = e, \quad \Psi(g^{-1}) = (\Psi(g))^{-1}.$$  

Suppose now that $G = C_n$, a cyclic group. It turns out that the automorphisms of $C_n$ depend very much on the properties of $n$ as an integer.
THEOREM If $G = C_n$, then $G$ has $\phi(n)$ different automorphisms, given by

$$x \in G \implies \Psi(x) = x^k, \quad \gcd(k, n) = 1.$$  

PROOF Suppose $\Psi$ is an automorphism of $G = \langle a \rangle$. Since $\Psi(a) \in G$, there is a $k$ so that $\Psi(a) = a^k$. It follows that

$$\Psi(a^2) = \Psi(a)\Psi(a) = a^k a^k = a^{2k},$$

$$\Psi(a^3) = \Psi(a)\Psi(a) = a^{2k} a^k = a^{3k}$$

and so on, so $\Psi(a^i) = a^{ik}$. It is now easy to check that $\Psi(a^i)\Psi(a^j) = \Psi(a^{i+j})$.

The only condition we need to look at is that $\Psi$ be a bijection, in other words,

$$\{e, a^k, a^{2k}, \ldots, a^{(n-1)k}\} = \{e, a, a^2, \ldots, a^{n-1}\}$$

This will happen if and only if the order of $a^k$ in $G$ is equal to $n$. But we have seen that this order is $\frac{n}{\gcd(n, k)}$, so we get an automorphism if and only if $\gcd(n, k) = 1$.  

\[\Box\]
If you didn’t want to use the that theorem, you could say this: if $\Psi$ is a bijection, there must be an $r$ so that $a^{rk} = a$; that is, $rk \equiv 1 \mod n$, and this implies $gcd(k, n) = 1$. And, if $a^{rk} = a$, $(\Psi(a^r) = a)$, then $a^{(ir)k} = a^i$, or $\Psi(a^{ir}) = a^i$.

What are the automorphisms of $V = \{I, X, Y, Z\}$? If $\Psi$ is an automorphism, then $\Psi(I) = I$, and it is easy to check that if

$$\{\Psi(X), \Psi(Y), \Psi(Z)\} = \{X, Y, Z\},$$

then $\Psi$ will be an automorphism, so there are $3!$ different automorphisms.

It is not hard to show that for any group $G$, the set of automorphisms forms a group under composition. It is often called $Aut(G)$. I will only talk about this if there is class interest!
The last topic today is the subgroups of $C_2 \times C_4$. To simplify notation, write $C_2 = \{e, a\}$ and $C_4 = \{e, b, b^2, b^3\}$, where $a^2 = e$ and $b^4 = e$. (The identities are technically different.) If you prefer, you can make $a = [1]_2$ and $b = [1]_4$ as an arithmetic version of this.

Then the elements of the group are

$$\{(e, e), (e, b), (e, b^2), (e, b^3), (a, e), (a, b), (a, b^2), (a, b^3)\}$$

What is the order of $(a^j, b^k)$? It’s the smallest $r$ so that $(a^j, b^k)^r = (e, e)$; that is,

$$a^{jr} = e, b^{kr} = e \iff jr \equiv 0 \mod 2, \quad kr \equiv 0 \mod 4.$$ 

It isn’t terrible hard to see that $(e, e)$ has order 1, $(e, b^2)$, $(a, e)$, $(a, b^2)$ all have order 2, and the other elements: $(e, b)$, $(e, b^3)$, $(a, b)$, $(a, b^3)$ all have order 4. It follows that the subgroups of shape $\langle x \rangle$ are:
\( \{(e, e), (e, e), (e, b^2)\}, \{(e, e), (a, e)\}, \{e, e\}, (a, b^2)\} \)

\( \{(e, e), (e, b), (e, b^2), (e, b^3)\}, \{(e, e), (a, b), (e, b^2), (a, b^3)\} \)

A subgroup of \( C_2 \times C_4 \) will have order dividing \(|C_2 \times C_4| = 8\), and so be 1,2,4,8. The only subgroup of order 1 is \((e, e)\), and the only subgroup of order 8 is the whole group.

Furthermore, if \( H \) is a subgroup of order 2, then it has to look like \( \{(e, e), x\} \), where \( x \) has order 2, so it’s in the list above. In the remaining case, \( H \) has order 4. If it has an element of order 4, then that’s \( H \), and it’s in the list.

What’s left? There are four elements of order less than four, and this is the only possibility. You’ve already proved that

\( \{(e, e), (e, b^2), (a, e), (a, b^2)\} \)

is a subgroup!
WORKSHEET PROBLEM
For a change, this one is a bit more theoretical. It’s not hard if you follow the definitions carefully.

1. Prove that in any group, for any $g, h \in G$,

$$(gh)^{-1} = h^{-1}g^{-1}$$

Hint: Consider the product $(gh)(h^{-1}g^{-1})$ and apply associativity.

2. Suppose $G$ is an abelian group and define $\Psi(g) = g^{-1}$. Prove that $\Psi$ is an automorphism of $G$.

That is: prove that $\Psi$ is a bijection and $\Psi(gh) = \Psi(g)\Psi(h)$ for all $g, h \in G$. 
1. By associativity,
\[(gh)(h^{-1}g^{-1}) = g(hh^{-1})g^{-1} = geg^{-1} = gg^{-1} = e.\]

2. If \(g \in G\), then \(g = (g^{-1})^{-1}\), hence \(\Psi(g^{-1}) = g\), so \(\Psi\) is onto or surjective. If \(\Psi(g) = \Psi(h)\), then \(g^{-1} = h^{-1}\), so \(g = (g^{-1})^{-1} = (h^{-1})^{-1} = h\), so \(\Psi\) is one-to-one or injective. Thus \(\Psi\) is a bijection.

Finally, since \(G\) is an abelian group,
\[\Psi(gh) = h^{-1}g^{-1} = g^{-1}h^{-1} = \Psi(g)\Psi(h).\]

Bonus. Suppose we don’t know anything about \(G\), but \(\Psi\) is an automorphism, then
\[\Psi(gh) = \Psi(g)\Psi(h) \implies h^{-1}g^{-1} = g^{-1}h^{-1}\]
\[\implies (h^{-1}g^{-1})^{-1} = (g^{-1}h^{-1})^{-1} \implies gh = hg.\]
So, if \(\Psi\) is an automorphism, then \(G\) is abelian.