Suppose that the order of an element a in G is n and n is finite. Then we know that $a^n = e$, where e is the identity element in G. Multiply both sides (left or right) by the inverse of a^n which is $(a^{-1})^n$. Thus

$$a^n = e \Leftrightarrow (a^{-1})^n \cdot a^n = (a^{-1})^n \cdot e \Leftrightarrow e = (a^{-1})^n$$

Clearly, a^{-1} has the same order as element a and is also the inverse of a. Now, if the order of a happens to be infinite, then a^{-1} must also be of infinite order otherwise it would contradict what was just proven above.

3.14 If H and K are subgroups of G, show that $H \cap K$ is a subgroup of G.

Suppose that H and K are both subgroups of G. Then by definition, both are non-empty and both contain the identity, e. Since, $e \in H$ and $e \in K$, then $e \in H \cap K$, which makes $H \cap K$ non-empty. Now, to prove that $H \cap K$ is a subgroup, by theorem 3.1, we show that when $a, b \in H \cap K$ then $ab^{-1} \in H \cap K$. So, let $a, b \in H \cap K$, which means $a, b \in H$ and $a, b \in K$. But we already know that H and K are subgroups, so we know that $ab^{-1} \in H$ and $ab^{-1} \in K$. Hence we have $ab^{-1} \in H \cap K$.

3.19 Prove theorem 3.6.

If $C(a) = G$, then we are done. So let us assume that $C(a) \neq G$. Showing that $e \in C(a)$ is trivial, since $e \cdot a = a \cdot e = a$. Next, suppose that $b, c \in C(a)$. Then, $(bc)a = b(ca) = b(ac) = (ba)c = (ab)c = a(bc)$, which shows that $bc \in C(a)$. Now, we take some $b \in C(a)$ and show that b^{-1} is also in $C(a)$. So,

$$\begin{aligned} b \cdot a &= a \cdot b \\ a &= b^{-1} \cdot a \cdot b && \text{multiply on left by inverse of b} \\ a \cdot b^{-1} &= b^{-1} \cdot a && \text{multiply on right by inverse of b} \end{aligned}$$

Thus $b^{-1} \in C(a)$ whenever b is.

3.27 Suppose a group contains elements a and b such that $|a| = 4, |b| = 2$, and $a^3 b = ba$. Find $|ab|$.

$$e = ee = a^4 b^2 = aa^3 bb = a(a^3 b)b = a(ba)b = (ab)(ab) = (ab)^2$$

First thing to note is that $|a| \neq |b|$, which means by Exercise 3.4 that one is not an inverse to the other. We get the second inequality from the order of a and b, then we use associativity, followed by the given equality, followed by more associativity, to conclude that $|ab| = 2$.

3.28 Consider the elements $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$ from $SL(2, \mathbb{R})$. Find $|A|, |B|$, and $|AB|$. Does your answer surprise you?

The last equality comes from row 1:column 1 and row 2:column 2 both using (1), while row 1:column 2 and row 2:column 1 use (2).
Using the just proven formula, we can see that the order of
$\begin{bmatrix} \cos 60^\circ & -\sin 60^\circ \\ \sin 60^\circ & \cos 60^\circ \end{bmatrix}$ is going to be 6, since $\cos 360^\circ = 1$ and $\pm \sin 360^\circ = 0$. The order of
$\begin{bmatrix} \cos(\sqrt{2})^\circ & -\sin(\sqrt{2})^\circ \\ \sin(\sqrt{2})^\circ & \cos(\sqrt{2})^\circ \end{bmatrix}$ is infinite because in order to get the identity matrix, θ must equal $0, 360^\circ, 720^\circ, \ldots$, this is only possible if n were an irrational number, but since n is a positive integer then the identity can never be reached.

3.34 $U(15)$ has six cyclic subgroups. List them.

The six cyclic subgroups of $U(15)$ are as follows:
$\langle 2 \rangle = \{1, 2, 4, 8\}$
$\langle 4 \rangle = \{1, 4\}$
$\langle 8 \rangle = \{1, 8\}$
$\langle 7 \rangle = \langle 13 \rangle = \{1, 7, 4, 13\}$
$\langle 11 \rangle = \{1, 11\}$
$\langle 14 \rangle = \{1, 14\}$

3.44 Let $H = \{A \in GL(2, \mathbb{R}) \mid \det A$ is a power of $2\}$. Show that H is a subgroup of $GL(2, \mathbb{R})$.

First, we check if the identity is in H. Well, the determinant of the identity matrix is 1 which is equal to 2^0, so $e \in H$ and H is nonempty. Next, we let $A, B \in H$ and show that $AB \in H$ as well. Well, the determinant of A is 2^k and the determinant of B is 2^n for some $k, n \in \mathbb{Z}$, so by Example 2.9 on page 45, $\det(AB) = \det(A) \cdot \det(B) = 2^k \cdot 2^n = 2^{k+n}$. Since $k + n$ must be an integer, then the determinant of AB must be a power of 2 and we get that $AB \in H$. Lastly, we need to show that $A^{-1} \in H$ whenever $A \in H$ to satisfy Theorem 3.2. Clearly, for any $A \in GL(2, \mathbb{R})$ there exists an inverse, $A^{-1} \in GL(2, \mathbb{R})$ otherwise this would contradict $GL(2, \mathbb{R})$ being a group. So let $A \in H$ as well, then we know that $\det(AA^{-1}) = \det(A) \cdot \det(A^{-1}) = 2^k \cdot \det(A^{-1}) = e$, for some $k \in \mathbb{Z}$. Since this is true in $GL(2, \mathbb{R})$, then $\det(A^{-1})$ must be 2^{-k}, which is a power of 2 and hence $A^{-1} \in H$ as well.

3.45 Let H be a subgroup of $\mathbb{R}$ under addition. Let $K = \{2^a \mid a \in H\}$. Prove that K is a subgroup of $\mathbb{R}^*$ under multiplication.

Firstly $0 \in H$ because H is a subgroup of $\mathbb{R}$ with addition. Here we know that $2^0 = 1 \in K$. So K is nonempty. Now if $a, b \in K$, then $a = 2^k$ and $b = 2^n$ for some $k, n \in H$. Furthermore $ab = 2^k 2^n = 2^{k+n}$ and with $k, n \in H$ we know that $k + n \in H$ so $ab \in K$. Now if $c \in K$, then $\exists z \in H$ such that $c = 2^z$. With $z \in H$, then $-z \in H$ because H is a group under addition. Thus $2^{-z} \in K$. Thus

We can say that $\langle a^3\rangle \cap \langle a^2\rangle = \langle a^{21}\rangle \cap \langle a^{10}\rangle$, by Theorem 4.2, since $\langle a^{21}\rangle = \langle a^{\gcd(24,21)}\rangle = \langle a^3\rangle$ and $\langle a^{21}\rangle = \langle a^{\gcd(24,10)}\rangle = \langle a^2\rangle$. So looking at some of the elements of $\langle a^3\rangle = \{\ldots, a^3, a^6, a^9, \ldots\}$ and looking at some of the elements of $\langle a^2\rangle = \{\ldots, a^2, a^4, a^6, \ldots\}$, we can see that $a^6 \in \langle a^3\rangle \cap \langle a^2\rangle$. Now, we can deduce that a^6 is actually a generator of $\langle a^3\rangle \cap \langle a^2\rangle$ since all elements of $\langle a^3\rangle$ are some multiple of 3 while all elements of $\langle a^2\rangle$ are multiples of 2 thereby making the all the elements in common multiples of 6 and $\langle a^6\rangle = \langle a^{21}\rangle \cap \langle a^{10}\rangle$. Furthermore, 6 happens to be the lowest common multiple of 2 and 3, which leads us to a more general form, by the same argument as above, of finding the generator of some subgroup when $|a| = d$, $\langle a^m\rangle \cap \langle a^n\rangle = \langle a^{\gcd(m,d)}\rangle \cap \langle a^{\gcd(n,d)}\rangle$, by theorem 4.2, then $\langle a^s\rangle \cap \langle a^r\rangle = \langle a^t\rangle$, where $s = \gcd(m, d)$, $r = \gcd(n, d)$, and $t = \operatorname{lcm}(s, r)$.

T1 Any common multiple of 2 integers is divisible by the lcm of those 2 numbers.
Proof: Let $m, n \in \mathbb{Z}$. Given any $c \in \mathbb{Z}$, c is a common multiple of m and n, we need to show $\operatorname{lcm}(m, n) | c$. So, let $d = \gcd(m, n)$. Then $m = dm'$ and $n = dn'$. Given c, a common multiple of m and n, then $c = m \cdot k = dm' \cdot k$ and $c = n \cdot l = dn' \cdot l$. Immediately we see that $d | c$. We want to show that $n' | k$. If $n' = 1$ then the result follows. If not, then we know that the $\gcd(m', n') = 1$ (from our first hw. assignment), thus n' is the product of primes, none of which divide m'. But $n' | (c/d) = m'k$ and n' does not divide m', which implies that $n' | k$. Thus $d \cdot m' \cdot n' | c$. With that fact, we see that $d \cdot m' \cdot n' \leq$ all common multiples of m and n. Moreover, $dm'n' = m \cdot n' = n \cdot m'$, so $dm'n'$ is a common multiple, so it is the $\operatorname{lcm}(m, n)$.

4.15 Let G be an Abelian group and let $H = \{g \in G \mid |g| \text{ divides } 12\}$. Prove that H is a subgroup of G. Is there anything special about 12 here? Would your proof be valid if 12 were replaced by some other positive integer? State the general result.

Let's prove the general result first. Let $H = \{g \in G : |g| \text{ divides } m\}$ where $m \in \mathbb{N}$. First we note that $e \in G$ and $|e| = 1$ and 1 divides any m, so that $e \in H$ and H is nonempty. Next, to show that $a \in H$ has an inverse in H, we know that $|a| = |a^{-1}|$ by Exercise 3.4, which means that $|a^{-1}|$ divides m as well. Now if we show $ab \in H$ then we can conclude that H is a subgroup of G by theorem 3.2 so let $a, b \in H$ and $n = |a|$ and $k = |b|$. Then we know that the $\operatorname{lcm}(n, k) | m$ by T1. It follows then that since G is Abelian that $(ab)^t = a^t b^t = e$, where $t = \operatorname{lcm}(n, k)$. Furthermore, $|ab| = r \leq t$ but r must divide t and $t|m$ then $r|t$ by transitivity, concluding that ab must be in H. Now going back and answering the first questions. H must subgroup of G when $m = 12$ since we proved it for all positive integers. There is nothing special about 12 since 12 is only one integer from the entire set of natural numbers. Yes the proof would be valid if we replaced any positive integer.

4.18 If a cyclic group has an element of infinite order, how many elements of finite order does it have?

$$\begin{aligned}
5^{15} \bmod 7 &= (5^7 \bmod 7)\cdot(5^7 \bmod 7)\cdot(5 \bmod 7)\\
&= (5 \bmod 7)\cdot(5 \bmod 7)\cdot(5 \bmod 7)\\
&= (5^3 \bmod 7)\\
&= 126 \bmod 7\\
&= 6
\end{aligned}$$

where the second equality (above and below) is from Fermat's Little Theorem.

$$\begin{aligned}
7^{13} \bmod 11 &= (7^{11} \bmod 11)\cdot(7^2 \bmod 11)\\
&= (7 \bmod 11)\cdot(49 \bmod 11)\\
&= (7\cdot 5 \bmod 11)\\
&= 35 \bmod 11\\
&= 2
\end{aligned}$$

7.22 Suppose that G is a group with more than one element and G has no proper, nontrivial subgroups. Prove that $|G|$ is prime. (Do not assume at the outset that G is finite.)

Suppose that G is a group with more than one element and G has no proper, nontrivial subgroups. Now, let g be any nonidentity element in G. Then $\langle g\rangle$ is a subgroup of G. But since G has no proper subgroups, it must be that $\langle g\rangle = G$, which means that G is cyclic. Hence it must follow that G can only be finite, otherwise $\langle g^2\rangle$ is a proper subgroup and a contradiction. So by theorem 4.3, we know if $k \mid n = |G|$, then there is a subgroup of order k, yet this means that k cannot be anything other than 1 or n (otherwise we would have a proper subgroup), so it must be that the order of G is prime.

7.26 Let $|G| = 8$. Show that G must have an element of order 2.

Let g be any nonidentity element in G. Then by Corollary 2, $|g|$ divides $|G|$. Since $|G| = 8$, $|g|$ must be 2, 4, or 8. The case where $|g| = 2$ is clear and we're done. Otherwise, $|g| = 4$ or $|g| = 8$, then $|g^2| = 2$ or $|g^4| = 2$, respectively and again we're done.

7.28 Show that $\mathbb{Q}$, the group of rational numbers under addition, has no proper subgroup of finite index.

For the sake of contradiction, let us suppose that H is a proper subgroup of $\mathbb{Q}$ under addition with a finite index. Then there exist an element, $z \in \mathbb{Q}\backslash H$, which also means that $\frac{z}{2} \notin H$. Notice now for every $n \in \mathbb{N}$, either $(\frac{z}{2}+\frac{z}{n}) \notin H$ or $(\frac{z}{2}-\frac{z}{n}) \notin H$, otherwise $[(\frac{z}{2}+\frac{z}{n})+(\frac{z}{2}-\frac{z}{n})] \in H$ and that implies that $z \in H$.

Thus there exists a $k \in \mathbb{N}$ with $(\frac{z}{2} \pm \frac{z}{n}) \notin H$ such that $\frac{z}{2} + H = \frac{z}{2} \pm \frac{z}{k} + H$, which we know must be true since H has a finite index. Now for the positive case,

$$\left(\frac{z}{2} + \frac{z}{k}\right) - \frac{z}{2} = \frac{z}{k} \in H \Rightarrow \left\langle \frac{z}{k} \right\rangle \subseteq H \Rightarrow z \in H$$

or for the negative case,

$$\frac{z}{2} - \left(\frac{z}{2} - \frac{z}{k}\right) = \frac{z}{k} \in H \Rightarrow \left\langle \frac{z}{k} \right\rangle \subseteq H \Rightarrow z \in H$$

Contradiction since there does not exist a $k \in \mathbb{N}$ such that $\frac{z}{2} + H = \frac{z}{2} \pm \frac{z}{k} + H$. Thus there is no proper subgroups of $\mathbb{Q}$ under addition with finite index.

7.33 Let G be a group of order p^n where p is prime. Prove that the center of G cannot have order p^{n-1}.

For the sake of contradiction, let $|Z(G)| = p^{n-1}$. Then, there are p elements in G that are not in $Z(G)$. So, take one of those elements, let's say $g \in G \setminus Z(G)$, and look at the centralizer of g. Since g always commutes with itself, it follows that $g \in C(g)$. Furthermore, g commutes with all the elements from the center, so $Z(G) \subseteq C(g)$. Now, we know by theorem 3.6 that $C(g) \leq G$ and from Lagrange's theorem that $|C(g)|$ must divide $|G|$. But from what we've said, $|C(g)|$ must be strictly larger than $|Z(G)|$. Thus it can only be that $|C(g)|$ is p^n. This means that $G = C(g)$, which implies that g commutes with every element of G and must be in the center. Contradiction since g was chosen such that $g \notin Z(G)$.

7.47 Determine all finite subgroups of $\mathbb{C}^*$, the group of nonzero complex numbers under multiplication.

The n^{th} roots of unity are those complex numbers, x, such that $x^n = 1$. In fact, by the fundamental theorem of algebra, there are n such roots for any $n \in \mathbb{N}$. Furthermore, these roots form a cyclic subgroup in $\mathbb{C}^*$ under multiplication and we can find them by $e^{(2\pi ik)/n}$ for any $n \in \mathbb{N}$, $k = 0, 1, \ldots, n-1$. Thus, $\{e^{(2\pi ik)/n} \mid k = 0, 1, \ldots, n-1\}$ is a cyclic subgroup of order n in $\mathbb{C}^*$ under multiplication for any $n \in \mathbb{N}$ and, moreover, this finds all the finite subgroups of $\mathbb{C}^*$.

8.2 Show that $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ has seven subgroups of order 2.

$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 = \{(0,0,0), (0,1,0), (0,0,1), (0,1,1), (1,0,0), (1,0,1), (1,1,0), (1,1,1)\}$. So, (0, 0, 0) is the identity and with any nonidentity element, there being 7 in total, forms a subgroup. Note that this is possible since any nonidentity element has an order of 2 and thus must be its own inverse.

8.10 How many elements of order 9 does $\mathbb{Z}_3 \oplus \mathbb{Z}_9$ have?