1. For this problem, one can use either the elementary divisor decomposition (p. 163) or the invariant factor decomposition. The former turns out to be easier for this problem, but we’ll do it both ways. We will write cyclic groups additively.

Solution A: (using the elementary divisor decomposition). By theorem 5 (p. 163), $G$ must be isomorphic to $\mathbb{Z}_{p^2} \times \mathbb{Z}_q$ or to $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_q$. But $\mathbb{Z}_{p^2} \times \mathbb{Z}_q$ is cyclic (prop. 6(1), page 165), so $G$ must be $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_q$. Recall that the order of an element $(x,y,z)$ is the least common multiple of $|x|$, $|y|$, and $|z|$.

Now all nonzero elements of $\mathbb{Z}_p$ have order $p$, and similarly for $\mathbb{Z}_q$. Thus

- If $x$ or $y$ (or both) are nonzero and $z \neq 0$, then $(x,y,z)$ has order $pq$. There are $(p^2 - 1)(q - 1) = p^2q - p^2 - q + 1$ such elements.
- If $x = y = 0$ and $z \neq 0$, then $(x,y,z)$ has order $q$. There are $q - 1$ such elements.
- If $x$ or $y$ (or both) are not zero and if $z = 0$, then $(x,y,z)$ has order $p$. There are $p^2 - 1$ such elements.

That leaves $(x,y,z) = (0,0,0)$, which has order 1.

In particular, the greatest order of any element is $pq$.

Solution B: In the invariant factor decomposition, $n_1$ must be divisible by each of the prime factors of $|G|$ (see page 161). Thus $n_1$ is divisible by $p$ and by $q$, and therefore by $pq$. Since $|G|$ is divisible by $n_1$, this means $n_1 = p^2q$ or $n_1 = pq$. But $n_1 < |G|$ since we are told that $G$ is not cyclic. Thus $n_1 = pq$, and therefore $n_2 = p$. So $G \cong \mathbb{Z}_{pq} \times \mathbb{Z}_p$.

Let us write $\mathbb{Z}_{pq}$ and $\mathbb{Z}_p$ additively. Now the order of $(a,b) \in G$ is

$$\text{lcm}(|a|,|b|).$$

The order of an element $\bar{a} \in \mathbb{Z}_{pq}$ is $pq/(a,pq)$. We may take $0 \leq a < pq$. If $a$ is a multiple of $p$ but not $q$, then $(a,pq) = p$, so $|\bar{a}| = q$. There are $q - 1$ such $a$’s, namely $p, 2p, 3p, \ldots, (q-1)p$. Likewise if $a$ is a multiple of $q$ but not $p$, then $|\bar{a}| = p$. There are $p - 1$ such $a$’s, namely $q, 2q, \ldots, (p-1)q$. If $a$ is a multiple of $p$ and $q$, then $a = 0$ and $|\bar{a}| = 1$. The other $pq - (p - 1) - (q - 1) - 1 = pq - p - q + 1 = (p-1)(q-1)$ elements have order $pq$.

Now $\mathbb{Z}_p$ has one element (the identity) of order 1 and $p - 1$ elements of order $p$.

Thus we have the following table:

<table>
<thead>
<tr>
<th></th>
<th>1 : 1</th>
<th>$p : q - 1$</th>
<th>$q : p - 1$</th>
<th>$pq : (p - 1)(q - 1)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 : 1</td>
<td>1 : 1</td>
<td>$p : q - 1$</td>
<td>$q : p - 1$</td>
<td>$pq : (p - 1)(q - 1)$</td>
</tr>
<tr>
<td>$p : p - 1$</td>
<td>$p : p - 1$</td>
<td>$p : (p - 1)(q - 1)$</td>
<td>$pq : (p - 1)^2$</td>
<td>$pq : (p - 1)^2(q - 1)$</td>
</tr>
</tbody>
</table>

Order of element: number of elements with that order
The numbers across the top refer to elements \( \bar{a} \) of \( \mathbb{Z}_{pq} \). The numbers down the left side refer to elements \( \bar{b} \) of \( \mathbb{Z}_p \). The numbers in the table refer to the corresponding elements \((\bar{a}, \bar{b})\) of \( G \cong \mathbb{Z}_{pq} \times \mathbb{Z}_p \).

For example, looking at row 2 and column 3 of the table, we see that there are \( p - 1 \) elements \( \bar{a} \) of order \( q \) in \( \mathbb{Z}_{pq} \), \( p - 1 \) elements \( \bar{b} \) of order \( p \) in \( \mathbb{Z}_p \), and from these we get \((p - 1)^2\) elements \((\bar{a}, \bar{b})\) of order \( pq \) in \( G \).

Altogether, \( G \) has:

- 1 element of order 1;
- \( p - 1 \) elements of order \( q \);
- \((p - 1) + (q - 1) + (p - 1)(q - 1) = pq - 1\) elements of order \( p \); and
- \((p - 1)(q - 1) + (p - 1)^2(q - 1) + (p - 1)^2 = p^2q - pq - p + 1\) elements of order \( pq \).

In particular, the largest order is \( pq \).

2. Note that

\[
((1, r)(x, 1))(y, 1) = (x^{-1}, r)(y, 1) = (x^{-1}y^{-1}, r) = ((yx)^{-1}, r),
\]

whereas

\[
(1, r)((x, 1)(y, 1)) = (1, r)(xy, 1) = ((xy)^{-1}, r).
\]

Thus the operation is associative if and only if these are equal for every \( x \) and \( y \), i.e., if and only

\[
(xy)^{-1} = (yx)^{-1}
\]

or, equivalently, \( xy = yx \).

So the operation is associative if and only if \( G \) is abelian. This proves (a). To prove (b), we just have to check that there is an identity element (there is, namely \((1, 1)\)) and that every element has an inverse. Note that \((x, 1)\) has inverse \((x^{-1}, 1)\) and that \((x, r)\) is its own inverse.

3. (a). Suppose \( p = mn \). Then

\[
0 = p1 = (m1)(n1).
\]

Since \( F \) is a field, this means \( m1 \) or \( n1 \) is 0. Since \( p \) is the order of 1 (in \((F, +)\)), this means \( p \) divides \( m \) or \( n \). Since \( p = mn \), this means \( m = p \) and \( n = 1 \) or \( m = 1 \) and \( n = p \). Thus \( p \) is prime.

(b) Let \( x \) be a nonzero element of \( F \). Then

\[
1 + 1 + \cdots + 1 (m\text{-times}) = 0
\]

if and only if

\[
x + x + \cdots + x (m\text{-times}) = 0.
\]

(We can deduce one equation from the other by multiplying by \( x \) or by \( x^{-1} \).) Thus all nonzero elements have the same order.

(c) Let \( q \) be a prime factor of \(|F|\). By Cauchy’s theorem, \( F \) (as an additive group) has an element of order \( q \). Hence by (a), \( q = p \). Thus \(|F|\) is a power of \( p \).