I sketch out the proof of various exercises. I place a [...] where extra work would be good.

Exercise. 1.3.30.
Proof. (Sketch)
Suppose $\bar{a}^2 = 0$ in $\mathbb{Z}_n$ implies that $\bar{a} = 0$. We want to prove $n$ is square free. By prime factorization, there exists distinct primes $p_i$ and positive integers $n_i$ such that $n = p_1^{n_1} \cdots p_r^{n_r}$. We want to show $n_i = 1$ for all $i$. Suppose, without loss of generality $n_1 > 1$. Then let $a = p_1^{n_1-1}p_2^{n_2} \cdots p_r^{n_r}$. [...] Then $\bar{a}^2 = 0$, but $\bar{a} \neq 0$. Contradiction.

Note that proofs by contradiction can often be rephrased as a direct proof of the contrapositive. In this case, we have shown that if "$n$ is not square free" then "$\bar{a}^2 = 0$ in $\mathbb{Z}_n$ does not imply $\bar{a} = 0".

Exercise. 1.3.32.
Proof. (Sketch)
Suppose $f(\bar{a}) = f(\bar{b})$. Then $\bar{a}^{p-2} = \bar{b}^{p-2}$. Then $1 = [...] = \bar{a} \bar{b}^{p-2}$. Then $\bar{b} = [...] = \bar{a}$. Thus $f$ is one-to-one. Because $|\mathbb{Z}_p|$ is finite, $f$ is also onto. We conclude every element of $\mathbb{Z}_p$ has a $(p-2)$th root.

Exercise. 1.4.5
Proof. (Sketch using Exercise 1.4.26)
Suppose $\tau \sigma = (1 \ 2 \ 3 \ 4)$ and $\sigma \tau = (1 \ 2 \ 3 \ 4)$. Then
\[
\sigma \tau \sigma = \sigma (1 \ 2 \ 3 \ 4) \\
(1 \ 2 \ 3 \ 4) = \sigma (1 \ 2 \ 3 \ 4) \\
(1 \ 2 \ 3 \ 4) = \sigma (1 \ 2 \ 3 \ 4) \sigma^{-1}.
\]
But by Exercise 1.4.26, $\sigma (1 \ 2 \ 3 \ 4) \sigma^{-1}$ is a 4-cycle.
(I realized the easier proof)

Look at the parity.

Exercise. 1.4.23
Proof. (Sketch)
Let us follow the hint. $\sigma \neq \varepsilon$ implies there exists $k$ such that $\sigma k = l$ with $k \neq l$. Now since $n \geq 3$, there exists $m \notin \{k, l\}$. Let $\gamma = (k \ m)$. Now we simply have to show that $\sigma \gamma \neq \gamma \sigma$.

Let's see. We have $\sigma \gamma k = \sigma m =?$. That wasn’t any good. Next, $\sigma \gamma m = \sigma k = l$.

On the other hand $\gamma \sigma m =?$. At this point you might say, what the heck? Well, let's try $\gamma \sigma k = \gamma l = \gamma$. 1
Putting our thinking caps on, we realize that \(\sigma \gamma k = \sigma m \neq l\) because \(\sigma k = l\) and permutations are injective mappings. Thus \(\sigma \gamma \neq \gamma \sigma\).

(Sketch using Exercise 1.4.26)

Repeat the first line of previous proof: \(\sigma \neq \varepsilon [\ldots] m \notin \{k, l\}\). Let \(\gamma = (k \ m)\). We have \(\sigma \gamma \neq \gamma \sigma\) if and only if \(\sigma \gamma \sigma^{-1} \neq \gamma\). But \(\sigma \gamma \sigma^{-1} = (\sigma k \ \sigma m) = (l \ \sigma m)\). Thus \(\sigma \gamma \sigma^{-1} l = \sigma m\) while \(\gamma l = l\). We conclude \(\sigma \gamma \sigma^{-1} \neq \gamma\) and hence \(\sigma \gamma \neq \gamma \sigma\). \(\square\)

**Exercise. 1.4.26 (Generalization)**

One can take the result of Exercise 1.4.26 and show that \(\sigma \gamma \sigma^{-1}\) has the same cycle structure as \(\gamma\) for any \(\gamma \in S_n \setminus \{\varepsilon\}\). More precisely, if \(\gamma \neq \varepsilon\) has the cycle decomposition

\[
( k_{1,1} \ k_{1,2} \ldots \ k_{1,n_1} ) \ldots ( k_{m,1} \ k_{m,2} \ldots \ k_{m,n_m} ),
\]

show that

\[
\sigma \gamma \sigma^{-1} = (\sigma k_{1,1} \ \sigma k_{1,2} \ldots \ \sigma k_{1,n_1}) \ldots (\sigma k_{m,1} \ \sigma k_{m,2} \ldots \ \sigma k_{m,n_m}).
\]

**Proof.** (Sketch)

If \(\gamma = \delta_1 \delta_2 \ldots \delta_m\) then

\[
\sigma \gamma \sigma^{-1} = \sigma \delta_1 \delta_2 \ldots \delta_m \sigma^{-1} = \sigma \delta_1 \sigma^{-1} \sigma \delta_2 \sigma^{-1} \ldots \sigma \delta_m \sigma^{-1}.
\]

The result follows from 1.4.26. \(\square\)

**Exercise. 1.4.27c**

**Proof.** (Sketch)

If we can show the result for an arbitrary cycle, we can show it for an arbitrary permutation (cyclic decomposition).

By 1.4.27a, if we can show the result for an arbitrary transposition \((a \ b)\) then we can show it an arbitrary cycle. Without loss of generality we have \(a < b\).

Write \(b = a + n\) for some \(n \geq 1\). If \(b = a + 1\), we’re done. So suppose \(n \geq 1\).

Let us attempt to reduce \((a \ a + n)\). We’d like to have something like

\[
(a \ a + n) = (\sigma(a) \ \sigma(a + 1)) = \sigma(a \ a + 1) \sigma^{-1}.
\]

In fact, this tells us that \(\sigma(a) = a\) and \(\sigma(a+1) = a+n\). Define \(\sigma = (a + 1 \ a + n)\).

In a clean proof, we might modify the above with the following: if \((a \ b)\) satisfies \(|b-a| = 1\), we’re done. Otherwise \((a \ b)\) can be written as a product of transpositions \((c \ d)\) for which \(|d-c| < |b-a|\). WLOG \(a < b\). Then for \(\sigma = (a + 1 \ b)\), we have

\[
\sigma(a \ a + 1) \sigma^{-1} = (\sigma(a) \ \sigma(a + 1)) = (a \ b).
\]

I’d like to emphasize how the “nicer” write-up differs from my initial thought process. Depending on your audience, sometimes the proof that illustrates the thought process is good. However, a clean proof is often elegant. \(\square\)

**Exercise. 1.4.27d**

**Proof.** (Sketch)

The hint refers to 1.4.27b, but I think 1.4.27c seems more useful.

By 1.4.27c, if you can do it for \((k \ k + 1)\) with \(k \in \{1, \ldots, n - 1\}\) then you can do it for any permutation.
There is nothing to show for \( k = 1 \). \((1 \ 2) = (1 \ 2)\). For \( k = 2 \), we have \( \sigma (1 \ 2) \sigma^{-1} = (2 \ 3) \). In general, [...] and we have \( \sigma^{k-1} (1 \ 2) (\sigma^{k-1})^{-1} = (k \ k+1) \).

**Exercise.** 1.4.28

*Proof. (Sketch)*

Part a: \( \sigma^2 = (1 \ 3 \ 5 \ \cdots \ 2k-1) (2 \ 4 \ 6 \ \cdots \ 2k) \). Rigorous clarification would be to consider the space of objects as elements in \( \mathbb{Z}_n \) and that \( \sigma \) is equivalent to the map \( \bar{k} \mapsto k+1 \) [see part c]. Thus \( \sigma^2 \) is the map \( \bar{k} \mapsto k+2 \) [see part c].

Technically we don't need part c to prove parts a and b. Part a would be done as follows: if \( 1 \leq i \leq 2k-2 \) then \( \sigma^2 i = \sigma(i+1) = i+2 \). Thus we confirmed the proposed equality except for the mappings \( 2k-1 \mapsto 1 \) and \( 2k \mapsto 2 \). Manually we have \( \sigma^2(2k-1) = \sigma(2k) = 1 \) and \( \sigma^2(2k) = \sigma(1) = 2 \).

Part b: We follow the rigorous argument of part a. \( \sigma^m \) is the map \( \bar{k} \mapsto k+m \) [see part c]. Thus for \( 0 \leq i \leq m-1 \), we have

\[
( i \ i+m \ i+2m \ \cdots \ i+(q-1)m )
\]

We double-check that \( i+(q-1)m \mapsto i+(q-1)m+m = i+qm = i \). [...]

Similar to part a, we don't need part c. If \( 1 \leq j \leq n-m \), then \( \sigma^m j \mapsto j+m \).

For \( n-m+1 \leq j \leq n \) then we can write \( j = n-m+i \) for some \( 1 \leq i \leq m \). Rewriting \( j \), we obtain \( j = i+(q-1)m \) and so

\[
\sigma^m j = \sigma^m(i+(q-1)m)
= \sigma \sigma^m(i+(q-1)m)
= [...] 
= \sigma^i
= \sigma^{i-1} 1
= 1 + (i-1)
= i
\]

as desired.

Part c: Much the same as what I have written in the latter parts of a and b.

Part d: The book suggests that \( \sigma^m \) is a cycle of length \( p \). This would mean that, modulo \( p \), we have

\[
\sigma^m = (0 \ m \ 2m \ \cdots \ (p-1)m)
\]

If this is to be a cycle, then the elements \( km \) must be unique for \( 0 \leq k \leq p-1 \).

Suppose \( \overline{k_1 m} = \overline{k_2 m} \). Since \( p \) is prime and \( 1 \leq m \leq p-1 \), then \( m \) is relatively prime with \( p \). Thus, \( \overline{m} \) has an inverse mod \( p \) and [...] so we conclude \( \overline{k_1} = \overline{k_2} \). □