Exercises 10:

(4) Cosets of $\langle 4\rangle$ in $\mathbb{Z}_{12}$:

$\langle 4\rangle = \{0,4,8\}$
$1+\langle 4\rangle = \{1,5,9\}$
$2+\langle 4\rangle = \{2,6,10\}$
$3+\langle 4\rangle = \{3,7,11\}$

Since $\langle 4\rangle \cup (1+\langle 4\rangle) \cup (2+\langle 4\rangle) \cup (3+\langle 4\rangle) = \mathbb{Z}_{12}$, these are all of the cosets of $\langle 4\rangle$.

(6) Left cosets of $\{\rho_0,\mu_2\}$ in D_4 (using the notation of the book):

$\{\rho_0,\mu_2\}$
$\rho_1 + \{\rho_0,\mu_2\} = \{\rho_1, \delta_2\}$
$\rho_2 + \{\rho_0,\mu_2\} = \{\rho_2, \mu_1\}$
$\rho_3 + \{\rho_0,\mu_2\} = \{\rho_3, \delta_1\}$

Since the union of these sets is all of D_4, these are all of the left cosets of $\{\rho_0,\mu_2\}$.

(13) The index of $\langle 3\rangle$ in $\mathbb{Z}_{24}$:

$|\langle 3\rangle| = \frac{24}{\gcd(3,24)} = 24/3 = 8$

So $|\mathbb{Z}_{24} : \langle 3\rangle| = 24/8 = 3$.

(16) $\mu = (1\ 2\ 4\ 5)(3\ 6)$ in S_6.

$\mu^2 = (1\ 4)(2\ 5)$
$\mu^3 = (1\ 5\ 4\ 2)(3\ 6)$
$\mu^4 = e$
$\Rightarrow |\langle\mu\rangle| = 4$

So, $|S_6 : \langle\mu\rangle| = |S_6|/|\langle\mu\rangle| = 6!/4 = 60$.

(20) This is impossible. In an abelian gp, left cosets & right cosets coincide.

(21) The improper subgp G of any gp G.

(22) Let $G = \mathbb{Z}_6$, $H = \{e\}$. Then the left cosets of H are:
$H,\ 1+H,\ 2+H,\ 3+H,\ 4+H,\ 5+H$, which partitions G into 6 cells.

(23) Impossible. There must be at least one element in each cell, so the gp must must have at least 12 elements for this to be possible.

(24) This is impossible. The # of cells in the partition of G is the index of the subgp H in G, and is equal to $|G|/|H|$. Since 6 is not divisible by 4, no such subgp H exists.

(28) We first show that if $g^{-1}hg \in H\ \forall g\in G$ & $\forall h\in H$, then $g^{-1}Hg = H$. It is clear that $g^{-1}Hg \subseteq H$, so we need only show $H \subseteq g^{-1}Hg$.
$g^{-1}Hg \subseteq H \Rightarrow H \subseteq gHg^{-1}$ (left mult. by g & right mult. by g^{-1}). Given any $g\in G$, let $y = g^{-1}$. Then $g^{-1}Hg \subseteq H \subseteq yHy^{-1} = g^{-1}Hg \Rightarrow H = g^{-1}Hg$.
We next show $gH = Hg\ \forall g\in G$. Let $g\in G$ & $x\in Hg$, so that $x = hg$ for some $h\in H$. Then $g^{-1}x = g^{-1}hg \in g^{-1}Hg = H \Rightarrow g^{-1}x \in H \Rightarrow x \in gH$. Thus $Hg \subseteq gH$. By a similar argument, starting with $y\in gH$, we can show $g^{-1}y \in H$, so $y \in gH$.

(29) Suppose $gH = Hg$ $\forall g \in G$, & consider $g^{-1}hg$ for some $g \in G$ & some $h \in H$. Since $Hg = gH$, $\exists h' \in H$ s.t. $hg = gh'$. Thus $g^{-1}hg = g^{-1}gh' = h' \in H$, as desired.

(34) Let G be a gp, $H \le G$ s.t. $|G:H| = 2$. Then H has 2 left cosets & 2 right cosets. Since H is both a left & right coset, the 2nd left & 2nd right coset must be $\{g \in G \mid g \notin H\}$.

(40) Let G be a gp w/ order n, & let $a \in G$. Then $\langle a \rangle \le G$, so $|\langle a \rangle| = k$ must divide n by Lagrange's thm. Let $n/k = d$. Then $a^n = a^{kd} = (a^k)^d = e^d = e$, as desired.

(43) $H, K \le G$. $a \sim b \Leftrightarrow a = hbk$ for some $h \in H$ & $k \in K$.

(a) $\sim$ is an equivalence relation:

- reflexive: $a = eae$, & $e \in H$, $e \in K$ since H & K are subgps. Therefore $a \sim b$.
- symmetric: Suppose $a \sim b$. Then $\exists h \in H$, $k \in K$ s.t. $a = hbk$. So $b = h^{-1}ak^{-1}$, & since H & K are subgps, $h^{-1} \in H$ & $k^{-1} \in K$. Therefore, $b \sim a$.
- transitive: Suppose $a \sim b$ & $b \sim c$. Then $\exists h_1, h_2 \in H$, $k_1, k_2 \in K$ s.t. $a = h_1 b k_1$ & $b = h_2 c k_2$. Thus, $a = h_1 h_2 c k_2 k_1$. Since H & K are subgps, $h_1 h_2 \in H$ & $k_2 k_1 \in K$.

(b) Suppose $a \sim b$. Then $a = hbk \Rightarrow b = h^{-1}ak^{-1}$, so $b \in HaK$. (here we use that $H = H^{-1}$!)

<u>Exercises 11</u>:

(16) $\mathbb{Z}_2 \times \mathbb{Z}_{12} \simeq \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3$
$\mathbb{Z}_4 \times \mathbb{Z}_6 \simeq \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_6$
So yes, they are isomorphic.

(18) $\mathbb{Z}_8 \times \mathbb{Z}_{10} \times \mathbb{Z}_{24} \simeq \mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_8 \times \mathbb{Z}_3$
$\mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_{40} \simeq \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_8 \times \mathbb{Z}_5$, so no, they are not isomorphic by FTFGAG.

(23) $32 = 2^5$
$\mathbb{Z}_{32}$; $\mathbb{Z}_2 \times \mathbb{Z}_{16}$; $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_8$; $\mathbb{Z}_4 \times \mathbb{Z}_8$; $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$; $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_4$;
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

(39) Let $F = \{g \in G \mid |g| < \infty\}$.

- closure: Let $g, h \in F$. Then $|g| = n < \infty$ & $|h| = m < \infty$. Consider $(gh)^{nm} = g^{nm} h^{nm}$, since G is abelian. Then
$$(gh)^{nm} = (g^n)^m \cdot (h^m)^n = e^m \cdot e^n = e \cdot e = e \Rightarrow |gh| \le nm < \infty.$$
- identity: $|e| = 1 < \infty \Rightarrow e \in F$.
- inverses: Let $g \in F$. Since $|g^{-1}| = |g| < \infty$, $g^{-1} \in F$.

Therefore, $F \le G$.

(47) $H = e \cup \{g \in G \mid |g| = 2\}$.

- closure: Let $h, g \in H$. If $h = e$, then $hg = g \in H$, & if $g = e$, then $hg = h \in H$. If $h \neq e$ & $g \neq e$, then $|h| = |g| = 2$. Since H is abelian, $(hg)^2 = h^2 g^2 = e \cdot e = e \Rightarrow |hg| \leq 2$. If $|hg| = 2$, then $hg \in H$. If $|hg| = 1$, then $hg = e \in H$. ✓
- identity: $e \in H$ by assumption ✓
- inverses: Let $g \in H$. If $g = e$, then $g^{-1} = e^{-1} = e \in H$. If $g \neq e$, then $|g| = 2 \Rightarrow |g^{-1}| = 2 \Rightarrow g^{-1} \in H$ ✓

Therefore, $H \leq G$.

(49) Consider S_4 which is not abelian. Then $(1\,2), (2\,3)$ have order 2, but $(1\,2)(2\,3) = (1\,2\,3)$ has order 3, so H is not closed and so cannot be a subgp of S_4.

(53) Let G be an abelian gp, p a prime, & $|G| = p^k$ for some k. Let $g \in G$. Then $|g| = |\langle g \rangle|$, which must divide $|G|$ by Lagrange's thm. Since the only divisors of p^k are powers of p, $|g|$ is a power of p.
Since this proof does not use that G is abelian, this assumption can be dropped.

(54) By FTFGAG, there are decompositions of $G, H, \& K$, unique up to order, as:

$$G \cong \mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_n^{r_n}} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$
$$H \cong \mathbb{Z}_{q_1^{k_1}} \times \cdots \times \mathbb{Z}_{q_m^{k_m}} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$
$$K \cong \mathbb{Z}_{l_1^{s_1}} \times \cdots \times \mathbb{Z}_{l_t^{s_t}} \times \mathbb{Z} \times \cdots \times \mathbb{Z}.$$

Also, $G \times K$ & $H \times K$ decompose as:

$$G \times K \cong (\mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_n^{r_n}} \times \mathbb{Z} \times \cdots \times \mathbb{Z}) \times (\mathbb{Z}_{l_1^{s_1}} \times \cdots \times \mathbb{Z}_{l_t^{s_t}} \times \mathbb{Z} \times \cdots \times \mathbb{Z}), \;\&$$
$$H \times K \cong (\mathbb{Z}_{q_1^{k_1}} \times \cdots \times \mathbb{Z}_{q_m^{k_m}} \times \mathbb{Z} \times \cdots \times \mathbb{Z}) \times (\mathbb{Z}_{l_1^{s_1}} \times \cdots \times \mathbb{Z}_{l_t^{s_t}} \times \mathbb{Z} \times \cdots \times \mathbb{Z}),$$

and by FTFGAG, these are unique up to order. Since $G \times K \cong H \times K$, these decompositions must be the same up to order, & therefore

$$\mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_n^{r_n}} \times \mathbb{Z} \times \cdots \times \mathbb{Z} \cong \mathbb{Z}_{q_1^{k_1}} \times \cdots \times \mathbb{Z}_{q_m^{k_m}} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$

& thus $G \cong H$.

<u>Additional exercises</u>

(1) (a) We must prove λ_g is a bijection.

- injective: let $x, y \in G$ s.t. $\lambda_g(x) = \lambda_g(y)$. Then $gx = gy$, & so $x = y$ by left cancellation.
- surjective: Let $y \in G$. Then $g^{-1}y \in G$ & $\lambda_g(g^{-1}y) = g(g^{-1}y) = y$.

Therefore, $\lambda_g \in S_G$.

(b) We first show φ is a homomorphism. Let $g, h \in G$, & let $x \in G$. Then
$\lambda_g \circ \lambda_h(x) = \lambda_g(hx) = ghx = \lambda_{gh}(x)$, so $\lambda_g \lambda_h = \lambda_{gh}$
Thus $\varphi(gh) = \lambda_{gh} = \lambda_g \lambda_h = \varphi(g)\varphi(h)$.
We next show φ is injective. Let $g, h \in G$ s.t. $\varphi(g) = \varphi(h)$. Then $\lambda_g = \lambda_h$, so for all $x \in G$, $\lambda_g(x) = \lambda_h(x) \Rightarrow gx = hx \Rightarrow g = h$.
Finally, by the definition of $\varphi(G)$, φ is surjective onto $\varphi(G)$. Therefore, $G \cong \varphi(G)$.

(c) We have already shown that the image of a homomorphism is a subgp of the target gp, so G is isomorphic to a subgp of S_G.

② (a) • homomorphism: let $(g_1,h_1),(g_2,h_2)\in G_1\times G_2$. Then
$\pi((g_1,h_1)(g_2,h_2)) = \pi((g_1g_2, h_1h_2)) = g_1g_2 = \pi((g_1,h_1))\,\pi((g_2,h_2))$ ✓

• Surjective: let $g\in G_1$. Then $(g,e_2)\in G_1\times G_2$ (where $e_2\in G_2$ is the identity), & $\pi((g,e_2))=g$.

• not injective (unless $G_2=\{e_2\}$!): Let $h\in G_2$ & $h\neq e_2$. Then $\forall g\in G_1$, $\pi((g,e_2)) = g = \pi((g,h))$.

(b) • homomorphism: let $g,h\in G_1$. Then $\iota(gh) = (gh,e_2) = (g,e_2)(h,e_2) = \iota(g)\iota(h)$.

• injective: let $g,h\in G_1$ s.t. $\iota(g)=\iota(h)$. Then $(g,e_2) = \iota(g) = \iota(h) = (h,e_2)$. Thus $g=h$.

• not surjective (unless $G_2=\{e_2\}$!); Consider $(g,h)\in G_1\times G_2$, where $h\in G_2$, $h\neq e_2$, & $g\in G_1$. Then $\forall g'\in G_1$, $\iota(g')=(g',e_2)\neq(g,h)$, as $e_2\neq h$.

③ Fix $i\in\{1,\dots,n\}$, & consider the map $\iota: G_i \to \prod_{j=1}^{n} G_j$ defined by $\iota(g) = (e_1,\dots,e_{i-1},g,e_{i+1},\dots,e_n)$, where $e_j\in G_j$ is the identity. By a similar argument as in 2(b), ι is an injective homomorphism. Moreover, ι is surjective onto its image, $\iota(G_i)$, which is a subgp of $\prod_{j=1}^{n} G_j$. Therefore, G_i is isomorphic to a subgp of G.

④ Let G be a gp of prime order p. Then since $p\geq 2$, $\exists g\in G$ s.t. $g\neq e$. Consider $H=\langle g\rangle$. Then by Lagrange's Thm, $|H|$ divides p, so $|H|=1$ or p. Since $g\neq e$, $|H|\neq 1$. Thus $|H|=p$, so $G=H=\langle g\rangle$. Therefore, G is cyclic.