CHAPTER 8

Section 8.1

1. If $(a, b) \in G \times H$ then the order is $|(a, b)| = \text{lcm}\{|a|, |b|\}$. With this information the numerical questions here are easily done.

2. $4 \cdot 2 \cdot 6 \cdot 4 = 192$.

3. (a) Answered in the text. (b) $\{(0, 0)\}$ is the subgroup of 1 element; there are 7 subgroups of 2 elements; there are 7 subgroups of 4 elements; there is 1 subgroup of 8 elements (namely, the whole group).

4. Define $\varphi : G \times H \to H \times G$ by $\varphi(x, y) = (y, x)$ and verify that it is an isomorphism.

5. $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic.

6. (a) $\mathbb{Z}_{12} \cong \mathbb{Z}_3 \times \mathbb{Z}_4$. Explicitly let $A = \langle [4]_{12} \rangle$ and $B = \langle [9]_{12} \rangle$ and show that $\mathbb{Z}_{12} = A \times B$.
   (b) $\mathbb{Z}_{15} \cong \mathbb{Z}_3 \times \mathbb{Z}_5$
   (c) $\mathbb{Z}_{30} \cong \mathbb{Z}_2 \times \mathbb{Z}_{15} \cong \mathbb{Z}_3 \times \mathbb{Z}_{10} \cong \mathbb{Z}_5 \times \mathbb{Z}_6$

7. ($\Rightarrow$) Clear since G_i is isomorphic to a subgroup of the product.
($\Leftarrow$) $(a_1, a_2, \ldots)(b_1, b_2, \ldots) = (a_1b_1, a_2b_2, \ldots) = (b_1a_1, b_2a_2, \ldots) = (b_1, b_2, \ldots)(a_1, a_2, \ldots)$.

8. Since $\pi_i(e_1, \ldots, e_{i-1}, a_i, e_{i+1}, \ldots, e_n) = a_i$ the projection map is surjective. The homomorphism property follows quickly from the definitions.

9. No. $\mathbb{Z}_4 \times \mathbb{Z}_2$ has no element of order 8.

10. (a) Since f, g are bijective it is routine to check that θ is bijective. Also $\theta((a, b)\cdot(a', b')) = \theta(aa', bb')$ $= (f(aa'), g(bb')) = (f(a)f(a'), g(b)g(b')) = (f(a), g(b))\cdot(f(a'), g(b')) = \theta(a, b)\cdot\theta(a', b')$.
    (b) Induction on n. The case $n = 2$ is done in (a). Suppose $n > 2$. By the inductive hypothesis $G_1 \times \cdots \times G_{n-1} \cong H_1 \times \cdots \times H_{n-1}$. Apply (a) to complete the proof.

11. Let $\alpha : K \to M \times N$ be an isomorphism with $\alpha(x) = (\alpha_1(x), \alpha_2(x))$. Define $\varphi : H \times K \to H \times M \times N$ by $\varphi(h, k) = (h, \alpha_1(k), \alpha_2(k))$. Verify that φ is an isomorphism.

12. (a) The homomorphism π_i of Exercise 8 has G_i^* as its kernel.
    (b) Define $\delta_i : G_i \to G_1 \times \cdots \times G_n$ by $\delta_i(x) = (e_1, \ldots, e_{i-1}, x, e_{i+1}, \ldots, e_n)$. Check that δ_i is an injective homomorphism with image G_i^*.
    (c) For any g in the direct product verify that $g = \delta_1(\pi_1(g))\cdots\delta_n(\pi_n(g)) \in G_1^*\cdots G_n^*$. The uniqueness follows since the projection π_i picks out the i^{th} component.

13. (a) Closure under multiplication and inverses is easily verified.
(b) ($\Rightarrow$) Answered in the text. ($\Leftarrow$) $G \times G \times G$ is abelian so every subgroup is normal.

14. If k is any common multiple of $|a_1|, \ldots, |a_n|$ then $a_i^k = e_i$ for every index i. Therefore $(a_1, \ldots, a_n)^k = (e_1, \ldots, e_n)$. The order of this element is the smallest positive such k. That is the lcm.

15. Define $\sigma \in S_n$ by $\sigma(j) = i_j$. Define the map f from $G_1 \times \cdots \times G_n$ to $G_{i_1} \times \cdots \times G_{i_n}$ by $f(a_1, \ldots, a_n) = (a_{\sigma(1)}, \ldots, a_{\sigma(n)})$. Verify that this f is an isomorphism.

16. View $G = NK$ as an internal direct product so that $xy = yx$ for every $x \in N$ and $y \in K$. For any $a \in M$ we have $(xy)^{-1}a(xy) = y^{-1}(x^{-1}ax)y = x^{-1}ax \in M$ since M is normal in N.

17. Every element $r \in \mathbb{Q}^*$ can be uniquely written as $r = \varepsilon \cdot |r|$ where $\varepsilon = \pm 1$ and $|r|$ is the absolute value of r. Apply Theorem 8.1.

18. Every $z \in \mathbb{C}^*$ can be uniquely as $z = r(\cos\theta + i \cdot \sin\theta)$ where $r \in \mathbb{R}^*$ and $\theta \in \mathbb{R}$. Moreover r is uniquely determined by z, and θ is determined (mod 2π). Define $f: \mathbb{C}^* \to \mathbb{R}^* \times \mathbb{R}/\mathbb{Z}$ by $f(z) = (r, [\theta/2\pi)$ for the r, θ defined above. Verify that f is an isomorphism.

19. (a) $f^*(xy) = (f_1(xy), \ldots, f_n(xy)) = (f_1(x)f_1(y), \ldots, f_n(x)f_n(y)) = f^*(x)f^*(y)$. Also $\pi_i(f^*(x)) = \pi_i(f_1(x), \ldots, f_n(x)) = f_i(x)$.
(b) If g is any such homomorphism then as in Exercise 12 $g(x) = \delta_1(\pi_1(g(x)))\cdots\delta_n(\pi_n(g(x)) = \delta_1(f_1(x))\cdots\delta_n(f_n(x) = f^*(x)$.

20. Suppose $g \in G$ can be expressed in 2 ways: $g = a_1\cdots a_n = b_1\cdots b_n$ where $a_i, b_i \in N_i$. Then $(a_1^{-1}b_1)\cdots(a_n^{-1}b_n) = e$ since G is abelian. Then the hypothesis implies $a_i^{-1}b_i = e$ for each i, so that $a_i = b_i$. Apply Theorem 8.1.

21. If $G = H \times K$ then use δ_i and π_i as in Exercise 12. Conversely suppose δ_i and π_i are given. Define $H^* = \delta_1(H)$ and $K^* = \delta_2(K)$. These are subgroups of G, automatically normal since G is abelian. Since $\pi_i \circ \delta_i$ is the identity, δ_i is injective so that $H \cong H^*$ and $K \cong K^*$. The condition $\delta_1\pi_1 + \delta_2\pi_2 = \iota_G$ implies $H^* + K^* = G$. The conditions $\pi_i\delta_j = 0$ imply that $H^* \cap K^* = \{0\}$, and Theorem 8.3 applies.

22. Let $g \in G$ and $h \in H$ be generators, so $|g| = n$ and $|h| = m$. Lagrange's Theorem implies that $n \mid |G|$ and $m \mid |H|$. By Exercise 14, $|(g, h)| = \operatorname{lcm}\{n, m\}$. The result follows since $\operatorname{lcm}\{n, m\} = nm$ if and only if $(n, m) = 1$.

23. (a) Answered in the text. (b) Use the same example.

24. No. Use the example of 23(a) noting that M is normal in S_3.

25. Induction on k. Let $H = N_1\cdots N_{k-1}$. Then H is a normal subgroup (see Exercise 7.6.18) and by hypothesis $H \cap N_k = \langle e\rangle$. By Theorem 8.3 $G \cong H \times N_k$. Apply the induction hypothesis to H.

26. We use a modified statement and prove it by induction on k.
Claim. Let N_i be normal subgroups of a finite group G. Then $|N_1 \cdots N_k|$ divides $|N_1| \cdots |N_k|$ with equality if and only if $N_1 \cdots N_k \cong N_1 \times \cdots \times N_k$.
Proof. Suppose $k \geq 2$ and let $H = N_1 \cdots N_{k-1}$. Then H is normal and $|N_1 \cdots N_k| = |H| \cdot |N_k| / |H \cap N_k|$, using the Second Isomorphism Theorem (see Exercise 7.8.24). By the induction hypothesis (or trivially if $k = 2$) this divides $|N_1| \cdots |N_{k-1}| \cdot |N_k| / |H \cap N_k|$ which divides $|N_1| \cdots |N_k|$. Equality holds here if and only if $|H| = |N_1| \cdots |N_{k-1}|$ and $H \cap N_k = \langle e \rangle$. By induction (or trivially if $k = 2$), this occurs if and only if $H \cong N_1 \times \cdots \times N_{k-1}$ and $H \cap N_k = \langle e \rangle$. Apply Theorem 8.3.

27. (a) Use the subgroups in the answer to Exercise 23.
(b) Let $N = \langle r_1 \rangle$ and $H = \langle h \rangle$.
(c) Use $N = A_4$ and $H \ \langle (12) \rangle$.

28. Claim. If G is nonabelian with $|G| < 12$ then G is indecomposable.
Proof. If not then $G \cong A \times B$ for proper subgroups A, B. Then $|A|$, $|B| \leq |G|/2 < 6$ so that A, B are abelian (see Theorems 7.28 and 7.29). But then G would also be abelian (see Exercise 7).
This Claim settles (a), (b)
(c) Any two nonzero subgroups of $\mathbb{Z}$ meet nontrivially. (Compare Exercise 30.)

29. The only nonzero subgroups are $\langle 1 \rangle, \langle p \rangle, \langle p^2 \rangle, \ldots \langle p^{n-1} \rangle$. Since any two of these meet nontrivially, the group is indecomposable.

30. If A_1, A_2 are nonzero subgroups of $\mathbb{Q}$ let $a_i/b_i \in A_i$ be nonzero elements. Then $a_1a_2 = (a_2b_1) \cdot a_1/b_1 = (a_1b_2) \cdot a_2/b_2$ is in $A_1 \cap A_2$. Then $\mathbb{Q}$ cannot be the direct product of A_1 and A_2.

31. $\mathbb{Z}$ is indecomposable but $\mathbb{Z}_6$ is decomposable.

32. Apply the definition of "indecomposable".

33. This is a straightforward check of the definitions.

34. If $c = (c_1, c_2, \ldots) \in \sum G_i$ and $a = (a_1, a_2, \ldots) \in \prod G_i$ then $a^{-1}ca = (a_1^{-1}c_1a_1, a_2^{-1}c_2a_2, \ldots)$. Whenever $c_j = e_j$ we also have $a_j^{-1}c_ja_j = e_j$. Therefore $a^{-1}ca \in \sum G_i$ and it is normal.

35. The proof of Theorem 8.1 is easily adapted to this case.

36. Define $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ by $f([a]_{mn}) = ([a]_m, [a]_n)$ and note that f is a ring homomorphism.
If $(m, n) = 1$ then the kernel is $\{0\}$ and f is injective. Since the orders of these rings are equal it follows that f is an isomorphism. Since isomorphic rings have isomorphic unit groups the result follows. (Compare Lemma 8.8 and Corollary 13.5.)

37. Let $G = G_1 \times \cdots \times G_n$ with projections $\pi_i : G \to G_i$. By hypothesis there is a unique $g^* : G \to H$ with $\tau_i \circ g^* = \pi_i$. Exercise 19 provides a unique homomorphism $f^* : H \to G$ with $\pi_i \circ f^* = \tau_i$. Now

$g^*f^* : H \to H$ is the unique homomorphism with $\tau_i \circ g^*f^* = \tau_i$. It follows that $g^*f^* = \iota_H$. Similarly $f^*g^* = \iota_G$. Therefore f^* and g^* are isomorphisms.

Section 8.2

1. Answered in the text.

2. pG is the image of the homomorphism $f : G \to G$ defined: $f(x) = px$. Checking the homomorphism property is routine.

3. (a), (c), (e), (g) are answered in the text.
(b) $\mathbb{Z}_{15}$ (d) $\mathbb{Z}_8 \oplus \mathbb{Z}_9$, $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9$, $\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$, $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$.
(f) Use the decompositions: $2^4 = 2^3 2^1 = 2^2 2^2 = 2^2 2^1 2^1 = 2^1 2^1 2^1 2^1$ combined with $3^2 = 3^1 3^1$ to get 10 non-isomorphic groups.
(h) $1160 = 2^3 5^1 29^1 = 2^2 2^1 5^1 29^1 = 2^1 2^1 2^1 5^1 29^1$ yields 3 groups.

4. Since $f(x) = px$ is a homomorphism we have $pG = pG_1 + \cdots + pG_n$. This sum is easily seen to be direct.

5. (a), (c) are answered in the text. (b) $2, 2, 2^2, 3, 3, 3^2$ (d) $2, 2^2, 2^2, 2^4, 3, 3, 3, 5, 5, 5^2$

6. (a) 250 (b) 6, 6, 36 (c) 2, 10, 20, 40 (d) 2, 60, 60, 1200

7. (a) 2, 2, and 2, 2 (b) 16 and 16 (c) 2, 4 and 2, 4
(d) 2, 2, 2, 2 and 2, 2, 2, 2

8. Elements of G(p) are $n/p^k + \mathbb{Z}$.

9. (a) Answered in the text. (b) Since $n/2^k + \mathbb{Z} = 2(n/2^{k+1} + \mathbb{Z})$ we see that $2 \cdot G(2) = G(2)$ when $G = \mathbb{Q}/\mathbb{Z}$.

10. The homomorphism property is easy to check. Suppose $a \in G$ is given and let $p^k = |a|$. Since $(p, n) = 1$ there exist integers x, y such that $nx + p^k y = 1$. Then $a = x(na) + y(p^k a) = xf(a)$.
Injective. If $f(a) = 0$ then $a = 0$. Surjective. $a = f(xa)$.

11. Note that $p\mathbb{Z}_{p^n} = \{0\}$ if and only if $n = 1$. Apply Theorem 8.7.

12. The Fundamental Theorem 8.7 says that G is isomorphic to a direct sum of cyclic groups of prime power order. Since $|G|$ is the product of these prime powers, some power of p must occur. Then one of the direct summands must be $\mathbb{Z}_{p^k}$ for some $k \geq 1$. Then G contains an element of order p^k and hence an element of order p by Theorem 7.8.

13. Answered in the text.

14. Exercise 13 implies that $|G(p_i)| = p_i^{k_i}$ for some k_i. By Theorem 8.5 we know that $p^t m = |G| = |G(p_1)| \cdots |G(p_n)| = p_1^{k_1} \cdots p_n^{k_n}$ where $p = p_1$ and $p_1, \ldots, p_n$ are distinct primes. It follows that $t = k_1$.

15. Say $|G| = p^t m$ where $(p, m) = 1$. Then $n \le t$. The Fundamental Theorem implies that $G(p) \cong \mathbb{Z}_{p^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{k_s}}$ where $t = k_1 + \cdots + k_s$. Note that $p\mathbb{Z}_{p^k}$ is a subgroup of order p^{k-1}. Altering one summand in this way we find subgroups of every order $p^t, p^{t-1}, \ldots, p^2, p$.

16. This occurs if and only if n is squarefree (*i.e.* either $n = 1$ or n is a product of one or more distinct primes).

17. (a), (b) Compare the elementary divisors and apply Theorem 8.12.

18. Using Exercise 15 it follows that if $d \mid n$ (and $d > 0$) there is a subgroup N of G with $|N| = d$. Applying this to $d = n/k$ we use $H = G/N$.

19. (a) Answered in the text. (b) If $a + T$ is of finite order in G/T, $n(a + T) = 0 + T$ for some positive integer n. Then $na \in T$ so it has finite order, say k. But then $kna = 0$ and a itself has finite order, so that $a \in T$. Then $0 + T$ is the only element of finite order in G/T.

20. Not necessarily. As in the Hint, $(1, 1) + (-1, 0) = (0, 1)$ is a sum of two elements of infinite order equal to one of finite order in $\mathbb{Z} \oplus \mathbb{Z}_3$.

21. Let $h \in G$ with $f(h) = 1$, and set $H = \langle h \rangle$. Let K be the kernel of f. For any $x \in G$ we have $f(x) = f(h^n)$ for some $n \in \mathbb{Z}$ so that $xh^{-n} \in K$ and $x \in h^n K \subseteq HK$. Then $G = HK$ and certainly $H \cap K = \langle e \rangle$. Apply Theorem 8.3.

22. First let us suppose G and H are p-groups. Let $N_G(m)$ be the number of elements of G with order p^m. Recall that $\mathbb{Z}_{p^n}$ ha s unique subgroup of order p^k for every $k = 1, 2, \ldots, n$ (by Exercise 7.3.40). Therefore the number of elements of order p^k in $\mathbb{Z}_{p^n}$ is a function $\varphi(p^k)$ independent of n, as long as $n \ge k$. (This is often called the Euler φ-function.)

Now suppose the invariant factors of G are $p, p, \ldots, p^2, p^2, \ldots$ where there are k_j copies of p_j, for each j, and each $k_j \ge 0$. Then $N_G(p) = (k_1 + k_2 + k_3 + \cdots)\varphi(p)$, $N_G(p^2) = (k_2 + k_3 + \cdots)\varphi(p^2)$, $N_G(p^3) = (k_3 + \cdots)\varphi(p^3)$, *etc.* Consequently, $k_m = N_G(p^{m+1})/\varphi(p^{m+1}) - N_G(p^m)/\varphi(p^m)$ is determined entirely by the values of N_G. Therefore if $N_G = N_H$ it follows that G and H have the same elementary divisors and hence are isomorphic.

The extension of the argument beyond the case of p-groups is left to the reader.

23. The equation $x^m = e$ has at most m solutions in G. The proof of Theorem 7.41 (or Corollary 8.11) applies to G.

24. Given the invariant factors $m_1, m_2, \ldots, m_t$ in a divisor chain, we can re-build the elementary divisors: Factor $m_j = p_1^{k_{1j}} \cdots p_s^{k_{sj}}$. The divisor conditions imply: $0 \le k_{i1} \le k_{i2} \le \cdots \le k_{it}$ for each $i = 1, 2, \ldots, s$.

The elementary divisors are then easily read off this array: $p_1^{k_{11}}, p_1^{k_{12}}, \ldots, p_1^{k_{1t}}, p_2^{k_{21}}, \ldots, p_2^{k_{2t}}, \ldots, p_s^{k_{s1}}, \ldots, p_s^{k_{st}}$, where we omit any entry equal to 1. Now apply Theorem 8.12.

25. By Lemma 8.4: If $a \in G$ then $a = \sum a_p$ where $a_p \in G(p)$. The sum is taken over all prime numbers p, noting that $a_p = 0$ for all but finitely many p (since $a_p \neq 0$ only if p divides $|a|$). The proof of the uniqueness is the same as in the proof of Theorem 8.5, using the finiteness of the sums to reduce to the case there. By Exercise 8.1.5 conclude that $G \cong \sum G(p)$.