Homework 3 Solutions

Ch 7: 4, 6, 9, 35, 36, 48, 52, 53, 69, 77

4. Find all left cosets of $H = \{1, 11\}$ in $U(30)$. We can verify that H is a subgroup, namely, $11^2 = 121 = 1 \bmod 30$. $U(30) = \{1, 7, 11, 13, 17, 19, 23, 29\}$ and the cosets are H, $7H = \{7, 17\}$, $13H = \{13, 23\}$, and $19H = \{19, 29\}$.

6. We have actually done this one before.

9. Let $H, K < G$ and $g \in G$. Clearly $g(H \cap K) \subseteq gH$ and $g(H \cap K) \subseteq gK$ so $g(H \cap K) \subseteq gH \cap gK$. Conversely, suppose $g' \in gH \cap gK$ so $g' = gh = gk$ and thus $g^{-1}g' \in H \cap K$ and $g' = g(g^{-1}g') \in H \cap K$.

35. Suppose $H < K < G$ we know $[G : H] = |G|/|H| = (|G|/|K|)(|K|/|H|) = [G : K][K : H]$ and $|H| = [H : K]$.

36. Suppose $K < H < G$ with $[G : K] = p$ (prime). We know $[G : K] = [G : H][H : K]$ and since p is prime, either $[G : H] = 1$ and $H = G$ or $[H : K] = 1$ and $H = K$.

48. Let G be abelian of order 15. Suppose G has no element of order 15. Then every element has order 5 or 3 (except for e). Suppose $H, K < G$ with $|H| = 5$ and $|K| = 3$, then $|HK| = |H||K|/|H \cap K| = 15$ thus $HK = G$. But $H =< h >$ and $K =< k >$ since 5 and 3 are prime and $|hk| = 15$, which is a contradiction.

So possibly, all elements are of order 3. But then $< h > \cap < h' > = \{e\}$ for $< h' > \neq < h >$. Let $< h_1 >, < h_2 >, \ldots, < h_7 >$ be all of the subgroups of order 3. The problem is that we would get $< h_1 >< h_2 >$ as a subgroup and $| < h_1 >< h_2 > | = 3^2 = 9 \not| 15$.

A similar argument works with all subgroups of order 5.

52. Let $|G| = pq^n$ where p and q are prime and $p > q^n$. If there were $a \in G$ and $|a| = p^i q^j$ where $i \in \{0, 1\}$ and $j \in \{1, \ldots, n\}$, then we get $|a^{p^i q^{j-1}}| = q$. So if there were no element of order q, then we know all elements are of order p. But then $< a > \cap < b > = \{e\}$ or $< a > = < b >$ for every $a, b \in G$. But then $| < a, b > | \geq |a||b| = p^2 > |G|$ which is a contradiction.

53. Let $|G| = 21$, and there is exactly one subgroup of order 3. Then there must be a subgroup H of order 7. If G is not cyclic, then there must be another subgroup K of order 7, and then $|HK| = 49$, which is a contradiction. Thus G must be cyclic. This argument does work for any G with $|G| = pq$ where $q < p$ and there is a unique subgroup of order q.

69. Let $G = \{(1), (12)(34), (1234)(56), (13)(24), (1432)(56), (56)(13), (14)(23), (24)(56)\}$

a. Find the stab(1) and orb(1).

$$\text{stab}(1) = \{(1), (24)(56)\}\text{and } \text{orb}(1) = \{1, 2, 3, 4\}.$$

b. Find the stab(3) and orb(3).

$$\text{stab}(3) = \{(1), (24)(56)\}\text{and } \text{orb}(3) = \{3, 4, 1, 2\}.$$

c. Find the stab(5) and ord(5).

$$\text{stab}(5) = \{(1), (12)(34), (13)(24), (14)(23)\}\text{and } \text{orb}(5) = \{5, 6\}.$$

77. It is actually clear that the eight-element group is isomorphic to D_4. Namely, let $\gamma = \beta^2 = (12)(34)$ and $\alpha = (1234)$ satisfy

$$\alpha^4 = e, \quad \gamma^2 = e, \quad \alpha\gamma\alpha\gamma = e$$

This makes the group D_4.

Ch 8: 21, 26, 31, 56, 57, 70, 77, 78, 79, 80

21. Let G and H be groups with $(g, h) \in G \times H$. Find a necessary and sufficient condition for $\langle (g, h) \rangle = \langle g \rangle \times \langle h \rangle$.

We know $|\langle (g, h) \rangle = \text{lcm}(|g|, |h|)$ and $|\langle g \rangle \times \langle h \rangle| = |g| \cdot |h|$ so

$$\langle (g, h) \rangle = \langle g \rangle \times \langle h \rangle \iff \gcd(|g|, |h|) = 1 \iff \langle g \rangle \times \langle h \rangle \text{ is cyclic}$$

26. $S_3 \times \mathbb{Z}_2$ is isomorphic to which of the following: $\mathbb{Z}_{12}$, $\mathbb{Z}_6 \times \mathbb{Z}_2$, A_4, D_6.

$S_3 \times \mathbb{Z}_2$ is not abelian so that rules out $\mathbb{Z}_{12}$ and $\mathbb{Z}_6 \times \mathbb{Z}_2$. $S_3 \times \mathbb{Z}_2$ has only two elements of order 6 $((1, 2, 3), 1)$ and $((3, 2, 1), 1)$ while A_4 has 8. So the only viable option is D_6.

Let $r = ((1, 2, 3), 1)$, then we have that $|r| = 6$, let $f = ((1, 2), 1)$, then $|f| = 2$, and $(rf)(rf) = \big(((1, 2, 3), 1)((1, 2), 1)\big)\big(((1, 2, 3), 1)((1, 2), 1)\big) = ((1, 2, 3)(1, 2), 1 + 1)((1, 2, 3)(1, 2), 1 + 1) = ((1, 3), 0)((1, 3), 0) = ((1, 3)(1, 3), 0 + 0) = ((), 0)$.

This actually shows that $S_3 \times \mathbb{Z}_2 \simeq D_6$ as D_6 is the only 12 element group with elements r, f satisfying $r^6 = e$ and $r^i \neq e$ for $0 < i < 6$, $f^2 = e$, and $rfrf = e$.

31. What is the order of the largest cyclic subgroup of $\mathbb{Z}_6 \times \mathbb{Z}_{10} \times \mathbb{Z}_{15}$. We know $|(n, m, k)| = \text{lcm}(m, n, k)$ here $\text{lcm}(6, 10, 15) = 30$ and could be achieved with $(1, 0, 3)$, $(2, 5, 3)$, etc.

Same idea works for finding the largest cycle in $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}$ the order will be $\text{lcm}(n_1, \ldots, n_m)$.

Note: Let $N = n_1 n_2 \cdots n_m$ and $N_i = N/n_i$

$$\text{lcm}(n_1, \ldots, n_m) = \frac{N}{\gcd(N_1, \ldots, N_m)}$$

56. Let $G = \{ax^2 + bx + c \mid a, b, c \in \mathbb{Z}_3\}$ with addition defined as the usual polynomial addition. Show that $G \simeq \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$. Generalize.

Showing that $G \simeq \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ requires (1) giving the bijection, which is clear, namely, $(a, b, c) \mapsto ax^2 + bx + c$, and (2) showing that this is an isomorphism, which is also clear.

Generalizing can happen in a variety of ways. First, we could note that $G^{\oplus n} \simeq \{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \mid a_i \in G\}$ and more generally as $\sum_{i=1}^{n} G_i \simeq \{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \mid a_i \in G_i\}$. Here $n = \infty$ works too.

57. g^i in $G = \langle g \rangle$ is a generator iff $\gcd(i, n) = 1$ where $i = |g|$. So for what n are there just two i relatively prime to n, or equivalently, when is $U(n) \simeq \mathbb{Z}_2$? This happens for $n = 3, 4, 6$.

70. Prove $D_8 \times D_3 \not\simeq D_6 \times D_4$. $D_8 \times D_4$ has an element of order 24, namely (r, r') where r and r' are the rotations by $2\pi/8$ and $2\pi/3$ respectively. This is because $|(r, r')| = \operatorname{lcm}(8, 3) = 24$. But the largest $|(a, b)|$ can be in $D_6 \times D_4$ is $\operatorname{lcm}(6, 4) = 12$.

72. For p and q odd primes, explain why $U(p^m q^n)$ is not cyclic. $U(p^m q^n) \simeq U(p^m) \oplus U(q^n) \simeq \mathbb{Z}_{(p-1)p^{m-1}} \oplus \mathbb{Z}_{(q-1)q^{n-1}}$. The largest order of an element of $U(p^m q^n)$ is thus $\operatorname{lcm}((p-1)p^{m-1}, (q-1)q^{n-1}) = \frac{(p-1)p^{m-1}(q-1)q^{n-1}}{\gcd((p-1)p^{m-1},(q-1)q^{n-1})}$. Since $2 \mid p - 1$ and $2 \mid q - 1$ we know that $\gcd((p-1)p^{m-1}, (q-1)q^{n-1}) \geq 2$ and thus $\operatorname{lcm}((p-1)p^{m-1}, (q-1)q^{n-1}) \leq \frac{(p-1)p^{m-1}(q-1)q^{n-1}}{2} < (p-1)p^{m-1}(q-1)q^{n-1} = \varphi(p^m q^n) = |U(p^m q^n)|$.

77. $U(7 \cdot 17) \simeq Z_6 \times \mathbb{Z}_{16}$. Let $(a, b) \in Z_6 \times \mathbb{Z}_{16}$, then $|(a, b)| = \operatorname{lcm}(|a|, |b|)$ but $|a| \mid 6$ and $|b| \mid 16$ and thus $\operatorname{lcm}(|a|, |b|) \mid \operatorname{lcm}(6, 16) = 48$ and thus $x^{48} = e$ for all $x \in Z_6 \times \mathbb{Z}_{16}$.

Similarly, $U(p \cdot q) \simeq \mathbb{Z}_{p-1} \times \mathbb{Z}_{q-1}$ and the order of any element of $\mathbb{Z}_{p-1} \times \mathbb{Z}_{q-1}$ must divide $\operatorname{lcm}(p - 1, q - 1)$ and thus $x^{\operatorname{lcm}(p-1,q-1)} = e$ and there is an $x \in \mathbb{Z}_{p-1} \times \mathbb{Z}_{q-1}$ so that $x^i \neq e$ for $i < \operatorname{lcm}(p - 1, q - 1)$.

78. $U(200) = U(2^3 5^2) \simeq U(2^3) \times U(5^2) \simeq \mathbb{Z}_{2^2} \times \mathbb{Z}_{5 \cdot 4} = \mathbb{Z}_4 \times Z_{20}$. $U(50) \times U(4) \simeq U(5^2) \times U(2) \times U(4) \simeq \mathbb{Z}_{5 \cdot 4} \times \mathbb{Z}_2 = \mathbb{Z}_2 \times \mathbb{Z}_{20}$. So $U(200) \not\simeq U(50) \times U(4)$.

$U_{50}(200) \simeq \mathbb{Z}_4$ being just $\{1, 51, 101, 151\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \not\simeq \mathbb{Z}_2 \simeq U(4)$.

These do not contradict the theorem since $\gcd(200, 50) \neq 1$.

79. Let $p > 2$ be prime. $U_p(p^n) = \{m \in U(p^n) \mid m \bmod p = 1\}$. So $U_p(p^n) = \{mp + 1 \mid mp + 1 < p^n\} = \{mp + 1 \mid m < p^{n-1}\}$. Since $U(p^n) \simeq \mathbb{Z}_{p^{n-1}(p-1)}$ is cyclic, we know $U_p(p^n)$ is cyclic of size p^{n-1} and thus is isomorphic to $\mathbb{Z}_{p^{n-1}}$.

80. Find the smallest integer so that $x^k = 1$ for $x \in U(100)$. $U(100) = U(2^2 \cdot 5^2) \simeq U(2^2) \times U(5^2) \simeq \mathbb{Z}_2 \times \mathbb{Z}_{20}$. $\operatorname{lcm}(2, 20) = 20$ so $x^{20} = 1$ for all $x \in U(100)$. (See 78 for a few more details.)

Ch 9: 9, 12, 18, 21, 35, 63, 64, 78, 82, 86

9. Suppose H has index 2, then for $a \in G$ so that $a \notin H$ we know $G - H = aH = Ha$. For $a \in H$, trivially, $aH = H = Ha$. Thus for any $a \in G$, $aH = Ha$ and so H is normal.

12. Let G be abelian and $H < G$, then $H \lhd G$ and $(aH)(bH) = (ab)H = (ba)H = (bH)(aH)$ so G/H is abelian.

18. Let $k \mid n$ we know $|k| = n/k$ and so $|\mathbb{Z}_k/\langle k \rangle| = k$, we also know that $\mathbb{Z}_n/\langle k \rangle$ is cyclic, so $\mathbb{Z}_k/\langle k \rangle \simeq \mathbb{Z}_k$.

We could use a later result

$$\mathbb{Z}_n/k\mathbb{Z}_n = (\mathbb{Z}/n\mathbb{Z})/(k\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/k\mathbb{Z} = \mathbb{Z}_k$$

More generally, if $K \triangleleft H \triangleleft G$, then

$$(G/K)/(H/K) \simeq G/H$$

21. If $a \in G$ has order pq, then $G = \langle a \rangle$ and G is cyclic. If there is no element of order qp, then take $a \in G$, then $|a|$ is p or q. Suppose $|a| = q$, then $G/\langle a \rangle$ is cyclic of order p, say $\langle b/\langle a \rangle \rangle = G/\langle a \rangle$.

Then $|ab| = pq$, for suppose $(ab)^i = a^i b^i = e$. If $p \not| i$, then $b^i\langle a \rangle \neq \langle a \rangle$ and so $b^i \notin \langle a \rangle$ and thus $b^i a^i \neq e$. So $p|i$, so $i = mp$. Suppose $b^p = a^j$, if $b^p = e$, then $b^i a^i = a^m \neq e$ unless $q|m$ and so $|ab| = pq$. If $b^p = a^j \neq e$, then a^j is a generator of $\langle a \rangle$ so if needs be, replace a with a^j so that $b^p = a$. But then $b^i = b^{pm} = a^m \neq e$ unless $q|m$. In this case $|b| = pq$.

35. Note that $\langle 3 \rangle \cap \langle 6 \rangle = \{1\}$ since $3^a = 6^b$ iff $a = b = 0$. $\langle 3 \rangle\langle 6 \rangle \cap \langle 10 \rangle = \{1\}$ since $3^a 6^b = 10^c$ iff $a = b = c = 0$. So G is the internal direct product.

The situation is different for H as $3^{-1}6^2 = 12^1$ so $\langle 12 \rangle \subseteq \langle 3 \rangle\langle 6 \rangle$.

63. Let G have two normal subgroups of order 3, say $\langle a \rangle$ and $\langle b \rangle$, then $H = \langle a \rangle\langle b \rangle$ is a subgroup of order 9, so $9 \mid |G|$ and thus $|G| \neq 24$.

64. Let G' be the subgroup of G generated by elements S of the form $x^{-1}y^{-1}xy$.

a. Let $g \in G'$ and $a \in G$, then $a^{-1}gag^{-1} \in S$ so $a^{-1}ga \in G'$ and we have $a^{-1}G'a \subseteq G'$ so G' is normal in G.

b. $(aG')(bG') = (ab)G' = (ba)G'$, since $(ba)^{-1}(ab) \in G'$, so G/G' is abelian.

c. If G/N is abelian, then for all $a, b \in G$, $(ab)N = (aN)(bN) = (bN)(aN) = (ba)N$ and so $(ba)^{-1}(ab) \in N$ and hence $S \subseteq N$ and thus $G' < N$.

d. The exact same argument we gave in (a), where we replace G' by H works.

78. $U(60) = U(4 \cdot 3 \cdot 5) = U(4) \times U(3) \times U(5) = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$. This has no element of order 8.

82. $U(80) = U(16 \cdot 5) = U(2^4) \times U(5) = U_5(80) \times U_{16}(80) = \{1, 11, 21, 31, 41, 51, 61, 71\} \times \{1, 17, 33, 49\} = \{1, 11, 41, 51\} \times \{1, 71\} \times \{1, 17, 33, 49\} \simeq \mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_4 = \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_4$.

So the internal direct product is $\langle 11 \rangle\langle 71 \rangle\langle 17 \rangle$.

86. Let $H < G$ and define $N(H) = \{x \in G \mid xHx^{-1} = H\}$. $H \triangleleft N(H) < G$ and for $H \triangleleft K < G$, $K < N(H)$.

That $N(H)$ is closed under products and inverses is clear. That $H \triangleleft N(H)$ is also clear. Moreover, if $H \triangleleft K < G$, then $K < N(H)$ is clear.

Ch 10: 7 - 10, 24, 27, 46, 49, 50, 52, 56, 57, 61

7. $G \underset{\phi}{\to} H \underset{\sigma}{\to} K$. It is clear that $\sigma\phi : G \to K$ is a homomorphism, for example, $(\sigma\phi)(g_1 g_2) = \sigma(\phi(g_1 g_2)) = \sigma(\phi(g_1)\phi(g_2)) = \sigma(\phi(g_1))\sigma(\phi(g_2)) = (\sigma\phi)(g_1)(\sigma\phi)(g_2)$.

If ϕ and σ are onto, then $H \simeq G/\ker(\phi)$ and $K \simeq G/\ker(\sigma\phi) \simeq$ so

$$|G| = |K|[G : \ker(\sigma\phi)] = |H|[G : \ker(\phi)]$$

so

$$[\ker(\sigma\phi) : \ker(\phi)] = |\ker(\sigma\phi)|/|\ker(\phi)| = (|G|/|\ker(\phi)|)/(G/\ker(\sigma(\phi))|$$
$$= [G : \ker(\phi)]/[G : \ker(\sigma\phi)] = |H|/|K|$$

8. Let $G \leq S_n$ and define

$$\operatorname{sgn}(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd} \end{cases}$$

Clearly, $\operatorname{sgn}(\sigma_1\sigma_2) = \operatorname{sgn}(\sigma_1)\operatorname{sgn}(\sigma_2)$ and $\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma)^{-1}$, so sgn is a homomorphism. $\ker(\operatorname{sgn}) = A_n \cap G$. This shows that $\mathbb{Z}_2 \simeq G/(A_n \cap G)$ nd so $[G : A_n \cap G] = 2$.

9. $\pi_G : G \times H \to G$ given by $\pi_G((g, h)) = g$ is clearly a homomorphism. For example, $\pi_G((g_1, h_1)(g_2, h_2)) = \pi_G((g_1g_2, h_1h_2)) = g_1g_2 = \pi_H((g_1, h_1))\pi_G((g_2, h_2))$. $\ker(\pi_G) = \{e_G\} \times H \simeq K$. So it makes sense to write, $(G \times H)/H = G$.

10. Let $G \leq D_n$ and define $\phi : G \to -1, 1 \simeq \mathbb{Z}_2$ by

$$\phi(x) = \begin{cases} 1 & \text{if } x \text{ is a rotation} \\ -1 & \text{if } x \text{ is a reflection} \end{cases}$$

Since rotation×rotation and reflection×reflection is a rotation, and reflection×rotation and rotation×reflection is a reflection ϕ is a homomorphism.

$\ker(\phi) =$ rotations.

24. Suppose $\phi : \mathbb{Z}_{50} \to \mathbb{Z}_{15}$ is a group homomorphism with $\phi(7) = 6$.

a. What is $\phi(x)$? Since $\gcd(7, 50) = 1$ we know that 7^{-1} exists in $U(50)$. Note that $50 - 7^2 = 1$ so $-7^2 \bmod 50 = 1$ and hence $7^{-1} = -7 = 43 \bmod 50$ so $43 \times 7 = 1 \mod 50$. $\phi(43 \cdot 7) = 43 \cdot \phi(7) \bmod 15 = 43 \cdot 6 \mod 15 = 3$ so $\phi(1) = 3$ and thus $\phi(x) = x \cdot 3 \bmod 15 = (x \bmod 15)(3) \bmod 15$. (As a check $\phi(7) = 7 \cdot 3 \bmod 15 = 21 \bmod 15 = 6$.)

b. $\operatorname{Img}(\phi) = \langle 3 \rangle = \{0, 3, 6, 9, 12\}$ (in $\mathbb{Z}_{15}$).

c. $\phi(x) = (x \bmod 15)(3) \bmod 15 = 0$ iff $5 \mid x \bmod 15$ so $\ker(\phi) = \langle 5 \rangle = \{0, 5, 10, 15, 20, 25, 30, 35, 40, 45\}$ (in $\mathbb{Z}_{50}$). As a "check" $|\mathbb{Z}_{50}|/|\ker(\phi)| = 50/10 = 5 = |\operatorname{Img}(\phi)|$.

d. $\phi^{-1}(12) = \{x \mid \phi(x) = 3x \bmod 15 = 12\} = 4 + \ker(\phi) = \{4, 9, 14, 19, 24, 29, 34, 39, 44, 49\}$.

27. Determine all homomorphisms $\phi : \mathbb{Z}_n \to \mathbb{Z}_n$. We have $n = 1 + \cdots + 1$ (n times) and so $\phi(n) = \phi(1) + \cdots + \phi(1)$ (n times) and so $\phi(n) = n \cdot \phi(1) \bmod n = \langle \phi(1) \rangle$. So for any $k \in \mathbb{Z}_n$ we define $\phi : \mathbb{Z}_n \to \langle k \rangle$ by $\phi(1) = k$ and $\phi(m) = m \cdot k \bmod n$.

Question What about characterizing homomorphisms $\phi : \mathbb{Z}_n \to \mathbb{Z}_m$? Notice that $\operatorname{Img}(\phi) \mid m$ and $|\ker(\phi)| \mid n$ so that $n = |\operatorname{Img}(\phi)||\ker(\phi)|$. So $|\operatorname{Img}(\phi)| \mid n$ as well! So the upshot is that $\phi(1) \mid \gcd(n, m)$. Is that the only condition?

46. Show that every homomorphic image of $\mathbb{Z}_m \times \mathbb{Z}_n$ has the form $\mathbb{Z}_s \times \mathbb{Z}_t$. Where $s \mid m$ and $t \mid n$. It is clear that $\phi((1, 0))$ and $\phi((0, 1))$ determines ϕ completely and we can pick any

$a \in \mathbb{Z}_m$ and $b \in \mathbb{Z}_m$ and set $\phi((1,0)) = a$ and $\phi((0,1)) = b$ and $\phi\mathbb{Z}_m\mathbb{Z}_n \to \langle a\rangle_{\mathbb{Z}_m} \times \langle b\rangle_{\mathbb{Z}_n} \simeq \mathbb{Z}_{|a|} \times \mathbb{Z}_{|b|}$. and we know $|a| \mid m$ and $|b| \mid n$.

49. If $K < G$ and $N \triangleleft G$, then

$$(KN)/N \simeq K/(K \cap N)$$

Notice $N \triangleleft KN$ and $K \cap N \triangleleft K$ since $N \triangleleft G$. So the claim "makes sense." Try defining $\phi : K \to KN/N$ by $\phi(k) = kN$.

This is clearly onto and well defined. It is a homomorphism since $\phi(kk') = (kk')N = k(k'N \cdot N) = k(Nk')N = (kN)(k'N) = \phi(k)\phi(k')$. We have $\phi(k) = N \iff k \in N$ so that $\ker(\phi(= K \cap N)$. Thus we have $K/\ker(\phi) = K/(K \cap N) \simeq \text{Img}(\phi) = KN/N$.

50. Suppose $N \triangleleft M \triangleleft G$, then $(G/N)/(M/N) \simeq G/M$.

Define $\phi : G/N \to G/M$ by $\phi(g/N) = g/M$. Suppose $g/N = g'/N$, then $(g')^{-1}g \in N \subseteq M$ and so $(g')^{-1}g \in M$ and $g/M = g'/M$. So the map is well-defined. Since $\phi((g/N)(g'/N)) = \phi((gg')/N) = (gg')/M = (g/M)(g'/M) = \phi(g/N)\phi(g'/N)$.

Noe $\phi(g/N) = e/M$ iff $g/M = e/M$ iff $g \in M$ so $\ker(\phi) = M/N$ and we have

$$(G/N)/\ker(\phi) = (G/N)/(M/N) \simeq \text{Img}(\phi) = G/M$$

52. Let $k \mid n$ and $\phi : U(n) \to U(k)$ be given by $x \mapsto x \bmod k$. This is a homomorphism that is onto since if $\gcd(m,k) = 1$, then $\gcd(m,n) = 1$ and $\phi(m) = m$. $\ker(\phi) = \{m \in U(n) \mid \phi(m) = m \bmod k = 1\} = U_k(n)$.

56. Suppose $\mathbb{Z}_{10}$ and $\mathbb{Z}_{15}$ are homomorphic images of G, then $|G| = 10|N| = 15|M|$ where $N, M \triangleleft G$. One thing is that $30 \mid |G|$. In general, if H and K are homomorphic images of G, then $|H|, |K| \mid |G|$ so $\text{lcm}(|H|, |K|) \mid |G|$.

57. Suppose for all p prime, $\mathbb{Z}_p$ is a homomorphic image of G, then since $|G| = |\mathbb{Z}_p||\ker(\phi)| = p|\ker(\phi)|$, we have $p \mid |G|$. Thus G must be infinite. $\mathbb{Z}$ is an example as is $\sum_{i=1}^{\infty} \mathbb{Z}_p$.

61. Define $\phi : G \to \text{Inn}(G)$ by $\phi(g) = (\sigma_g : x \mapsto gxg^{-1})$. Then ϕ is a homomorphism by previous results and $\ker(\phi) = \{g \mid \sigma_g = \text{id}\}$ now $\sigma_g = \text{id}$ iff for all $x \in G$, $gxg^{-1} = x$ iff $g \in Z(G)$.

66. Suppose $H, K \triangleleft G$ with $H \cap K = \{e\}$. Prove that G is isomorphic to a subgroup on $G/H \oplus G/K$.

Define $\phi : G \to G/H \oplus G/K$ by $g \mapsto (gH, gK)$. This is a homomorphism since $\phi(gh) = (gHhH, gKhK) = (gH, gK)(hH, hK)$ and $\phi(e) = (eH, eK)$. Next, $g \in \ker(\phi) \iff (gH, gK) = (eH, eK)$, this means $g \in H \cap K$, but then $g = e$. So ϕ is one-one and thus $G \simeq \text{Img}(\phi)$.

Ch 11: 14 - 18, 33, 39

14. If G is abelian and $m = p_1p_2 \cdots p_k \mid |G|$ where $p_1, p_2, \ldots, p_k$ are **distinct** primes, then G has a cyclic subgroup of order m.

This follows since we know G is isomorphic to $\sum_i^m \mathbb{Z}_{q_i}^{n_i}$ where q_i are, not necessarily distinct, primes. We know that $p_i = q_{j_i}$ for some j_i and hence we can find a subgroup isomorphic to $\mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_k} \simeq \mathbb{Z}_{p_1p_2\cdots p_k}$.

15. Let's just tackle the final part. Suppose $|G| = p_1^{m_1} \cdots p_k^{m_k}$ where p_i are distinct primes and $m_i \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$.

Let $P(n)$ be the number of partitions of n, that is the number of ways of writing $n = n_1 + n_2 + \cdots + n_l$ where $n_1 \geq n_2 \geq \cdots \geq n_l \geq 1$. Then clearly, the number of such groups is $\prod_{i=1}^{k} P(m_i)$.

16. Using the $p(n)$ to be the number of partitions of n, then the number of abelian groups of order p^r is $p(r)$, then number of order $p^r q$ is $p(r)p(1) = p(r)$ (so no change), the number of order $p^r q^2$ is $p(r)p(2) = p(r)(2)$ (so twice the number).

17. For $|G| = 16$ and $x + x + x + x = 0$ to always be true, it must be that $|x| \in 2, 4$ so the factors must include one of order 2 or one of order 4. Thus $\mathbb{Z}_8 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbb{Z}_4$, $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ are the unique such abelian groups (up to isomorphism).

18. There are $p(4)^n$ many abelian groups of order $p_1^4 p_2^4 \cdots p_n^4$. $p(4) = 5^n$ (the partitions are: 4,31,22,21,1111)

33. If G is an abelian group of order 4 and $|a| = |b| = 4$ with $a^2 \neq b^2$, then $G \simeq \mathbb{Z}_4 \times \mathbb{Z}_4$. The only other option is $\mathbb{Z}_{16}$, but then the unique subgroup of order 4 in $\langle 4 \rangle$ and the only two generators are 4 and 12.

39. Say we have an abelian group of order $p_1^{m_1} \cdots p_k^{m_k}$ and each $m_i = m_{i,1} + \cdots + m_{i,l_i}$ where $m_{j,s} \geq m_{j,s+1} > 0$ is a partition of m_i so that

$$G \simeq \left(\mathbb{Z}_{{p_1}^{m_{1,1}}} \times \cdots \times \mathbb{Z}_{p_1^{m_{1,l_1}}}\right) \times \left(\mathbb{Z}_{{p_2}^{m_{2,1}}} \times \cdots \times \mathbb{Z}_{p_1^{m_{2,l_2}}}\right) \times \cdots \times \left(\mathbb{Z}_{{p_k}^{m_{k,1}}} \times \cdots \times \mathbb{Z}_{p_k^{m_{k,l_k}}}\right)$$

So we just need to find primes $q_{i,j}$ for $i = 1, \ldots, k$ and $j = 1, \ldots, l_i$ so that $p_i^{m_{i,j}} \mid q_{i,j} - 1$, that is $q_{i,j} = p_1^{m_{i,j}} \cdot t + 1$. Dirichlet's Theorem provides the needed primes $q_{i,j}$.