Homework 2 Solutions

Ch 4: 4, 13, 20, 23, 33, 48, 55, 71, 76, 78

4. $\langle 3\rangle = \{3, 6, 9, 12, 15, 17\}$ Since $\gcd(3, 15) = 3$ we know $\langle 15\rangle = \langle 3\rangle$. Similarly, $\langle a^3\rangle = \langle a^{15}\rangle = \{a^3, a^6, a^9, a^{12}, a^{15}, a^{17}\}$.

13. $a \in \langle 10\rangle \cap \langle 12\rangle$ iff $10 \mid a$ and $12 \mid a$ so $\langle 10\rangle \cap \langle 12\rangle$ is generated by $\mathrm{lcm}(10, 12) = 60$. similarly, $\langle a^{60}\rangle = \langle a^{10}\rangle \cap \langle a^{12}\rangle$.

20. D_n has n many two-element cyclic subgroups, the reflections, and one subgroup isomorphic to $\mathbb{Z}_n$, the rotations. For every divisor d of n, there will be one cyclic subgroup isomorphic to $\mathbb{Z}_d$. Thus D_{p^n} has $(n + 1) + n = 2n + 1$ cyclic subgroups and D_{qp} has $4 + pq$ many.

23. Clearly, $(ab)^{\mathrm{lcm}(|a|,|b|)} = e$ so $|ab| \le \mathrm{lcm}(|a|, |b|)$. If $|ab| = r < \mathrm{lcm}(|a|, |b|)$, then say $d = \mathrm{lcm}(|a|, |b|)$ and $d = qr + s$ where $0 \le s < r$, then

$$e = (ab)^d = (ab)^{qr+s} = ((ab)^r)^q (ab)^a = e^r (ab)^s = (ab)^s$$

So $(ab)^s = e$ and $0 \le s < r$, which contradicts the choice of r unless $s = 0$. So $r|d$.

If $\gcd(|a|, |b|) = 1$, then $\mathrm{lcm}(|a|, |b|) = |a| \cdot |b|$ suppose $r = r_a r_b$ where $r_a \mid |a|$ and $r_b \mid |b|$. Notice that $b^{-r_b} = a^{r_a}$ and if $|a| = r_a n_a$ and $|b| = r_b n_b$ and $n_a < n_b$, then

$$e = (a^{r_a})^{n_a} = (b^{-r_b})^{n_a} = (b^{r_b n_a})^{-1}$$

but this is a contradiction since $r_b r_a < r_b n_b = |b|$.

33. See the discussion in (20) above. The point is that if $d \mid n$, then there is a single cyclic subgroup of order d and that will have $\phi(d)$ many generators.

55. If an element of $\mathbb{C}$ satisfies $z^n = 1$, then z is an n^{th} root of unity and thus $z = \omega_n^k$ where $\omega_n = e^{\frac{2\pi}{n}}$. The elements $\{1, \omega_n, \omega_n^2, \ldots, \omega_n^{n-1}\}$ is a cyclic group with generator ω_n. Thus it has $\phi(n)$ many generators.

71. If $H < \langle a\rangle, \langle b\rangle$, then $|H| \mid \gcd(|a|, |b|) = \gcd(10, 24) = 2$. So the only options for $|H$ are 2 and 1.

76. If $|x| = n$ and $\langle x^r\rangle \subseteq \langle x^s\rangle \subseteq$, then $\langle x^{\gcd(r,n)}\rangle = \langle x^r\rangle \subseteq \langle x^s\rangle = \langle x^{\gcd(s,n)}\rangle \subseteq$ So we must have $\gcd(s, n) \mid \gcd(r, n)$ which reduces to just $\gcd(s, n) \mid r$.

78. $\langle r^1 5\rangle = \{e, r^{15}, r^{30}, r^{45}\} < D_{60}$. For the non-cyclic group use $\{e, r^{30}, f, r^{30} f\}$.

Ch 5: 3, 5, 9, 23, 25, 28, 43, 46, 57, 72

3. Write each given permutation as a product of disjoint cycles.

a.

$$(1,2,3,5)(4,1,3) = (1,5)(2,3,4)$$

b.

$$(1,3,2,5,6)(2,3)(4,6,5,1,2) = (1,2,4)(3,5)$$

c.

$$(1,2)(1,3)(2,3)(1,4,2) = (1,4)(2,3)$$

5. What is the order of each of the given permutations?

a. $|(124)(357)| = \operatorname{lcm}(3,3) = 3$

b. $|(124)(3567)| = \operatorname{lcm}(3,4) = 12$

c. $|(124)(35)| = \operatorname{lcm}(3,2) = 6$

d. $|(124)(357869)| = \operatorname{lcm}(3,6) = 6$

e. $|(1235)(24567)| = |(1243567)| = 7$

f. $|(345)(245)| = |(25)(34)| = \operatorname{lcm}(2,2) = 2$

9. Write $((14562)(2345)(136)(235))^{10}$ as a product of disjoint cycles.

$$((14562)(2345)(136)(235))^{10} = ((153)(46))^{10} = (153)^{10}(46)^{10} = (153)^9(153) = (153)$$

23. What are all possible orders of elements of S_6, A_6, A_7?

We just have to consider lists of lengths of disjoint sequences. For S_6 we have (6), (5, 1), (4, 2), (4, 1, 1), (3, 3), (3, 2, 1), (3, 1, 1, 1), (2, 2, 2), (2, 2, 1, 1), (2, 1, 1, 1, 1), and (1, 1, 1, 1, 1, 1). These have orders: 6, 5, 4, 3, 6, 3, 2, 2, 2, and 1.

Which of these are in A_6? (5, 1), (4, 2), (3, 3), (3, 1, 1, 1), (2, 2, 1, 1), (1, 1, 1, 1, 1, 1), so the orders are 5, 4, 3, 2, and 1.

A similar idea works for A_7. The permutations that are even are: (7), (5, 1, 1), (4, 2, 1), (3, 3, 1), (3, 2, 2), (2, 2, 1, 1, 1), (1, 1, 1, 1, 1, 1, 1) with orders, 7, 5, 4, 3, 6, 2, 1.

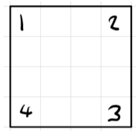
25. Let $\beta = (1,3,5,7,9,8,6)(2,4,10)$ what is the smallest integer so that $\beta^n = \beta^{-5}$? We have $|\langle\beta\rangle| = 21$ so $\beta^{-5} = \beta^{21-5} = \beta^{18}$, since $-5 = 21 - 5 = 16 \bmod 21$.

28. Suppose $H < S_n$ and $|H|$ is odd. Then no $h \in H$ can be odd, since if h is odd then $|h|$ even and $|h| \mid H$. To see that when h is odd, then $|h|$ is even, consider $h = c_1 c_2 \cdots c_k$ where these are disjoint cycles of length $n_1, n_2, \cdots, n_k$. For h to be odd we must have an odd number of even length cycles and thus $\operatorname{lcm}(n_1, \ldots, n_k) = |h|$ is even.

43. $\operatorname{stab}(a) \neq \emptyset$ since $e \in \operatorname{stab}(a)$. If $g, h \in \operatorname{stab}(a)$, then clearly $(gh)(a) = g(h(a)) = g(a) = a$ so $gh \in \operatorname{stab}(a)$. Also, $h^{-1}(a) = a$ so $h^{-1} \in \operatorname{stab}(a)$.

46. If α is an n-cycle, then $\langle\alpha\rangle$ is cyclic of order n so we know that $\langle\alpha^i\rangle = \langle\alpha^{\gcd(i,n)}\rangle$ and $|\alpha^i| = n/\gcd(i,n)$. So if $k \mid n$, then $\langle\alpha^k\rangle \simeq \mathbb{Z}_{n/k}$. (In the sense of Ch 6.)

57. We have $H = (1,2)(4,3)$, $R = (1,2,3,4)$ and the entire group is R^i and $R^i H$ for $i = 0,1,2,3$. Now $R^0, R^2, H, R^2 H$ are even.



72. This is a computation (perhaps not the best choice of a problem)

$$\begin{aligned}\sigma(4) * \sigma^2(5) * \sigma^3(7) * \sigma^4(2) * \sigma^5(3) &= (2 * 9) * (5 * 5) * 6 \\ &= (6 * 0) * 6 = 6 * 6 = 0\end{aligned}$$

The check digit is 0, since $0 * 0 = 0$

73. Show that every element off S_n can be written from $(1, k)$.

$$(n_1, n_2, \ldots, n_m) = (1, n_m)(1, n_{m-1}) \cdots (1, n_1)(1, n_m)$$

Just work this out:

$$(1,1)(n_1, n_2, n_3, \ldots, n_m)$$

Ch 6: 6, 15, 16, 18, 19, 31, 42, 43, 65, 75

6. This is sort of trivial, but also important.

The first thing is probably the most relevant, it says that if we preserve the operations, then the inverse automatically preserves the operations. Clearly, if $\phi : G \simeq H$, then $\phi^{-1} H \to G$ is a bijection. We must show that $\phi^{-1}(h_1 h_2) = \phi^{-1}(h_1)\phi^{-1}(h_2)$. For this we note that

$$\phi(\phi^{-1}(h_1)\phi^{-1}(h_2)) = \phi(\phi^{-1}(h_1))\phi(\phi^{-1}(h_2)) = h_1 h_2$$

and

$$\phi(\phi^{-1}(h_1 h_2)) = h_1 h_2$$

since ϕ is 1-1 it must be that $\phi^{-1}(h_1 h_2) = \phi^{-1}(h_1)\phi^{-1}(h_2)$. So $G \underset{\phi}{\simeq} H \implies H \underset{\phi^{-1}}{\simeq} G$. So symmetry holds.

If $G \underset{\phi}{\simeq} H \underset{\psi}{\simeq} K$, then $G \underset{\psi \circ \phi}{\simeq} K$. So transitivity holds.

Finally, $G \underset{\mathrm{id}}{\simeq} G$. So reflexivity holds.

15.

	H	V
ϕ_{R_0}	H	V
$\phi_{R_{90}}$	$R_{90} H R_{90}^{-1} = R_{90}^2 H = V$	H
ϕ_H	$HHH^{-1} = H$	$HVH^{-1} = R_{90} V = D'$
ϕ_D	$DHD^{-1} = R_{270} D = V$	$DVD^{-1} = R_{90} D = H$

16. Find G and H so that $G \not\simeq H$ but $\mathrm{Aut}(A) \simeq \mathrm{Aut}(H)$. The book provides examples in the theorem $\mathrm{Aut}(\mathbb{Z}_n) \sim U(n)$. For p prime $U(p) \sim \mathbb{Z}_{p-1}$ so for p prime $\mathrm{Aut}(Z_p) \simeq \mathbb{Z}_{p-1}$. It is true that $U(2p) \simeq \mathbb{Z}_{p-1}$. (See here.) The upshot is that for all prime p:

$$\mathbb{Z}_p \not\simeq \mathbb{Z}_{2p} \text{ and } \mathrm{Aut}(\mathbb{Z}_p) = U(p) = U(2p) = \mathrm{Aut}(\mathbb{Z}_{2p})$$

As a really simple case $\mathbb{Z}_3 \not\simeq \mathbb{Z}_6$, but $\mathrm{Aut}(\mathbb{Z}_3) = U(3) \simeq \mathbb{Z}_2 = U(6) = \mathrm{Aut}(\mathbb{Z}_6)$. Actually, $\mathrm{Aut}(\mathbb{Z}_4) \simeq U(4) \simeq \mathbb{Z}_2$.

18. If $G \simeq H$, then $\mathrm{Aut}(G) \simeq \mathrm{Aut}(G)$.

This is simple. Let $\phi : G \to H$ be an isomorphism and define $\Phi : \mathrm{Aut}(G) \to \mathrm{Aut}(H)$ by $\Phi(\psi)(h) = \phi(\psi(\phi^{-1}(h)))$. We must show that Φ preserves the group operations and is 1-1 and onto.

Preserves composition: Let $\psi_1, \psi_2 \in \mathrm{Aut}(G)$

$$\Phi(\psi_1 \circ \psi_2)(h) = (\phi \circ \psi_1 \circ \psi_2 \circ \phi^{-1})(h)$$

while

$$\begin{aligned}(\Phi(\psi_1) \circ \Phi(\psi_2))(h) &= \phi(\psi_1(\phi^{-1}(\Phi(\psi_2)(h)))) \\ &= \phi(\psi_1(\phi^{-1}(\phi(\psi_2(\phi^{-1}(h)))))) \\ &= (\phi \circ \psi_1 \circ \phi \circ \phi^{-1} \circ \psi_2 \circ \phi^{-1})(h) \\ &= (\phi \circ \psi_1 \circ \psi_2 \circ \phi^{-1})(h)\end{aligned}$$

Preserves inverses: This basically follows from the above.

Φ is one-to-one: If $\phi \circ \psi_1 \circ \phi^{-1} = \phi \circ \psi_2 \circ \phi^{-1}$, then by appropriately applying ϕ or ϕ^{-1} to each side we get $\psi_1 = \psi_2$.

Φ is onto: Let $\rho \in \mathrm{Aut}(H)$, then $\psi = \phi^{-1} \circ \rho \circ \phi \in \mathrm{Aut}(G)$ and clearly, $\Phi(\psi) = \rho$.

19. We have basically done this in previous homework.

31. Let $r \in U(n)$ and show that $\alpha : \mathbb{Z}_n \to \mathbb{Z}_n$ defined by $\alpha(n) = rm \bmod n$ is an automorphism.

$\alpha(m+k) = r(m+k) \bmod n = (rm+rk) \bmod n = (rm \bmod n) + (rk \bmod n) = \alpha(m) + \alpha(k)$. That $\alpha(-k) = -\alpha(k)$ is essentially the same. Suppose $\alpha(m) = \alpha(m')$, then $(rm - rm') = r(m - m') = 0 \bmod n$ but then $n \mid r(m - m')$ and as $r \in U(n)$, $n \mid m - m'$, so $m = m'$ and α is 1-1. Let $m \in \mathbb{Z}_n$, then $r(r^{-1}m) = m \bmod n$. So α is onto.

42. For $\mathbb{Z}_{15}$ consider $\alpha = (1, 2, 3, 4, 5)(6, 7, 8)$ which has order 15. $U(16) = \{1, 3, 5, 7, 9, 11, 13, 15\}$, or $|U(16)| = \phi(16) = 2^3(2 - 1) = 8$. So Cayley's Theorem suffices for this. D_8 is literally a subgroup of S_8, in fact $D_8 = \langle (0, 7)(1, 6)(2, 5)(3, 4), (0, 1, 2, 3, 4, 5, 6, 7) \rangle$.

43. This is pretty straightforward. $\phi : a + ib \mapsto \left[\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right]$.

$$(a+ib)(c+id) = (ac-bd) + i(ad+bc) \mapsto \begin{bmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{bmatrix} = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} c & -d \\ d & c \end{bmatrix}$$

$$(a+ib) + (c+id) \mapsto \begin{bmatrix} a+c & = (b+d) \\ b+d & a+c \end{bmatrix} = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} + \begin{bmatrix} c & -d \\ d & c \end{bmatrix}$$

The multiplicative inverse is interesting

$$z^{-1} = (a+ib)^{-1} = \frac{a-ib}{a^2+b^2} = \frac{\bar{z}}{\bar{z}z} \mapsto \frac{1}{a^2+b^2} \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}^{-1}$$

65. We have already seen that $D_n = \{e, r, \ldots, r^{n-1}, h, rh, \ldots, r^{n-1}h\}$. Any automorphism is determined by $h \mapsto r^i h$ and $r \mapsto r^k$ where $\gcd(k, n) = 1$. So there are $n \times \phi(n)$ many automorphisms.

75. Just map

$$\phi(\sigma) = \begin{cases} \sigma & \sigma \text{ even} \\ \sigma(n, n+1) & \sigma \text{ odd} \end{cases}$$

So

$$\begin{aligned} \phi(\sigma_1)\phi(\sigma_2) &= \begin{cases} \sigma_1(n, n+1)\sigma_2(n, n+1) & \sigma_1, \sigma_2 \text{ odd} \\ \sigma_1\sigma_2(n, n+1) & \sigma_1 \text{ even and } \sigma_2 \text{ odd} \\ \sigma_1(n, n+1)\sigma_2 & \sigma_1 \text{ odd and } \sigma_2 \text{ even} \\ \sigma_1\sigma_2 & \sigma_1, \sigma_2 \text{ even} \end{cases} \\ &= \begin{cases} \sigma_1\sigma_2 & \sigma_1, \sigma_2 \text{ odd} \\ \sigma_1\sigma_2(n, n+1) & \sigma_1 \text{ even and } \sigma_2 \text{ odd} \\ \sigma_1\sigma_2(n, n+1) & \sigma_1 \text{ odd and } \sigma_2 \text{ even} \\ \sigma_1\sigma_2 & \sigma_1, \sigma_2 \text{ even} \end{cases} \\ &= \phi(\sigma_1\sigma_2) \end{aligned}$$

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 $| < h_1 >< h_2 > | = 3^2 = 9 \nmid 15$.

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.