Homework 2 Solutions

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

4. $\langle 3\rangle = \{3, 6, 9, 12, 15, 18\}$ Since $\gcd(3, 15) = 3$ we know $\langle 15\rangle = \langle 3\rangle$. Similarly, $\langle a^3\rangle = \langle a^{15}\rangle = \{a^3, a^6, a^9, a^{12}, a^{15}, a^{18}\}$.

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 $\operatorname{lcm}(10, 12) = 60$. 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 $p^n + (n + 1)$ since p^n has $n + 1$ divisors $p^0, p^1, \cdots, p^n$ cyclic subgroups and D_{qp} has $pq + 4$ many since pq has divisors $1, p, q, pq$.

23. Clearly, $(ab)^{\operatorname{lcm}(|a|,|b|)} = e$ so $|ab| \mid \operatorname{lcm}(|a|, |b|)$. Note that commutativity of a and b is used here.

If $|ab| = r$, then $a^r b^r = e$ and so $a^r = b^{-r} \in \langle a\rangle \cap \langle b\rangle = \{e\}$, since $|\langle a\rangle \cap \langle b\rangle| \mid \gcd(|a|, |b|) = 1$. But this means that $a^r = e = b^r$ and so $|a| \mid r$ and $|b| \mid r$ and so $\operatorname{lcm}(|a|, |b|) \mid |ab|$.

Thus $\operatorname{lcm}(|a|, |b|) = |ab|$.

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.

48. Let G be abelian and $G^k = \{x^k \mid x \in G\}$. Let $g = a^k \in G^k$ and $h = b^k \in G^k$ for $a, b \in G$, then as G is commutative $(ab)^k = a^k b^k = gh$ so $gh \in G^k$. Similarly, $(a^k)^{-1} = (a^{-1})^k$. So G^k is a subgroup of G. Let us see that $G^k = G^{\gcd(k,n)}$, where $n = |G|$.

Let $g \in G^k$, then so $g = a^k$. Let $d = \gcd(k, n)$, then $k = md$ $a^k = (a^m)^d$ so $G^k \subseteq G^d$.

Now suppose $h = a^d \in G^d$, then $xk + yn = d$ for some $x, y \in \mathbb{Z}$. But then $h = a^d = (a^x)^k (a^n)^y = (a^x)^k$. So $h \in G^k$. So $G^d \subseteq G^k$.

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 $\langle x^r\rangle \subseteq \langle x^s\rangle$, then $\langle x^{\gcd(r,n)}\rangle = \langle x^r\rangle \subseteq \langle x^s\rangle = \langle x^{\gcd(s,n)}\rangle$ 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. $|(1\ 2\ 4)(3\ \ 57)| = \text{lcm}(3,3) = 3$

b. $|(1\ 2\ 4)(3\ 5\ 6\ 7)| = \text{lcm}(3,4) = 12$

c. $|(1\ 2\ 4)(3\ 5)| = \text{lcm}(3,2) = 6$

d. $|(1\ 2\ 4)(3\ 5\ 7\ 8\ 6\ 9)| = \text{lcm}(3,6) = 6$

e. $|(1\ 2\ 3\ 5)(2\ 4\ 5\ 6\ 7)| = |(1\ 2\ 4)(3\ 5\ 6\ 7)| = \text{lcm}(3,4) = 12$

f. $|(3\ 4\ 5)(2\ 4\ 5)| = |(2\ 5)(3\ 4)| = \text{lcm}(2,2) = 2$

9. Write $((1\ 4\ 5\ 6\ 2)(2\ 3\ 4\ 5)(1\ 3\ 6)(2\ 3\ 5))^{10}$ as a product of disjoint cycles.

$((1\,4\,5\,6\,2)(2\,3\,4\,5)(1\,3\,6)(2\,3\,5))^{10} = ((1\,5\,3)(4\,6))^{10} = (1\,5\,3)^{10}(4\,6)^{10} = (1\,5\,3)^{9}(1\,5\,3) = (1\,5\,3)$

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.

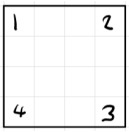
25. Let $\beta = (1,3,5,7,9,8,6)(2,4,10)$ what is the smallest integer so that $\beta^n = \beta^{-5}$? We have $|\langle\beta\rangle| = 21$ so $\beta^{-5} = \beta^{21-5} = \beta^{16}$, since $-5 = 21 - 5 = 16 \bmod 21$.

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 $h = c_1c_2\cdots c_k$ 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 $\text{lcm}(n_1, \ldots, n_k) = |h|$ is even.

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

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^iH for $i = 0,1,2,3$. Now R^0, R^2, H, R^2H 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 $(1,k)$. You know every $\sigma \in S_n$ can be written as $\sigma_1 \cdots \sigma_k$ where these are disjoint cycles. So, to argue that 2-cycles of the form $(1\ k)$ suffice, it is enough to show that any cycle can be written as a product of such 2-cycles. This works:

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

Just work this out, basically, with input n_i nothing happens until you hit $\cdots(1\ n_{i+1})(1\ n_i)\cdots$. Here you see that $n_i \mapsto 1 \mapsto n_{i+1}$ so $n_i \mapsto n_{i+1}$ and then nothing happens in the rest.

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 $\phi^{-1}(h_1h_2) = \phi^{-1}(h_1)\phi^{-1}(h_2)$. For this we note that

$$\phi(\phi^{-1}(h_1)\phi^{-1}(h_2)) = \phi(\phi^{-1}(h_1))\phi(\phi^{-1}(h_2)) = h_1h_2$$

and

$$\phi(\phi^{-1}(h_1h_2)) = h_1h_2$$

since ϕ is 1-1 it must be that $\phi^{-1}(h_1h_2) = \phi^{-1}(h_1)\phi^{-1}(h_2)$. 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, $G \underset{\text{id}}{\simeq} G$. So reflexivity holds.

15.

	H	V
ϕ_{R_0}	H	V
$\phi_{R_{90}}$	$R_{90}HR_{90}^{-1} = R_{90}^2H = V$	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

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