Homework #5 Solutions

p 83, #16. In order to find a chain

$$\langle a_1 \rangle \leq \langle a_2 \rangle \leq \cdots \leq \langle a_n \rangle$$

of subgroups of $\mathbb{Z}_{240}$ with n as large as possible, we start at the top with $a_n = 1$ so that $\langle a_n \rangle = \mathbb{Z}_{240}$. In general, given $\langle a_i \rangle$ we will choose $\langle a_{i-1} \rangle$ to be the largest proper subgroup of $\langle a_i \rangle$. We will make repeated use of the fundamental theorem of cyclic groups which tells us that a cyclic group of order m has a unique subgroup of order d for any $d|m$.

The largest proper subgroup of $\mathbb{Z}_{240}$ has size 120 and is $\langle 2 \rangle$. Since $|2| = 120$, the largest proper subgroup of $\langle 2 \rangle$ has size 60 and is $\langle 4 \rangle$. Since $|4| = 60$, the largest proper subgroup of $\langle 4 \rangle$ has size 30 and is $\langle 8 \rangle$. Since $|8| = 30$, the largest proper subgroup of $\langle 8 \rangle$ has order 15 and is $\langle 16 \rangle$. Since $|16| = 15$, the largest possible subgroup of $\langle 16 \rangle$ has order 5 and is $\langle 48$. Finally, since $|48| = 5$ is prime, the only proper subgroup of $\langle 48 \rangle$ is $\langle 0 \rangle$. Therefore, we have produced the maximal chain

$$\langle 0 \rangle \leq \langle 48 \rangle \leq \langle 16 \rangle \leq \langle 8 \rangle \leq \langle 4 \rangle \leq \langle 2 \rangle \leq \langle 1 \rangle$$

which has length 7. Notice that the chain

$$\langle 0 \rangle \leq \langle 120 \rangle \leq \langle 60 \rangle \leq \langle 30 \rangle \leq \langle 15 \rangle \leq \langle 5 \rangle \leq \langle 1 \rangle$$

also has length 7, but is produced in the opposite way, i.e. by starting with $\langle 0 \rangle$ and at each stage choosing $\langle a_{i+1} \rangle$ as the smallest subgroup containing $\langle a_i \rangle$.

p 83, # 20. Let $x \in G$. Since $x^{35} = e$, we know that $|x| = 1, 5, 7$ or 35. Since $|G| = 35$, if G contains an element x of order 35, then $G = \langle x \rangle$ as desired. On the other hand, if G contains an element x of order 5 and and element y of order 7, then, since G is abelian

$$(xy)^{35} = x^{35}y^{35} = ee = e$$

so that the order k of xy divides 35. That is, $|xy| = 5, 7$ or 35. If $|xy| = 5$ then

$$e = (xy)^5 = x^5y^5 = ey^5 = y^5$$

which means that $7 = |y|$ divides 5, a contradiction. Likewise, we have a similar problem if $|xy| = 7$. It follows that $|xy| = 35$, and as above that G is cyclic.

So, what we need to do is show that G *must* have an element of order 5 and an element of order 7. We argue by contradiction. If G has no elements of order 5 then every non-identity element of G has order 7. That is, there are 34 elements in G or order 7. However, by the corollary to Theorem 4.4, the number of elements in G of order 7 is divisible by $\phi(7) = 6$, and 34 is *not* divisible by 6. Likewise, if G had no element of order 7 then G would contain 34 elements of order 5, and this number would have to be divisible by $\phi(5) = 4$, which is also impossible. It follows that G must have at least one element of order 5 and at least one of order 7. As we pointed out above, this forces G to be cyclic.

This argument *does not* work if 35 is replaced by 33, because $33 = 3 \cdot 11$ and $\phi(3) = 2$ *does* divide $32 = 33 - 1$, and so we cannot eliminate the case that G consists only of elements of orders 1 or 3. Nevertheless, we will see later that every abelian group of order 33 is, indeed, cyclic.

p 84, # 36. ($\Rightarrow$) Suppose that G is the union of the proper subgroups H_i, for $i \in I$ (I is some indexing set). Let $a \in G$. Then there is an $i \in I$ so that $a \in H_i$, and by closure we have $\langle a \rangle \leq H_i$. Since $H_i \neq G$, it must be the case that $\langle a \rangle \neq G$. Since $a \in G$ was arbitrary, we conclude that G cannot be cyclic.

($\Leftarrow$) Now suppose that G is not cyclic. For any $a \in G$ we know that (1) $a \in \langle a \rangle$ and (2) $\langle a \rangle \neq G$. It follows that

$$G = \bigcup_{a \in G} \langle a \rangle$$

expresses G as the union of proper subgroups.

p 84, # 40. The proof of the fundamental theorem of cyclic groups shows that if $0 \neq H \leq \mathbb{Z}$ then $H = \langle a \rangle$ where a is the least positive integer in H. Since $H = \langle m \rangle \cap \langle n \rangle$ consists of all the integers that are common multiples of m and n, it must be the case that $H = \langle a \rangle$ where a is the least common multiple of m and n. That is

$$\langle m \rangle \cap \langle n \rangle = \langle \mathrm{lcm}(m, n) \rangle.$$

p 85, # 56. It is enough to show that $U(2^n)$ has two distinct elements of order 2, say a and b. For then $U(2^n)$ will have the non-cyclic subgroup $\{1, a, b, ab\}$.

Let $a = 2^n - 1$ and $b = 2^{n-1} - 1$. Since $n \geq 3$, we see that $a, b \neq 1$. So to show that a and b have order 2 in $U(2^n)$ we need only show that $a^2 \bmod 2^n = b^2 \bmod 2^n = 1$. Well

$$\begin{aligned} a^2 &= (2^n - 1)^2 = 2^{2n} - 2^{n+1} + 1 = 2^n(2^n - 2) + 1 \\ b^2 &= (2^{n-1} - 1)^2 = 2^{2n-2} - 2^n + 1 = 2^n(2^{n-2} - 1) + 1 \end{aligned}$$

which give the desired conclusion since $n > 2$.

p 85, # 60.

Proposition 1. *Let $|x| = n$. Then $\langle x^r \rangle \subset \langle x^s \rangle$ if and only if $(n, s)|(n, r)$*

Proof. ($\Rightarrow$) Suppose that $\langle x^r \rangle \subset \langle x^s \rangle$. Then $|x^r|$ divides $|x^s|$. Since $|x^r| = n/(n, r)$ and $|x^s| = n/(n, s)$, this means there is a k so that $kn/(n, r) = n/(n, s)$. That is, $k(n, s) = (n, r)$, which is what we sought to show.

($\Leftarrow$) Now suppose that $(n, s)|(n, r)$. Then, as above, we can show that $n/(n, r)|n/(n, s)$. Since $|x^s| = n/(n, s)$, the fundamental theorem of cyclic groups implies that $\langle x^s \rangle$ has a unique subgroup, H, of order $n/(n, r)$. But $n/(n, r)$ also divides $n = |x|$, so $\langle x^r \rangle$ is the unique subgroup of $\langle x \rangle$ of order $n/(n,r)$. Since H is a subgroup of $\langle x \rangle$ with this property, it must be the case that $\langle x^r \rangle = H \subset \langle x^s \rangle$.

$\square$

p 85, # 64. Let $x \in Z(G)$, $x \neq e$. By hypothesis, $|x| = p$, a prime. Let $y \in G$, $y \neq e, x^{-1}$. Then $|y| = q$ and $|xy| = l$, both primes. Since $x \in Z(G)$ we see that

$$e = (xy)^l = x^l y^l$$

so that

$$x^{-l} = y^l.$$

But $|x^{-l}| = |x^l| = p/(l,p)$ and $|y^l| = q/(l,q)$ and so

$$\frac{p}{(l,p)} = \frac{q}{(l,q)}.$$

or

$$p(l,q) = q(l,p).$$

Since l, p, q are prime, this is only possible if $p = q = l$. That is, for any $y \in G$, $|y| = p = |x|$.

p 92, # 34. Let H denote the unique nontrivial proper subgroup of G. Assume that G is not cyclic. Then for any $x \in G$, $x \neq e$, $\langle x \rangle = H$. That is, for any $x \in G$ we have $x \in H$, i.e.

$$G \leq H$$

which is impossible. Therefore G must be cyclic.

If $|G| = \infty$ then G has infinitely many subgroups, which is prevented by our hypotheses. It follows that $|G| = n$ for some $n \in \mathbb{Z}^+$. Since the subgroups of a cyclic group of order n correspond to the divisors of n, the only way G can have exactly one nontrivial proper subgroup is if n has exactly one nontrivial proper divisor. This can only occur if $n = p^2$, p prime.

Permutation Exercise 1. We must verify the 4 axioms that define a group.
0. *Closure.* Let $f, g \in A(S)$. Since f and g are both one-to-one and onto, it follows from general set theory that $f \circ g$ is also one-to-one and onto. Hence $f \circ g \in A(S)$ and so $A(S)$ is closed under composition.

1. *Associativity.* Let $f, g, h \in A(S)$. As above, it is a well known result in set theory that function composition is associative, i.e. $f \circ (g \circ h) = (f \circ g) \circ h$. This verifies that the operation in $A(S)$ is associative.

2. *Identity.* Define $1_S : S \to S$ by $1_S(x) = x$ for all $x \in S$. This is clearly one-to-one and onto and so $1_S \in A(S)$. Furthermore, 1_S serves as the identity in $A(S)$. To see this, let $f \in A(S)$. Then for any $x \in S$ we have

$$(f \circ 1_S)(x) = f(1_S(x)) = f(x) = 1_S(f(x)) = (1_S \circ f)(x).$$

Since $x \in S$ was arbitrary this shows that $f \circ 1_S = f = 1_S \circ f$, and since $f \in A(S)$ was arbitrary we have shown that 1_S is the identity in $A(S)$.

3. *Inverses.* Let $f \in A(S)$. Once again, general set theory tells us of the existence of a function $g \in A(S)$ with the property that $f(g(x)) = g(f(x)) = x$ for all $x \in S$. We claim that g is the inverse of f. For any $x \in S$ we have

$$1_S(x) = x = f(g(x)) = (f \circ g)(x)$$

so that $f \circ g = 1_S$. Similar reasoning shows that $g \circ f = 1_S$ as well, and so we conclude that g is the inverse of f.

Permutation Exercise 2. We apply the two-step subgroup test. Let $f \in G$. Since $f(a) = a$ we have

$$a = f^{-1}(f(a)) = f^{-1}(a)$$

so that $f^{-1} \in G$. If $g \in G$ as well, then $g(a) = a$ and so

$$(f \circ g)(a) = f(g(a)) = f(a) = a$$

which proves that $f \circ g \in G$. It follows that $G \leq A(S)$.

p 112, # 2.

Proposition 2. *The order of the k-cycle $\sigma = (a_1 a_2 \cdots a_k)$ is k.*

Proof. It is clear that $\sigma^k = \epsilon$. We must show that k is the smallest positive integer with this property. Since $\sigma^i(a_1) = a_{1+i}$ for any $1 \leq i \leq k-1$ and $a_j \neq a_1$ for $j \neq 1$, we see that $\sigma^i \neq \epsilon$ for any $1 \leq i \leq k-1$. It follows that $|\sigma| = k$. □

p 112, # 4. a. It is easy to see that the permutation in question is

$$(12)(356)$$

and since these cycles are disjoint the order is $\mathrm{lcm}(2, 3) = 6$.

b. In this case our permutation is

$$(1753)(264)$$

and since these cycles are disjoint the order is $\mathrm{lcm}(4, 3) = 12$.

p 113, # 18a. We see that

$$\alpha = (12345)(678)$$

and

$$\beta = (23847)(56)$$

and

$$\alpha\beta = (12345)(678)(23847)(56) = (12485736)$$

p 114, # 24. We know that the disjoint cycle structures of elements of S_7 correspond to partitions of 7, and that the lcm of the numbers in these partitions give the orders of the elements of S_7. To find the elements of order 5, therefore, we must find the partitions of 7 for which the lcm of the terms is 5. The only such partition is

$$7 = 5 + 1 + 1$$

and so the only elements of S_7 with order 5 must be the product of a 5-cycle and 2 1-cycles, all disjoint. Since 1-cycles are trivial, we conclude that the only elements in S_7 of order 5 are the 5-cycles. We now count these.

The number of 5-tuples of elements of $\{1, 2, 3, 4, 5, 6, 7\}$ is $7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 = 7!/2!$. Since a given 5-cycle corresponds to exactly 5 5-tuples (i.e. we can write a 5-cycle as starting with any one of its elements), we see that the number of 5-cycles in S_7 is

$$\frac{7!}{2!5} = 7 \cdot 6 \cdot 4 \cdot 3 = 504.$$

p 114, # 28. We first notice that

$$\beta = (14523)$$

which has order 5. Since 99 mod 5 = 4 we see that

$$\beta^{99} = \beta^4 = \beta^{-1} = (13254).$$

p 114, # 32. Since β is the product of two disjoint cycles of lengths 7 and 3, $|\beta| = \text{lcm}(3, 7) = 21$. Since the equation $\beta^n = \beta^{-5}$ is the same as $\beta^{n+5} = \epsilon$, and the smallest value for which the last equation holds satisfies $n + 5 = 21$, we must have $n = 21 - 5 = 16$.

p 114, # 36. Since (1234) has order 4, $H = \langle (1234) \rangle$ is a cyclic subgroup of order 4 in S_4. On the other hand, (12) and (34) both have order 2 and commute, so that $K = \{\epsilon, (12), (34), (12)(34)\}$ is a non-cyclic subgroup of order 4 in S_4.

p 114, # 46. Let $\sigma \in Z(S_n)$. Then for any $\tau \in S_n$ we have $\sigma\tau = \tau\sigma$ or, equivalently,

$$\sigma\tau\sigma^{-1} = \tau.$$

By carefully choosing τ we will show that $\sigma(i) = i$ for all $i \in \{1, 2, \ldots, n\}$, i.e. that $\sigma = \epsilon$.

We start by taking $\tau = (12)$. We have

$$(12) = \sigma(12)\sigma^{-1} = (\sigma(1)\,\sigma(2)),$$

the latter equality having been proven in class. This means that we must have $\sigma(1) = 1$ or 2. Since $n \geq 3$, we can also choose $\tau = (13)$ which yields

$$(13) = \sigma(13)\sigma^{-1} = (\sigma(1)\,\sigma(3))$$

so that $\sigma(1) = 1$ or 3. The only way this is compatible with our previous conclusion is if $\sigma(1) = 1$. Now fix any $i \in \{1, 2, \ldots, n\}$, $i \neq 1$. If we let $\tau = (1i)$ then we get

$$(1i) = \sigma(1i)\sigma^{-1} = (\sigma(1)\,\sigma(i)) = (1\,\sigma(i))$$

which tells us that $\sigma(i) = i$. We have therefore shown that $\sigma(i) = i$ for every $i \in \{1, 2, \ldots, n\}$. As we noted above, this means that $\sigma = \epsilon$, and it follows that $Z(S_n) = \{\epsilon\}$.