HOMEWORK 4 SOLUTIONS TO SELECTED PROBLEMS

1. Chapter 3, Problem 18 (Graded)

Let H and K be subgroups of G. Then e, the identity, must be in H and K, so it must be in $H \cap K$. Thus, $H \cap K$ is nonempty, so we can use either Theorem 3.1 or Theorem 3.2 (the one-step and two-step subgroup tests). *Be careful: before you can use the subgroup tests, you must show that the proposed subgroup is nonempty. This usually requires you to show that e is in the set.*

1.1. **Using the One-step Subgroup Test.** Let a and b be elements of $H \cap K$. Then a and b are in H, so $ab^{-1} \in H$ since H is a subgroup of G. Also, a and b are in K, so $ab^{-1} \in K$. Hence $ab^{-1} \in H \cap K$, and therefore, $H \cap K$ is a subgroup of G.

1.2. **Using the Two-step Subgroup Test.** Let a and b be elements of $H \cap K$. Then a and b are in H, so $ab \in H$ and $a^{-1} \in H$ since H is a subgroup of G. Also, a and b are in K, so $ab \in K$ and $a^{-1} \in K$. Hence $ab \in H \cap K$ and $a^{-1} \in H \cap K$, and therefore, $H \cap K$ is a subgroup of G.

1.3. **Intersections of More Than Two Subgroups.** Note that both proofs generalize to intersections of any number of subgroups. No matter what, we need to show e is in the intersection (which is true since it is in every subgroup) and when using the subgroup tests, we only look at two elements a and b in the intersection and use the fact that a and b are in each of the subgroups.

2. Chapter 3, Problem 20 (Graded)

Let $z \in C(a)$. Then

$$za = az$$

We want a similar equation, but with a replaced by a^{-1}. Multiply both sides by a^{-1} on the left:

$$a^{-1}za = a^{-1}az$$
$$a^{-1}za = z$$

Multiply both sides by a^{-1} on the right:

$$a^{-1}zaa^{-1} = za^{-1}$$
$$a^{-1}z = za^{-1}$$

In other words,

$$za^{-1} = a^{-1}z$$

Thus, z commutes with a^{-1}, so for any element $a \in G$, $C(a) \subseteq C(a^{-1})$.

In particular,

$$C(a^{-1}) \subseteq C((a^{-1})^{-1}) = C(a),$$

so $C(a) = C(a^{-1})$.

Alternatively, to prove $C(a^{-1}) \subseteq C(a)$, you could start with $z \in C(a^{-1})$:

$$a^{-1}z = za^{-1}$$

and multiplying both sides by a on the left, then multiplying both sides by a on the right to get

$$za = az.$$

3. Chapter 3, Problem 24 (Not Graded)

Let us use the contrapositive: let a and b be two (possibly equal) elements of a group, and suppose $a^2 = b^2$ and $a^3 = b^3$. We need to show that $a = b$. Remember that the negation of an "or" statement is an "and" statement.

Since $a^2 = b^2$, we can take the inverse of both sides to get

$$a^{-2} = b^{-2}.$$

Since $a^3 = b^3$, we will multiply the left side of the above equation by a^3 and the right side by b^3:

$$a^{-2}(a^3) = b^{-2}(b^3)$$
$$a^1 = b^1$$

Hence $a = b$.

4. Chapter 3, Problem 32 (Not Graded)

First, since n is even, in Z_n,

(1) An odd number plus an odd number is even (even if we need to reduce mod n).
(2) An odd number plus an even number is odd.
(3) An even number plus an even number is even.

This is because in order to determine the remainder mod n, we subtract a multiple of n from the sum. See the division algorithm on page 3 of the textbook with the sum as a, and $q = n$. Since n is even, $a - bn$ and a are either both odd or both even.

Let H be a subgroup of Z_n. Note that 0, the identity element, is in H. Now, either H has no odd elements, or H has at least one odd element. If H has at least one odd element, we need to prove that the number of odd elements in H equals the number of even elements (and hence half of the elements of H are even).

Since H has at least one odd element, let us call it a. Suppose there are j odd elements in H (including a) and there are k even elements in H (including 0).

Write the odd elements as

$$a = g_1, g_2, \ldots g_j.$$

What happens if we add a to each of these?

$$g_1 + a, g_2 + a, \ldots, g_j + a.$$

Note that these are j distinct elements: if $g_r + a = g_s + a$, then by canceling a, we get $g_r = g_s$. Furthermore, all j of them are even (since all of them are an odd number plus an odd number). Most importantly, all of them are in H, since H is a subgroup and hence is closed. So

$$g_1 + a, g_2 + a, \ldots, g_j + a$$

is a list of j distinct even elements in H. But it might not be all of them. Could there be even numbers in H which are not equal to a plus some odd number in H?

Still, at least we can say that j out of k even elements in H can be written as an odd element of H plus a. Hence

$$j \leq k.$$

Write the even elements as

$$0 = h_1, h_2, \ldots, h_k.$$

Let us add a to each of these:

$$h_1 + a, h_2 + a, \ldots, h_k + a.$$

Again, these are k distinct elements of H, and all of them are odd (even plus odd is odd). But there may be odd numbers in H which cannot be written as a plus an even number in H, so

$$k \leq j.$$

Therefore, $j = k$. That is, the number of odd elements in H equals the number of even elements in H.

5. Chapter 3, Problem 60 (Graded)

Let G be a finite group with more than one element. Then there is an element $a \in G$ with the following properties:

(1) $a \neq e$
(2) $|a|$ is finite (since $|G|$ is finite)
(3) $|a| > 1$ since $a \neq e$

Let $n = |a|$. Then $n > 1$, $a^n = e$ and $a^m \neq e$ for any integer $1 \leq m < n$.

The problem is that n might not be prime. But what will happen is that we will find a power of a which will have prime order.

Since $n > 1$, we can factor n as a product of primes:

$$n = p_1 p_2 \ldots p_{k-1} p_k.$$

Then

$$a^{(p_1 p_2 \cdots p_{k-1} p_k)} = e$$

5.1. **Using Theorem 4.2.** We can use Theorem 4.2 to determine the order of $a^{(p_1 p_2 \cdots p_{k-1})}$:

$$\left|a^{(p_1 p_2 \cdots p_{k-1})}\right| = |a| / \gcd\left(|a|, p_1 p_2 \ldots p_{k-1}\right)$$

$$|a| / \gcd\left(|a|, p_1 p_2 \ldots p_{k-1}\right) = n / \gcd(n, p_1 p_2 \ldots p_{k-1}) = n / \left(p_1 p_2 \ldots p_{k-1}\right) = p_k.$$

Hence

$$\left|a^{(p_1 p_2 \cdots p_{k-1})}\right| = p_k,$$

so $a^{(p_1 p_2 \cdots p_{k-1})}$ is an element with prime order p_k.

5.2. **Without Theorem 4.2.** We have

$$\left(a^{(p_1p_2\cdots p_{k-1})}\right)^{p_k} = a^{(p_1p_2\cdots p_{k-1}p_k)} = e,$$

so

$$\left|a^{(p_1p_2\cdots p_{k-1})}\right| \leq p_k.$$

Let q be an integer with $1 \leq q < p_k$. We need to show that

$$\left(a^{(p_1p_2\cdots p_{k-1})}\right)^{q} \neq e.$$

Since $0 < p_1p_2\ldots p_{k-1}q < p_1p_2\ldots p_{k-1}p_k$, we know

$$a^{(p_1p_2\cdots p_{k-1}q)} \neq e.$$

Thus,

$$\left(a^{(p_1p_2\cdots p_{k-1})}\right)^{q} = a^{(p_1p_2\cdots p_{k-1}q)} \neq e,$$

and therefore,

$$\left|a^{(p_1p_2\cdots p_{k-1})}\right| = p_k,$$

so $a^{(p_1p_2\cdots p_{k-1})}$ is an element with prime order p_k.

6. Chapter 4, Problem 22 (graded)

Let G be a group with three elements. One of them is the identity, e. Let us call the other two elements a and b. To prove that G is cyclic, we need to show that $G = \langle a\rangle$. (We could also show $G = \langle b\rangle$ as well. It turns out that $\langle a\rangle = \langle b\rangle$ in this problem).

Let us fill out a Cayley table. We can fill in the rows and columns for e first:

$\times$	e	a	b
e	e	a	b
a	a	?	?
b	b	?	?

Right now, we have $G = \{e, a, b\}$ and $\langle a\rangle = \{a, a^2, \ldots\}$. We need to prove that $a^2 = b$ and $a^3 = e$ in order to show $G = \langle a\rangle$.

First, we have $ae = a$ according to the Cayley table. Hence $a^2 \neq a$ (each element can only appear once in each row and column of the interior of the Cayley table) and $ab \neq a$. We also have $ab \neq b$ (b cannot appear twice in the same column). Hence $ab = e$. Similarly, $ba \neq b$ and $ba \neq a$, so $ba = e$:

$\times$	e	a	b
e	e	a	b
a	a	?	e
b	b	e	?

We can fill in the remaining entries since each element can only appear once in each row and column of the interior of the Cayley table:

$\times$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Hence $a^2 = b$, so $a^3 = a \cdot a^2 = ab = e$. Therefore, $G = \langle a\rangle = \{a, a^2, e\}$.

7. Chapter 4, Problem 42 (Not Graded)

Let G be a group with infinite order. If G has an element a of infinite order, then the subgroups $\langle a\rangle$, $\langle a^2\rangle$, $\langle a^3\rangle$,... are an infinite collection of subgroups of G.

However, it is possible that every element of G has finite order. We can proceed by contradiction. Suppose that G has a finite number of subgroups. Then it has a finite number of cyclic subgroups. Each cyclic subgroup has order equal to the order of its generator (by Corollary 1, page 74), and since every element of G has finite order, this means that all the cyclic subgroups have finite order (finitely many elements). So we have finitely many cyclic subgroups of finite order (basically, what could happen is that even though G has infinitely many elements, the cyclic subgroups the elements generate may overlap with each other so much that there is only finitely many of them). Let m be the total number of distinct cyclic subgroups ($m < \infty$). Let n be the order of the cyclic subgroup with the largest order.

If $a \in G$, then $a \in \langle a\rangle$. Hence

$$G \subseteq \bigcup_{a\in G} \langle a\rangle .$$

Therefore,

$$|G| \leq \left|\bigcup_{a\in G} \langle a\rangle\right| \leq m \cdot n < \infty.$$

$\left|\bigcup_{a\in G} \langle a\rangle\right|$ is bounded above by the number of cyclic subgroups (m) multiplied by the size of the largest cyclic subgroup (n).

This contradicts the fact that G has infinite order. Therefore, G has infinitely many cyclic subgroups (and hence infinitely many subgroups).

8. Chapter 4, Problem 52 (Graded)

$U(49)$ is a cyclic group with 42 elements. To determine the number of generators, we must count the number of elements in $U(49)$ whose order equals the order of the group, 42. By Theorem 4.4, page 79, the number of elements of order 42 in a cyclic group of order 42 is $\phi(42)$, the number of positive integers less than 42 and relatively prime to 42.

8.1. **The Function ϕ is Multiplicative in Certain Cases.** Since $42 = 6\cdot 7$, and $\gcd(6, 7) = 1$, $\phi(42) = \phi(6) \cdot \phi(7) = 2 \cdot 6 = 12$. Thus, $U(49)$ has 12 generators.

8.2. **Listing the Numbers Coprime to 42.** To determine which integers are coprime to 42, first factor 42 as a product of primes. It helps to list the primes in increasing order:

$$42 = 2 \cdot 3 \cdot 7$$

Now list the numbers from 1 to 41:

1	8	15	22	29	36
2	9	16	23	30	37
3	10	17	24	31	38
4	11	18	25	32	39
5	12	19	26	33	40
6	13	20	27	34	41
7	14	21	28	35	

First, cross out the numbers which are divisible by 2, the first prime which divides 42. Then cross out the numbers divisible by 3, and then cross out the numbers divisible by 7. The leftover numbers are coprime to 42. Count them, and that is $\phi(42)$.

1	~~8~~	~~15~~	~~22~~	29	~~36~~
~~2~~	~~9~~	~~16~~	23	~~30~~	37
~~3~~	~~10~~	17	~~24~~	31	~~38~~
~~4~~	11	~~18~~	25	~~32~~	~~39~~
5	~~12~~	19	~~26~~	~~33~~	~~40~~
~~6~~	13	~~20~~	~~27~~	~~34~~	41
~~7~~	~~14~~	~~21~~	~~28~~	~~35~~	

Leftovers: 1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41

$$\phi(42) = 12$$

Thus, $U(49)$ has 12 generators. Beware, the leftover numbers are not necessarily the generators!