Math 641 Abstract Algebra

Questions for Section 6: Cyclic Groups

1. State the Division Algorithm.
2. Apply the Division Algorithm using \( m = 15 \) and \( n = 200 \).

Remark: Questions 3 through 6 deal with Theorem 6.6.

3. In the second sentence, \( m \) is the smallest positive integer such that \( a^m \in H \). What guarantees the existence of \( m \)?
4. The goal is to show \( H = \langle a^m \rangle \). So let \( b \in H \) be given, and write \( b = a^n \). Want to show \( a^n = (a^m)^q \) somehow. Method: \( n = mq + r \) for some \( 0 \leq r < m \). Therefore \( a^n = a^{mq + r} \). Why does this imply \( a^r \in H \)?
5. Why does this imply \( r = 0 \)?
6. Why does this imply \( a^n = (a^m)^q \)?

Remark: Questions 7 through 11 deal with the greatest common divisor of two integers.

7. Fix \( r, s \in \mathbb{Z} \). Let \( H = \{ nr + ms : n, m \in \mathbb{Z} \} \). Name three elements in \( H \), given that \( r = 6 \) and \( s = 8 \).
8. Fix \( r, s \in \mathbb{Z} \). Let \( H = \{ nr + ms : n, m \in \mathbb{Z} \} \). Given that \( H \) is a subgroup of \( \langle \mathbb{Z}, + \rangle \), why can we say \( H = d\mathbb{Z} \) for some positive integer \( d \)?
9. Explain why \( d \) divides \( r \). Explain why \( d \) divides \( s \).
10. If \( k > 0 \) divides \( r \) and \( s \), explain why \( k \) divides \( d \).
11. Why does this imply that \( d \) is the smallest positive divisor of \( r \) and \( s \)?
12. Let \( G \) be a finite group generated by \( a \), and assume 4 is the smallest positive integer such that \( a^4 = e \). Describe the isomorphism between \( G \) and \( \langle \mathbb{Z}_4, +_r \rangle \).
13. Is it safe to say that \( G \cong \langle \mathbb{Z}_m, +_m \rangle \) whenever \( G \) is a finite group generated by \( a \) and \( m \) is the smallest positive integer such that \( a^m = e \)?

Remark: Questions 14 through 24 deal with Theorem 6.14

14. The hypotheses in Theorem 6.14 are that \( G = \langle a \rangle \), \( |G| = n \), and \( H = \langle a^r \rangle \). Why is \( n \) the order of \( a \)?
15. Suppose that \(a^k = e\) for some positive integer \(k\). Using the division algorithm, we can say that \(k = nq + r\) for some \(0 \leq r < n\). Why does this imply that \(a^r = e\)? Why does this in turn imply that \(r = 0\)? Why does \(r = 0\) imply that \(n\) divides \(k\)?

16. To compute \(|H|\), we must compute the order of \(a^s\). So we compute the list \(a^s, a^{2s}, a^{3s}, \ldots, a^{ms}\), where \(m\) is the first integer such that \(a^{ms} = e\). Why does this imply that \(m\) is the smallest positive integer such that \(n\) divides \(ms\)?

17. Our goal is to compute \(m\), the order of \(a^s\) and therefore the size of \(H\). Let \(d = \gcd(n, s)\). We know that \(d = un + vs\) for some integers \(u, v\), and we know \(d\) divides both \(n\) and \(d\), so we have \(1 = un_0 + vn_0\), where \(n_0 = \frac{n}{d}\) and \(s_0 = \frac{s}{d}\) are integers. Why does this imply that \(\gcd(n_0, s_0) = 1\)?

18. Why is \(\frac{ms}{n}\) equal to \(\frac{ms_0}{n_0}\)?

19. Why is \(\frac{ms_0}{n_0}\) an integer?

20. We know now that \(n_0\) divides \(ms_0\). Why does this imply that \(n_0\) divides \(m\)? (See page 62.)

21. We know by algebra that the smallest integer \(m\) such that \(n\) divides \(ms\) is the same as the smallest one such that \(n_0\) divides \(ms_0\). In other words, \(m\) is the smallest integer such that \(n_0\) divides \(m\). Why does this imply that \(m = n_0\)? Hence \(|H| = n_0 = \frac{n}{d} = \frac{n}{\gcd(n, s)}\).

22. If \(\langle a^s \rangle = \langle a^t \rangle\), then both subgroups have the same size. Why does this imply that \(\gcd(n, s) = \gcd(n, t)\)?

Conversely, knowing that \(s\) and \(t\) are two positive integers such that \(\gcd(n, s) = \gcd(n, t)\), how do we know that \(\langle a^s \rangle = \langle a^t \rangle\)? We will show in the next two questions that \(\langle a^p \rangle = \langle a^{\gcd(n, p)} \rangle\) for all \(p\), which will imply that \(\langle a^s \rangle = \langle a^{\gcd(n, s)} \rangle = \langle a^{\gcd(n, t)} \rangle = \langle a^s \rangle\).

23. Write \(\gcd(n, p) = d\). Then \(d\) divides \(p\). Why does this imply that \(a^p \in \langle a^d \rangle\)? Why does this in turn imply that \(\langle a^p \rangle \subseteq \langle a^d \rangle\)?

24. Given \(\gcd(n, p) = d\), we know that \(un + vp = d\) for some integers \(u\) and \(v\). Why does this imply that \(a^{up} = a^{d}\)? Why does this in turn imply that \(a^d \in \langle a^p \rangle\)? Therefore \(\langle a^d \rangle \subseteq \langle a^p \rangle\). Combining this with Question 23 we see that \(\langle a^p \rangle = \langle a^d \rangle = \langle a^{\gcd(n, p)} \rangle\).
Homework for Section 6 (only the starred problems will be graded):

1, 5, 11*, 18*, 19, 22*, 33, 35, 37, 45*, 55*

Hints:

11. If $s$ is a generator of $\langle \mathbb{Z}_{60}, +_{60} \rangle$ then $s$ has order 60. Using group notation, $s = 1 + 1 + 1 + \cdots = 1^s$. We know that 1 is a generator of $\langle \mathbb{Z}_{60}, +_{60} \rangle$. So the order of $s$ is $\frac{60}{\gcd(60, s)}$ by Theorem 6.14. This implies that $\gcd(60, s) = 1$. So the number of generators has to be the number of values of $s$ between 0 and 59 which satisfy $\gcd(60, s) = 1$.

18. As in Problem 11, we can write 30 = 1^{30} using group notation in $\langle \mathbb{Z}_{42}, +_{42} \rangle$. Now apply Theorem 6.14.

22. For each $k \in \mathbb{Z}_{12}$ compute $\langle k \rangle$. Many of the groups obtained will be the same, since the nature of the group depends only on $\gcd(12, k)$ (as we saw in Question 24). Now arrange the subgroups in a diagram similar to Figure 5.12, page 52.

45. Assume the group operation in $\mathbb{Z}$ is addition. Verify Conditions 1, 2, 3 of Theorem 5.14, page 52.

55. To show that $\langle \mathbb{Z}_p, +_p \rangle$ has no non-trivial subgroups means that every subgroup not equal to $\{0\}$ must be equal to $\mathbb{Z}_p$. We know that all the subgroups are cyclic and have the form $\langle a \rangle$ for some $a \in \mathbb{Z}_p$. You must show that if $a \neq 0$ then $a$ has order $p$. Write $a = 1^a$ in group notation. Use the formula for the order of $a$, combined with the fact that $p$ is a prime number, to show that $a$ has order $p$ when $a \neq 0$. 