Abstract Algebra **Thomas Judson** **Chapter 4 Exercises**

1. Prove or disprove each of the following statements.

(a) $U(8)$ is cyclic.

(b) All of the generators of $\mathbb{Z}_{60}$ are prime.

(c) $\mathbb{Q}$ is cyclic.

(d) If every proper subgroup of a group G is cyclic, then G is a cyclic group.

(e) A group with a finite number of subgroups is finite.

2. Find the order of each of the following elements.

(a) $5 \in \mathbb{Z}_{12}$

(b) $\sqrt{3} \in \mathbb{R}$

(c) $\sqrt{3} \in \mathbb{R}^*$

(d) $-i \in \mathbb{C}^*$

(e) 72 in $\mathbb{Z}_{240}$

(f) 312 in $\mathbb{Z}_{471}$

3. List all of the elements in each of the following subgroups.

(a) The subgroup of $\mathbb{Z}$ generated by 7

(b) The subgroup of $\mathbb{Z}_{24}$ generated by 15

(c) All subgroups of $\mathbb{Z}_{12}$

(d) All subgroups of $\mathbb{Z}_{60}$

(e) All subgroups of $\mathbb{Z}_{13}$

(f) All subgroups of $\mathbb{Z}_{48}$

(g) The subgroup generated by 3 in $U(20)$

(h) The subgroup generated by 5 in $U(18)$

(i) The subgroup of $\mathbb{R}^*$ generated by 7

(j) The subgroup of $\mathbb{C}^*$ generated by i where $i^2 = -1$

(k) The subgroup of $\mathbb{C}^*$ generated by $2i$

(l) The subgroup of $\mathbb{C}^*$ generated by $(1+i)/\sqrt{2}$

(m) The subgroup of $\mathbb{C}^*$ generated by $(1+\sqrt{3}\,i)/2$

4. Find the subgroups of $GL_2(\mathbb{R})$ generated by each of the following matrices.

(a) $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

(b) $\begin{pmatrix} 0 & 1/3 \\ 3 & 0 \end{pmatrix}$

(c) $\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$

(d) $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$

(e) $\begin{pmatrix} 1 & -1 \\ -1 & 0 \end{pmatrix}$

(f) $\begin{pmatrix} \sqrt{3}/2 & 1/2 \\ -1/2 & \sqrt{3}/2 \end{pmatrix}$

5. Find the order of every element in $\mathbb{Z}_{18}$.

6. Find the order of every element in the symmetry group of the square, D_4.

7. What are all of the cyclic subgroups of the quaternion group, Q_8?

8. List all of the cyclic subgroups of $U(30)$.

9. List every generator of each subgroup of order 8 in $\mathbb{Z}_{32}$.

10. Find all elements of finite order in each of the following groups. Here the "$*$" indicates the set with zero removed.

(a) $\mathbb{Z}$ (b) $\mathbb{Q}^*$ (c) $\mathbb{R}^*$

11. If $a^{24} = e$ in a group G, what are the possible orders of a?

12. Find a cyclic group with exactly one generator. Can you find cyclic groups with exactly two generators? Four generators? How about n generators?

13. For $n \leq 20$, which groups $U(n)$ are cyclic? Make a conjecture as to what is true in general. Can you prove your conjecture?

14. Let

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$

be elements in $GL_2(\mathbb{R})$. Show that A and B have finite orders but AB does not.

15. Evaluate each of the following.

(a) $(3 - 2i) + (5i - 6)$
(b) $(4 - 5i) - \overline{(4i - 4)}$
(c) $(5 - 4i)(7 + 2i)$
(d) $(9 - i)\overline{(9 - i)}$
(e) i^{45}
(f) $(1 + i) + \overline{(1 + i)}$

16. Convert the following complex numbers to the form $a + bi$.

(a) $2 \operatorname{cis}(\pi/6)$
(b) $5 \operatorname{cis}(9\pi/4)$
(c) $3 \operatorname{cis}(\pi)$
(d) $\operatorname{cis}(7\pi/4)/2$

17. Change the following complex numbers to polar representation.

(a) $1 - i$
(b) -5
(c) $2 + 2i$
(d) $\sqrt{3} + i$
(e) $-3i$
(f) $2i + 2\sqrt{3}$

18. Calculate each of the following expressions.

(a) $(1 + i)^{-1}$
(b) $(1 - i)^6$
(c) $(\sqrt{3} + i)^5$
(d) $(-i)^{10}$
(e) $((1 - i)/2)^4$
(f) $(-\sqrt{2} - \sqrt{2}\,i)^{12}$
(g) $(-2 + 2i)^{-5}$

19. Prove each of the following statements.

(a) $|z| = |\overline{z}|$
(b) $z\overline{z} = |z|^2$
(c) $z^{-1} = \overline{z}/|z|^2$
(d) $|z + w| \leq |z| + |w|$
(e) $|z - w| \geq ||z| - |w||$
(f) $|zw| = |z||w|$

20. List and graph the 6th roots of unity. What are the generators of this group? What are the primitive 6th roots of unity?

21. List and graph the 5th roots of unity. What are the generators of this group? What are the primitive 5th roots of unity?

22. Calculate each of the following.

(a) $292^{3171} \pmod{582}$

(b) $2557^{341} \pmod{5681}$

(c) $2071^{9521} \pmod{4724}$

(d) $971^{321} \pmod{765}$

23. Let $a, b \in G$. Prove the following statements.

(a) The order of a is the same as the order of a^{-1}.

(b) For all $g \in G$, $|a| = |g^{-1}ag|$.

(c) The order of ab is the same as the order of ba.

24. Let p and q be distinct primes. How many generators does $\mathbb{Z}_{pq}$ have?

25. Let p be prime and r be a positive integer. How many generators does $\mathbb{Z}_{p^r}$ have?

26. Prove that $\mathbb{Z}_p$ has no nontrivial subgroups if p is prime.

27. If g and h have orders 15 and 16 respectively in a group G, what is the order of $\langle g \rangle \cap \langle h \rangle$?

28. Let a be an element in a group G. What is a generator for the subgroup $\langle a^m \rangle \cap \langle a^n \rangle$?

29. Prove that $\mathbb{Z}_n$ has an even number of generators for $n > 2$.

30. Suppose that G is a group and let a, $b \in G$. Prove that if $|a| = m$ and $|b| = n$ with $\gcd(m, n) = 1$, then $\langle a \rangle \cap \langle b \rangle = \{e\}$.

31. Let G be an abelian group. Show that the elements of finite order in G form a subgroup. This subgroup is called the *torsion subgroup* of G.

32. Let G be a finite cyclic group of order n generated by x. Show that if $y = x^k$ where $\gcd(k, n) = 1$, then y must be a generator of G.

33. If G is an abelian group that contains a pair of cyclic subgroups of order 2, show that G must contain a subgroup of order 4. Does this subgroup have to be cyclic?

34. Let G be an abelian group of order pq where $\gcd(p, q) = 1$. If G contains elements a and b of order p and q respectively, then show that G is cyclic.

35. Prove that the subgroups of $\mathbb{Z}$ are exactly $n\mathbb{Z}$ for $n = 0, 1, 2, \ldots$.

36. Prove that the generators of $\mathbb{Z}_n$ are the integers r such that $1 \leq r < n$ and $\gcd(r, n) = 1$.

37. Prove that if G has no proper nontrivial subgroups, then G is a cyclic group.

38. Prove that the order of an element in a cyclic group G must divide the order of the group.

39. For what integers n is -1 an nth root of unity?

40. If $z = r(\cos\theta + i\sin\theta)$ and $w = s(\cos\phi + i\sin\phi)$ are two nonzero complex numbers, show that

$$zw = rs[\cos(\theta + \phi) + i\sin(\theta + \phi)].$$

41. Prove that the circle group is a subgroup of $\mathbb{C}^*$.

42. Prove that the nth roots of unity form a cyclic subgroup of $\mathbb{T}$ of order n.

43. Let $\alpha \in \mathbb{T}$. Prove that $\alpha^m = 1$ and $\alpha^n = 1$ if and only if $\alpha^d = 1$ for $d = \gcd(m, n)$.

44. Let $z \in \mathbb{C}^*$. If $|z| \neq 1$, prove that the order of z is infinite.

45. Let $z = \cos\theta + i\sin\theta$ be in $\mathbb{T}$ where $\theta \in \mathbb{Q}$. Prove that the order of z is infinite.

Programming Exercises.

(1) Write a computer program that will write any decimal number as the sum of distinct powers of 2. What is the largest integer that your program will handle?

(2) Write a computer program to calculate $a^x \pmod{n}$ by the method of repeated squares. What are the largest values of n and x that your program will accept?

References and Suggested Readings.

[1] Koblitz, N. *A Course in Number Theory and Cryptography.* 2nd ed. Springer, New York, 1994.

[2] Pomerance, C. “Cryptology and Computational Number Theory—An Introduction,” in *Cryptology and Computational Number Theory*, Pomerance, C., ed. Proceedings of Symposia in Applied Mathematics, vol. 42, American Mathematical Society, Providence, RI, 1990. This book gives an excellent account of how the method of repeated squares is used in cryptography.