Do the following exercises from Judson:
Chapter 4, Section 4.4: 7, 11, 14, 22 (b), (d); 30

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

► **Solution.** $Q_8 = \{\pm 1, \pm I, \pm J, \pm K\}$. The distinct cyclic subgroups are

- $\langle 1 \rangle = \{1\}$
- $\langle -1 \rangle = \{\pm 1\}$
- $\langle I \rangle = \langle -I \rangle = \{1, -1, I, -I\}$
- $\langle K \rangle = \langle -J \rangle = \{1, -1, K, -K\}$
- $\langle J \rangle = \langle -K \rangle = \{1, -1, J, -J\}$

◄

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

► **Solution.** If $a^k = e$, then the order of a divides k. Thus, the possible orders of a are the divisors of 24, that is, 1, 2, 3, 4, 6, 8, 12, 24. ◄

14. Let $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}$ be elements of $\mathrm{GL}_2(\mathbb{R})$. Show that A and B have finite orders, but AB does not.

► **Solution.** $A^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$, $A^3 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, $A^4 = (A^2)^2 = I$ so the order of A is 4.

$B^2 = \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix}$, $B^3 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ so the order of B is 3.

$AB = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$ and for each $n \in \mathbb{N}$, $(AB)^n = \begin{bmatrix} 1 & -n \\ 0 & 1 \end{bmatrix} \neq I$. Thus, the order of AB is infinite. ◄

22. (b) Calculate $2257^{341} \pmod{5681}$.

► **Solution.** Use repeated squares:

$$\begin{aligned}
2257^{2^1} &= 2257^2 \pmod{5681} &&= 5099 \\
2257^{2^2} &= 5099^2 \pmod{5681} &&= 3545 \\
2257^{2^3} &= 3545^2 \pmod{5681} &&= 653 \\
2257^{2^4} &= 653^2 \pmod{5681} &&= 334 \\
2257^{2^5} &= 334^2 \pmod{5681} &&= 3617 \\
2257^{2^6} &= 3817^2 \pmod{5681} &&= 5027 \\
2257^{2^7} &= 5027^2 \pmod{5681} &&= 1641 \\
2257^{2^8} &= 1641^2 \pmod{5681} &&= 87
\end{aligned}$$

Since $341 = 2^0 + 2^2 + 2^4 + 2^6 + 2^8$,

$$\begin{aligned}
2257^{341} &= 2257^{2^0+2^2+2^4+2^6+2^8} \pmod{5681} \\
&= 2257^{2^0} \cdot 2257^{2^2} \cdot 2257^{2^4} \cdot 2257^{2^6} \cdot 2257^{2^8} \pmod{5681} \\
&= 2257 \cdot 3545 \cdot 334 \cdot 5027 \cdot 87 \pmod{5681} \\
&= 2876 \pmod{5681}.
\end{aligned}$$

◀

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

▶ **Solution.** Use repeated squares after first reducing mod 765. $971 = 206 pmod 765$ so $971^{321} \pmod{765} = 206^{321} \pmod{765}$ and

$$\begin{aligned}
206^{2^1} &= 206^2 \pmod{765} && = 361 \\
206^{2^2} &= 361^2 \pmod{765} && = 271 \\
206^{2^3} &= 271^2 \pmod{765} && = 1
\end{aligned}$$

Thus, $206^{2^k} = 1 \pmod{765}$ for all $k \geq 3$. Since $321 = 2^0 + 2^6 + 2^8$ it follows that

$$\begin{aligned}
971^{321} &= 206^{321} \pmod{765} \\
&= 206^{2^0+2^6+2^8} \pmod{765} \\
&= 206^{2^0} \cdot 206^{2^6} \cdot 206^{2^8} \pmod{765} \\
&= 206 \cdot 1 \cdot 1 \pmod{765} \\
&= 206 \pmod{765}.
\end{aligned}$$

◀

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

▶ **Solution.** Let c be an arbitrary element of $\langle a \rangle \cap \langle b \rangle$. Then $c = a^k$ and the order of c divides the order m of a. Also, $c = b^l$ so the order of c divides the order n of b. Thus, the order of c is a common divisor of a and b and hence a divisor of the $\gcd(m, n) = 1$. Thus, the order of c is 1 and the only element with order 1 is the identity e, so that $c = e$. Since c was an arbitrary element of $\langle a \rangle \cap \langle b \rangle$ it follows that $\langle a \rangle \cap \langle b \rangle = \{e\}$. ◀

Exercises not from the text:

1. Find all generators of the cyclic group $G = \langle g \rangle$ if:

   (a) $|g| = 18$ (b) $|G| = \infty$

▶ **Solution.** (a) g^k is a generator of G if and only if $\gcd(k, 18) = 1$. Thus, the generators are g^k for $k \in \{1, 5, 7, 11, 13, 17\}$.

(b) The only generators are g and g^{-1}. ◀

2. Let $G = \langle g \rangle$ with $|g| = 24$. List all of the generators for the unique subgroup of G of order 8.

▶ **Solution.** The unique subgroup of G of order 8 is the cyclic subgroup $\langle g^3 \rangle$. The generators of this cyclic group are all of the powers $(g^3)^k$ where $\gcd(k\,8) = 1$. Thus, $k = 1, 3, 5, 7$ so the generators of $\langle g^3 \rangle$ are g^3, g^9, g^{15}, and g^{21}. ◀

3. In each case determine whether G is cyclic.

(a) $G = U(12)$ (b) $G = U(11)$

▶ **Solution.** (a) $U(12) = \{1, 5, 7, 11\}$ and $1^2 = 1$, $5^2 = 1$, $7^2 = 1$, and $11^2 = 1$ so all elements have order 2, and hence cannot generate all of $U(12)$. Thus, $U(12)$ is not cyclic.

(b) $U(11)$ is cyclic. In fact, $U(11) = \langle 2 \rangle$ since the powers of 2 modulo 11 fill up all of the 10 elements of $U(11) = \mathbb{Z}_{11} \setminus \{0\}$. ◀

4. Let $|g| = 18$ in a group G. Compute:

(a) $|g^8|$ (b) $|g^5|$ (c) $|g^3|$

▶ **Solution.** (a) $|g^8| = 18/\gcd(8, 18) = 18/2 = 9$.

(b) $|g^5| = 18/\gcd(5, 18) = 18$.

(c) $|g^3| = 18/3 = 6$. ◀

5. In each case find all the subgroups of $G = \langle g \rangle$ and draw the lattice diagram.

(a) $|g| = p^2$, where p is prime. **Answer:** $\langle e \rangle$, $\langle g^p \rangle$, $\langle g \rangle$.

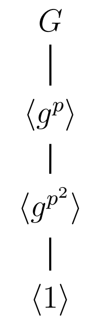
▶ **Solution.** Subgroups are $\langle 1 \rangle$, $\langle g^p \rangle$, $\langle g \rangle = G$. The subgroup diagram for G is

$$\begin{array}{c} G \\ | \\ \langle g^p \rangle \\ | \\ \langle 1 \rangle \end{array}$$

◀

(b) $|g| = p^3$, where p is prime. **Answer:** $\langle e \rangle$, $\langle g^{p^2} \rangle$, $\langle g^p \rangle$, $\langle g \rangle$.

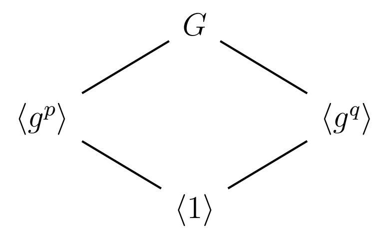
▶ **Solution.** Subgroups are $\langle 1\rangle$, $\langle g^{p^2}\rangle$, $\langle g^p\rangle$, $\langle g\rangle = G$. The subgroup diagram for G is



◀

(c) $|g| = pq$, where p and q are distinct primes. **Answer:** $\langle e\rangle$, $\langle g^p\rangle$,$\langle g^q\rangle$, $\langle g\rangle$.

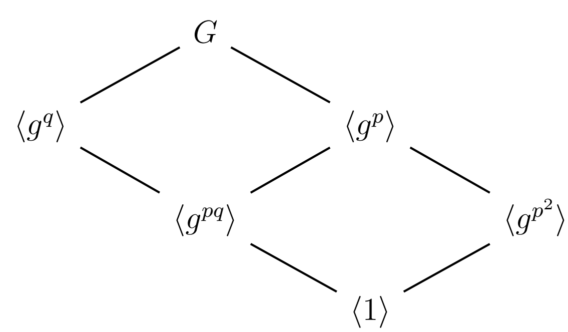
▶ **Solution.** Subgroups are $\langle 1\rangle$, $\langle g^p\rangle$, $\langle g^q\rangle$, $\langle g\rangle$. The subgroup diagram for G is



◀

(d) $|g| = p^2q$, where p and q are distinct primes. **Answer:** $\langle e\rangle$, $\langle g^{p^2}\rangle$, $\langle g^{pq}\rangle$, $\langle g^p\rangle$,$\langle g^q\rangle$, $\langle g\rangle$.

▶ **Solution.** Subgroups are $\langle 1\rangle$, $\langle g^{p^2}\rangle$, $\langle g^p\rangle$, $\langle g^q\rangle$, $\langle g^{pq}\rangle$, $\langle g\rangle$. The subgroup diagram for G is



◀

6. Let $|g| = 40$. List all of the elements of $\langle g\rangle$ that have order 10.

▶ **Solution.** Since the order of g^k is $40/\gcd(k, 40)$ we need all k with $\gcd(k, 40) = 4$. This is all integers of the form $4r$ where $\gcd(r, 40) = 1$. Hence $r = 1, 3, 7, 9$, so $k = 4$, 12, 28, 36. ◀

7. Prove that $H = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \middle| n \in \mathbb{Z} \right\}$ is a cyclic subgroup of $\mathrm{GL}_2(\mathbb{R})$.

   ▶ **Solution.** Let $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. Then $A \in \mathrm{GL}_2(\mathbb{R})$ since it is invertible because $A^{-1} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$. It is sufficient to show that $H = \langle A \rangle$. But for $n > 0$, $A^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$, which is easy to see by induction, and $A^{-n} = (A^{-1})^n = \begin{bmatrix} 1 & -n \\ 0 & 1 \end{bmatrix}$. Thus, H consists of all the powers of A, so it is a cyclic subgroup with generator A. ◀