Reading:

1. For this assignment: § 3.4 and 3.5 and class notes (Lectures 13-15).
2. For next week's classes: § 3.6.

Problems:

Problem 1: Recall Theorem 14.1 from class:

Theorem 14.1. *Let G be a finite cyclic group, $n = |G|$ and x a generator of G. Let $k \in \mathbb{Z}$. The following hold:*

   (i) *Every subgroup of G is cyclic and is equal to $\langle x^d \rangle$ where d is a positive divisor of n.*
   (ii) *If d and d' are distinct positive divisors of n, then $\langle x^d \rangle \neq \langle x^{d'} \rangle$*
   (iii) *x^k is a generator of G $\iff$ $gcd(n, k) = 1$.*
   (iv) *$\langle x^k \rangle = \langle x^d \rangle$ where $d = gcd(n, k)$*
   (v) *$o(x^k) = n/gcd(n, k)$*

Part (iv) was proved in class. The goal of this problem is to prove the other parts. Note that parts (i)-(iii) are proved in the book, but in this problem you are asked to give slightly different proofs, following the outline given below.

First use the definition of the order from class to prove that if d is a positive divisor of n, then $o(x^d) = n/d$. Then use this fact, Corollary 13.2 from class (= Definition 3.22 from the book) and (iv) to prove (v).

Next prove the following lemma:

Lemma. *Let H be a finite group of order n and $y \in H$. Then y is a generator of H $\iff$ $o(y) = n$.*

Then use this lemma and (v) to prove (iii).

Next use Corollary 3.25 (from the book) and (iv) to prove (i). Finally, use (v) and Corollary 13.2 to prove (ii).

Problem 2:

   (a) List all generators of $(\mathbb{Z}_{12}, +)$ and $(\mathbb{Z}_{15}, +)$
   (b) List all subgroups of $(\mathbb{Z}_{12}, +)$ and $(\mathbb{Z}_{15}, +)$ (without repetitions)

Problem 3: (practice) Prove that the relation $\cong$ of "being isomorphic" is an equivalence relation (Claim 15.1 from class).

Hint: To prove that $\cong$ is symmetric, show that if $\varphi : G \to G'$ is an isomorphism, then the inverse map $\varphi^{-1} : G' \to G$ is also an isomorphism. Since the inverse of a bijection is a bijection, you only need to show that $\varphi^{-1}(uv) = \varphi^{-1}(u)\varphi^{-1}(v)$ for all $u, v \in G'$. To prove this, take any $u, v \in G'$,

and let $x = \varphi^{-1}(u), y = \varphi^{-1}(v)$. Then $\varphi(x) = u$ and $\varphi(y) = v$; at this point you can use the fact that φ is a isomorphism.

Problem 4:

(a) Let $G = (\mathbb{Z}_6, +)$ and $G' = (\mathbb{Z}_7^\times, \cdot)$. Prove that $G' \cong G$ and find an explicit isomorphism $\varphi : G \to G'$. **Hint:** Use Theorem 15.2 from class.

(b) (practice) Use map φ from (a) to show (explicitly) that the multiplication tables of G and G' can be obtained from each other by relabeling of elements.

Problem 5:

(a) Let $G = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in \mathbb{R} \right\}$. Prove that G is a subgroup of $GL_2(\mathbb{R})$.

(b) Let G be the group from part (a). Find an isomorphism φ from $(\mathbb{R}, +)$ to G (and prove that φ is an isomorphism).

(c) (bonus) $H = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R} \text{ and } a^2 + b^2 \neq 0 \right\}$ with matrix multiplication (note that H is a group by Problem 5 in Homework #6). Prove that H is isomorphic to $(\mathbb{C} \setminus \{0\}, \cdot)$ (nonzero complex numbers with multiplication).

Problem 6: Let G be a group from Problem 2 in Homework #5: $G = \mathbb{R} \setminus \{-1\}$ as a set, and the operation $*$ on G is defined by $x * y = xy + x + y$. Prove that $(G, *)$ is isomorphic to $(\mathbb{R} \setminus \{0\}, \cdot)$ and find an explicit isomorphism between those groups.

Problem 7: Let $\varphi : G \to G'$ be an isomorphism, and let $g \in G$.

(a) Prove by induction that $\varphi(g^n) = \varphi(g)^n$ for every $n \in \mathbb{N}$.

(b) Prove that if $n \in \mathbb{N}$, then $g^n = e_G$ if and only if $\varphi(g)^n = e_{G'}$ (where e_G is the identity element of G and $e_{G'}$ is the identity element of G'). **Hint:** Use (a) and the fact that an isomorphism must send identity element to identity element (Theorem 3.30 from the book).

(c) Use (b) to prove that $o(g) = o(\varphi(g))$ (Proposition 15.3 from class). Thus isomorphisms preserve orders of elements.

Problem 8: Let G be a group and $g, h \in G$.

(a) Prove that the elements $g^{-1}hg$ and h have the same order by direct computation.

(b) Now prove that $g^{-1}hg$ and h have the same order without any computations by using Problem 7(c) and Example 3 from Lecture 15.

(c) Prove that gh and hg have the same order. **Hint:** Use (a) (or (b)).

Hint for (a): Let $n = o(h)$, so that $h^n = e$. First show that $(g^{-1}hg)^n = e$ as well (if you do not see how to do this, start with $n = 2$, see the pattern, then generalize). Note that the equality $(g^{-1}hg)^n = e$ DOES NOT mean that $o(g^{-1}hg) = n$. It only means that $o(g^{-1}hg) \leq n = o(h)$ as there

could exist $m < n$ such that $(g^{-1}hg)^m = e$ as well. Show that the latter is impossible by contradicting the assumption $n = o(h)$.

Problem 9: Let D_8 be the octic group (the group of isometries of a square) and Q_8 the quaternion group defined in Exercise 3.1.34.

    (a) Find the order of each element in both D_8 and Q_8.

    (b) Prove that D_8 and Q_8 are not isomorphic. **Hint:** Use Problem 7(c).

Note: If you are using 7th edition, replace Corollary 3.25 by Corollary 3.21, Definition 3.22 by Definition 3.18 and Exercise 3.1.34 by Exercise 3.1.28.