I.3. Cyclic Groups

1. Let $a, b \in G$. Show that $|a| = |a^{-1}|$, $|ab| = |ba|$ and for any $c \in G$, $|a| = |cac^{-1}|$.

**Proof** We only present the proof when the orders of the elements involved are finite. The case when they are infinite can be discussed similarly.

Let $m = |a|$ and $n = |a^{-1}|$. From $a^m = e$, we have $e = (a^{-1})^m$ by multiplying $(a^{-1})^m$ both sides. Thus $n|m$. (Therefore, if $m < \infty$, then $n < \infty$ as well). By symmetry, $m|n$ and so $m = n$.

Now let $s = |ab|$ and $t = |ba|$. By the definition of order, and by associative law, we have $a(ba)^{s-1}b = (ab)^s = e$. It follows that $(ba)^s = b(a(ba)^{s-1})b^{-1} = beb^{-1} = e$, and so $t|s$. (Therefore, if $s < \infty$, then $t < \infty$ as well). By symmetry, $t|s$ also.

Finally, let $a' = ac^{-1}$ and $b' = c$. By what we have just shown, $|a| = |a'b'| = |b'a'| = |cac^{-1}|$.

3. Let $G$ be an Abelian group of order $pq$ with $(p, q) = 1$. Show that $G$ is cyclic if and only if there exist elements $a, b \in G$ such that $|a| = p$ and $|b| = q$.

**Proof**: Suppose that $G = \langle x \rangle$. Then $|x| = |G| = pq$. Let $a = x^q$ and $b = x^p$. Then

$$|a| = |x^q| = \frac{pq}{(pq, q)} = p \quad \text{and} \quad |b| = |x^p| = \frac{pq}{(pq, p)} = q.$$ 

Conversely, assume the existence of such elements $a$ and $b$. Let $x = ab$ and $n = |x|$. Since $G$ is Abelian, $x^{pq} = (ab)^{pq} = (a^p)^q(b^p)^{p} = e$, and so $n|(pq)$. Also, $a^n = a^n b^n (b^{-n}) = (ab)^n (b^{-1})^n = (b^{-1})^n$. Note that (by Ex. I-3.1) $|b^{-1}| = |b| = q$. It follows that $|a^n| = p/(p, n)$ and $|(b^{-1})^n| = q/(n, q)$, and so $p(n, q) = q(n, p)$. Since $(p, q) = 1$, we must have $p|(n, p)$, and so $p|n$. By symmetry, $q|n$ also, and so by $(p, q) = 1$, $(pq)|n$. Together with $n|(pq)$, we have $n = pq$, and so $G = \langle x \rangle$.

4. If $f : G \to H$ is a homomorphism, $a \in G$, and $f(a)$ has finite order in $H$, then $|a|$ is infinite or $|f(a)|$ divides $|a|$.

**Proof**: Let $n = |f(a)|$. Assume that $|a| = m < \infty$. Then $a^m = e_G$. Since $f$ is a homomorphism, $f(e_G) = e_H$, and so $(f(a))^m = f(a^m) = f(e_G) = e_H$. Thus $n|m$. 

1
7. Let \( p \) be prime and \( H \) a subgroup of \( \mathbb{Z}(p^\infty) \).

(a) Every element of \( \mathbb{Z}(p^\infty) \) has finite order \( p^n \) for some \( n \geq 0 \).
(b) If at least one element of \( H \) has order \( p^k \) and no element of \( H \) has order greater than \( p^k \), then \( H \) is the cyclic subgroup generated by \( 1/p^k \), whence \( H \cong \mathbb{Z}_{p^k} \).
(c) If there is no upper bound on the orders of elements of \( H \), then \( H = \mathbb{Z}(p^\infty) \).
(d) The only proper subgroup of \( \mathbb{Z}(p^\infty) \) are the finite cyclic groups \( C_n = \langle 1/p^k \rangle \), \( (n = 1, 2, \ldots) \). Furthermore, \( \langle 0 \rangle = C_0 < C_1 < C_2 < \cdots \).

(c) As shown above, if \( (a, p) = 1 \), then \( \frac{a}{p} \) is an element of \( \mathbb{Z}_p \). Therefore, if for any integer \( N \), there is an element \( \frac{a}{p^k} \) in \( H \) with \( (a, p) = 1 \) such that \( |\frac{a}{p^k}| = p^k > N \), then \( H \) must have a sequence of elements \( \frac{a_1}{p^{k_1}}, \frac{a_2}{p^{k_2}}, \ldots, \frac{a_n}{p^{k_n}}, \ldots \) such that \( k_1 < k_2 \cdots < k_n < \cdots \) and \( \lim_{n \to \infty} k_n = \infty \). As shown in the proof of Part (b), once \( \frac{a}{p^k} \in H \), then for each \( i \in \{1, 2, \ldots, k\} \), \( \frac{1}{p^i} \in H \). It follows that \( \{1/p^n | n \in \mathbb{N}^* \} \subseteq H \), and so by Ex. I-2.16, \( H = \mathbb{Z}(p^\infty) \).

(d) Let \( H \) be a subgroup of \( \mathbb{Z}(p^\infty) \). If \( |H| < \infty \), then the order of elements in \( H \) must
be bounded, and so by Part (b), there is an integer \( n \geq 0 \) such that \( H = C_n \). As when \( 0 \leq n < m, \frac{1}{p^m} \in C_m \) but \( \frac{1}{p^n} \notin C_n \), we have \( C_0 < C_1 < C_2 < \cdots \).

(e) Let \( H = \langle x_1, x_2, \cdots, x_k, \cdots \rangle \leq G \). Then
\[
H = \{ n_1 x_1 + n_2 x_2 + \cdots n_k x_k \mid k \in \mathbb{N}^*, n_1, n_2, \cdots, n_k \in \mathbb{Z} \}. \tag{1}
\]

Note that (Ex. I-2.16) \( \mathbb{Z}(p^\infty) = \langle \{ \frac{1}{p^k} \mid k \in \mathbb{N}^* \} \rangle \). Thus
\[
\mathbb{Z}(p^\infty) = \{ n_1 \frac{1}{p} + n_2 \frac{1}{p^2} + \cdots n_k \frac{1}{p^k} \mid k \in \mathbb{N}^*, n_1, n_2, \cdots, n_k \in \mathbb{Z} \}. \tag{2}
\]

It follows that a natural way to define a map \( f : H \rightarrow \mathbb{Z}(p^\infty) \) (hoping this map is an isomorphism) is to define, for each \( i \in \mathbb{N}^* \), \( f(x_i) = \frac{1}{p^i} \), and linearly extend it to the whole group \( H \):
\[
f(n_1 x_1 + n_2 x_2 + \cdots n_k x_k) = n_1 \frac{1}{p} + n_2 \frac{1}{p^2} + \cdots n_k \frac{1}{p^k}. \tag{3}
\]

However, the representation of elements in \( H \) given above is not unique. For example, when \( n = p + 1, nx_2 = x_1 + x_2 \), and so \( f(nx_1) \) may be equal to both \( \frac{n-2}{p} \) and \( \frac{1}{p} + \frac{1}{p^2} \).

Thus we must show that \( n \frac{2}{p} = \frac{1}{p} + \frac{1}{p^2} \) (in this case, it is easy). We prove a few claims first.

**Claim 1** \( |x_n| = p^n \) for each \( n \in \mathbb{N}^* \).

**Proof:** This follows from the assumption that \( |x_1| = p \) and the recurrence definition \( x_k = px_{k+1} \) for each \( k \). Assume that \( |x_k| = p^k \). Let \( s = |x_{k+1}| \). Then \( p^{k+1} x_{k+1} = p^k x_k = 0 \), and so \( s \) must be a factor of \( p^{k+1} \). Since \( p \) is a prime, \( s = p^i \) for some integer \( i \leq k + 1 \). If \( i \leq k \), then \( p^{i-1} x_k = p^i x_{k+1} = 0 \), and so \( |x_k| < p^k \), a contradiction. Hence \( s = p^{k+1} \).

**Claim 2** If \( p^b \mid (n' - n) \), then \( n' x_k = n x_k \) and \( f(n' x_k) = f(n x_k) \).

**Proof:** Claim 1 implies the first half of the statement. Write \( n' = mp^k + n \). Then \( f(n' x_k) = (n + p^k) \frac{1}{p^k} = n \frac{1}{p^k} = f(nx_k) \) (assuming that \( f \) is well-defined).

**Claim 3** If \( n' = np + n \), then \( n' x_k = m x_{k+1} + n x_k \), and \( f(n' x_k) = f(n x_k) + f(m x_{k+1}) \).

**Proof:** The first half statement follows from the definition of the \( x_n \)'s, and the second half follows from the definition of \( f \) (assuming that \( f \) is well-defined).

By Claims 1 and the first halves of Claims 2 and 3 (therefore we do not assume that \( f \) is well-defined yet), for any \( h \in H \), we can find integers \( k, n_1, n_2, \cdots, n_k \) such that \( |n_i| < p \) such that \( h = n_1 x_1 + n_2 x_2 + \cdots + n_k x_k \), called the **reduced form** of \( h \). **Remark:** Even in
reduced forms, the presentation of \( h \in H \) is not unique. For example, when \( p = 3 \), then
\[
x_1 - x_2 - x_3 = 3x_2 - x_2 - x_3 = 2x_2 - x_3 = x_2 + 3x_3 - x_3 = x_2 + 2x_3.
\]

**Claim 4** If \( h = n_1x_1 + n_2x_2 + \cdots n_kx_k \in H \) is in reduced form such that \( n_1/p + n_2/p_2 + \cdots + n_k/p^k \in \mathbb{Z} \), then \( h = 0 \), the additive identity of \( H \).

**Proof:** Note that \( \frac{n_1p^{k-1} + n_2p^{k-2} + \cdots + n_k}{p^k} \in \mathbb{Z} \) if and only if \( p^k| (n_1p^{k-1} + n_2p^{k-2} + \cdots + n_k) \).

However, as \( |n_i p^{k-i}| < p^{k-i+1}, |n_1p^{k-1} + n_2p^{k-2} + \cdots + n_k| < p^k \). Hence we must have \( n_1p^{k-1} + n_2p^{k-2} + \cdots + n_k = 0 \). However, since \( |n_2p^{k-2}| < p^{k-1}, |n_3p^{k-3}| < p^{k-2}, \cdots, |n_k| < p \), it follows that \( |n_2p^{k-2} + \cdots + n_k| \) is at most
\[
|n_2p^{k-2}| + \cdots + |n_k| < |n_2p^{k-2}| + \cdots + |n_{k-1}|p + p < \cdots < |n_2p^{k-2}| + p^{k-2} < p^{k-1},
\]
and so we must have \( n_1 = n_2 = \cdots = n_k = 0 \).

**Claim 5** Assume that \( h \in H \) such that \( h \) has two reduced forms,
\[
h = n_1x_1 + n_2x_2 + \cdots + n_kx_k = n'_1x_1 + n'_2x_2 + \cdots + n'_kx_k.
\]

We can write \( n'_k - n_k = \epsilon_k p + r_k \) where \( 0 \leq r_k < p \) and \( |\epsilon_k| \leq 1 \). Inductively, for \( i < k \), we can write \( n'_i - n_i + \epsilon_{i+1} = \epsilon_i + r_i \), where \( 0 \leq r_i < p \) and \( |\epsilon_i| \leq 1 \). Then \( r_1 = r_2 = \cdots = r_k = 0 \).

**Proof:** Note that
\[
(n'_1 - n_1)x_1 + (n'_2 - n_2)x_2 + \cdots + (n'_k - n_k)x_k = 0.
\]

Since \( |n_i| < p \) and \( |n'_i| < p \), we have \( |n'_i - n_i| \leq 2p - 2 \), and we can write \( n'_k - n_k = \epsilon_k p + r_k \) where \( 0 \leq r_k < p \) and \( |\epsilon_k| \leq 1 \). Inductively, for \( i < k \), write \( n'_i - n_i + \epsilon_{i+1} = \epsilon_i + r_i \), where \( 0 \leq r_i < p \) and \( |\epsilon_i| \leq 1 \). Thus writing the left hand side of the equality above in reduced form, we have
\[
r_1x_1 + r_2x_2 + \cdots + r_kx_k = 0,
\]
By Claim 4, \( r_1 = r_2 = \cdots = r_k = 0 \).

Now we are ready to show that \( f \) is well defined. Consider the generic case and assume that \( h \in H \) such that \( h \) has two reduced form,
\[
(n'_1 - n_1)x_1 + (n'_2 - n_2)x_2 + \cdots + (n'_k - n_k)x_k = 0. \tag{4}
\]
We need to show that
\[
\frac{(n'_1 - n_1)}{p} + \frac{(n'_2 - n_2)}{p} + \cdots + \frac{(n'_k - n_k)}{p^k} \in \mathbb{Z}. \tag{5}
\]
We argue by induction on $k$ to show that (4) implies (5). Suppose that $k = 1$. By Claim 5, (4) holds if and only if $n'_1 - n_1 = \pm p$, and so (5) holds trivially. Assume that we have (4), and that for smaller values of $k$, (4) implies (5).

By Claim 5, either $n'_k = n_k$, whence by induction, (5) holds; or $|n'_k - n_k| = p$. Without loss of generality, we assume that $n'_k = n_k + p$. By the recurrence definition of the $x_n$’s, (4) becomes,

$$ (n'_1 - n_1)x_1 + (n'_2 - n_2)x_2 + \cdots + (n'_{k-1} - n_{k-1} + 1)x_{k-1} = 0. $$

By induction,

$$ m = \frac{(n'_1 - n_1)}{p} + \frac{(n'_2 - n_2)}{p^2} + \cdots + \frac{(n'_{k-1} - n_{k-1} + 1)}{p^{k-1}} \in \mathbb{Z}. \quad (6) $$

But (6) implies that

$$ \frac{(n'_1 - n_1)}{p} + \frac{(n'_2 - n_2)}{p^2} + \cdots + \frac{(n'_k - n_k)}{p^k} = \frac{(n'_1 - n_1)}{p} + \frac{(n'_2 - n_2)}{p^2} + \cdots + \frac{(n'_{k-1} - n_{k-1})}{p^{k-1}} + \frac{p}{p^k} = m \in \mathbb{Z}. $$

This proves that $f$ is well-defined.

Note that (1) and (2) imply that $f$ is onto and Claim 4 shows that $\ker(f) = \{0\}$, which indicates that $f$ is an injection, while (3) indicates that $f$ is a homomorphism.