Exercise. Describe all homomorphisms from $\mathbb{Z}_{24}$ to $\mathbb{Z}_{18}$.

Solution. We need some preliminary discussion before we try to define the homomorphisms to try to figure out how they might look like. Let $f : \mathbb{Z}_{24} \to \mathbb{Z}_{18}$ be a homomorphism. For any integer $k \geq 0$ notice that

$$f(k \mod 24) = f((1 \mod 24) + \cdots + (1 \mod 24)) \quad \text{(added } k \text{ times)}$$

$$= f(1 \mod 24) + \cdots + f(1 \mod 24)$$

$$= k \cdot f(1 \mod 24).$$

It follows that a homomorphism $f$ is completely determined by the value $f(1 \mod 24)$. Write $f(1 \mod 24) = n \mod 18$ where $n$ is an integer such that $0 \leq n \leq 17$. Notice that

$$24n \mod 18 = 24f(1 \mod 24)$$

$$= f(24 \mod 24)$$

$$= f(0 \mod 24)$$

$$= 0 \mod 18.$$

since any homomorphism maps the identity to identity. So 18 must divide $24n$, so 3 must divide $4n$, hence 3 must divide $n$. So $n$ must be among 0, 3, 6, 9, 12, 15.

The above discussion suggests how we might want to define our homomorphisms. We find that any such homomorphism must send $(1 \mod 24)$ to $(3k \mod 18)$ for some $k = 0, 1, \cdots, 5$. It follows that there are at most 6 possible homomorphisms from $\mathbb{Z}_{24} \to \mathbb{Z}_{18}$, given by $f_0, f_1, \cdots, f_5$ where

$$f_k(r \mod 24) = 3kr \mod 18 \quad \text{(1)}$$

for $k = 0, 1, \cdots, 5$. First we need to check that for each of this $k$, equation (1) gives a well defined function from $\mathbb{Z}_{24}$ to $\mathbb{Z}_{18}$. To this end, let $r, r' \in \mathbb{Z}$ such that $r \mod 24 = r' \mod 24$. Then $(r - r')$ is a multiple of 24. So $(3kr - 3kr') = 3k(r - r')$ is a multiple of $3 \times 24 = 72$. In particular, $(3kr - 3kr')$ is a multiple of 18. It follows that $(3kr \mod 18)$ only depends on the congruence class of $r$ modulo 24. So indeed equation (1) gives us a well defined function from $\mathbb{Z}_{24}$ to $\mathbb{Z}_{18}$. Now we verify that for any $r, s \in \mathbb{Z}$, we have

$$f_k(r \mod 24 + s \mod 24) = f_k((r + s) \mod 24) = 3k(r + s) \mod 18$$

$$= 3kr \mod 18 + 3ks \mod 18$$

$$= f_k(r \mod 18) + f_k(s \mod 18).$$

So each $f_k$ is indeed a homomorphism from $\mathbb{Z}_{24}$ to $\mathbb{Z}_{18}$.

At the risk of repeating ourselves, we recall that if $f : \mathbb{Z}_{24} \to \mathbb{Z}_{18}$ is any homomorphism, then $f(1 \mod 18)$ must be of the form $(3k \mod 18)$ for some $k = 0, 1, \cdots, 5$ and that any homomorphism $f$ is determined completely by the value of $f(1 \mod 18)$. For $k = 0, 1, \cdots, 5$, we have constructed a homomorphism $f_k$ such that $f_k(1 \mod 18) = 3k \mod 18$. It follows that there are six homomorphisms from $\mathbb{Z}_{24}$ to $\mathbb{Z}_{18}$ and these are given by $f_0, f_1, \cdots, f_5$ as defined in equation (1). □
2.

If $m$ is an integer, then $m\mathbb{Z}$ denotes the set of all integer multiples of $m$.

2.1. **Lemma.** Let $m, n$ be nonzero integers and $r = \text{lcm}(m, n)$. Then $m\mathbb{Z} \cap n\mathbb{Z} = r\mathbb{Z}$.

*Proof.* Let $x \in m\mathbb{Z} \cap n\mathbb{Z}$. Then $x$ is a multiple of $m$ and $x$ is a multiple of $n$. Hence $x$ is a multiple of $r$. So $x \in r\mathbb{Z}$. So $m\mathbb{Z} \cap n\mathbb{Z} \subseteq r\mathbb{Z}$. On the other hand $r$ is a multiple of $m$ and $n$, so $r \in m\mathbb{Z} \cap n\mathbb{Z}$. So $r\mathbb{Z} \subseteq m\mathbb{Z} \cap n\mathbb{Z}$ since $m\mathbb{Z} \cap n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. □

2.2. **Lemma.** Let $G$ be a group and $a$ be an element of $G$. Then $\langle a^m \rangle = \{a^k : k \in m\mathbb{Z}\}$.

*Proof.* If $k \in m\mathbb{Z}$, then $k$ has the form $k = mt$ for some integer $t$, so $a^k = a^{mt} \in \langle a^m \rangle$. Thus $\{a^k : k \in m\mathbb{Z}\} \subseteq \langle a^m \rangle$. On the other hand, if $g \in \langle a^m \rangle$, then $g$ has the form $g = a^{ms}$ for some integer $s$. Let $k = ms$. Then $g = a^k$ and $k \in m\mathbb{Z}$. So $g \in \{a^k : k \in m\mathbb{Z}\}$. □

2.3. **Lemma.** Let $G$ be a group and $a \in G$. Then show that $\langle a^m \rangle \cap \langle a^n \rangle = \langle a^{\text{lcm}(m, n)} \rangle$.

*Proof.* Write $r = \text{lcm}(m, n)$. From the previous lemma, we have

\[
\langle a^m \rangle \cap \langle a^n \rangle = \{a^k : k \in m\mathbb{Z}\} \cap \{a^k : k \in n\mathbb{Z}\}
= \{a^k : k \in m\mathbb{Z} \cap n\mathbb{Z}\}
= \{a^k : k \in r\mathbb{Z}\}
= \langle a^r \rangle.
\]

Here the first and the final equality follows from lemma 2.2 and the third equality follows from lemma 2.1. □

The above is a rather straightforward proof. On the next page you will find a more elaborate argument which also ends up giving a proof of the same statement in a much more long winded manner. But along the way we prove a bunch of things which are of some importance in themselves.
All through the following discussion, let $G$ be a group and let $a$ be an element of $G$ of finite order $|a| = d$. If $m$ is an integer, we shall write $m' = \gcd(m,d)$. Recall from the text that $|a^m| = d/m'$.

2.4. **Lemma.** If $m$ and $n$ are relatively prime nonzero integers, then $(mn)' = m'n'$.

*Proof.* Note that $m'$ is a factor of $m$ and $n'$ is a factor of $n$. Since $m$ and $n$ are relatively prime, so are $m'$ and $n'$. Since $m'$ and $n'$ each divide $d$, it follows that $m'n'$ divides $d$. Since $(m/m')$ and $(n/n')$ are each relatively prime to $d$, so is the product $(m/m')(n/n')$. Writing $mn = (m'n')((m/m')(n/n'))$, we find that $\gcd(mn,d) = m'n'$.

2.5. **Lemma.** Let $k,n$ be nonzero integers. If $k$ is a multiple of $n$, then $\langle a^k \rangle \subseteq \langle a^n \rangle$.

*Proof.* We can write $k = nt$ for some $t \in \mathbb{Z}$. So $a^k = a^{nt} \in \langle a^n \rangle$. So $\langle a^k \rangle \subseteq \langle a^n \rangle$.

2.6. **Lemma.** Let $m$ be a nonzero integer, then $\langle a^m \rangle = \langle a^{\gcd(m,d)} \rangle$.

*Proof.* Note that $m$ is a multiple of $m'$, so lemma 2.5 implies $a^m \in \langle a^{m'} \rangle$. Conversely, we can write $m' = \alpha m + \beta a$ for some integers $\alpha, \beta \in \mathbb{Z}$. So
\[a^{m'} = a^{\alpha m + \beta a} = a^m \in \langle a^m \rangle.\]

2.7. **Lemma.**

(a) If $b \in \langle a \rangle$, then $|b|$ divides $|a|$.

(b) If $k,m$ are nonzero integers such that $a^k \in \langle a^m \rangle$, then $m' \mid k'$.

*Proof.* (a) We can write $b = a^t$ for some nonzero integer $t$. So $|b| = |a|/t'$ is a factor of $|a|$.

(b) By part (a), we have $|a^k|$ divides $|a^m|$, that is, $|a|/k'$ divides $|a|/m'$. So $m'$ divides $k'$.

2.8. **Lemma.** Let $m, n$ be relatively prime nonzero integers. Then $\langle a^m \rangle \cap \langle a^n \rangle = \langle a^{mn} \rangle$.

*Proof.* Write $H = \langle a^m \rangle \cap \langle a^n \rangle$. By lemma 2.5 we have $\langle a^{mn} \rangle \subseteq \langle a^m \rangle$ and $\langle a^{mn} \rangle \subseteq \langle a^n \rangle$. So $\langle a^{mn} \rangle \subseteq H$.

Notice that $H$ is a subgroup of the cyclic group $\langle a^m \rangle$, so $H$ is cyclic. So $H = \langle a^k \rangle$ for some nonzero integer $k$. Since $a^k \in \langle a^m \rangle$ and $a^k \in \langle a^n \rangle$, lemma 2.7(b) implies that $m' \mid k'$ and that $n' \mid k'$. Since $m'$ and $n'$ are relatively prime, we have $m'n' \mid k'$. So $k'$ is a multiple of $m'n' = (mn)l'$ by lemma 2.4 and lemma 2.5 implies that $\langle a^k \rangle \subseteq \langle a^{(mn)} \rangle$. Now we obtain $H = \langle a^k \rangle = \langle a^k \rangle \subseteq \langle a^{(mn)} \rangle = \langle a^{mn} \rangle$, where the second and the final equality follows from lemma 2.6.

2.9. **Lemma.** Let $m$ and $n$ be two nonzero integers and $l = \text{lcm}(m,n)$. Then $\langle a^m \rangle \cap \langle a^n \rangle = \langle a^l \rangle$.

*Proof.* Since $a^{-m}$ and $a^m$ generate the same subgroup, without loss, we may assume that $m$ is a positive integer and similarly, that $n$ is a positive integer. Let $d = \gcd(m,n)$. Let $b = a^d$. Then $a^m = b^{m/d}$ and $a^n = b^{n/d}$. Now we have
\[\langle a^m \rangle \cap \langle a^n \rangle = \langle b^{m/d} \rangle \cap \langle b^{n/d} \rangle = \langle b^{mn/d^2} \rangle = \langle a^{mn/d} \rangle = \langle a^l \rangle\]
where the second equality follows from 2.8 since $(m/d)$ and $(n/d)$ are relatively prime and the last equality follows since $mn = dl$.
3. Sign of a permutation, even and odd permutations.

3.1. Definition. We want to define the “sign” of a permutation. We start with the polynomial \( P(x_1, \ldots, x_n) \) in \( n \) variables \( x_1, \ldots, x_n \) with \( n(n-1)/2 \) distinct linear factors \( (x_i - x_j) \) for \( 1 \leq i < j \leq n \). For example, if \( n = 4 \), then

\[
P(x_1, x_2, x_3, x_4) = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4).
\]

Let \( \alpha \in S_n \) be any permutation. Say that a pair \((i, j)\) is a crossing pair for \( \alpha \) if \( (i < j) \) and \( (\alpha^{-1} > \alpha^{-1}(j)) \), that is, when we represent \( \alpha \) in the form \( \left(1 \frac{1}{\alpha(2)} \cdots \frac{1}{\alpha(n)}\right) \) then in the second row “\( i \) is sitting under a bigger number than \( j \)”, that is, “\( i \) is sitting to the right of \( j \)”. Let \( N(\alpha) \) be set of crossing pairs for \( \alpha \)

\[
N(\alpha) = \{(i, j) : 1 \leq i < j \leq n, \alpha^{-1}(i) > \alpha^{-1}(j)\}.
\]

The number \( |N(\alpha)| \) is called the number of crossings of \( \alpha \).

Claim: The polynomial \( P(x_{\alpha(1)}, \ldots, x_{\alpha(n)}) \) also has \( n(n-1)/2 \) distinct linear factors. Upto a plus or minus sign, these factors are same as the factors of \( P(x_1, \ldots, x_n) \). More precisely, for each \( 1 \leq i < j \leq n \), either \((x_i - x_j)\) or \((x_j - x_i)\) is a factor of \( P(x_{\alpha(1)}, \ldots, x_{\alpha(n)}) \), but not both. If \((i, j) \notin N(\alpha)\), then \((x_i - x_j)\) is a factor, otherwise \((x_j - x_i)\) is a factor.

Proof of claim: Pick a pair \( i, j \) such that \( 1 \leq i < j \leq n \). Suppose \((i, j) \notin N(\alpha)\). Then \( \alpha^{-1}(i) < \alpha^{-1}(j) \), so \((x_{\alpha^{-1}(i)} - x_{\alpha^{-1}(j)})\) is a factor of \( P(x_1, \ldots, x_n) \). So \((x_{\alpha(\alpha^{-1}(i))} - x_{\alpha(\alpha^{-1}(j))}) = (x_i - x_j)\) is a factor of \( P(x_{\alpha(1)}, \ldots, x_{\alpha(n)}) \). On the other hand, suppose \((i, j) \in N(\alpha)\). Then \( \alpha^{-1}(j) < \alpha^{-1}(i) \), so \((x_{\alpha^{-1}(j)} - x_{\alpha^{-1}(i)})\) is a factor of \( P(x_1, \ldots, x_n) \). So \((x_{\alpha(\alpha^{-1}(j))} - x_{\alpha(\alpha^{-1}(i))}) = (x_j - x_i)\) is a factor of \( P(x_{\alpha(1)}, \ldots, x_{\alpha(n)}) \).

Thus we find that for each \( i, j \) such that \( 1 \leq i < j \leq n \), either \((x_i - x_j)\) or \((x_j - x_i)\) is a factor of \( P(x_{\alpha(1)}, \ldots, x_{\alpha(n)}) \). This already gives \( n(n-1)/2 \) distinct factors which is equal to the degree of the polynomial, so each of these factors must occur just once and there cannot be any more factors.

3.2. Example. Let \( a = (\frac{1}{2} \frac{2}{4} \frac{3}{4} \frac{3}{1} \frac{4}{1}) \). So \( a^{-1} = (\frac{1}{2} \frac{2}{4} \frac{3}{4} \frac{4}{1} \frac{1}{1}) \). Then \( N(a) = \{(1, 2), (1, 4), (3, 4)\} \) and \( P(x_{\alpha(1)}, x_{\alpha(2)}, x_{\alpha(3)}, x_{\alpha(4)}) = (x_2 - x_4)(x_2 - x_3)(x_4 - x_4)(x_4 - x_3)(x_3 - x_3) \) or \( P(x_{\alpha(1)}, \ldots, x_{\alpha(n)}) \). Observe that we get a contribution of \(-1\) for each crossing pair \((i, j)\).

From the claim above we find that the ratio \( P(x_{\alpha(1)}, \ldots, x_{\alpha(n)})/P(x_1, \ldots, x_n) \) is equal to either \(1\) or \(-1\). Define

\[
\text{sign}(\alpha) = \frac{P(x_{\alpha(1)}, \ldots, x_{\alpha(n)})}{P(x_1, \ldots, x_n)}.
\]

The number \( \text{sign}(\alpha) \) is called the sign of the permutation \( \alpha \).

3.3. Theorem. If \( \alpha, \beta \in S_n \), then \( \text{sign}(\alpha \beta) = \text{sign}(\alpha) \text{sign}(\beta) \), that is, the sign is multiplicative. In other words, the function \( \text{sign} : S_n \to \{-1, 1\} \) is a group homomorphism.

Proof. By definition of sign of a permutation, we have

\[
\text{sign}(\alpha \beta) = \frac{P(x_{\alpha(\beta(1))}, \ldots, x_{\alpha(\beta(n))})}{P(x_1, \ldots, x_n)} = \frac{P(x_{\alpha(1)}, \ldots, x_{\alpha(n)})}{P(x_1, \ldots, x_n)} \cdot \frac{P(x_{\alpha(\beta(1))}, \ldots, x_{\alpha(\beta(n))})}{P(x_{\alpha(1)}, \ldots, x_{\alpha(n)})} \quad (2)
\]

Notice that the first fraction in the right hand side of (2) is equal to \( \text{sign}(\alpha) \). Introduce the variables \( y_1 = x_{\alpha(1)}, \ldots, y_n = x_{\alpha(n)} \). Then \( y_{\beta(1)} = x_{\alpha(\beta(1))}, \ldots, y_{\beta(1)} = x_{\alpha(\beta(1))} \). Writing the
second fraction in the right hand side of (2) in terms of the variables \(y_1, \cdots, y_n\), we get
\[
\frac{P(x_{\alpha(1)}, \cdots, x_{\alpha(n)})}{P(x_{\alpha(1)}, \cdots, x_{\alpha(n)})} = \frac{P(y_{\beta(1)}, \cdots, y_{\beta(n)})}{P(y_1, \cdots, y_n)} = \text{sign(\(\beta\))}.
\]
Now equation (2) implies that \(\text{sign(\(\alpha\beta\))} = \text{sign(\(\alpha\)) \text{sign(\(\beta\))}}\).

3.4. Remark. Note that \(\text{sign(id)} = 1\). Further, since sign of a permutation is either 1 or \(-1\), we have
\[
\text{sign(\(\alpha^{-1}\))} = \text{sign(\(\alpha\))}^{-1} = \text{sign(\(\alpha\))}
\]
and
\[
\text{sign(\(\alpha\beta\alpha^{-1}\))} = \text{sign(\(\alpha\)) \text{sign(\(\beta\)) \text{sign(\(\alpha\))}^{-1}} = \text{sign(\(\beta\))}.
\]

3.5. Lemma. The sign of a flip (or a transposition) is \(-1\).

Proof. Directly verify from the definition that \(\text{sign(1 2)} = -1\) (left as an exercise). Let \((i \ j)\) be any flip. Then Pick a permutation \(\alpha\) such that \(\alpha(1) = i\) and \(\alpha(2) = j\). Then \((i \ j) = \alpha(1 2)\alpha^{-1}\). So \(\text{sign(i j)} = \text{sign(\(\alpha\)) \text{sign(12)} \text{sign(\(\alpha\))}^{-1}} = \text{sign(1 2)} = -1\).

3.6. Theorem. (a) If a permutation can be written as a product of a even number of flips, then it has sign 1.
(b) If a permutation can be written as a product of a odd number of flips, then it has sign -1.
(c) If a permutation can be written as a product of a even number of flips, then it cannot be written as a product of an odd number of flips and vice versa.

Proof. Let \(\alpha\) be a permutation. Suppose \(\alpha = \beta_1 \cdots \beta_{2k}\) where each \(\beta_j\) is a flip. Then
\[
\text{sign(\(\alpha\))} = \text{sign(\(\beta_1\))} \cdots \text{sign(\(\beta_{2k}\))} = (-1)^{2k} = 1.
\]
Note that the first equality above holds since sign is multiplicative (see theorem 3.3) and the second equality holds by lemma 3.5. This proves part (a). The proof of (b) is exactly similar. Part (c) follows from part (a) and (b) since a permutation has a well defined sign.

The theorem above prompts the next definition.

3.7. Definition. A permutation is called even if it can be written as a product of even number of flips, otherwise the permutation is called odd. Notice that the notion of even and odd permutations make sense because of part (c) of the theorem 3.6. Also notice that an even permutation is just another name for a permutation that have sign 1 and that an odd permutation is just another name for a permutation that have sign \(-1\). We may restate some of the above facts about sign of a permutation, in terms of even and odd permutations as follows. These facts follow directly from the corresponding facts about sign of a permutation.

- The identity is an even permutation while each flip is odd.
- Since the sign of a permutation is multiplicative, the product of two even permutations is even and the product of two odd permutations is even. The product of an even and an odd permutation is odd. The inverse of an even permutation is even and the inverse of an odd permutation is odd.
- In particular, the set of even permutations form a subgroup of \(S_n\). This subgroup is called the alternating group and is denoted by \(A_n\).

3.8. Exercise: Show that \(\text{sgn(\(\alpha\))} = (-1)^{|\text{N(\(\alpha\))}|}\). (Hint: Look at the proof of the claim in 3.1)
4. Some exercises: November 11.

4.1. Exercise. Prove or disprove: There is a non-cyclic abelian group of order 20.

Solution. Let $G = \mathbb{Z}_2 \times \mathbb{Z}_{10}$. Let $g_1, g_2 \in G$. We can write these elements in the form $g_1 = (\alpha_1, \beta_1)$ and $g_2 = (\alpha_2, \beta_2)$ for some $\alpha_1, \alpha_2 \in \mathbb{Z}_2$ and $\beta_1, \beta_2 \in \mathbb{Z}_{10}$. The composition law on $G$ is defined by

$$g_1 + g_2 = (\alpha_1 + \beta_1, \alpha_2 + \beta_2)$$

It follows that $g_1 + g_2 = g_2 + g_1$ for all $g_1, g_2 \in G$, so $G$ is abelian.

Note that $|G| = |\mathbb{Z}_2||\mathbb{Z}_{10}| = 20$. Let $g \in G$. Then $g$ has the form $g = (a \mod 2, b \mod 10)$ for some $a, b \in \mathbb{Z}$. So $10g = (10a \mod 2, 10b \mod 10) = (0 \mod 2, 0 \mod 10)$ and this is the identity of $G$. So every element of $G$ has order at most 10. In particular $G$ does not have any element of order 20, so $G$ is not cyclic. So there is a non-cyclic abelian group of order 20.

$\square$

4.2. Exercise. Let $\phi : G \to H$ be a group homomorphism. Show that $\phi^{-1}\{e_H\} = \{e_G\}$ if and only if $\phi$ is one to one. Here $e_G$ and $e_H$ denotes the identities of $G$ and $H$ respectively. Also recall that $\phi^{-1}\{e_H\}$ is defined as the set $\phi^{-1}\{e_H\} = \{g \in G : \phi(g) = e_H\}$.

Solution. Suppose $\phi$ is one to one. Since $\phi$ is a homomorphism, we know that $\phi(e_G) = e_H$. Since $\phi$ is one to one, more than one element in $G$ cannot map to $e_H$, so $\phi^{-1}\{e_H\}$ can have at most one element. It follows that $\phi^{-1}\{e_H\} = \{e_G\}$.

Conversely, suppose $\phi^{-1}\{e_H\} = \{e_G\}$. Let $a, b \in G$ such that $\phi(a) = \phi(b)$. Then

$$\phi(ab^{-1}) = \phi(a)\phi(b)^{-1} = \phi(a)\phi(a)^{-1} = e_H.$$ 

So $ab^{-1} \in \phi^{-1}\{e_H\} = \{e_G\}$. In other words, $ab^{-1} = e_G$, so $a = b$. Hence $\phi$ is one to one.

$\square$

4.3. Exercise. Let $G$ be a group. Let $a, b \in G$ such that $|a| = m$ and $|b| = n$. If $\gcd(m, n) = 1$, then show that $\langle a \rangle \cap \langle b \rangle = \{e\}$.

Solution. Let $e$ denote the identity of $G$. Since $\gcd(m, n) = 1$, there exists integers $r$ and $s$ such that $mr + ns = 1$. Let $x \in \langle a \rangle \cap \langle b \rangle$. Since $x \in \langle a \rangle$ we can write $x = a^t$ for some $t \in \mathbb{Z}$ and hence

$$x^m = a^{tm} = (a^m)^t = e^t = e.$$ 

Similarly, since $x \in \langle b \rangle$ and $|b| = n$, we have $x^n = e$. So

$$x = x^{mr + ns} = (x^m)^r(x^n)^s = e^re^s = e.$$ 

$\square$

4.4. Exercise. (a) Calculate the order of $(6 \mod 17)$ in $U(17)$. Show that $U(17)$ is a cyclic group with generator $(6 \mod 17)$.

(b) What is the remainder obtained when $14^{2491}$ is divided by 17? You may use the fact that $2491 = 155.16 + 11$.

Proof. (a) We calculate $6^2 \equiv 2 \mod 17$. So $6^4 \equiv 4 \mod 17$ and $6^8 \equiv 16 \equiv -1 \mod 17$ and $6^{16} \equiv 1 \mod 17$. Write $a = 6 \mod 17$. So $a^{16} = 1 \mod 17$, hence the order of $a$ is a factor of 16. But we already saw that $a^n \neq 1 \mod 17$ for $n = 1, 2, 4, 8$. It follows that the order of $a$ in $U(17)$ is 16. Since 17 is a prime, we have $U(17) = \{n \mod 17 : 1 \leq n \leq 16, n \in \mathbb{Z}\}$. So $U(17)$ has order 16. Since we found an element of order 16 in $U(17)$, it follows that $U(17)$ is cyclic and $a$ is a generator for this cyclic group.

(b) We have $14^{2491} \equiv 14^{11} \mod 17$. Since $14^2 \equiv 10 \mod 17$, we can write $14^{2491} = (14^2)^{1245} \cdot 14 \equiv 10^{1245} \cdot 14 \mod 17$. Now we need to calculate $10^{1245} \mod 17$. We have $10^4 \equiv -1 \mod 17$, so $10^{1245} \equiv (10^4)^{311} \cdot 10 \equiv (-1)^{311} \cdot 10 \equiv -10 \equiv 7 \mod 17$. Therefore, $14^{2491} \equiv 7 \mod 17$.

6
(b) Since $U(17) = \langle a \rangle$, we can write $(14 \mod 17) = a^k$ for some integer $k$. Now $a^{2491} = a^{155 \cdot 16 + 11} = a^{11}$ since $a^{16} = 1 \mod 17$. So

$$(14 \mod 17)^{2491} = a^{2491k} = a^{11k} = (14 \mod 17)^{11}.$$ 

Now we have $14^2 \equiv (-3)^2 \equiv 9 \mod 17$,

$14^4 \equiv 81 \equiv (-4) \mod 17$, $14^8 \equiv 16 \equiv -1 \mod 17$. So

$$14^{11} = 14^8 \cdot 14^2 \cdot 14 \equiv (-1) \cdot 9 \cdot (-3) \equiv 27 \equiv 10 \mod 17.$$ 

So $14^{2491} \equiv 10 \mod 17$. So the remainder is 10. \qed

4.5. Exercise. Find an element $a$ of largest order in $S_8$. What is the order of $a$? Find $a^{157}$.

Proof. Let $n_1 \geq n_2 \geq \cdots \geq n_k$ be a non-increasing sequence of natural numbers with $n_1 + n_2 + \cdots + n_k = 8$. We shall say that a permutation $\sigma \in S_8$ has cycle type $(n_1, \cdots, n_k)$ if $\sigma$, when written as a product of disjoint cycles, consists of $k$ cycles of length $n_1, n_2, \cdots, n_k$ respectively. For example, the permutation $(1468)(253)(7)$ has cycle type $(4, 3, 1)$. Note that if a permutation has cycle type $(n_1, \cdots, n_k)$, then its order is the least common multiple of the numbers $n_1, \cdots, n_k$. We can list all the cycle types in $S_8$ by listing all nonincreasing sequences of natural numbers $(n_1, \cdots, n_k)$ such that $\sum_k n_k = 8$. There are 22 such cycle types. They are

$$(8), (7, 1), (6, 2), (6, 1, 1) (5, 3), (5, 2, 1), (5, 1, 1, 1),$$

$$(4, 4), (4, 3, 1), (4, 2, 2), (4, 2, 1, 1), (4, 1, 1, 1, 1)$$

$$(3, 3, 2), (3, 3, 1, 1), (3, 2, 2, 1), (3, 2, 1, 1, 1), (3, 1, 1, 1, 1, 1)$$

$$(2, 2, 2, 2), (2, 2, 2, 1, 1), (2, 2, 1, 1, 1, 1), (2, 1, 1, 1, 1, 1, 1).$$

Looking at the least common multiples, we find that the largest order occurs for cycle type $(5, 3)$. So $a = (1 \ 2 \ 3 \ 4 \ 5) (6 \ 7 \ 8)$ is an element of largest order in $S_8$. One has $|a| = 15$. So $a^{15} = e$ where $e$ denotes the identity permutation. So $a^{157} = (a^{15})^{10} a^7 = a^7$. Write $b = (1 \ 2 \ 3 \ 4 \ 5)$ and $c = (6 \ 7 \ 8)$. The cycles $b$ and $c$ are disjoint, so they commute, that is, $bc = cb$. So $a^7 = (bc)^7 = b^7 c^7$. Since $b$ has order 5 and $c$ has order 3, we have $b^5 = b^2 = (1 \ 3 \ 5 \ 2 \ 4)$ and $c^2 = c = (6 \ 7 \ 8)$. Finally, we get

$$a^{157} = a^7 = b^7 c^7 = b^5 c^5 = (1 \ 3 \ 5 \ 2 \ 4) (6 \ 7 \ 8).$$ \qed

4.6. Exercise. Let $\phi : G \to H$ be a group homomorphism. Let $N = \{ g \in G : \phi(g) = e_H \}$. Show that $N$ is a subgroup of $G$.

Solution. Since $\phi$ is a group homomorphism, we have $\phi(e_G) = e_H$, so $e_G \in N$.

Let $a, b \in N$. Then $\phi(a) = e_H$ and $\phi(b) = e_H$. Since $\phi$ is a homomorphism, we have $\phi(ab) = \phi(a) \phi(b) = e_H e_H = e_H$. So $ab \in N$ if $a$ and $b$ belong to $N$.

Finally, let $a \in N$. Then $\phi(a) = e_H$. Since $\phi$ is a homomorphism, we have $\phi(a^{-1}) = (\phi(a))^{-1} = e_H^{-1} = e_H$. So $a^{-1} \in N$ if $a \in N$.

It follows that $N$ is a subgroup of $G$. \qed
5. NORMAL SUBGROUP AND QUOTIENT GROUP

We begin by stating a couple of elementary lemmas.

5.1. **Lemma.** Let $A$ and $B$ be subsets of a group $G$. If $g, h \in G$, then $g(hA) = (gh)A$. If $A \subseteq B$ and $g \in G$, then $gA \subseteq gB$.

The proofs of the lemma above will be left as exercise. We often use easy results like these without mentioning explicitly.

5.2. **Lemma.** Let $\phi : G \to H$ be a group homomorphism and let $N = \ker(\phi)$. Then $\phi^{-1}(\phi(g)) = gN = Ng$ for all $g \in G$.

**Proof.** Take $g \in G$. Let $x \in \phi^{-1}(\phi(g))$ or in other words, $\phi(x) = \phi(g)$. Then

$$\phi(g^{-1}x) = \phi(g)^{-1}\phi(x) = \phi(g)^{-1}\phi(g) = e_H,$$

so $g^{-1}x \in N$, or in other words $x \in gN$. Thus $\phi^{-1}(\phi(g)) \subseteq gN$. Conversely, if $x \in gN$, then $x = gn$ for some $n \in N$, so $\phi(x) = \phi(g)\phi(n) = \phi(g)e_H = \phi(g)$, so $x \in \phi^{-1}(\phi(g))$. Thus $gN \subseteq \phi^{-1}(\phi(g))$. This proves $\phi^{-1}(\phi(g)) = gN$. A similar argument shows that $\phi^{-1}(\phi(g)) = Ng$ (Exercise: Write out this argument). \hfill \Box

5.3. **Definition.** Let $G$ be a group. A subgroup $N$ of $G$ is called a normal subgroup if $gN = Ng$ for all $g \in G$. In this case we need not distinguish between left and right cosets. So we simply talk of cosets of $N$.

5.4. **Lemma.** Let $G$ be a group and $N$ be a subgroup of $G$. The following are equivalent.

(a) $gN = Ng$ for all $g \in G$.

(b) $gNg^{-1} = N$ for all $g \in G$.

(c) If $g \in G$ and $n \in N$, then $gng^{-1} \in N$.

**Proof.** Suppose (a) holds. Then $gNg^{-1} = (gN)g^{-1} = (Ng)g^{-1} = N(gg^{-1}) = N$. Thus (a) implies (b). Clearly (b) implies (c). Assume (c). Let $x \in gN$. Then $x \in gn$ for some $n \in N$. So $x = gng^{-1}g \in Ng$ since $gng^{-1} \in N$ by our assumption. Thus $gN \subseteq Ng$. Similarly show that $Ng \subseteq gN$. So $gN = Ng$. Thus (c) implies (a). \hfill \Box

5.5 (Motivating the construction of a quotient). Lemma 5.2 says that kernels of homomorphisms are normal subgroups. Conversely, we shall see that all normal subgroups appear as kernels of homomorphisms. Let $G$ be a group and let $N$ be a normal subgroup of $G$. We shall construct a onto group homomorphism $\pi : G \to Q$ such that $\ker(\pi) = N$. This group $Q$ will be called the quotient of $G$ by the normal subgroup $N$ and will be denoted by $Q = G/N$.

To motivate the construction, suppose we have an onto group homomorphism $\pi : G \to Q$ and let $\ker(\pi) = N$. Let $q \in Q$. Since $\pi$ is onto, we can pick an element $g \in G$ such that $\pi(g) = q$. Then Lemma 5.2 gives us $\pi^{-1}(q) = gN$. In words, this says that the preimages of elements of $Q$ are just the cosets of $N$. So the elements of $Q$ are in one to one correspondence with the set of cosets of $N$ in $G$. Also verify that if $q_1$ and $q_2$ are two elements of $Q$ such that $\pi^{-1}(q_1) = g_1N$ and $\pi^{-1}(q_2) = g_2N$, then $\pi^{-1}(q_1q_2) = g_1g_2N$ (Exercise: verify this). This suggests the definition that follows.

5.6. **Definition.** Let $G$ be a group and $N$ be a normal subgroup. Let $G/N$ denote the set of cosets of $N$ in $G$. Let $C$ and $D$ be two cosets of $N$ in $G$. We say that an element $c \in G$
is a representative of the coset $C$ if $c \in C$. Choose a representative $c$ of the coset $C$ and a representative $d$ of the coset $D$.

**Claim:** The coset $cdN$ only depends on the cosets $C$ and $D$ and does not depend on the choice of the representatives $c$ and $d$.

**Proof.** Let $c_1$ be another representative of $C$ and $d_1$ be another representative of $D$. Then $c_1c^{-1} \in N$ and $d_1d^{-1} \in N$. Since $N$ is normal, $c(d_1d^{-1})c^{-1} \in N$ as well. So

$$(c_1d_1)(cd)^{-1} = c_1d_1d^{-1}c^{-1} = (c_1c^{-1})c(d_1d^{-1})c^{-1} \in N.$$ 

So $c_1d_1 \in Ncd = cdN$. So $c_1d_1N = cdN$. \qed

Define a binary operation on $G/N$ as follows: Given two cosets $C$ and $D$, we choose coset representatives $c$ and $d$ of $C$ and $D$ respectively and let $(C,D)$ to be the coset $cdN$. The claim we just proved imply that this procedure gives a well defined binary operation on $G/N$.

Let us reiterate the definition of the binary operation in slightly different words. If $c \in C$ and $d \in D$, then $C = cN$ and $D = dN$. So our definition says

$$(cN)(dN) = cdN.$$ 

Let us also reiterate that we have already argued this is a well defined operation on $G/N$ and this argument required the fact that $N$ is a normal subgroup.

Next one verifies that $G/N$ with the binary operation just defined becomes a group where the identity is the coset $N$ and inverse of $gN$ is $g^{-1}N$. This group $G/N$ is called the quotient of $G$ by $N$. There is a canonical onto function from $\pi : G \to G/N$ given by $\pi(g) = gN$. Verify that $\pi$ is a homomorphism and $\ker(\pi) = N$.

**5.7. Example.** Verify that $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$.

### 6. Constructing Homomorphisms

**6.1. Lemma.** Let $G$ be a group and $a \in G$. Then there exists a homomorphism $\phi : \mathbb{Z} \to G$ given by $\phi(n) = a^n$ for all $n \in \mathbb{Z}$. This $\phi$ is the unique homomorphism from $\mathbb{Z}$ to $G$ such that $\phi(1) = a$.

**Sketch of proof.** Define $\phi(n) = a^n$ for all $n \in \mathbb{Z}$. Verify that $\phi : \mathbb{Z} \to G$ is a homomorphism such that $\phi(1) = a$. Let $\phi' : \mathbb{Z} \to G$ be any homomorphisms such that $\phi'(1) = a$. Then $\phi'(n) = a^n = \phi(n)$ for all $n \in \mathbb{Z}$. So $\phi' = \phi$. \qed

The above lemma says that constructing homomorphisms from $\mathbb{Z}$ to any group is easy. You can send 1 to anything you want and the homomorphism is completely determined once you decide where 1 goes.

**6.2. Corollary.** The map $\phi(k) = k \mod n$ is the unique homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}_n$ such that $\phi(1) = 1 \mod n$. The kernel of this homomorphism is $n\mathbb{Z}$.

**6.3. Lemma.** Let $\phi_1 : G \to H_1$ and $\phi_2 : G \to H_2$ be two homomorphisms. Then there is a homomorphism $\phi : G \to H_1 \times H_2$ given by $\phi(G) = (\phi_1(G), \phi_2(G))$.

**6.4. Theorem.** Let $A, B, C$ be three groups and let $f : A \to B$ and $g : A \to C$ be two homomorphisms.

(i) if there exists a homomorphism $h : B \to C$ such that $h \circ f = g$, then $\ker(f) \subseteq \ker(g)$. 


(ii) Suppose $f$ is onto and $\ker(f) \subseteq \ker(g)$.

(a) Then there exists a unique homomorphism $h : B \to C$ such that $h \circ f = g$.

(b) If $g$ is onto, then so is $h$.

(c) If $\ker(g) = \ker(f)$, then $h$ is one to one.

(d) If $g$ is onto and $\ker(g) = \ker(f)$, then $h$ is an isomorphism.

Proof. (i) Exercise.

(ii) (a) Uniqueness: Suppose $h, h'$ be two homomorphisms such that $h \circ f = g = h' \circ f$. Pick $b \in B$. Since $f$ is onto there exists $a \in A$ such that $f(a) = b$. Then $h(b) = h(f(a)) = g(a) = h'(f(a)) = h'(b)$. So $h = h'$. Thus there can be at most one $h$ with the given properties.

Existence: Let $b \in B$. Suppose $a, a' \in A$ such that $f(a) = f(a') = b$. Then $f(a^{-1}a') = e$, so $(a^{-1}a') \in \ker(f)$, so $(a^{-1}a') \in \ker(g)$, so $g(a^{-1}a') = e$, so $g(a) = g(a')$. Thus we observe that “$g$ takes the same value on all the elements of $A$ that map to $b$”. Given $b \in B$, we can pick $a \in A$ such that $f(a) = b$ (since $f$ is onto) and then define $h(b) = g(a)$. Because of our observation, this procedure gives us a well defined function $h : B \to C$. Verify that $h$ is a homomorphism. Now suppose $a \in A$. Let $b = f(a)$. So $a$ is an element of $A$ such that $f(a) = b$. So $h(b) = g(a)$, or $h(f(a)) = g(a)$. So $h \circ f = g$. This proves part (a).

(b) Now suppose $g$ is onto. Let $c \in C$. Then there exists $a \in A$ such that $g(a) = c$. It follows that $h(f(a)) = c$, so $h$ is onto. This proves part (b).

(c) Now suppose $\ker(f) = \ker(g)$. To show $h$ is one to one, it is enough to verify that $\ker(h) = e_B$. Let $b \in \ker(h)$, that is, $h(b) = e_C$. Pick $a \in A$ such that $f(a) = b$. Then $g(a) = h(f(a)) = h(b) = e_C$, so $a \in \ker(g) = \ker(f)$, so $b = f(a) = e_B$. So $\ker(h) = e_B$. This proves part (c). Part (d) follows from part (b) and (c).

6.5. Corollary. Let $m, n$ be positive integers. Then there exists a unique homomorphism $h : \mathbb{Z}_{mn} \to \mathbb{Z}_m$ such that $h(1 \ mod \ mn) = 1 \ mod \ m$.

Sketch of proof. Let $f : \mathbb{Z} \to \mathbb{Z}_{mn}$ and $g : \mathbb{Z} \to \mathbb{Z}_m$ be the homomorphisms $f(k) = k \ mod \ mn$ and $g(k) = k \ mod \ m$. Then $\ker(f) = mn\mathbb{Z} \subseteq m\mathbb{Z} = \ker(g)$. Now apply the above theorem.

It is convenient to represent the statement of theorem [6.4] in a diagrammatic language. Let us denote an onto homomorphism $f : A \to B$ by a double headed arrow $f : A \leftrightarrow B$. The theorem [6.4] says that

\[
\begin{array}{ccc}
A & \xrightarrow{g} & C \\
\downarrow{f} & & \downarrow{h} \\
B & & \end{array}
\]

with $\ker(f) \subseteq \ker(g)$, there exists a unique $h : B \to C$ such that the following diagram commutes:

\[
\begin{array}{ccc}
A & \xrightarrow{g} & C \\
\downarrow{f} & & \downarrow{h} \\
B & & \end{array}
\]

(3)

Saying that the diagram commutes is a pictorial way of saying that $g = h \circ f$. 

10
6.6. **Theorem** (The first isomorphism theorem). Let \( \psi : G \to H \) be a group homomorphism. Let \( K = \ker(\psi) \). Let \( \phi : G \to G/K \) be the natural quotient homomorphism: \( \phi(g) = gK \). Then there is a unique isomorphism \( \eta : G/K \to \psi(G) \) such that \( \psi = \eta \circ \phi \).

**Proof.** Recall that kernels of homomorphisms are normal subgroups, so \( K \) is normal in \( G \). From given data, we get the following diagram of homomorphisms

\[
\begin{array}{ccc}
G & \xrightarrow{\psi} & \psi(G) \\
\downarrow{\phi} & & \downarrow{\circlearrowright}\eta \\
G/K & & \\
\end{array}
\]

Note that the horizontal arrow is simply the given map \( \psi \), but we consider it as a map to the subgroup \( \psi(G) \) of \( H \). So \( \psi : G \to \psi(G) \) is an onto homomorphism. From the definition of the quotient map, we have \( \ker(\phi) = K = \ker(\psi) \). So by theorem 6.4(d), we get an isomorphism \( \eta : G/K \to \psi(G) \), such that the following diagram commutes:

\[
\begin{array}{ccc}
G & \xrightarrow{\psi} & \psi(G) \\
\downarrow{\phi} & & \downarrow{\circlearrowright}\eta \\
G/K & & \\
\end{array}
\]

Saying that the above diagram commutes is just a pictorial way of saying \( \psi = \eta \circ \phi \). \( \square \)

Let \( G \) be a group and \( N \) be a normal subgroup. The quotient homomorphism \( G \to G/N \) collapses the normal subgroup \( N \) to the identity in \( G/N \). In this way, considering the quotient group \( G/N \) lets us forget the structure inside \( N \). The correspondence theorem below says that taking quotient by \( N \) “retains the subgroup structure in \( G \) above \( N \)”. So passing to the quotient group \( G/N \) lets us disregard what was happening inside \( N \) and focus solely on what happens “above” \( N \). Thus, the quotient construction becomes an important simplifying tool.

6.7. **Theorem** (the correspondence theorem). Let \( N \) be a normal subgroup of \( G \). Then there is a natural inclusion preserving bijection between

\[
\{ \text{set of subgroups of } G \text{ containing } N \} \to \{ \text{set of subgroups of } G/N \}
\]

Under this bijection, a subgroup \( H \) of \( G \) such that \( H \supseteq N \) corresponds to the subgroup \( H/N \) of \( G/N \). Under the above correspondence, normal subgroups on the left hand side correspond to normal subgroups on the right hand side.

The proof of the correspondence theorem is left as a routine exercise. We want to move on to the second and the third isomorphism theorems. These theorems let us compare the subgroup structures in groups with subgroup structures in various quotients. Before stating them we need a lemma. The proof of the lemma is left as an exercise.

6.8. **Lemma.** Let \( H \) and \( K \) be two subgroups of a group \( G \). Then \( HK \) is a subgroup of \( G \) if and only if \( HK = KH \).

**Proof.** Suppose \( HK = KH \). Let \( c, c' \in HK \). Then there exists \( h, h' \in H \) and \( k, k' \in K \) such that \( c = hk \) and \( c' = h'k' \). Note that \( kh' \in KH = HK \), so \( kh' = h''k'' \) for some \( h'' \in H \) and
\[k'' \in K.\] Then \(cc' = hh'k' = hh''k'' \in HK\) since \(hh'' \in H\) and \(k''k \in K\). Thus \(HK\) is closed under multiplication. Let \(c \in HK\). Then there exists \(h \in H\) and \(k \in K\) such that \(c = hk\). Now \(c^{-1} = k^{-1}h^{-1} \in KH = HK\). So \(HK\) is closed under taking inverses. Clearly \(e_G\) belongs to \(HK\). It follows that \(HK\) is a subgroup. This proves one implication. The other implication is left as an exercise. \(\square\)

6.9. Theorem (The second isomorphism theorem). Let \(N\) be a normal subgroup of \(G\). Let \(H\) be a subgroup of \(G\). Then \(HN\) is a subgroup of \(G\) and \(H \cap N\) is a normal subgroup of \(H\) and \(H/H \cap N \cong HN/N\).

Sketch of proof. Since \(N\) is normal in \(G\), we have \(gN = Ng\) for all \(g \in G\). So \(HN = NH\). By lemma 6.8, it follows that \(HN\) is a subgroup of \(G\). Verifying \(H \cap N\) is a normal subgroup of \(H\) is left as a routine exercise. Now let \(\psi\) be the composition of homomorphisms:

\[
H \longrightarrow \text{inclusion} \longrightarrow HN \longrightarrow \text{quotient map} \longrightarrow HN/N.
\]

So \(\psi : H \rightarrow HN/N\) is given by \(\psi(h) = hN\). Note that \(\psi\) is a homomorphism since both the inclusion and the quotient map are homomorphisms. Now verify that \(\psi\) is onto and \(\ker(\psi) = H \cap N\). Then the second isomorphism theorem follows from the first isomorphism theorem. \(\square\)

6.10. Theorem (The third isomorphism theorem). Let \(H\) and \(N\) be normal subgroups of \(G\) with \(N \subset H \subset G\). Then there is a natural isomorphism \(G/N \cong H/\overline{H}\).

Proof. Consider the following diagram of homomorphisms:

\[
\begin{array}{ccc}
G & \longrightarrow & G/H \\
\phi_H \downarrow & & \downarrow \psi \\
G/N & \longrightarrow & \\
\phi_N & & \\
\end{array}
\]

where both the arrows \(\phi_N\) and \(\phi_H\) are the natural quotient homomorphisms. Note that \(\ker(\phi_N) = N \subset H = \ker(\phi_H)\). So by theorem 6.4(c), we have a onto homomorphism \(\psi : G/N \rightarrow G/H\) such that the following diagram commutes:

\[
\begin{array}{ccc}
G & \longrightarrow & G/H \\
\phi_H \downarrow & & \downarrow \psi \\
G/N & \longrightarrow & \\
\phi_N & & \\
\end{array}
\]

If \(g \in G\), then one has \(\psi(gN) = \psi \circ \phi_N(g) = \phi_H(g) = gH\). Now verify that \(\ker(\psi) = H/N\) and apply the first isomorphism theorem. \(\square\)

Let \(G_1\) and \(G_2\) be two groups. Let us consider the product group \(G_1 \times G_2\). The product comes with natural projection maps \(\pi_1 : G_1 \times G_2 \rightarrow G_1\) and \(\pi_2 : G_1 \times G_2 \rightarrow G_2\) given by \(\pi_1(g_1, g_2) = g_1\) and \(\pi_2(g_1, g_2) = g_2\). It is easy to verify that \(\pi_1\) and \(\pi_2\) are onto homomorphisms. The next theorem tells us how to construct homomorphism to a product.

6.11. Theorem. Let \(G_1, G_2, G\) be groups. Given homomorphisms \(f_1 : G \rightarrow G_1\) and \(f_2 : G \rightarrow G_2\), there exists a unique homomorphism \(f : G \rightarrow G_1 \times G_2\) such that \(\pi_1 \circ f = f_1\) and \(\pi_2 \circ f = f_2\) (where \(\pi_1\) and \(\pi_2\) are the natural projections).
sketch of proof. Define \( f : G \to G_1 \times G_2 \) by \( f(g) = (f_1(g), f_2(g)) \) and verify that \( f \) is a homomorphism and that \( \pi_1 \circ f = f_1 \) and \( \pi_2 \circ f = f_2 \) \( \square \)

6.12. Theorem. Let \( H, K \) be two normal subgroups of a group \( G \) such that \( H \cap K = \{e\} \). Then show that \( G \) is isomorphic to a subgroup of \( G/H \times G/K \).

sketch of proof. Let \( \phi_H : G \to G/H \) and \( \phi_K : G \to G/K \) be the natural quotient homomorphisms. By 6.11 we get a homomorphism \( \phi : G \to G/H \times G/K \), given by

\[
\phi(g) = (\phi_H(g), \phi_K(g)) = (gH, gK).
\]

Let \( g \in \ker(\phi) \). Then \( (gH, gK) \) is the identity in \( G/H \times G/K \). This means \( gH \) is the identity in \( G/H \) and \( gK \) is the identity in \( G/K \). To say \( gH \) is the identity in \( G/H \), means \( gH = H \), so \( g \in H \). Similarly, we get \( g \in K \). So \( g \in H \cap K = \{e\} \). So \( \ker(\phi) = \{e\} \) and hence \( \phi \) is a one to one homomorphism. So \( \phi : G \to G/H \times G/K \) gives an isomorphism \( \phi : G \to \phi(G) \) and \( \phi(G) \) is a subgroup of \( G/H \times G/K \). \( \square \)

6.13. Theorem. Let \( H \) and \( K \) be two subgroups of a finite group \( G \) such that \( K \) is normal in \( G \), \( H \cap K = \{e\} \) and \( HK = G \). Then show that \( |G| = |H| \cdot |K| \).

Proof. By the second isomorphism theorem, we know that \( HK \) is a subgroup of \( G \) and \( H \cap K \) is a normal subgroup of \( H \) and that \( H/H \cap K \cong HK/K \). Now since \( H \cap K = \{e\} \) and \( HK = G \), we get

\[
H \cong H/\{e\} = H/H \cap K \cong HK/K \cong G/K.
\]

So \( |H| = |G/K| = |G|/|K| \). \( \square \)

Infact, given the hypothesis of 6.13 it follows that \( G \cong H \times K \) (Exercise: show this). In this situation, one says that \( G \) is the internal direct product of \( H \) and \( K \).

6.14. Theorem. Let \( H, K \) be two normal subgroups of a finite group \( G \) such that \( H \cap K = \{e\} \) and \( HK = G \). Then show that \( G \) is isomorphic to \( G/H \times G/K \).

Proof. By 6.12 we have an one to one homomorphism \( \phi : G \to G/H \times G/K \) given by \( \phi(g) = (gH, gK) \). By 6.13 we have \( |G| = |K| \cdot |H| \). So \( |G/H| = |G|/|H| = |K| \) and \( |G/K| = |G|/|K| = |H| \). So

\[
|G/H \times G/K| = |G/H| \cdot |G/K| = |K| \cdot |H| = |G|.
\]

By 6.12, we have an one to one homomorphism \( \phi : G \to G/H \times G/K \) given by \( \phi(g) = (gH, gK) \). Since \( G \) and \( G/H \times G/K \) have the same size, the map \( \phi \) must be onto as well. So \( \phi : G \to G/H \times G/K \) is an isomorphism. \( \square \)

The following result, known as the Chinese remainder theorem is a special case of the above considerations, but we shall state and prove it directly.

6.15. Theorem. Let \( m, n \) be two nonzero integers. If \( m \) and \( n \) are relatively prime, then \( \mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n \).

Proof. By 6.5 we have a natural homomorphisms \( \mathbb{Z}_{mn} \to \mathbb{Z}_m \) and \( \mathbb{Z}_{mn} \to \mathbb{Z}_n \) given by taking \( (k \mod mn) \) to \( (k \mod m) \) and to \( (k \mod n) \) respectively. By 6.11 this gives a homomorphism \( f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n \) given by

\[
f(k \mod mn) = (k \mod m, k \mod n)
\]
Let \( k \in \mathbb{Z} \) such that \((k \mod mn) \in \ker(f)\), then \((k \mod m, k \mod n) = (0 \mod m, 0 \mod n)\). In other words \( m \) and \( n \) divide \( k \). Since \( m \) and \( n \) are relatively prime, this means \( mn \) divides \( k \), so \( k \mod mn \) is the identity of \( \mathbb{Z}_{mn} \). So \( \ker(f) \) is just the identity of \( \mathbb{Z}_{mn} \), hence \( f: \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n \) is one to one. Since \( |\mathbb{Z}_{mn}| = mn = |\mathbb{Z}_m| \cdot |\mathbb{Z}_n| = |\mathbb{Z}_m \times \mathbb{Z}_n| \), the map \( f \) must be onto as well. So \( f \) is an isomorphism.

\[\square\]

6.16. Corollary. Let \( m \) and \( n \) be relatively prime non-zero integers. Then
(a) \( U(mn) \simeq U(m) \times U(n) \).
(b) For a positive integer \( n \) let \( \phi(n) \) be the Euler Totient function defined as the number of integers \( k \) such that \( 1 \leq k < n \) and \( k \) is relatively prime to \( n \). For example \( \phi(p) = (p - 1) \) if \( p \) is a prime number. One has \( \phi(mn) = \phi(m)\phi(n) \).
(c) Let \( n \) be a positive integer. Let \( n = p_1^{e_1} \cdots p_r^{e_r} \) be the prime factorization of \( n \). Then \( \phi(n) = n(1 - p_1^{-1}) \cdots (1 - p_r^{-1}) \).

\( \square \)

**sketch of proof.** Consider the isomorphism \( f: \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n \) given in 6.15. Since \( f \) is onto, given any \((\alpha, \beta) \in U(m) \times U(n)\), there exists \( k \in \mathbb{Z} \) such that \( f(k \mod mn) = (\alpha, \beta) \). This means \((k \mod m) = \alpha \) and \((k \mod n) = \beta \) are relatively prime to \( m \) and \( n \) respectively, so \( k \) is relatively prime to \( mn \), that is, \((k \mod mn) \in U(mn)\). Conversely, if \((k \mod mn) \in U(mn)\), then \( f(k \mod mn) = (k \mod m, k \mod n) \in U(m) \times U(n)\). So the restriction of \( f \) to \( U(mn) \) gives an onto map \( f: U(mn) \to U(m) \times U(n) \). Since \( f \) is one to one, so is the restriction. Finally verify that \( f \) is also a homomorphism for the multiplicative groups \( U(mn) \) to \( U(m) \times U(n) \). This proves part (a). Part (b) follows immediately, since \( |U(n)| = \phi(n) \). Part (c) follows from part (b) and the easy observation that \( \phi(p^r) = p^r(1 - p^{-1}) \) for a prime number \( p \).
7. Few more exercises

7.1. Exercise. Let $p$ be a prime. Let $G$ be a group of order $p^2$. Show that $G \simeq \mathbb{Z}/p^2\mathbb{Z}$ or $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Proof. Let $G^*$ denote the set of non-identity elements of $G$. If $G$ has an element of order $p^2$, then we $G \simeq \mathbb{Z}/p^2\mathbb{Z}$. Otherwise each element of $G^*$ must have order $p$. So all nontrivial proper subgroups of $G$ are isomorphic to $\mathbb{Z}/p\mathbb{Z}$ and any two of these distinct subgroups intersect trivially. Pick $x \in G^*$. Write $H = \langle x \rangle$ and pick $y \in G - H$. We shall argue that either $\langle x \rangle$ or $\langle y \rangle$ is normal in $G$.

Suppose $\langle x \rangle$ is not normal in $G$. Then we claim that $H$ has exactly $p$ distinct conjugates subgroups $\{y^rHy^{-r} : 0 \leq r < p\}$. To prove the claim, note that if $H$ is not normal in $G$, then $N_G(H) = H$. It is easy to see that every element of $G$ can be written as $y^i x^j$ for $0 \leq i < p$ and $0 \leq j < p$. So any conjugate of $H$ has the form $y^rHy^{-r}$ for some $0 \leq r < p$. If $y^rHy^{-r} = y^rHy^{-s}$ for some $0 \leq r < s < p$, then that would imply $y^{s-r} \in N_G(H) - H$, a contradiction. This proves the claim.

Now notice that if $y \notin H$, so $y \notin y^rHy^{-r}$ for any $r$. So $\langle y \rangle$ is distinct from the conjugates of $H$. It follows that the $(p + 1)$ subgroups $H, yHxy^{-1}, \ldots, y^{p-1}H y^{-(p-1)}, \langle y \rangle$ are all distinct and hence any two of them intersect trivially. By counting the elements in these subgroups we find that $G$ must be the union of these subgroups. Now $xyx^{-1}$ must belong to one of these subgroups. If $xyx^{-1}$ belongs to some conjugate of $H$, then $y$ belongs to some conjugate of $H$ which is a contradiction. So we must have $xyx^{-1} \notin \langle y \rangle$, which implies that $\langle y \rangle$ is normal in $G$. Thus we have argued that either $\langle x \rangle$ or $\langle y \rangle$ is normal in $G$. In particular, $G$ has a normal subgroup of order $p$.

Without loss, suppose $\langle x \rangle$ is normal in $G$. Then $yxy^{-1} = x^r$ for some $r$. So $y^{-1}xy = y^{p-1}xy^{-(p-1)} = x^{p-1} = x$ by Fermat’s little theorem. It follows that $yx = xy$. So $G$ is abelian. Now it is easy to see that $\langle x \rangle \times \langle y \rangle \rightarrow G$ given by $(a,b) \mapsto ab$ is an isomorphism. □

7.2. Exercise. Describe the homomorphisms from $\mathbb{Z}_{24}$ to $\mathbb{Z}_{18}$.

Sketch of proof. Let $\pi : \mathbb{Z} \rightarrow \mathbb{Z}_{24}$ be the natural quotient homomorphism: $\pi(n) = n$ mod 24. For $k = 0, 1, \ldots, 5$, define the homomorphisms $g_k : \mathbb{Z} \rightarrow \mathbb{Z}_{18}$ by $g_k(r) = 3rk$ mod 18. Notice that $g_k(24m) = 72mk$ mod 18 = 0 mod 18. So $\ker(\pi) = 24\mathbb{Z} \subseteq \ker(g_k)$. Thus there exists $f_k : \mathbb{Z}_{24} \rightarrow \mathbb{Z}_{18}$ such that the following diagram commutes:

$$
\begin{array}{ccc}
\mathbb{Z} & \xrightarrow{g_k} & \mathbb{Z}_{18} \\
\pi \downarrow & & \downarrow f_k \\
\mathbb{Z}_{24} & \xrightarrow{f_k} & \mathbb{Z}_{18}
\end{array}
$$

In other words we have found six homomorphisms $f_k : \mathbb{Z}_{24} \rightarrow \mathbb{Z}_{18}$ given by $f_k(m$ mod 24) = $f_k(\pi(m)) = g_k(m) = 3km$ mod 18 for $0 \leq k \leq 5$.

Now suppose $f : \mathbb{Z}_{24} \rightarrow \mathbb{Z}_{18}$ be any homomorphism. Let $f(1$ mod 24) = $m$ mod 18. Then Note that 0 mod 18 = $f(24$ mod 24) = $24m$ mod 18, so $24m$ must be a multiple of 18, so $m$ must be a multiple of 3. Hence $f(1$ mod 24) = $3k$ mod 24 for some $k$. So for any $r \in \mathbb{Z}$, we have $f(r$ mod 24) = $rf(1$ mod 24) = $3rk$ mod 18 = $f_k(r$ mod 24). So $f = f_k$ for some $k$. It follows that $f_k$'s are all the possible homomorphisms from $\mathbb{Z}_{24}$ to $\mathbb{Z}_{18}$. □
7.3. **Exercise.** (a) Let \( \tau_1 \) and \( \tau_2 \) be two transpositions in \( S_n \). Show that \( \tau_1 \tau_2 \) can be written as a product of 3-cycles.

(b) Prove that every element of \( A_n \) can be written as a product of 3-cycles.

**Proof.** (a) Let \( \tau_1 = (i \ j) \) and \( \tau_2 = (k \ l) \). Suppose \( \{i, j\} \) and \( \{k, l\} \) are disjoint. Then notice that \( \tau_1 \tau_2 = (i \ j \ k)(j \ k \ l) \); so \( \tau_1 \tau_2 \) is a product of 2-cycles. Next suppose \( \{i, j\} \) and \( \{k, l\} \) have one element in common. By renaming the elements if necessary, without loss, we may assume that the common element is \( j = k \). Then \( \tau_1 \tau_2 = (j \ l \ i) \) is a three cycle. The remaining possibility is \( \tau_1 = \tau_2 \). In this case \( \tau_1 \tau_2 \) is the identity permutation, which is also the (empty) product of 3-cycles. This proves part (a).

(b) Let \( \sigma \) be any permutation in \( A_n \). Since \( \sigma \) is an even permutation, we can write \( \sigma = \tau_1 \tau_2 \cdots \tau_{2n} \) where \( \tau_j \) are transpositions. From part (a) we know that for \( j = 1, \ldots, n \), the product \( \tau_{2j-1} \tau_{2j} \) can be written as a product of 3-cycles. Multiplying these together, we find that \( \sigma \) can also be written as a product of 3-cycles. \( \square \)

7.4. **Exercise.** Consider the group \( \mathbb{R}^3 \). Let \( H = \{(x_1, x_2, x_3) \in \mathbb{R}^3 : x_1 + 2x_2 - x_3 = 0\} \). Show that \( H \) is a normal subgroup of \( \mathbb{R}^3 \). Show that \( \mathbb{R}^3/H \simeq \mathbb{R} \).

**Proof.** The identity of the additive group \( \mathbb{R}^3 \) is \( \mathbf{0} = (0, 0, 0) \). Notice that \( \mathbf{0} \in H \) so \( H \neq \emptyset \).

Let \( x = (x_1, x_2, x_3) \) and \( y = (y_1, y_2, y_3) \) be two elements of \( H \).

Then \( x_1 + 2x_2 - x_3 = 0 \) and \( y_1 + 2y_2 - y_3 = 0 \). It follows that the coordinates of 
\[
(x_1 - y_1) + 2(x_2 - y_2) - (x_3 - y_3) = (x_1 + 2x_2 - x_3) + (y_1 + 2y_2 - y_3) = 0.
\]

So \( x - y \in H \) if \( x, y \in H \). This directly proves that \( H \) is a subgroup of \( \mathbb{R}^3 \). Since \( \mathbb{R}^3 \) is abelian, any subgroup is automatically normal.

Alternatively, we can argue as follows: Now define \( f : \mathbb{R}^3 \rightarrow \mathbb{R} \) by
\[
f(x_1, x_2, x_3) = x_1 + 2x_2 - x_3.
\]

Let \( x = (x_1, x_2, x_3) \) and \( y = (y_1, y_2, y_3) \) be two elements of \( \mathbb{R}^3 \). Then we verify that
\[
f(x + y) = f(x_1 + y_1, x_2 + y_2, x_3 + y_3)
= (x_1 + y_1) + 2(x_2 + y_2) - (x_3 + y_3)
= (x_1 + 2x_2 - x_3) + (y_1 + 2y_2 - y_3)
= f(x) + f(y).
\]

So \( f \) is a group homomorphism. Looking at the definition of \( H \), we notice \( H = \ker(f) \). Since the kernel of any homomorphism is a normal subgroup, we find that \( H \) is a normal subgroup of \( \mathbb{R}^3 \). Given any \( x \in \mathbb{R} \), we notice that \( f(x, 0, 0) = x \), so \( f \) is an onto homomorphism. Thus by the first isomorphism theorem, we get an isomorphism \( \mathbb{R}^3/H \simeq \mathbb{R} \). \( \square \)

7.5. **Exercise.** Let \( G \) be a group and \( a, b \in G \). Suppose \( a \) has order \( m \) and \( b \) has order \( n \). If \( \gcd(m, n) = 1 \), then show that \( \langle a \rangle \cap \langle b \rangle = \{e\} \).

**Proof.** Let \( x \in \langle a \rangle \cap \langle b \rangle \). Since \( x \in \langle a \rangle \), we have \( x = a^t \) for some \( t \in \mathbb{Z} \). Since \( a^m = e \), it follows that \( x^m = a^{tm} = e \). Similarly since \( x \in \langle b \rangle \), we get \( x^n = e \). Since \( \gcd(m, n) = 1 \), there exists \( r, s \in \mathbb{Z} \) such that \( mr + ns = 1 \). It follows that \( x = x^{mr+ns} = (x^m)^r(x^n)^s = e^re^s = e \). \( \square \)
7.6. Exercise. Let $G$ be a group. An element of $G$ is called a commutator if it has the form $aba^{-1}b^{-1}$ for some $a,b \in G$.

(a) If $c$ is a commutator and $g \in G$. Then show that $c^{-1}$ is a commutator and that $g cg^{-1}$ is a commutator.

(b) Let $G'$ be the set of all elements of $G$ that can be written as a product of commutators. Then show that $G'$ is a normal subgroup of $G$.

(c) Let $N$ be a normal subgroup of $G$. Show that $G/N$ is abelian if and only if $N$ contains $G'$.

Proof. (a) Let $c$ be a commutator. Then $c$ has the form $c = aba^{-1}b^{-1}$ for some $a,b \in G$. Note that $c^{-1} = bab^{-1}a^{-1}$. So $c^{-1}$ is also a commutator. Also, notice that $gcg^{-1} = gaba^{-1}b^{-1}g^{-1} = (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1}$. Thus $gcg^{-1}$ is also a commutator. This proves part (a).

(b) Note that $e = eee^{-1}e^{-1}$ can be written as a commutator. Let $x \in G'$. Then $x = c_1c_2 \cdots c_n$ where each $c_j$ is a commutator. Then $x^{-1} = c_n^{-1} \cdots c_1^{-1}$. From part (a), we know that each $c_j^{-1}$ is a commutator. It follows that $x^{-1}$ is also a product of commutators, so $x^{-1} \in G'$. Now let $x, y \in G'$. Then we can write $x = c_1 \cdots c_n$ and $y = d_1 \cdots d_m$ where each $c_j$ and $d_j$ is a commutator. Then $xy = c_1 \cdots c_n d_1 \cdots d_m$ is also a product of commutators, so $xy \in G'$. Thus $G'$ is a subgroup of $G$. Now suppose $x \in G'$ and $g \in G$. Then we can write $x = c_1 \cdots c_n$ where each $c_j$ is a commutator. Then $g x g^{-1} = (g c_1 g^{-1}) \cdots (g c_n g^{-1})$. From part (a) we know that each $gc_jg^{-1}$ is a commutator. So we find that $g x g^{-1}$ is also a product of commutators, so $g x g^{-1} \in G'$. Thus $G'$ is a normal subgroup of $G$.

(c) Let $N$ be a normal subgroup of $G$ such that $G/N$ is abelian. Let $a, b \in G$. Then in the factor group $G/N$, we have $abN = aNbN = bNaN = baN$. It follows that $(ab)(ba)^{-1} \in N$, that is, $aba^{-1}b^{-1} \in N$. So $N$ contains all the commutators. Since $N$ is a subgroup, it follows that $N$ contains all the products of commutators, so $N$ contains $G'$.

□