SECTION 1

2. Assume that \( n \) is a natural number. Let \( d_0, d_1, \ldots, d_r \in \{0, \ldots, 9\} \) be its decimals, read from right to left; that is, \( n = d_0 + d_1 10 + d_2 10^2 + \cdots + d_r 10^r \).

   e) Show that \( n \equiv d_0 - d_1 + d_2 - \cdots \pmod{11} \).

   \[ \begin{align*}
   \text{Proof.} \quad & \text{Note that } 10 \equiv -1 \pmod{11}, \text{ so by properties of modular arithmetic we have } \\
   & d_i 10^i \equiv d_i (-1)^i \pmod{11}. \text{ This gives us that } \\
   & n \equiv d_0 + d_1 10 + d_2 10^2 + \cdots + d_r 10^r \pmod{11} \\
   & n \equiv d_0 - d_1 + d_2 - \cdots + d_r (-1)^r \pmod{11}. 
   \end{align*} \]

   \[ \square \]

   f) The definition of modular equivalence tell us that if \( a \equiv b \pmod{k} \), then \( a \) and \( b \) have the same remainder after division by \( k \). We apply this fact and the previous exercise: write 2015 in base 10 as

   \[ 2015 = 5 + 1 \cdot 10 + 0 \cdot 10^2 + 2 \cdot 10^3 \]

   the previous exercise tells us that

   \[ 2015 \equiv 5 - 1 + 0 - 2 \pmod{11} \]

   \[ 2015 \equiv 2 \pmod{11}. \]

   Hence 2015 has remainder 2 after division by 11.
SECTION 2

2. Suppose that $*$ is an associative and commutative binary operation on a set $S$. Show that the subset

$$T := \{ a \in S \mid a * a = a \}$$

of $S$ is closed under $*$. 

Proof. To show that $T$ is closed under $*$ we need to show that if $a, b \in T$ then $a * b \in T$, which occurs if and only if $(a * b) * (a * b) = a * b$.

Let $a, b \in T$, then by associativity we have that

$$(a * b) * (a * b) = a * (b * a) * b$$

by commutativity we have that

$$a * (b * a) * b = a * (a * b) * b$$

and lastly again by associativity we get that

$$(a * b) * (a * b) = (a * a) * (b * b).$$

Since $a, b$ are both elements of $T$ they have the property that $a * a = a$ and $b * b = b$, hence

$$(a * b) * (a * b) = (a * a) * (b * b) = (a) * (b) = a * b.$$ 

Which shows that $a * b \in T$. 

SECTION 3

2. Assume that $(G, *)$ and $(H, \square)$ are groups and that $f : (G, *) \rightarrow (H, \square)$ is a homomorphism.

a) Let $e_G$ and $e_H$ denote the identity elements of $G$ and $H$, respectively. Show that $f(e_G) = e_H$.

b) Show that one has $f(a^{-1}) = f(a)^{-1}$ for ever $a \in G$.

Proof. a) $f(e_G) = f(e_G * e_G) = f(e_G) \square f(e_G)$ and so by multiplying by $f(e_G)^{-1}$ we get that $e_H = f(e_G)$.

b) Let $a \in G$, then using part (a) we get that

$$f(a) \square f(a^{-1}) = f(a * a^{-1}) = f(e_G) = e_H$$

which implies that $f(a^{-1})$ is the inverse of $f(a)$, i.e. $f(a^{-1}) = f(a)^{-1}$. 

1. Let $G$ be a group and let $H$ be a non-empty subset of $G$.
   
   a) Show that $H$ is a subgroup of $G$ if and only if for all $a, b \in H$ one has $ab^{-1} \in H$.
   
   b) Assume that $H$ is finite. Show that $H$ is a subgroup of $G$ if and only if for all $a, b \in H$ one has $ab \in H$. (Hint: Consider the set $\{a, a^2, a^3, \ldots\}$ for an element $a \in H$ to see that $1 \in H$ and $a^{-1} \in H$.)

   **Proof.** 
   
   a) If $H$ is a subgroup then clearly $a, b \in H$ implies $b^{-1} \in H$ and $ab^{-1} \in H$.
   
   Going the other direction, assume $H$ has the property that $a, b \in H$ implies $ab^{-1} \in H$ for all $a, b \in H$.
   
   Applying the property with elements $a, a$, we get that $aa^{-1} \in H$, so $e \in H$.
   
   Applying the property with elements $e, a$ for all $a \in H$, we get that $ea^{-1} \in H$, so $a^{-1} \in H$ for all $a \in H$.
   
   Applying the property with elements $a, b^{-1}$ for all $a, b \in H$, we get that $a(b^{-1})^{-1} \in H$, so $ab \in H$ for all $a, b \in H$.
   
   Since $H$ is nonempty we can apply these properties.

   b) If $H$ is a subgroup then clearly $a, b \in H$ implies $ab \in H$ for all $a, b \in H$.
   
   Going the other direction, assume $H$ has the property that $a, b \in H$ implies $ab \in H$ for all $a, b \in H$. Then $H$ is automatically closed under products, it remains to show that $H$ contains the identity and is closed under inverses.
   
   Using the hint, let $a \in H$ and consider the set $S = \{a, a^2, a^3, \ldots\}$, by the given property we know that $S \subset H$. We also know that $H \subset G$. Since $G$ is finite, $S$ must also be finite. This implies that $a^m = a^n$ for some $m \neq n \in \mathbb{N}$.
   
   Without loss of generality, assume $m > n$. Multiplying the equation $a^m = a^n$ by $a^{-n}$ (which exists in $G$), we get that $a^{m-n} = e$. This gives us that $a^{m-n} = e \in S \subset H$.
   
   So $H$ contains the identity.
   
   Note that $a^{m-n} = aa^{m-n-1} = e$, so $a^{m-n-1}$ must be the inverse of $a$, since $m > n$ we have that $a^{m-n-1} = a^{-1} \in S \subset H$. So $H$ is closed under inverses.

   \[\square\]

8. Let $f : G \to H$ be a homomorphism between groups $G$ and $H$.
   
   a) If $U$ is a subgroup of $G$ then $f(U)$ is a subgroup of $H$.
   
   b) If $V$ is a subgroup of $H$ then $f^{-1}(V)$ is a subgroup of $G$.

   **Proof.** 
   
   a) To show $f(U)$ is a subgroup, need to show it contains the identity $e_H$, that it is closed under inverses, and that it is closed under products.
   
   Since $U$ is a subgroup, $e_G \in U$, and since $f$ is a homomorphism $f(e_G) = e_H$, so necessarily $f(e_G) = e_H \in f(U)$.
Assume $h \in f(U) = \{ f(g) : g \in U \}$, then there exists a $g$ such that $f(g) = h$. Since $U$ is a subgroup it is closed under inverses, in particular $g^{-1} \in U$ and so $f(g^{-1}) = f(g)^{-1} = h^{-1} \in f(U)$.

Assume $h_1, h_2 \in f(U)$, then there exist $g_1, g_2 \in U$ such that $f(g_1) = h_1$ and $f(g_2) = h_2$. Since $U$ is a subgroup it is closed under products, in particular $g_1 g_2 \in U$ and so $f(g_1 g_2) = f(g_1) f(g_2) = h_1 h_2 \in f(U)$.

b) To show $f^{-1}(V)$ is a subgroup, need to show it contains the identity $e_G$, that it is closed under inverses, and that it is closed under products.

Since $f$ is a homomorphism and $V$ is a subgroup of $H$, we know that $f(e_G) = e_H \in V$, so $e_G \in f^{-1}(V)$.

Assume $g \in f^{-1}(V)$, we want to show $g^{-1} \in f^{-1}(V)$. Since $g \in f^{-1}(V)$ we know that $f(g) \in V$, and since $f$ is a homomorphism $f(g^{-1}) = f(g)^{-1}$. We know $V$ is a subgroup so it is closed under inverses, so in particular $f(g)^{-1} = f(g^{-1}) \in V$, so then $g^{-1} \in f^{-1}(V)$.

Assume $g_1, g_2 \in f^{-1}(V)$, we want to show that $g_1 g_2 \in f^{-1}(V)$. Since $f$ is a homomorphism $f(g_1) f(g_2) = f(g_1 g_2)$, and $V$ is a subgroup so it is closed under products, so in particular $f(g_1) f(g_2) \in V$, so $f(g_1 g_2) \in V$ which implies $g_1 g_2 \in f^{-1}(V)$.

\[ \square \]

SECTION 5

5. Let $G = \langle a \rangle$ be a cyclic group of order $n$. Show that, for every divisor $d$ of $n$, there exists a subgroup of $G$ whose order is $d$.

**Proof.** Let $d$ be a divisor of $n$, then $n = kd$ for some integer $k$. By proposition 5.12,

$$o(a^k) = \frac{n}{gcd(k, n)} = \frac{n}{k} = d$$

and so $\langle a^k \rangle$ is a subgroup of $G$ of order $o(a^k) = d$. \[ \square \]

6. Let $f : G \to H$ be a homomorphism between two groups $G$ and $H$. Assume that $a \in G$ is an element of finite order $n \in \mathbb{N}$. Show that the order of $f(a)$ divides $n$.

**Proof.** The element $a$ is of order $n$, so $a^n = e_G$. Since $f$ is a homomorphism we can show that $f(a)^n = f(a^n)$ (argument for this is included below), so we get that

$$f(a)^n = f(a^n) = f(e_G) = e_H.$$ 

By corollary 5.11 applied to $f(a)$, we get that $f(a)^n = e_H$ if and only if $o(f(a))$ divides $n$, this completes the proof.

*The following proof of $f(a)^n = f(a^n)$ is included for completeness, but is simple enough and used often enough that we don’t require students to prove it in this exercise.*
Prove by induction on \( n \).

Base case: \( n = 1 \) is clear, \( f(a)^1 = f(a) \).

Inductive step: assume \( f(a)^n = f(a^n) \), we want to prove that \( f(a)^{n+1} = f(a^{n+1}) \).

Since \( f \) is a homomorphism \( f(a^{n+1}) = f(a \cdot a^n) = f(a) f(a^n) \), by the inductive assumption \( f(a^n) = f(a)^n \) we get that \( f(a^{n+1}) = f(a) f(a^n) = f(a)^{n+1} \).

\[ \square \]

SECTION 6

2. Let \( n \in \mathbb{N} \), let \( \sigma \in \text{Sym}(n) \) and let \((a_1, \ldots, a_k)\) be a \( k \)-cycle in \( \text{Sym}(n) \). Show that \( \sigma \circ (a_1, \ldots, a_k) \circ \sigma^{-1} = (\sigma(a_1), \ldots, \sigma(a_k)) \).

**Proof.** Showing that
\[
\sigma \circ (a_1, \ldots, a_k) \circ \sigma^{-1} = (\sigma(a_1), \ldots, \sigma(a_k))
\]
holds is equivalent to showing
\[
\sigma \circ (a_1, \ldots, a_k) = (\sigma(a_1), \ldots, \sigma(a_k)) \circ \sigma \tag{0.1}
\]
which is the version we prove here.

To show the left hand side (LHS) and right hand side (RHS) of (0.1) are equivalent permutations, we will show that applying the permutation on the LHS to a letter \( x \) is the same as applying the RHS permutation to the same letter.

*We will denote the application of a permutation \( \tau \) to a letter \( x \) by \( \tau[x] \), this is not entirely standard notation, but I find it useful when thinking of permutations in cycle notation as functions.*

If \( x = a_i \) for some \( 1 \leq i \leq k \), then applying the LHS to \( x \) gives
\[
\sigma \circ (a_1, \ldots, a_k)[x] = \sigma \circ (a_1, \ldots, a_k)[a_i]
\]
\[
= \sigma[a_i+1]
\]
\[
= [\sigma[a_i+1]]
\]

If \( x \neq a_i \) for any \( 1 \leq i \leq k \), then applying the LHS to \( x \) gives
\[
\sigma \circ (a_1, \ldots, a_k)[x] = \sigma[x]
\]
\[
= [\sigma[x]]
\]

Now we compare to applying the RHS permutation.

If \( x = a_i \) for some \( 1 \leq i \leq k \), then applying the RHS to \( x \) gives
\[
(\sigma(a_1), \ldots, \sigma(a_k)) \circ \sigma[x] = (\sigma(a_1), \ldots, \sigma(a_k)) \circ \sigma[a_i]
\]
\[
= (\sigma(a_1), \ldots, \sigma(a_k))[\sigma(a_i)]
\]
\[
= [\sigma[a_i+1]]
\]
If $x \neq a_i$ for any $1 \leq i \leq k$, then applying the RHS to $x$ gives

$$(\sigma(a_1), \ldots, \sigma(a_k)) \circ \sigma[x] = (\sigma(a_1), \ldots, \sigma(a_k))[\sigma x].$$

$$= [\sigma x].$$

So we see that the LHS permutation and the RHS permutation act identically as functions, hence they are equal.

7. Assume that $\sigma$ is a $k$-cycle. Show that if $k$ is even then $\sigma$ is odd and if $k$ is odd then $\sigma$ is even.

Proof. Let $\sigma = (a_1, \ldots, a_k)$, we prove by induction that we can write $\sigma$ as a product of $k - 1$ transpositions.

Base case: If $k = 2$ then $\sigma = (a_1, a_2)$, which is 1 transposition, so we are done.

Inductive assumption: any $(k - 1)$-cycle can be written as a product of $k - 2$ transpositions.

Inductive step: Let $\sigma = (a_1, \ldots, a_k)$ be a $k$-cycle, then

$$(a_1, \ldots, a_k) = (a_1, \ldots, a_{k-1}) \circ (a_{k-1}, a_k).$$

By the inductive assumption we know that $(a_1, \ldots, a_{k-1})$ can be written as a product of $k - 2$ transpositions (because it is a $k - 1$ cycle, the inductive assumption applies here). Moreover $(a_{k-1}, a_k)$ is a transposition, so altogether this implies that $(a_1, \ldots, a_k)$ can be written as a product of $k - 1$ transpositions.

By Theorem 6.13, the parity of $\sigma$ (even/odd) is equal to the parity of the number of transpositions it can be written as. We have shown that a $k$-cycle $\sigma$ can be written as a product of $k - 1$ transpositions, hence if the integer $k$ is even (resp. odd), then the $k$-cycle $\sigma$ must be odd (resp. even).

\[ \square \]

SECTION 7

1. b) Assume that $G = \langle t_1, t_2 \rangle$ is a finite group which is generated by two involutions $t_1, t_2$, i.e., elements of order 2 and assume that $n := o(t_1 t_2) \geq 3$. Show that $G \cong D_{2n}$.

Proof. We define a homomorphism

$$\phi : G \rightarrow D_{2n}$$

$$t_1 \rightarrow \rho$$

$$t_2 \rightarrow \sigma \rho.$$

Note: even though we have only defined where the map sends $t_1$ and $t_2$, this is enough to know where every element of $G$ is sent. This follows from the fact that
G is generated by $t_1$ and $t_2$ and that we require $\phi$ to be a homomorphism, so for example we know $\phi(t_1 t_2 t_1) = \phi(t_1)\phi(t_2)\phi(t_1) = \rho\sigma\rho\rho = \rho\sigma$.

Similarly we can define an homomorphism in the reverse direction

$$\psi : D_{2n} \to G$$

$$\sigma \mapsto t_2t_1$$

$$\rho \mapsto t_1$$

It’s not difficult to check that these maps are in fact inverses of each other, it suffices to check this on the generators.

$$[\phi \circ \psi](\sigma) = \phi(\psi(\sigma)) = \phi(t_2t_1) = \phi(t_2)\phi(t_1) = (\sigma\rho)(\rho) = \sigma$$

$$[\phi \circ \psi](\rho) = \phi(\psi(\rho)) = \phi(t_1) = \rho$$

and

$$[\psi \circ \phi](t_1) = \psi(\phi(t_1)) = \psi(\rho) = t_1$$

$$[\psi \circ \phi](t_1) = \psi(\phi(t_1)) = \psi(\sigma\rho) = \psi(\sigma)\psi(\rho) = (t_2t_1)(t_1) = t_2.$$  

These maps are not unique, there are in fact $n \cdot \Phi(n)$ unique isomorphisms between $G$ and $D_{2n}$ where $\Phi$ is Euler’s totient function.

$\square$

SECTION 8

1. Show that $V := \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ is a subgroup of Alt(4) and compute its left and right cosets. Do the left and right cosets of $V$ yield the same partitioning of Alt(4).

Proof. The left cosets of $V$ in Alt(4) can be computed to be

$$1V = \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

$$(1,2,3)V = \{(1,2,3)1, (1,2,3)(1,2)(3,4), (1,2,3)(1,3)(2,4), (1,2,3)(1,4)(2,3)\}$$

$$= \{(1,2,3), (1,3,4), (2,4,3), (1,4,2)\}$$

$$(1,3,2)V = \{(1,3,2)1, (1,3,2)(1,2)(3,4), (1,3,2)(1,3)(2,4), (1,3,2)(1,4)(2,3)\}$$

$$= \{(1,3,2), (2,3,4), (1,2,4), (1,4,3)\}.$$  

The right cosets of $V$ in Alt(4) can be computed to be
\[ V^1 = \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \]

\[ V(1,2,3) = \{(1,2,3), (1,2)(3,4)(1,2,3), (1,3)(2,4)(1,2,3), (1,4)(2,3)(1,2,3)\} \]
\[ = \{(1,2,3), (2,4,3), (1,4,2), (1,3,4)\} \]

\[ V(1,3,2) = \{(1,3,2), (1,2)(3,4)(1,3,2), (1,3)(2,4)(1,3,2), (1,4)(2,3)(1,3,2)\} \]
\[ = \{(1,3,2), (1,4,3), (2,3,4), (1,2,4)\} \]

We use the same representatives for no reason other than laziness, this is not guaranteed to work in general. We observe that yes, the left and right coset decompositions yield the same partitioning of \(\text{Alt}(4)\). We will see later that this implies that \(V\) is a normal subgroup of \(\text{Alt}(4)\).

\[ \square \]

**SECTION 9**

3. Let \(G\) be a group

   c) Show that if \(f : G \to H\) is a group isomorphism then \(f(Z(G)) = Z(H)\).

**Proof.**

We show inclusion both ways.

To show \(f(Z(G)) \subseteq Z(H)\), we need to show for every \(y \in f(Z(G))\) that \(hy = yh\) for all \(h \in H\).

By definition \(f(Z(G)) = \{y \in H : y = f(x)\text{ for some }x \in Z(G)\}\), and so we get that \(hy = hf(x)\) for some \(x \in Z(G)\). Since \(f\) is an isomorphism, a fortiori it is a surjection, so for every \(h \in H\) there is a \(g \in G\) such that \(f(g) = h\). So then

\[ hy = hf(x) = f(g)f(x) \]

but since \(f\) is a homomorphism \(f(g)f(x) = f(gx)\). Since \(x \in Z(G)\), we know that \(gx = xg\) for every \(g \in G\), and so we get that

\[ f(g)f(x) = f(gx) = f(xg) = f(x)f(g) = yh \]

as desired.

To show that \(Z(H) \subseteq f(Z(G))\) we note that since \(f\) is an isomorphism, so there exists an isomorphism \(f^{-1} : H \to G\) (such that \(f \circ f^{-1} = \text{id}_H\) and \(f^{-1} \circ f = \text{id}_G\)). So by the previous result applied to \(f^{-1} : H \to G\) we get that \(f^{-1}(Z(H)) \subseteq Z(G)\). Applying \(f\) to both sides gives us \(\text{id}_H(Z(H)) \subseteq f(Z(G))\), and so \(Z(H) \subseteq f(Z(G))\). \(\square\)
7. Assume that $G$ is a simple abelian group. Show that $G$ is cyclic and that the order of $G$ is prime.

**Proof.** Since $G$ is abelian, every subgroup of $G$ is normal, and the definition of *simple* means that the only normal subgroups of $G$ are $G$ itself and the trivial subgroup $\{e_G\}$. This implies that the only subgroups of $G$ are $G$ and $\{e_G\}$.

Let $x \in G$ be a nontrivial element (i.e. not the identity), then $\langle x \rangle$ is a subgroup of $G$. Since the only subgroups of $G$ are $G$ and $\{e_G\}$ and $x \neq e_G$, it must be that $G = \langle x \rangle$, so $G$ is cyclic.

To show that $G$ is of finite order, consider that also $\langle x^2 \rangle$ is also a subgroup of $G$. If $x^2 = e_G$ then $o(x) = 2$ and $G$ is cyclic of order 2 (which is prime), otherwise we must have $\langle x^2 \rangle = \langle x \rangle = G$. This implies that $x = x^{2k}$ for some $k$, hence $x^{2k-1} = e_G$, so $x$ has finite order.

Lastly we need to show that $o(x)$ is prime. Let $d = o(x)$, suppose $d = nk$ for some $n, k > 1$, then $o(x^k) = \frac{d}{\gcd(d, k)} = \frac{d}{k} = n$. So in particular $(x^k)$ is a subgroup of order $n$, which is strictly greater than 1 (so it cannot be $\{e_G\}$) and strictly less than $d$ (so it cannot be $G$), this contradicts the fact that the only subgroups of $G$ are $G$ and $\{e_G\}$. Hence $d$ must be prime.

*Note: throughout this exercise we are using the fact that $o(x) = |\langle x \rangle|$. 

---

**SECTION 10**

3. Let $M$ and $N$ be normal subgroups of a group $G$ and assume that $M \cap N = 1$.

   b) Assume additionally that $MN = G$. Show that the function $f : M \times N \to G$, $(a, b) \mapsto ab$, is an isomorphism. Here $M \times N$ denotes the direct product group formed from the groups $M$ and $N$.

**Proof.**  b) First we show that the function $f$ defined is a homomorphism. It is sufficient to show that

$$f((m_1, n_1) \cdot (m_2, n_2)) = f((m_1, n_1)) \cdot f((m_2, n_2)).$$

First we compute the left hand side

$$f((m_1, n_1) \cdot (m_2, n_2)) = f((m_1 m_2, n_1 n_2)) = m_1 m_2 n_1 n_2.$$

Now the right hand side

$$f((m_1, n_1)) \cdot f((m_2, n_2)) = (m_1 n_1) \cdot (m_2 n_2) = m_1 n_1 m_2 n_2.$$
By part (a), we know that \( n_1 m_2 = m_2 n_1 \), so then \( m_1 m_2 n_1 n_2 = m_1 n_1 m_2 n_2 \), which is what we needed to show that \( f \) is a homomorphism.

To show that \( f \) is an isomorphism, we now need only show that \( f \) is surjective and injective.

To show that \( f \) is surjective: note that every element of \( MN \) is of the form \( mn \) where \( m \in M \) and \( n \in N \). So to show \( f \) is surjective we need to find an element in \( M \times N \) which maps to \( mn \), namely \((m, n)\) gets mapped to \( mn \) by the function \( f \).

To show that \( f \) is injective: since \( f \) is a homomorphism, it suffices to show that \( \ker(f) \) is trivial (i.e. \( \ker(f) = \{e\} \)). By definition of the kernel

\[
\ker(f) = \{(m, n) \in M \times N : f((m, n)) = e\}
\]

\[
= \{(m, n) \in M \times N : mn = e\}
\]

\[
= \{(m, n) \in M \times N : n = m^{-1}\}
\]

so the elements in the kernel are pairs \((m, n)\) where \( n = m^{-1} \), but this implies that \( n = m^{-1} \in M \cap N = \{e\} \) (since \( n \in N \) and \( m^{-1} \in M \) and they are the same element), which of course implies that \((m, n) = (e, e)\).

\[
\square
\]

8. Let \( M \) and \( N \) be normal subgroups of a group \( G \) such that \( G/M \) and \( G/N \) are abelian. Show that \( G/(M \cap N) \) is abelian. (Hint: Show that \( f: G \to G/M \times G/N, a \to (aM, aN) \), is a homomorphism. Determine its kernel and use the first Isomorphism Theorem.)

**Proof.** Let’s follow the hint and consider the map

\[
f: G \to G/M \times G/N
\]

\[
a \to (aM, aN).
\]

To show that \( f \) is a homomorphism we show that \( f(ab) = f(a)f(b) \). We see that \( f(ab) = (abM, abN) \) and on the other hand \( f(a)f(b) = (aM, aN) \cdot (bM, bN) = (aMbM, aNbN) \). But since \( M \) and \( N \) are normal, \( a(Mb)M = a(bM)M \) and \( a(Nb)N = a(bN)N \).

Following the hint, let’s compute the kernel of this map.

\[
(f) = \{a \in G : f(a) = (eM, eN)\}
\]

\[
= \{a \in G : (aM, aN) = (eM, eN)\}.
\]

We observe that \( aM = eM \) if and only if \( a \in M \) and similarly \( aN = eN \) if and only if \( a \in N \), so we see that \( (aM, aN) = (eM, eN) \) if and only if \( a \in M \cap N \). So this of course implies that

\[
(f) = \{a \in G : a \in M \cap N\} = M \cap N.
\]
By the first isomorphism theorem we get that

\[ G / (M \cap N) = G / \ker(f) \cong \text{image}(f). \]

So \( G / (M \cap N) \) is isomorphic to the image of \( f \), which is a subgroup of \( G / M \times G / N \). Since \( G / M \times G / N \) is abelian, so is \( \text{image}(f) \) and hence so is \( G / (M \cap N) \). \qed

SECTION 11

1. Let \( X \) be a \( G \)-set via \( \ast \).

(a) Show that \( \text{stab}_G(x) := \{ g \in G \mid g \ast x = x \} \), the stabilizer of \( x \) in \( G \), is a subgroup of \( G \).

(b) Show that for \( g \in G \) and \( x \in X \) one has \( \text{stab}_G(g \ast x) = g \text{stab}_G(x) g^{-1} \).

(c) Let \( \rho : G \to \text{Sym}(X) \) denote the permutation representation of the \( G \)-set \( X \). Show that \( \ker(\rho) = \bigcap_{x \in X} \text{stab}_G(x) \).

(d) Show that for ever \( x \in X \) one has: \( x \in X^G \iff \text{stab}_G(x) = G \).

Proof. (a) To show \( \text{stab}_G(x) \) is a subgroup, we need to show

i. \( 1_G \in \text{stab}_G(x) \)

ii. If \( g, h \in \text{stab}_G(x) \) then \( gh \in \text{stab}_G(x) \)

iii. If \( g \in \text{stab}_G(x) \) then \( g^{-1} \in \text{stab}_G(x) \)

By definition \( g \in \text{stab}_G(x) \) if and only if \( g \ast x = x \), so this is what we will use to show elements belong to \( \text{stab}_G(x) \).

i. By the first axiom of group actions, \( 1_G \ast x' = x' \) for all \( x' \in X \), so in particular \( 1_G \ast x = x \). This shows \( 1_G \in \text{stab}_G(x) \).

ii. We assume \( g, h \in \text{stab}_G(x) \), this means \( g \ast x = x \) and \( h \ast x = x \). We want to show \((gh) \ast x = x \) because this would mean \( gh \in \text{stab}_G(x) \).

By the second axiom of group actions, \((gh) \ast x = g \ast (h \ast x) \). Since \( h \ast x = x \) and \( g \ast x = x \) this gives us that

\[(gh) \ast x = g \ast (h \ast x) = g \ast x = x \]

as desired.

iii. We assume \( g \in \text{stab}_G(x) \), this means that \( g \ast x = x \). We want to show that \( g^{-1} \ast x = x \). Again we compute the left hand side using the fact that \( g \ast x = x \)

\[ g^{-1} \ast x = g^{-1} \ast (g \ast x) = (g^{-1} g) \ast x = 1_G \ast x = x \]

as desired.
(b) We show \( \text{stab}_G(g \ast x) = \text{gstab}_G(x)g^{-1} \) by dual inclusion.

"\( \subseteq \)". We want to show \( \text{stab}_G(g \ast x) \subseteq \text{gstab}_G(x)g^{-1} \), this is equivalent to \( g^{-1}\text{stab}_G(g \ast x)g \subseteq \text{stab}_G(x) \).

Let \( h \in \text{stab}_G(g \ast x) \), then by definition \( h \ast (g \ast x) = g \ast x \). To show the desired inclusion, we need to show that \( g^{-1}hg \in \text{stab}_G(x) \), which is equivalent to showing \( (g^{-1}hg) \ast x = x \). We compute the left hand side of the desired equality

\[
(g^{-1}hg) \ast x = (g^{-1}h)(g \ast x) = g^{-1}(h \ast (g \ast x)) = g^{-1}(g \ast x) = (g^{-1}g) \ast x = 1_G \ast x = x
\]

as desired.

"\( \supseteq \)". We want to show that \( \text{stab}_G(g \ast x) \supseteq \text{gstab}_G(x)g^{-1} \). Let \( h \in \text{stab}_G(x) \), by definition this means \( h \ast x = x \). We want to show that \( ghg^{-1} \in \text{stab}_G(g \ast x) \), which is equivalent to \( (ghg^{-1}) \ast (g \ast x) = g \ast x \). Let’s expand the left hand side of the desired equality

\[
(ghg^{-1}) \ast (g \ast x) = (ghg^{-1}g) \ast x = (gh) \ast x = g \ast (h \ast x) = g \ast x
\]

as desired.

(c) By definition of the permutation representation \( \rho(g) := \sigma_g \) where \( \sigma_g \) is the bijection defined by the group action as follows

\[
\sigma_g : X \rightarrow X
\]

\[
x \mapsto g \ast x.
\]

The definition of the kernel is \( \ker(\rho) = \{ g \in G \mid \rho(g) = 1 \} \), (i.e. all the elements of \( G \) which get mapped to the identity element in the group \( \text{Sym}(X) \)). Here \( \text{Sym}(X) \) is the permutation group on the set \( X \) so the identity element is the trivial permutation (i.e. the permutation which sends every element \( x \in X \) to itself).

Now that we are clear about the definitions of all of the things involved let us see what we need to prove. We want to show that \( \ker(\rho) = \bigcap_{x \in X} \text{stab}_G(x) \).

By the definitions we wrote out above, we can see that \( g \in \ker(\rho) \) if and only if \( \rho(g) := \sigma_g \) is the trivial permutation. That is, if and only if

\[
\sigma_g(x) = x \quad \text{for all } x \in X.
\]

Again, by definition, \( \sigma_g(x) = g \ast x \), so this is really saying \( g \in \ker(\rho) \) if and only if \( g \ast x = x \) for all \( x \in X \).

Let us compare this condition to what it would mean for \( g \) to be an element in \( \bigcap_{x \in X} \text{stab}_G(x) \). Well, this means \( g \in \text{stab}_G(x) \) for all \( x \in X \), but as we recall from the definition of the stabilizer, this means that \( g \ast x = x \) for all \( x \in X \).

So we see that the condition for being in both subgroups is exactly the same, all we have done is unravel the definitions to see that they are in fact saying the same thing.
(d) Let \( x \in X^G \), the definition of \( X^G = \{ x \in X \mid g * x = x \text{ for all } g \in G \} \). So then \( g * x = x \) for all \( g \in G \), this means that \( g \in \text{stab}_G(x) := \{ g \in G \mid g * x = x \text{ for all } g \in G \} \), hence \( \text{stab}_G(x) = G \).

Similarly, if \( \text{stab}_G(x) = G \) then \( g * X = x \) for all \( g \in G \), which means \( x \in X^G \).

3. Show that \( \text{Inn}(G) \) is normal in \( \text{Aut}(G) \).

**Proof.** We start off by defining all the objects and making precise what we want to prove.

By definition \( \text{Inn}(G) \) is the group of automorphisms given by conjugation by elements of \( G \), precisely

\[
\text{Inn}(G) = \{ c_a : a \in G \}
\]

where \( c_a \) is the automorphism defined by

\[
c_a : G \to G \\
x \mapsto axa^{-1}.
\]

It won’t be relevant to this exercise, but it is also good to know (and to prove) that \( \text{Inn}(G) \cong G/Z(G) \). This is part of the reason we like inner automorphisms, because they are easily describable and the group \( \text{Inn}(G) \) is easily relatable to \( G \) itself.

On the other hand \( \text{Aut}(G) = \{ f : f : G \to G \text{ is an isomorphism} \} \) is just given abstractly as the group of all automorphisms. The group operation for both of these groups is composition of functions.

Now onto the content of the proof, we want to show that \( \text{Inn}(G) \) is normal in \( \text{Aut}(G) \), that is to say, we want to show that \( f \text{Inn}(G) f^{-1} = \text{Inn}(G) \) for all \( f \in \text{Aut}(G) \).

First we show \( f \text{Inn}(G) f^{-1} \subseteq \text{Inn}(G) \), let \( c_a \) be an element of \( \text{Inn}(G) \) then \( f \circ c_a \circ f^{-1} \) is in general another automorphism in \( \text{Aut}(G) \).

We want to show that \( f \circ c_a \circ f^{-1} \) is in fact contained in \( \text{Inn}(G) \), but everything in \( \text{Inn}(G) \) is an automorphism defined by conjugation by something, so if we can show \( f \circ c_a \circ f^{-1} \) is actually conjugation by something then we have shown this inclusion.

Let us ‘see’ what \( f \circ c_a \circ f^{-1} \) actually does...

\[
f \circ c_a \circ f^{-1} : G \to G \\
x \mapsto [f \circ c_a \circ f^{-1}](x)
\]

but what is \( [f \circ c_a \circ f^{-1}](x) \)? The automorphism \( f \) is just something arbitrary, so we can’t say much about that, we know how \( c_a \) acts though so we can say the following

\[
[f \circ c_a \circ f^{-1}](x) = [f \circ c_a](f^{-1}(x)) = f(a)f^{-1}(x)a^{-1} = f(a)f(f^{-1}(x))f(a^{-1}) = f(a)xf(a)^{-1}.
\]
Well, it appears as though applying $f \circ c_a \circ f^{-1}$ to the element $x$ is the same as conjugating $x$ by the element $f(a)$, the $x$ is arbitrary so in fact

$$f \circ c_a \circ f^{-1} : G \to G$$

$$x \mapsto [f \circ c_a \circ f^{-1}](x)$$

is the same as

$$c_{f(a)} : G \to G$$

$$x \mapsto f(a)x f(a)^{-1}$$

which is an inner automorphism by definition. So we see that $f \circ c_a \circ f^{-1} = c_{f(a)} \in \text{Inn}(G)$, which is what we wanted to show. This shows that $f \text{Inn}(G) f^{-1} \subseteq \text{Inn}(G)$.

The other direction asks us to show $f \text{Inn}(G) f^{-1} \supseteq \text{Inn}(G)$, but this is the same as $\text{Inn}(G) \supseteq f^{-1} \text{Inn}(G) f$, which is the same as what we showed above (except using $f^{-1}$ instead of $f$). The automorphism $f$ above was arbitrary, so we don't need to re-do the proof.

This shows $\text{Inn}(G)$ is normal in $\text{Aut}(G)$, and we are done. \qed

SECTION 12

1. Let $p$ be a prime, let $P$ be a $p$-group and let $Q < P$.

(a) Show that $N_P(Q) > Q$

(b) Show that if $[P : Q] = p$ then $Q \triangleleft P$.

Proof. (a) $N_P(Q)$ is the normalizer of $Q$ in $P$, let's define it.

$$N_P(Q) = \{g \in P : gQg^{-1} = Q\}$$

We want to show that $Q < N_P(Q)$, that is, we want to show that $qQq^{-1} = Q$ for every $q \in Q$.

There are a lot of ways to see that this is trivially true, one way is to recall that conjugation of a group by an element of the same group is an automorphism.

(b) Recall that $Q \triangleleft P$ if and only if $N_P(Q) = P$.

We know that $[P : Q] = [P : N_P(Q)][N_P(Q) : Q]$, and by assumption $[P : Q] = p$. Since $p$ is prime, we know that either $[N_P(Q) : Q] = 1$ or $p$.

If $[N_P(Q) : Q] = p$ then $[P : N_P(Q)] = 1$, which means $P = N_P(Q)$ which means $Q \triangleleft P$.

To show this we apply Lemma 12.2 which says the following:

If $G$ is a finite group and $H$ is a $p$-subgroup of $G$, then

$$[N_G(H) : H] \equiv [G : H] \pmod{p}.$$

When applied to our case (where $G = P$ and $H = Q$), we get that

$$[N_P(Q) : Q] \equiv [P : Q] \equiv 0 \pmod{p}.$$
so it must be the case that \([N_P(Q) : Q] = p\) and so \([P : N_P(Q)] = 1\) and so \(P = N_P(Q)\) and so \(Q \preceq P\).