Exercise 1.2.2

A group G is abelian if and only if the map $G \to G$ given by $x \mapsto x^{-1}$ is an automorphism.

Proof. ($\Rightarrow$) Suppose G is abelian. We want to show that the map $f : G \to G$ given by $f(x) = x^{-1}$ is an automorphism. First, we show that f is a homomorphism. Let $a, b \in G$ and consider $f(ab)$. We have

$$f(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = f(a)f(b),$$

where the third equality follows from the fact that G is abelian. Next, we show that f is bijective. To see that f is injective, suppose $f(a) = f(b)$ for some distinct $a, b \in G$. Then we have

$$f(a) = a^{-1} = b^{-1} = f(b).$$

Since inverses are unique in a group, we must have $a = b$, a contradiction. Thus, f is injective. To see that f is surjective, let $y \in G$. We want to find an $x \in G$ such that $f(x) = y$. Note that if we let $x = y^{-1}$, then we have

$$f(x) = x^{-1} = y.$$

Thus, f is surjective. Since f is a bijective homomorphism, it is an automorphism.

($\Leftarrow$) Suppose the map $f : G \to G$ given by $x \mapsto x^{-1}$ is an automorphism. We want to show that G is abelian. Let $a, b \in G$. Since f is a homomorphism, we have

$$f(ab) = f(a)f(b).$$

Expanding both sides, we have

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

Taking the inverse of both sides, we have

$$ab = (a^{-1}b^{-1})^{-1} = ba,$$

where the last equality follows from the property of inverses in a group. Thus, G is abelian. □

Exercise 1.2.3

Let Q_8 be the group (under ordinary matrix multiplication) generated by the complex matrices $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$, where $i^2 = -1$. Show that Q_8 is a nonabelian group of order 8. Q_8 is called the **quaternion group**. [*Hint:* Observe that $BA = A^3B$, whence every element of Q_8 is of the form A^iB^j. Note also that $A^4 = B^4 = I$, where $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity element of Q_8.]

Proof. Following the hint first we compute BA.

$$BA = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}.$$

Next we compute A^3B.

$$A^3B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^3 \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}.$$

Therefore we have that $BA = A^3B$ therefore we have that every element is of the form A^iB^j. Notice next that $A^4 = B^4 = I$ where I is the identity matrix. Thus, the possible values for i and j are $0, 1, 2, 3$. This gives us a total of $4 \cdot 4 = 16$ possible combinations of A^iB^j. However, we can reduce this number by noting that $A^2 = B^2$. Thus, we have the following distinct elements of Q_8:

$$I, A, A^2, A^3, B, AB, A^2B, A^3B.$$

Thus, $|Q_8| = 8$. Finally, we show that Q_8 is nonabelian. To see this, we compute AB and BA.

$$AB = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad BA = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}.$$

Since $AB \neq BA$, we conclude that Q_8 is nonabelian. □

Exercise 1.4.8

If H and K are subgroups of finite index of a group G such that $[G:H]$ and $[G:K]$ are relatively prime, then $G = HK$.

Proof. Let H and K be subgroups of finite index of a group G such that $[G:H]$ and $[G:K]$ are relatively prime. Let $[G:H] = m$ and $[G:K] = n$. We want to show that $G = HK$. Notice first that $H \cap K$ is a subgroup of both H and K. So by Theorem 1.4.5 we have that

$$\begin{aligned}[G:H\cap K] = [G:H][H:H\cap K] &\iff [G:H\cap K] = m[H:H\cap K]\\ [G:H\cap K] = [G:K][K:H\cap K] &\iff [G:H\cap K] = n[K:H\cap K]\end{aligned}$$

Then by substitution we have $m[H:H\cap K] = n[K:H\cap K]$. Since $(m,n) = 1$, we have $m|[K:H\cap K]$ and $n|[H:H\cap K]$. For brevity, let $[H:H\cap K] = a, [K:H\cap K] = b$. Then,

$$\begin{aligned}[G:H\cap K] &= mna\\ [G:H\cap K] &= mnb.\end{aligned}$$

This implies that $a = b$. By Proposition 1.4.8, $[H:H\cap K] \leq [G:K]$. This yields $na \leq n$, which forces $a = 1$. Then $[G:H\cap K] = [G:H][G:K]$ so by Proposition 1.4.9 we have that $G = HK$ as desired. □

Exercise 1.4.12

If H and K are subgroups of a group G, then $[H \vee K : H] \geq [K : H\cap K]$.

Proof. Let H and K be subgroups of a group G. Notice then that $H < H \vee K$ and $K < H \vee K$. From Theorem 1.4.8 we have that $[K:K\cap H] \leq [H\vee K:H]$, that is, $[H\vee K:H] \geq [K:K\cap H]$ as desired. □

Exercise 1.4.13

If $p > q$ are primes, a group of order pq has at most one subgroup of order p.
[*Hint:* Suppose H, K are distinct subgroups of order p. Show that $H \cap K = \langle e \rangle$; use Exercise 1.2.12 to get a contradiction.]

Proof. Let $p > q$ be primes and let G be a group of order pq. Suppose H, K are distinct subgroups of order p. We want to show that $H \cap K = \langle e \rangle$. To see this, let $x \in H \cap K$. Since H and K are subgroups of order p, we have that the order of any element in H or K must divide p by Lagrange's Theorem. Thus, the possible orders for x are 1 or p. If the order of x is 1, then we have that $x = e$. If the order of x is p, then we have that $\langle x \rangle = H = K$, a contradiction since we assumed that H and K are distinct. Therefore, we must have that the order of x is 1, and thus we have that $H \cap K = \langle e \rangle$.
Following the hint, we use Exercise 1.2.12 to get a contradiction.
We can see that $[K:H\cap K] = [K:\langle e\rangle] = p$. Next, we note that $H \vee K$ is a subgroup of G that contains both H and K. Thus, we have that $|H \vee K|$ must be a multiple of both $|H|$ and $|K|$. Since $|H| = |K| = p$, we have that $|H \vee K|$ must be a multiple of p. The possible multiples of p that are less than or equal to pq are p and pq. If $|H \vee K| = p$, then we have that $H \vee K = H = K$, a contradiction since we assumed that H and K are distinct. Thus, we must have that $|H \vee K| = pq$. Therefore, we have that $H \vee K = G$. We also have that $|G| = pq = [H\vee K:H]\cdot|H| = [H\vee K:H]\cdot p$. Dividing both sides by p, we have that $q = [H\vee K:H]$. Thus, we have that $[H\vee K:H] = q$.
Finally, we note that since $p > q$, we have that $[H\vee K:H] = q < p = [K:H\cap K]$. This contradicts Exercise 1.4.12 which states that $[H\vee K:H] \geq [K:H\cap K]$. Therefore, we conclude that a group of order pq has at most one subgroup of order p. □

Exercise 1.5.1

If N is a subgroup of index 2 in a group G, then N is normal in G.

Proof. Let N be a subgroup of index 2 in a group G. We want to show that N is normal in G. Choose $g \in G$ arbitrarily. If $g \in N$, then we have that $gN = N = Ng$. If $g \notin N$ then, since there are only two left cosets of N in G, and $g \notin N$ we must have that the cosets are gN and N. We also have that cosets partition G so we have that $G = N \cup gN$. Similarly, we have that the right cosets of N in G are Ng and N. Since cosets partition G, we have that $G = N \cup Ng$. Thus, we have that $gN = Ng$. Since $g \in G$ was arbitrarily chosen, we conclude that N is normal in G.

□

Exercise 1.5.6

Let $H < G$; then the set aHa^{-1} is a subgroup for each $a \in G$, and $H \cong aHa^{-1}$.

Proof. Let $H < G$. We want to show that the set aHa^{-1} is a subgroup for each $a \in G$, and that $H \cong aHa^{-1}$. First, we show that aHa^{-1} is a subgroup of G.
First we show that $aHa^{-1} < G$ for all $a \in G$.
Let $a \in G$ be arbitrarily chosen. Then, by definition we have that $aHa^{-1} = \{aha^{-1} | h \in H\}$. Let $x, y \in aHa^{-1}$ then we have that $x = ah_1a^{-1}$ and $y = ah_2a^{-1}$ for some $h_1, h_2 \in H$ by definition. Now consider xy^{-1}. We have

$$xy^{-1} = (ah_1a^{-1})(ah_2a^{-1})^{-1} = (ah_1a^{-1})(ah_2^{-1}a^{-1}) = ah_1h_2^{-1}a^{-1}.$$

Clearly, $ah_1h_2^{-1}a^{-1} \in aHa^{-1}$. Therefore, by Theorem 1.2.5 $aHa^{-1} < G$ for all $a \in G$ as a was arbitrarily chosen.
Next we show that $H \cong aHa^{-1}$.
Let $\varphi : H \to aHa^{-1}$ be given by $x \mapsto axa^{-1}$. We first show φ is a homomorphism.
Let $x, y \in H$ and consider $\varphi(xy)$,

$$\varphi(xy) = axya^{-1} = axeya^{-1} = axa^{-1}aya^{-1} = \varphi(x)\varphi(y).$$

Therefore φ is a homomorphism.
Next we show injectivity. Let x, y be distinct elements of H. For sake of contradiction, suppose $\varphi(x) = \varphi(y)$. Then we have

$$\varphi(x) = \varphi(y)$$

$$\begin{aligned} axa^{-1} &= aya^{-1} \\ \implies a^{-1}axa^{-1} &= a^{-1}aya^{-1} \\ \implies xa^{-1}a &= ya^{-1}a \\ \implies x &= y. \end{aligned}$$

This a contradiction, therefore we have that φ is injective.
Next we show surjectivity. Let $y \in aHa^{-1}$. We want to find an $x \in H$ such that $\varphi(x) = y$. Note that if we let $x = a^{-1}ya$, then we have

$$\varphi(x) = axa^{-1} = a(a^{-1}ya)a^{-1} = y.$$

Thus, φ is surjective.
Since φ is a bijective homomorphism, we conclude that $H \cong aHa^{-1}$ as desired.

□

Exercise 1.5.7

Let G be a finite group and H a subgroup of G of order n. If H is the only subgroup of G of order n, then H is normal in G.

Proof. Let G be a finite group and H a subgroup of G of order n. Suppose H is the only subgroup of G of order n. We want to show that H is normal in G. To see this, let $a \in G$ be arbitrarily chosen. We want to show that $aHa^{-1} = H$. First, we note that since H is a subgroup of G, we have that aHa^{-1} is also a subgroup of G. Then from Exercise 1.5.6, we have that $H \cong aHa^{-1}$. Thus, we have that $|H| = |aHa^{-1}| = n$. Since H is the only subgroup of G of order n, we must have that $aHa^{-1} = H$. Since $a \in G$ was arbitrarily chosen, we conclude that H is normal in G. □

Exercise 1.6.3

If $\sigma = (i_1 i_2 \dots i_r) \in S_n$ and $\tau \in S_n$, then $\tau\sigma\tau^{-1}$ is the r-cycle $(\tau(i_1)\tau(i_2)\dots\tau(i_r))$.

Proof. Let $\sigma = (i_1 i_2 \dots i_r) \in S_n$ and $\tau \in S_n$. We want to show that $\tau\sigma\tau^{-1}$ is the r-cycle $(\tau(i_1)\tau(i_2)\dots\tau(i_r))$. To see this, let $x \in \{1, 2, \dots, n\}$. We consider two cases.
Case 1: Suppose $x = \tau(i_k)$ for some $k \in \{1, 2, \dots, r\}$. Then we have

$$(\tau\sigma\tau^{-1})(x) = (\tau\sigma)(\tau^{-1}(x)) = (\tau\sigma)(i_k) = \tau(i_{k+1}),$$

where the last equality follows from the definition of σ and we take $i_{r+1} = i_1$. Thus, we have that $(\tau\sigma\tau^{-1})(\tau(i_k)) = \tau(i_{k+1})$ for all $k \in \{1, 2, \dots, r\}$.
Case 2: Suppose $x \neq \tau(i_k)$ for all $k \in \{1, 2, \dots, r\}$. Then we have

$$(\tau\sigma\tau^{-1})(x) = (\tau\sigma)(\tau^{-1}(x)) = (\tau)(\tau^{-1}(x)) = x,$$

where the second equality follows from the definition of σ since $\tau^{-1}(x) \neq i_k$ for all k. Thus, we have that $(\tau\sigma\tau^{-1})(x) = x$ for all x not in the set $\{\tau(i_1), \tau(i_2), \dots, \tau(i_r)\}$.
Combining both cases, we have that $\tau\sigma\tau^{-1}$ sends $\tau(i_k)$ to $\tau(i_{k+1})$ for all k and fixes all other elements. Therefore, we conclude that $\tau\sigma\tau^{-1}$ is the r-cycle $(\tau(i_1)\tau(i_2)\dots\tau(i_r))$ as desired.

□

Exercise 1.6.8

The group A_4 has no subgroup of order 6.

Proof. Suppose for sake of contradiction that A_4 has a subgroup H of order 6. Since $|A_4| = 12$, we have that the index of H in A_4 is given by

$$[A_4 : H] = \frac{|A_4|}{|H|} = \frac{12}{6} = 2.$$

Thus, we have that H is a subgroup of index 2 in A_4. From Exercise 1.5.1, we have that any subgroup of index 2 in a group is normal. Therefore, we have that H is normal in A_4.
Next, we note that since H is a subgroup of order 6, it must contain an element of order 3 by Cauchy's Theorem (Theorem 2.5.2). Then we have that since H is normal in A_4 and contains an element of order 3, we have that $H = A_4$ by Theorem 1.6.12 which is a contradiction since $|H| = 6$ and $|A_4| = 12$. Therefore, we conclude that A_4 has no subgroup of order 6.

□

Exercise 1.6.12

The center (Exercise 1.2.11) of the group D_n is $\langle e \rangle$ if n is odd and isomorphic to $\mathbb{Z}_2$ if n is even.

Proof. Let D_n be the dihedral group of order $2n$ with generators $\{r, s\}$ where r is a rotation of order n and s is a reflection of order 2. We want to show that the center of D_n is $\langle e \rangle$ if n is odd and isomorphic to $\mathbb{Z}_2$ if n is even. First, we consider the case when n is odd.
Case 1: Suppose n is odd. We want to show that the center of D_n is $\langle e \rangle$. To see this, let $x \in Z(D_n)$. We want to show that $x = e$. Since D_n is generated by a rotation r of order n and a reflection s of order 2, we have that any element in D_n can be written as either r^k or $r^k s$ for some integer k. We consider two cases.
Subcase 1: Suppose $x = r^k$ for some integer k. Since $x \in Z(D_n)$, we have that $xr = rx$. Thus, we have

$$r^k r = r r^k \implies r^{k+1} = r^{k+1},$$

which is true for all integers k. Next, since $x \in Z(D_n)$, we have that $xs = sx$. Thus, we have

$$r^k s = s r^k \implies r^{2k} = e,$$

where the last equality follows from the relation $sr^k s = r^{-k}$. Since n is odd, we have that $r^{2k} = e$ if and only if k is a multiple of n. Thus, we have that $x = r^k = e$.
Subcase 2: Suppose $x = r^k s$ for some integer k. Since $x \in Z(D_n)$, we have that $xr = rx$. Thus, we have

$$r^k s r = r r^k s \implies r^{k-1} s = r^{k+1} s \implies r^{-2} = e,$$

where the last equality follows from the relation $sr^k s = r^{-k}$. Since n is odd, we have that $r^{-2} = e$ is a contradiction. Therefore, we must have that $x \neq r^k s$ for any integer k.
Combining both subcases, we have that $x = e$. Since $x \in Z(D_n)$ was arbitrarily chosen, we conclude that $Z(D_n) = \langle e \rangle$ when n is odd.
Case 2: Suppose n is even. We want to show that the center of D_n is isomorphic to $\mathbb{Z}_2$. To see this, let $x \in Z(D_n)$. We want to show that x is either e or $r^{n/2}$. Since D_n is generated by a rotation r of order n and a reflection s of order 2, we have that any element in D_n can be written as either r^k or $r^k s$ for some integer k. We consider two cases.
Subcase 1: Suppose $x = r^k$ for some integer k. Since $x \in Z(D_n)$, we have that $xr = rx$. Thus, we have

$$r^k r = r r^k \implies r^{k+1} = r^{k+1},$$

which is true for all integers k. Next, since $x \in Z(D_n)$, we have that $xs = sx$. Thus, we have

$$r^k s = s r^k \implies r^{2k} = e,$$

where the last equality follows from the relation $sr^k s = r^{-k}$. Since n is even, we have that $r^{2k} = e$ if and only if k is a multiple of $n/2$. Thus, we have that $x = r^k$ is either e or $r^{n/2}$.
Subcase 2: Suppose $x = r^k s$ for some integer k. Since $x \in Z(D_n)$, we have that $xr = rx$. Thus, we have

$$r^k s r = r r^k s \implies r^{k-1} s = r^{k+1} s \implies r^{-2} = e,$$

where the last equality follows from the relation $sr^k s = r^{-k}$. Since n is even, we have that $r^{-2} = e$ is a contradiction. Therefore, we must have that $x \neq r^k s$ for any integer k.
Combining both subcases, we have that x is either e or $r^{n/2}$. Since $x \in Z(D_n)$ was arbitrarily chosen, we conclude that $Z(D_n) = \{e, r^{n/2}\}$ when n is even. Finally, we note that the set $\{e, r^{n/2}\}$ is isomorphic to $\mathbb{Z}_2$ since it is a group of order 2 under the operation of composition. Therefore, we conclude that the center of D_n is $\langle e \rangle$ if n is odd and isomorphic to $\mathbb{Z}_2$ if n is even as desired.

□