14.1. Work out the conjugacy classes of $D_5$.

**Solution.** Use the result in 12.10. Since $\{r^{2k}\}$ in $D_5$ contains all elements $\{r^ks\}$, the two classes $\{r^{2k}\}$ and $\{r^{2k+1}\}$ in $D_\infty$ now become one class in $D_5$. Therefore the conjugacy classes are

$$\{e\}, \{r, r^4\}, \{r^2, r^3\}, \{r^k\}.$$

14.5. Prove that the 3-cycles in $A_5$ form a single conjugacy class. Find two 5-cycles in $A_5$ which are not conjugate in $A_5$.

**Proof.** Two 3-cycles in $A_5$ contain at most 5 different elements and at least 3, we then have the following three cases:

Case (i). They have 3 different elements. If the two 3-cycles are identical, they are certainly conjugate. If not, they can be written as $(abc)$ and $(acb)$. Let $g = (bc)(de) \in A_5$, where $d, e$ are the other two elements, then $g(abc)g^{-1} = (acb)$.

Case (ii). They have 4 different elements. If the first one is $(abc)$, then the second one could be $(abd)$ or $(adb)$. But this two 3-cycles are conjugate by case (i), without loss of generality we assume it’s $(abd)$. Let $g = (cde) \in A_5$, again we have $g(abc)g^{-1} = (adb)$.

Case (iii). They have 5 different elements. Then they can be written as $(abc)$ and $(ade)$. Let $g = (bd)(ce)$.

Since we’ve exploited all possibilities, we conclude that all 3-cycles in $A_5$ form a conjugate class. Notice that the only $g \in S_5$ that conjugates $(12345)$ and $(13245)$, i.e. satisfies $g(12345)g^{-1} = (13245)$, is the 2-cycle $(23)$. Since $(23)$ is odd, $(12345)$ and $(13245)$ are not conjugate in $A_5$.

14.7. Work out the conjugacy classes and the centre of the quaternion group $Q$. What is the center of $S^3$?

**Solution.** $Q$ contains eight elements:

$$1, -1, i, -i, j, -j, k, -k.$$ 

Since 1 and $-1$ commute with all other elements, each of them forms a conjugacy class. Notice that

$$iji^{-1} = j^{-1}ij = -iji = -i, \quad kik^{-1} = k^{-1}ik = -kik = -i,$$

$i$ and $-i$ form a conjugacy class. Similarly we can find that there are other two conjugacy classes $\{j, -j\}$ and $\{k, -k\}$. Since an element in the centre if and only if it forms a conjugacy class itself, the centre of $Q$ is $\{1, -1\}$.

If $z = a + bi + cj + dk$ is an element in the centre of $S^3$, it commutes with all elements in $S^3$, in particular it commutes with $i, j$ and $k$. Notice that

$$i(a + bi + cj + dk)i^{-1} = iai^{-1} + i(bi)i^{-1} + i(cj)i^{-1} + i(dk)i^{-1} = a + bi - cj - dk,$$
it follows that $c$ and $d$ are zero. Similarly, we know $b$ and $k$ are zero by writing out $jzj^{-1} = z$ explicitly. Therefore $z = a$ is a real number, hence $1$ or $-1$. Notice that $\pm 1$ commute with all elements in $S^3$ since they commute with $i$, $j$ and $k$; we conclude the centre of $S^3$ is exactly $\{1, -1\}$.

15.1. If $H$ and $J$ are both subgroups of a group $G$, prove that $HJ$ is a subgroup of $G$ if and only if $HJ = JH$.

**Proof.** If $HJ = JH$, then for any $hj \in HJ$ where $h \in H$ and $j \in J$,

$$(hj)^{-1} = j^{-1}h^{-1} \in JH = HJ,$$

proving the existence of inverses. For any $h_1j_1, h_2j_2 \in HJ$ where $h_1, h_2 \in H$ and $j_1, j_2 \in J$, there are $h_3j_3 = j_1h_2$ since $HJ = JH$. Then

$$(h_1j_1)(h_2j_2) = h_1h_3j_3j_2 \in HJ,$$

i.e. $HJ$ is closed under multiplication, hence a subgroup.

Conversely, if $HJ$ is a subgroup, then for any $j \in J$ and $h \in H$, $h^{-1}j^{-1}$ is an element of $HJ$, thus its inverse

$$(h^{-1}j^{-1})^{-1} = jh \in JH,$$

i.e. $JH \subseteq HJ$. Then

$$(hj)^{-1} = j^{-1}h^{-1} = h_4j_4$$

for some $h_4 \in H$ and $j_4 \in J$,

$$hj = (h_4j_4)^{-1} = j^{-1}h_4^{-1} \in JH,$$

i.e. $HJ \subseteq JH$. Therefore we have $HJ = JH$.

15.2. Find all normal subgroups of $D_4$ and $D_5$. Generalise and deal with $D_n$ for arbitrary $n$.

**Solution.** We shall deal with $D_n$ directly. Let $N$ be a normal subgroup of $D_n$. If $r^k \notin N$ for any $k = 0, 1, \ldots, n - 1$, then $N$ is a subgroup of $\langle r \rangle$, hence the union of $\{r^k, r^{-k}\}$ where $r^k \in N$ since every element in $N$ implies both in $N$. From previous homework we know that $\{r^k, r^{-k}\}$ is a conjugacy class, thus $N$ is a union of conjugacy classes, in other words a normal subgroup. If $N$ contains an element $r^k$ for some $k$. There are two cases.

Case (i): $n$ is odd. From previous homework we know that all elements in the form $r^k$ form a conjugacy class. Since $N$ is normal, $N$ contains all elements in the class. In particular $N$ contains $s$ and $sr$ which generate $D_n$, thus $N = D_n$.

Case (ii): $n$ is even. There are two conjugacy classes formed by $r^k$ elements, namely $\{r^{\text{even}}s\}$ and $\{r^{\text{odd}}s\}$. Therefore either $\{s, r^2s\}$ or $\{r^{-1}s, rs\}$ is a subset of $N$. Since

$$(r^2s)s = (rs)(r^{-1}s) = r^2,$$
in either case $N$ contains $r^2$, hence all the $\frac{n}{2}$ even powers of $r$. Since each of the conjugacy classes has $\frac{n}{2}$ elements, that $N$ contains at least one of the classes implies that $N$ contains at least $n$ elements, hence exactly $n$ elements if $N$ is not $D_n$ itself. Notice that either conjugacy class along with even powers of $r$ forms a subgroup isomorphic to $D_{\frac{2n}{2}}$, in fact, it is the subgroup generated by $\{r^2, s\}$ or the one generated by $\{r^2, rs\}$. And it is normal because even powers of $r$ is the union of conjugacy classes $\{r^{\text{even}}, r^{\text{odd}}\}$. Therefore they're all possible normal subgroups other than $D_n$ itself. Notice that the argument works for $n = 2$ as well.

Finally we state the result in term of $n$. If $n$ is even, normal subgroups of $D_n$ are subgroups of $\langle r \rangle, \{r^{\text{even}}, r^{\text{even}}s\}, \{r^{\text{even}}, r^{\text{odd}}s\}$ and $D_n$. In case $n = 4$, all subgroups are:

$$\langle e \rangle, \langle r^2 \rangle, \langle r \rangle, \langle r^2, s \rangle, \langle r^2, rs \rangle, D_4.$$  

If $n$ is odd, normal subgroups are just subgroups of $\langle r \rangle$ and $D_n$, in case $n = 5$, they are:

$$\langle e \rangle, \langle r \rangle, D_5.$$  

15.5. Let $H$ be a normal subgroup of a group $G$, and let $J$ be a normal subgroup of $H$.

Then of course $J$ is a subgroup of $G$. Supply an example to show that $J$ need not be normal in $G$.

**Solution.** In the previous problem we showed that $H = \{e, r^2, s, r^2s\}$ is normal in $D_4$. Let $J = \{e, s\}$ a subgroup in $H$ that has index 2, hence normal in $H$. Again from the previous problem we know that $J$ is not normal in $D_4$.

15.14. Show that every element of the quotient group $\mathbb{Q}/\mathbb{Z}$ has finite order, but that only the identity element of $\mathbb{R}/\mathbb{Q}$ has finite order.

**Proof.** Take any element $[\frac{a}{b}] \in \mathbb{Q}/\mathbb{Z}$ where both $a$, $b$ are integers. $[\frac{a}{b}]$ stands for the equivalence class containing $\frac{a}{b}$, in other words all rationals that differ from $\frac{a}{b}$ by an integer. Observe that

$$b[\frac{a}{b}] = [b(\frac{a}{b})] = [a] = [0] \in \mathbb{Q}/\mathbb{Z},$$

the order of $[\frac{a}{b}]$ divides $b$, hence finite.

For any $[r] \in \mathbb{R}/\mathbb{Q}$, if it has finite order $n$, then

$$[nr] = n[r] = [0] \in \mathbb{R}/\mathbb{Q}.$$  

It then follows that $nr$ is a rational. Since $n \neq 0$, $r$ is also a rational, thus $[r]$ is the identity in $\mathbb{R}/\mathbb{Q}$.

16.1. Which of the following define homomorphisms from $\mathbb{C} - \{0\}$ to $\mathbb{C} - \{0\}$?

(a) $z \to z^*$  
(b) $z \to iz$

**Solution.** Only (a) defines a homomorphism.
Let \( z = a + bi \), then \( z^* = a - bi \). Since \( z \neq 0 \) implies that \( z^* \neq 0 \), \( z \rightarrow z^* \) is a map from \( \mathbb{C} - \{0\} \) to \( \mathbb{C} - \{0\} \). \( \mathbb{C} - \{0\} \) is a group under multiplication, we need to show that this map preserves multiplication, which is justified by the following identity:

\[
z_1^* z_2^* = (a_1 - b_1 i)(a_2 - b_2 i) = (a_1 a_2 - b_1 b_2) - (a_1 b_2 + b_1 a_2)i = (z_1 z_2)^* ,
\]

where \( z_k = a_k + b_k i \) for \( k = 1, 2 \).

Under the map defined in (b), 1 is mapped to \( i \), contradicting the fact that a homomorphism sends identity to identity.

16.2. Do any of the following determine homomorphisms for \( GL_n(\mathbb{C}) \) to \( GL_n(\mathbb{C}) \)?

(a) \( A \rightarrow A^t \quad \text{(b) } A \rightarrow A^2 \)

**Solution.** Neither of them defines a homomorphism.

Let \( A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \), then

\[
A^t B^t = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix},
\]

which is not equal to

\[
(AB)^t = \left( \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \right)^t = \begin{bmatrix} 1 & 2 \\ 0 & 2 \end{bmatrix}^t = \begin{bmatrix} 1 & 0 \\ 2 & 2 \end{bmatrix}.
\]

Therefore the map does not preserve multiplication.

**Remark:** What interesting is that this map could be a homomorphism. In the above argument we assumed the domain \( GL_n(\mathbb{C}) \) and the range \( GL_n(\mathbb{C}) \) are identically the same group. But if we change the definition of the multiplication in the second \( GL_n(\mathbb{C}) \) to \( A \times B = BA \), where the ”\( \times \)” is the formal multiplication for the group while \( BA \) is the usual matrix multiplication. Since \( (AB)^t = B^t A^t = A^t \times B^t \), this map defines a homomorphism.

The above \( A \) and \( B \) also disqualify map (c):

\[
A^2 B^2 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 8 \\ 0 & 4 \end{bmatrix},
\]

which is not equal to

\[
(AB)^2 = \begin{bmatrix} 1 & 2 \\ 0 & 2 \end{bmatrix}^2 = \begin{bmatrix} 1 & 6 \\ 0 & 4 \end{bmatrix}.
\]

16.5. Verify that the translations in \( D_\infty \) form a normal subgroup of \( D_\infty \) and that the corresponding quotient group is isomorphic to \( \mathbb{Z}_2 \).

**Proof.** Let \( H = \langle r \rangle \) be the subgroup of translations. Since it is the union of conjugacy classes \( \{r^k, r^{-k}\} \) and \( \{e\} \), where \( k \) is a positive integer, it is normal in \( D_\infty \). Notice that all \( r^k \)'s are equivalent under the relation defined by \( H \) where \( k \) is an integer. In fact we have

\[
(r^u s)(r^v s)^{-1} = (r^u s)(sr^{-v}) = r^{u-v} \in H.
\]
Therefore $G/H$ is the quotient group consisting of the only two equivalence classes induced by $H$. Since $\mathbb{Z}_2$ is the only group of order 2 (up to isomorphism), we must have $G/H \cong \mathbb{Z}_2$.

16.7. Each element

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

of $GL_2(\mathbb{C})$ gives rise to a so called **Möbius transformation**

$$z \rightarrow \frac{az + b}{cz + d}$$

of the extended complex plane $\mathbb{C} \cup \{\infty\}$. Show that these transformations form a group, the **Möbius group**, under composition of functions, and that this group is isomorphic to the quotient of $GL_2(\mathbb{C})$ by its centre.

**Proof.** Denote by $\varphi$ the map from $GL_2(\mathbb{C})$ to $M$ defined in the problem, where $M$ stands for the set of Möbius transformations. We first prove that

$$\varphi(A) \circ \varphi(B) = \varphi(AB)$$

where $\circ$ is composition of functions. Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ and $B = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$, then

$$\varphi(AB) = \varphi\left( \begin{bmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{bmatrix} \right) = (z \rightarrow \frac{(ae + bg)z + (af + bh)}{(ce + dg)z + (cf + dh)}).$$

On the other hand,

$$\varphi(A) \circ \varphi(B) = (z \rightarrow \frac{aez + f + b}{cez + f + d}) = \frac{a(eyz + f) + b(gyz + h)}{c(eyz + f) + d(gyz + h)},$$

proving the desired equality.

Since $M$ is defined as the image of $\varphi$, for any $\varphi(A)$ and $\varphi(B)$ in $M$,

$$\varphi(A) \circ \varphi(B) = \varphi(AB) \in M,$$

i.e. $M$ is closed under multiplication. Let $B$ be the identity matrix in $GL_2(\mathbb{Z})$, we have $\varphi(A) \circ \varphi(I) = \varphi(A)$. Similarly we can prove that $\varphi(I) \circ \varphi(A) = \varphi(A)$, thus $\varphi(I) = (z \rightarrow z)$ is the identity in $M$. We then let $B$ be $A^{-1} \in GL_2(\mathbb{C})$, the equality yields that $\varphi(A) \circ \varphi(A^{-1}) = \varphi(I)$, proving the existence of inverses. Now $M$ has group structure. Notice that $\varphi$ preserves multiplication in both groups, $\varphi$ is a homomorphism. Actually the above argument applies for any multiplication-preserving map from a group to a set, i.e. the map is a homomorphism from the domain group to its image.

The kernel of $\varphi$ consists of all matrices $A \in GL_2(\mathbb{C})$ such that $\varphi(A) = (z \rightarrow z)$, i.e. for any $z \in \mathbb{C} \cup \{\infty\}$,

$$z = \frac{az + b}{cz + d} \quad \text{where} \quad A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}. $$
Since $z$ is arbitrary, let $z = 0$ we have $b = 0$, then let $z$ tends to infinity it follows that $c = 0$, now we must have $a = d$ to make the equality hold. Therefore the kernel of $\varphi$ is all matrices in the form of $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$, we denote it by $K$. Alternatively, we can also write the above equation as

$$az + b = z(cz + d) = cz^2 + dz,$$

since the two polynomials on both sides must be identical, we have $b = z = 0$ and $a = c$. Now the First Isomorphism Theorem applies and we conclude that $M$ is isomorphic to the quotient of $GL_2(\mathbb{C})$ by the kernel. We need to prove $K$ is exactly the center of $GL_2(\mathbb{C})$.

Any element in $K$ can be written as $aI$ for some $a \in \mathbb{C}$ where $I$ is the identity matrix. Then $(aI)A = aA = A(aI)$ for any $A \in \mathbb{C}$, i.e. $K$ is in the center of $GL_2(\mathbb{C})$. Now let $Z = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be a matrix in the center, then it commutes with any matrix $A \in GL_2(\mathbb{C})$. Let $A = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$, then

$$\begin{bmatrix} a & b \\ 2c & 2d \end{bmatrix} = AZ = ZA = \begin{bmatrix} a & 2b \\ c & 2d \end{bmatrix},$$

it then follows that $b = c = 0$. We then choose $A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, using $b = c = 0$ we have

$$\begin{bmatrix} 0 & d \\ a & 0 \end{bmatrix} = AZ = ZA = \begin{bmatrix} 0 & a \\ d & 0 \end{bmatrix},$$

which implies that $a = d$. Therefore the center is exactly $K$. 