Question 1

Show that $(\mathbb{Z}/13\mathbb{Z})^\times \simeq \mathbb{Z}/12\mathbb{Z}$.

Solution: Consider $x \in (\mathbb{Z}/13\mathbb{Z})^\times$ such that $x \neq 0$, then $x^12 \equiv 1 \pmod{13}$ by the fermat's little theorem. Therefore, there must exists an element $x^{-1} = x^11 \in (\mathbb{Z}/13\mathbb{Z})^\times$ by the closure of group. Hence, the order of $(\mathbb{Z}/13\mathbb{Z})^\times$ is 12. Then, since we know that for any element x, $|x|\,|12$ by lagrange's theorem, and in $(\mathbb{Z}/13\mathbb{Z})^\times$, the followings hold

$$\begin{aligned}
[2^1] &\neq [1] \\
[2^2] = [4] &\neq [1] \\
[2^3] = [8] &\neq [1] \\
[2^4] = [3] &\neq [1] \\
[2^6] = [12] &\neq [1] \\
[2^12] &= [1]
\end{aligned}$$

. Therefore, the order of 2 is 12. Thus, 2 generates $(\mathbb{Z}/13\mathbb{Z})^\times$. This means that $(\mathbb{Z}/13\mathbb{Z})^\times$ is cyclic, and have the same order as $\mathbb{Z}/12\mathbb{Z}$. Thus, they are isomorphic.

Alternatively, one can construct an isomorphism $\varphi : (\mathbb{Z}/13\mathbb{Z})^\times \to \mathbb{Z}/12\mathbb{Z}$ by

$$\varphi([2]) = [1]$$

Which will follows that

$$\begin{aligned}
\varphi([4]) &= [2] \\
\varphi([8]) &= [3] \\
\varphi([3]) &= [4] \\
\varphi([6]) &= [5] \\
\varphi([12]) &= [6] \\
\varphi([11]) &= [7] \\
\varphi([9]) &= [8] \\
\varphi([5]) &= [9] \\
\varphi([10]) &= [10] \\
\varphi([7]) &= [11] \\
\varphi([1]) &= [0]
\end{aligned}$$

Which is a homomorphism, that is apparently surjective and injective. Therefore, φ is an isomorphism.

Question 2

Let $H < G$. Prove that the map $gH \mapsto Hg^{-1}$ is a bijection between the sets of left and right cosets.

Solution: Let f be a function that maps from gH to Hg^{-1}. Then firstly, for $gH = g'H$, we have that

$$Hg^{-1} = \left\{ hg^{-1} \mid h \in H \right\} = \left\{ (gh)^{-1} \mid h \in H \right\} = \left\{ (g'h)^{-1} \mid h \in H \right\} = Hg'^{-1}$$

So f is well-defined.

Next, for the surjectivity of f, let there be some right coset Hg. Then there must always be g^{-1} such that $f(g^{-1}H) = H(g^{-1})^{-1} = Hg$ by the property of inverse.

Lastly, for the injectivity, let consider that if $Hg = Hg'$, then it must follows that $g' \in \left\{ hg \mid h \in H \right\}$. Now, we can further deduce that

$$g'^{-1} \in \left\{ (hg)^{-1} \mid h \in H \right\} = \left\{ g^{-1}h \mid h \in H \right\}$$

So $g'gH = gH$, which means that $g'H = gH$.

Since f is a function from the set of left cosets to the set of right cosets such that f is surjective and injective, it must follows that f is a bijection between those two sets.

Question 3

Let $H < G$. Prove that $H \lhd G$ if and only if for any $g \in G$ there exists $g' \in G$ such that $gH = Hg'$.

Solution:
$(\Longrightarrow)$:

Assume that $H \lhd G$. Then for any $g \in G$, we know that $gHg^{-1} = H$, so $gH = Hg$. Thus there exists $g' = g$ such that $gH = Hg'$

$(\Longleftarrow)$:

Assume there for any $g \in G$ there is an element $g' \in G$ such that $gH = Hg'$. Then, since $g \in gH, g = hg'$ for some element $h \in H$. This means that $h^{-1}g = g'$ for that element $h \in H$.

Now, since $gH = Hg'$, and $g' = h^{-1}g$, we get that $gH = Hh^{-1}g = Hg$. Thus, $gHg^{-1} = H$, which means that $H \lhd G$ by definition.

Question 4

Let N be a subgroup of a cyclic group G. Prove that the quotient group G/N is cyclic.

Claim 1

All subgroups of a cyclic group is cylic.

Proof: Since a cyclic group G is generated by a single element, g, then each element in the subgroup $S \leq G$ is in G, which means that it must be some power of g. Then, let $S = \{ g^{a_1}, g^{a_2}, \dots \}$, so that it is possible to choose the smallest possitive a_i by the well ordering principle since $|S| < |G|$ is always countable, here note that the only infinite cyclic group G must be isomorphic to $\mathbb{Z}$, so let b be that element.

With the division algorithm, we know that for any a, $g^a = g^{mb+c}$ for some integer m and $0 \leq c < b$. The closure of the group asserts that g^c must be an element of S, but $0 \leq c < b$, so $c = 0$.

Hence, g^b generates S. □

Solution: Firstly, let notice that a cyclic group is an abelian group, since $r^n r^m = r^{n+m} = r^m r^n$ for any r, m, n. Now, let N be a subgroup of G, then N must be cyclic as per claim 1, so N must be abelian, and thus, normal.

Then G/N is a group of the left cosets. Let $G = \langle g \rangle$. Then we know that gN generates G/N. Firstly, notice if $gN = N$, then $g^k N = N$ for every k, making $GN = N$, which means that $G/N = 1$ is trivially cyclic.

So we are left with the case where $gN \neq N$. Now, let N ge generated by g^n with some integer n. Then we know that $g^k N \neq N$ for any $k < n$ since $g^k \notin N$, and moreover, $g^k \notin g^j N$ for any $j < k$ since g generates G so there is no element g^k in $g^j N$ for all $j < k < n$. This asserts that all of

$$N, gN, g^2N, \dots, g^{n-1}N$$

are all pairwise different.

Moreover, if N is generated by g^n, then there must be exactly n element of G/N which are as listed above, since any element of $g^\alpha \in G$ is in one of the partition of the n cosets as $g^\alpha = g^{kn+a} \in g^a N$ for some integer k and $0 \leq a < n$ by the division algorithm.

Since those n left cosets of G is all of the left cosets, we get that $G/N = \{ N, gN, g^2N, \dots, g^{n-1}N \}$, and that G/N is generated by gN, thus, G/N is cyclic.

Question 5

Let $H < G$ be a subgroup of finite index. Show that the set $\{ gHg^{-1} \mid g \in G \}$ is a finite set.

Solution: Consider that since $[G : H]$ is finite, then we can let $n = [G : H]$, which means that the quotient group $G/H = \{ g_1H, g_2H, \dots, g_nH \}$. Now, since G/H partitions G into n partitions, we know that for $g \in G$, $gH = g_iH$ for some g_i. This means that $g = g_ih$ for some $h \in H$. Thus,

$$gHg^{-1} = g_ihHh^{-1}g_i^{-1} = g_iHg_i^{-1}$$

From the equation, we know that $\{ gHg^{-1} \mid g \in G \} = \{ g_i H g_i^{-1} \}$ for previously defined g_i. Thus,

$$\left|\{ gHg^{-1} \}\right| \leq |G/H| = [G : H]$$

So, the set $\{ gHg^{-1} \mid g \in G \}$ is a finite set.

Question 6

Let N be a normal subgroup of a finite group G. Prove that N is the unique subgroup of order $|N|$ if $gcd(|N|, [G : N]) = 1$.

Solution: Let K be a normal subgroup of G with $n = |K| = |N|$. Then KN is must be subgroup of G since for $KN = \{ kn \mid k \in K, n \in N \}$, we have that for kn and $k'n'$ in KN, $kn(k'n')^{-1} = knn'^{-1}k'^{-1}$. But since N normal subgroup, $k'nn'^{-1}k'^{-1} \in N$, thus, $knn'^{-1}k'^{-1}$ is in KN.

Moreover, by the second isomorphism theorem, $|KN| = \frac{|K||N|}{|K \cap N|} = \frac{n^2}{|H \cap K|}$ and $|KN|$ divides $|G|$ by lagrange's theorem. Moreover, since $[G : N] = \frac{|G|}{n}$, we can deduce that $|KN|$ must be n since otherwise $\gcd(n, |G|\, n) \neq 1$.

Since $|KN| = n$, we get that $|K \cap N| = n$, thus, $K = N$. So, N is the unique subgroup of order $|N|$.

Question 7

Let p be an odd prime integer. Show that $p \equiv 1 \pmod 4$ if and only if $x^2 \equiv -1 \pmod p$ has an integer solution.

Solution:
($\Longrightarrow$):

if $p \equiv 1 \pmod 4$ then consider that $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group of order $p - 1$. Thus, let $(\mathbb{Z}/p\mathbb{Z})^\times$ be generated by $\langle r \rangle$, then there exists an element, $x = r^{\frac{p-1}{4}}$ such that the order of the element is 4. Hence, $x^4 \equiv 1 \pmod p$ but $x^2 \not\equiv 1 \pmod p$, so $x^2 \equiv -1 \pmod p$

($\Longleftarrow$):

if $x^2 \equiv -1 \pmod p$ for some integer x. Then $x \not\equiv 1 \pmod p$ and $x^3 \equiv -x \not\equiv 1 \pmod p$. Therefore, there exists an element $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ that is of degree 4. Now, by lagrange's theorem, 4 must divides $|(\mathbb{Z}/p\mathbb{Z})| = p - 1$. So, it follows that $p \equiv 1 \pmod 4$.

Question 8

Find all homomorphisms from S_3 to $\mathbb{Z}/3\mathbb{Z}$.

Solution: Note that we write the operator of both group using $\cdot$, abbrieviate using juxtaposition, and using x^n to denotes repeated operation even for $\mathbb{Z}/3\mathbb{Z}$.

Let us consider f as the homomorphism from S_3 ot $\mathbb{Z}/3\mathbb{Z}$. Trivially, we know that $f(id) = 0$. Next, let us consider $f((12)) = x$, then it must follows that $x^2 = 0$ since $(12)^2 = 0$. And as there is no element $x \neq 0$ in $ZMod[3]$ such that $x^2 = 0$. (As $1^2 = 2$ and $2^2 = 1$). So $f((12)) = 0$. Similar argument can be applied for (13) and (23) yielding that $f((12)) = f((23)) = f((13)) = 0$.

Next, let us consider the remaining two element of S_3, namely (123) and (132). We know that $(123) = (13)(23)$ and $(132) = (12)(13)$. So, $f((123)) = f((13)(23)) = 0 \cdot 0 = 0$, and similarly, $f((132)) = f((12)(13)) = 0 \cdot 0 = 0$. Thus, $f(x) = 0 \quad \forall x \in S_3$. is the only homomorphism from S_3 to $\mathbb{Z}/3\mathbb{Z}$.

Question 9

Show that the quotient group $\mathbb{R}/\mathbb{Z}$ is isomorphic to the unit circle $\{ z \in \mathbb{C} \mid |z| = 1 \}$.

Solution: Consider φ to be a epimorphism from $\mathbb{R}$ to the unit circle $\{ z \in \mathbb{C} \mid |z| = 1 \}$, with the following definition.

$$\varphi : x \mapsto f(x) = \cos(2\pi x) + i \sin(2\pi x)$$

Now, we will show that φ is well defined. Consider some $x = x'$ be a real number. Then it follows that $\cos(2\pi x) = \cos(2\pi x')$ and $\sin(2\pi x) = \sin(2\pi x')$ by the definition of the cos and sin functions. Hence, $f(x) = f(x')$, so φ is well-defined.

To show the surjectivity, let $z = (a+bi) \in \{ z \in \mathbb{C} \mid |z| = 1 \}$. Now, we know that $|z| = \sqrt{a^2+b^2} \geq a$, so $a \leq 1$ and $b \leq 1$. Moreover, $1 - a^2 = b^2$. So, it is possible to find such θ for which $a = \cos\theta$. This will ensure that $1 - a^2 = b^2 = 1 - \cos^2\theta = \sin^2\theta$. So, $z = (a+bi) = \cos\theta + i\sin\theta = f(\theta)$ for some $\theta \in \mathbb{R}$. Hence, φ is surjective.

Lastly, consider the kernel $\ker\varphi = \{ x \mid f(x) = 1 \}$. Then we know that $f(x) = 1$ if and only if $\cos(2\pi x) = 1$ and $\sin(2\pi x) = 0$. This occur if and only if $x \in \mathbb{Z}$ holds, by the periodicity of the functions. Hence, $\ker\varphi = \mathbb{Z}$.

Therefore, by the first isomorphism theorem, we have that $\mathbb{R}/\mathbb{Z} \simeq \{ z \in \mathbb{C} \mid |z| = 1 \}$.

Question 10

Find the class equation for D_{2n} when $n \in \mathbb{Z}$ with $n \geq 3$.

Solution: Firstly, consider that an element g of D_{2n} can always be written in the form of $f^i r^j$ for $i \in \{0,1\}$ and $j \in \{0, 1, \ldots, n-1\}$. Now, consider the conjugacy classes of D_{2n}.

$$\begin{aligned}
r^\alpha \cdot r^j &= r^{\alpha+j} \\
&= r^j \cdot r^\alpha \\
r^\alpha \cdot fr^j &= fr^{\alpha-j} \\
&= fr^j \cdot r^{\alpha-2j} \\
fr^\alpha \cdot r^j &= fr^{\alpha+j} \\
&= r^{-\alpha-j} f \\
&= r^j \cdot r^{-\alpha-2j} f \\
&= r^j \cdot fr^{\alpha+2j} \\
fr^\alpha \cdot fr^j &= ffr^{-\alpha} r^j \\
&= ffr^{-j} r^{-\alpha+2j} \\
&= fr^j \cdot fr^{-\alpha+2j}
\end{aligned}$$

From this, we split the problem into two cases of whether n is odd or even. We first discuss the scenario where n is odd.

If n is odd, then we can make a conjugacy class of r^k as $\{ r^k, r^{-k} \}$ since $\forall k, r^k \neq r^{-k}$ as n is odd. and the class containing fr must contain fr^{-1} and thus, contains fr^j for all $0 \leq j < n$. We could write the conjugacy classes of D_{2n} as

$$\{1\},\ \{r, r^{-1}\},\ \{r^2, r^{-2}\},\ \ldots,\ \left\{ r^{\frac{n-1}{2}}, r^{\frac{n+1}{2}} \right\},\ \{f, fr, \ldots, fr^{n-1}\}$$

Now, since all of the conjugacy classes, except for $\{1\}$ has 2 or more elements, the center of the group is $\{1\}$.

Since the class equation is

$$|D_{2n}| = |Z(D_{2n}| + [D_{2n} : C_{D_{2n}}(x)]$$

we need to find the centralizer of x for x in each class. Firstly, consider $x = r^\alpha$, then the centralizer $C_{D_{2n}}(x)$ is any r^j since they commute. But not fr^j since as shown above, $r^\alpha$and fr^j only if $r^\alpha = r^{\alpha-2j}$, which is when $j = 0$. And the centralizer of $x = f$ contains just f and 1 since $f \cdot r^j = r^j \cdot fr^{2j}$ and $f \cdot fr^j = fr^j \cdot fr^{2j}$. Since the index $[D_{2n} : C_{D_{2n}}(x)] = \frac{2n}{|C_{D_{2n}}(x)|}$, we get the following class equation.

$$|D_{2n}| = 1 + \frac{2n}{n} + \cdots + \frac{2n}{n} + \frac{2n}{2}$$

Where there is exactly $\frac{n-1}{2}$ numbers of $\frac{2n}{n}$ as there is $\frac{n-1}{2}$ classes of $\{ r^i, r^{-i} \}$, the number 1 represents the size of the center, and the number $\frac{2n}{2}$ is the index of the class that contain f.

Now, for the case that n is even. we can deduce the conjugacy classes by similar arguments, fr and fr^{-1} is not in the same conjugacy class. This is because i and $n-i$ will always be the same parity since n is even. This makes it so that fr^i and fr^{n-i} is of different parity, thus is in different class. As fr and fr^{-1} is not in the same class, the structure changed to

$$\{1\},\ \{r, r^{-1}\},\ \{r^2, r^{-2}\},\ \ldots,\ \{ r^{\frac{n}{2}}, r^{-\frac{n}{2}} \},\ \{f, fr^2, \ldots, f^{n-2}\},\ \{fr, fr^3, \ldots, fr^{n-1}\}$$

Now, since $\frac{n}{2} = n - \frac{n}{2}$, we get another element in the center $Z(D_{2n})$. Then, let us consider the centralizer of each representative of the classes. Firstly, notice that the centralizer of r^j remains the same except for $r^{\frac{n}{2}}$ which is in the center. Now, for $C_{D_{2n}}(f)$, we know that f commutes with 1, f and $r^{\frac{n}{2}}$ and $fr^{\frac{n}{2}}$ from the above equations. Since $f \cdot fr^{\frac{n}{2}} = fr^{\frac{n}{2}} \cdot fr^{-0+2\frac{n}{2}}$. Moreover, the equation above omit no extra solution apart from this 4 solutions as $f = fr^{2j}$ only at $j = \frac{n}{2}$ or $j = 0$. Similarly, for the centralizer $C_{D_{2n}}(fr)$, we know that fr commutes with 1, fr, $r^{\frac{n}{2}}$ and $fr^{\frac{n}{2}+1}$. And this are the only four solutions to the equation by similar arguments, which is that $fr = fr^{-1+2j}$ solves only at $j = 1, \frac{n}{2} + 1$, and fr^{1+2j} solves only at $j = 0, \frac{n}{2}$.

This makes the class equation of this case to be

$$|D_{2n}| = 2 + \frac{2n}{n} + \cdots + \frac{2n}{n} + \frac{2n}{4} + \frac{2n}{4}$$

Where the number 2 represents the size of the center, $\frac{n-2}{2}$ numbers of $\frac{2n}{n} = 2$ are the indices of each of the classes in the form $\left\{ r^j, r^{-j} \right\}$ from $j = 1, \ldots, n-2$, and two numbers of $\frac{2n}{4}$ are the indices of the classes with f and fr, ie. the class of fr^j for even and odd j respectively.