3.4.1 Find all the normal subgroups of D_4

Subgroups of D_4: Let R, F generate D_4

H1 $\{I\}$

H2 $\{I, R^2\}$

H3 $\{I, R, R^2, R^3\}$

H4 $\overset{a)}{\{I, F\}}$, $\overset{b)}{\{I, RF\}}$, $\overset{c)}{\{I, R^2F\}}$, $\overset{d)}{\{I, R^3F\}}$

H5 $\{I, F, R^2, R^2F\}$

H6 $\{I, RF, R^3F, R^2\}$

H1 is clearly normal since $gIg^{-1} = I$ for all $g \in G$

H2 is likewise normal since R^2 commutes with all $g \in G$,
so $gR^2g^{-1} = gg^{-1}R^2 = R^2 \quad \forall g \in G$

H3 is also normal

Check for generators of D_4, R and F

$RH3R^{-1} = \{RIR^3, RRR^3, RR^2R^3, RR^3R^3\} = \{I, R, R^2, R^3\} = H3$

$FH3F^{-1} = \{FIF, FRF, FR^2F, FR^3F\} = \{I, R^3, R^2, R\} = H3$

H4a),b),c),d) are not normal, check that $R\,H4a)R^{-1} \neq H4\,c)$ and so on

H5 is normal, since we can check that $FH5F = RH6R^3 = H5$ and F, R generate D_4

H6 is normal, since we can check that $FH6F = RH6R^3 = H6$

3.4.3 Let G be the affine group

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \middle| \, a, b \in \mathbb{Z}_5, \, a \neq 0 \right\}$$

with group operation given by matrix multiplication

Find a normal subgroup of order 5, and a normal subgroup of order 10

Let H be the sub group $H = \left\{ \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \middle| \, c \in \mathbb{Z}_5 \right\}$

Since $\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & c+d \\ 0 & 1 \end{pmatrix}$ H is a sub group

We compute

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & ac+b \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b+d \\ 0 & 1 \end{pmatrix}$$

So H is normal using the criterion

$gH = Hg \;\; \forall g \in G$ (pick $d = ac$)

Let $K < G$ be the subgroup :

$$K = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \;\middle|\; \begin{matrix} a = \pm 1 \\ \text{or } a = 1,4 \end{matrix} \quad b \in \mathbb{Z}_5 \right\}$$

$|K| = 10$. K is a subgroup since if $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} \in K$, then

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a a' & ab' + b \\ 0 & 1 \end{pmatrix} \in K$$

since $(\pm 1)(\pm 1) = \pm 1$

By an exercise from the previous week, K is normal, since $|K| = \dfrac{|G|}{2}$

3.4.4 Multiplication table for G/H where H is the subgroup of order 5

Cosets: $\begin{pmatrix}1&0\\0&1\end{pmatrix}H$

$\begin{pmatrix}2&0\\0&1\end{pmatrix}H = \left\{\begin{pmatrix}2&b\\0&1\end{pmatrix} \middle| b\in\mathbb{Z}_5\right\}$

$\begin{pmatrix}3&0\\0&1\end{pmatrix}H = \left\{\begin{pmatrix}3&b\\0&1\end{pmatrix} \middle| b\in\mathbb{Z}_5\right\}$

$\begin{pmatrix}4&0\\0&1\end{pmatrix}H = \left\{\begin{pmatrix}4&b\\0&1\end{pmatrix} \middle| b\in\mathbb{Z}_5\right\}$

Since H is normal, for any $g, g'\in H$ $(gH)(g'H)$

$= g(Hg')H$

$= gg'HH = gg'H$

	$\begin{pmatrix}1&0\\0&1\end{pmatrix}H$	$\begin{pmatrix}2&0\\0&1\end{pmatrix}H$	$\begin{pmatrix}3&0\\0&1\end{pmatrix}H$	$\begin{pmatrix}4&0\\0&1\end{pmatrix}H$
$\begin{pmatrix}1&0\\0&1\end{pmatrix}H$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}H$	$\begin{pmatrix}2&0\\0&1\end{pmatrix}H$	$\begin{pmatrix}3&0\\0&1\end{pmatrix}H$	$\begin{pmatrix}4&0\\0&1\end{pmatrix}H$
$\begin{pmatrix}2&0\\0&1\end{pmatrix}H$	$\begin{pmatrix}2&0\\0&1\end{pmatrix}H$	$\begin{pmatrix}4&0\\0&1\end{pmatrix}H$	$\begin{pmatrix}4&0\\0&1\end{pmatrix}H$	$\begin{pmatrix}3&0\\0&1\end{pmatrix}H$
$\begin{pmatrix}3&0\\0&1\end{pmatrix}H$	$\begin{pmatrix}3&0\\0&1\end{pmatrix}H$	$\begin{pmatrix}3&0\\0&1\end{pmatrix}H$	$\begin{pmatrix}2&0\\0&1\end{pmatrix}H$	$\begin{pmatrix}2&0\\0&1\end{pmatrix}H$
$\begin{pmatrix}4&0\\0&1\end{pmatrix}H$	$\begin{pmatrix}4&0\\0&1\end{pmatrix}H$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}H$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}H$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}H$

Recognize that

$G/H \cong \mathbb{Z}_5^*$

3.4.8 Show that the intersection of two normal subgroups $H_1, H_2 \subseteq G$ is normal

First note that $H_1 \cap H_2$ is a subgroup.

$g H_1 \cap H_2 g^{-1} \subseteq H_1$, for all $g \in G$ since H_1 is normal and $H_1 \cap H_2 \subseteq H_1$

similarity

$g H_1 \cap H_2 g^{-1} \subseteq H_2$

hence $g H_1 \cap H_2 g^{-1} \subseteq H_1 \cap H_2$

If G is a finite group we can argue that

Since $|g H_1 \cap H_2 g^{-1}| = |H_1 \cap H_2|$, we must have

$g H_1 \cap H_2 g^{-1} = H_1 \cap H_2 \quad \forall g \in G$ hence $H_1 \cap H_2$ is normal

Otherwise we argue that if

$g H_1 \cap H_2 g^{-1} \subseteq H_1 \cap H_2 \quad \forall g \in G$, then by

multiplying with g^{-1} from the left and g from the right we get

$H_1 \cap H_2 \subseteq g^{-1} H_1 \cap H_2 g \quad \forall g \in G$, but then also

$g^{-1} H_1 \cap H_2 g \subseteq H_1 \cap H_2$ so

$H_1 \cap H_2 \subseteq g^{-1} H_1 \cap H_2 g \subseteq H_1 \cap H_2$, hence we have equality

3.4.9. Let G be a cyclic group.
Prove that G/H is cyclic

Let a be a generator for G, and let n be the order of G.

The subgroup of G/H generated by aH will be:

$$aH, a^2H, a^3H, \dots, a^nH$$

which is a list containing all cosets of H
(If $H \neq \{id\}$ the cosets appear multiple times)

So aH generates G/H

3.4.11 If G is a group order 15, show that G has an element of order 3

If G is cyclic, generated by a, pick a^5

By Lagrange's theorem, the possible orders of elements of G are 1, 3, 5, 15. G has only one element of order 1, and if it has an element of order 15 it is cyclic

Assume for contradiction G only has elements of order 1 and 5, i.e. G has 14 elements of order 5. This is not possible. Let $H_1, H_2 \subseteq G$ be cyclic subgroups of order 5. Since any non-identity element of H_1 or H_2 generate their respective group, either $H_1 \cap H_2 = id$, or $H_1 = H_2$

So the number of order 5 elements is divisible by 4. To see this, let $a \in G$ be an element of order 5. It generates the group I, a, a^2, a^3, a^4. If b is not in this group, b generates the disjoint group I, b, b^2, b^3, b^4 etc, where all powers b^i $i \neq 5$ have order 5

3.5.1 Show that the exponential function is a group homomorphism $\phi: \mathbb{R} \to \mathbb{R}^+$. Is it an isomorphism

$$\phi(x+y) = e^{x+y} = e^x e^y$$

so ϕ is a group homomorphism

The Logarithm is an inverse, so it is an isomorphism

3.5.2 Let G, G' be finite groups and $T: G \to G'$ a group homomorphism. Show that the order of $T(g)$ divides the order of g

Let n be the order of g

$$T(g)^n = T(g^n) = T(id) = id$$

Since $T(g)^n = id$, the order of $T(g)$ must divide n

3.5.8 State whether the following statements are true or false

a) $f: \mathbb{Z} \to \mathbb{Z}$

$x \mapsto x^3$

No, consider $f(2) = 8$

$f(1) = 1$, so $f(1+1) \neq f(1) + f(1)$

b) $f: \mathbb{Z}_3 \to \mathbb{Z}_3$

$x \mapsto x^3$

Yes. $f(x+y) = (x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$

$= x^3 + y^3 = f(x) + f(y)$

Since $3 = 0$ in $\mathbb{Z}_3$

3.5.14

More generally, let H be a cyclic group and $T: H \to G$ any group homomorphism. Show that T is completely determined by its value on a generator of H

Let $H = \langle a \rangle$ and let $T, T': H \to G$ be group homomorphisms such that $T(a) = T'(a)$

Then for any $h \in H$, write $h = a^k$

$$T(h) = T(a^k) = T(a)^k = (T'(a))^k = T'(a^k) = T'(h)$$

Therefore $T = T'$

3.5.15 Let $\tau : \mathbb{Z}_n \to \mathbb{T}$ be defined by

$$\tau(x) = e^{\frac{2\pi i x}{n}}.$$

Show that τ is an injective group homomorphism

Show that its image is the n-th roots of unity

Check τ well-defined

$x \equiv y \pmod n \Rightarrow \tau(x) = \tau(y)$

$x = y + kn$ so $\tau(y) = e^{\frac{2\pi i x}{n}} \cdot e^{\frac{2\pi k n}{n}}$

$= e^{\frac{2\pi i x}{n}} = \tau(x)$

Group homomorphism

$\tau(x+y) = e^{\frac{2\pi i x+y}{n}} = e^{\frac{2\pi i x}{n}} e^{\frac{2\pi i y}{n}} = \tau(x)\tau(y)$

injective

If $\tau(x) = \tau(y)$, then $e^{\frac{2\pi i x}{n}} = e^{\frac{2\pi i y}{n}}$

So $1 = \dfrac{e^{\frac{2\pi i x}{n}}}{e^{\frac{2\pi i y}{n}}} = e^{\frac{2\pi i (x-y)}{n}}$

So $\frac{x-y}{n}$ is an integer i.e. $x \equiv y \pmod n$

To see the final statement, note that

$$(\tau(x))^n = \tau(nx) = \tau(0) = 1,$$

so $\tau(x)$ is always an n-th root of unity. Since τ is injective, and there are n n-th roots of unity and $|\mathbb{Z}_n| = n$, we must have that the image of τ is all the n-th roots of unity