Problem set 5 selected solutions

1. $\langle s \rangle = \{e, s\}$. $rsr^{-1} = sr^2 \notin \langle s \rangle$, so $\langle s \rangle$ is not normal in D_8

$\langle s, r^2 \rangle = \{e, s, sr^2, r^2\}$.

Clearly, $e \in N_{\langle s, r^2 \rangle}\langle s \rangle$ and $s \in N_{\langle s, r^2 \rangle}\langle s \rangle$.

$sr^2 s (sr^2)^{-1} = sr^2 s r^2 s = s^3 = s$, so $sr^2 \in N_{\langle s, r^2 \rangle}\langle s \rangle$

and $r^2 s r^{-2} = s r^{-4} = s$ so $r^2 \in N_{\langle s, r^2 \rangle}\langle s \rangle$. This shows that $\langle s \rangle$ is normal in D_8.

Finally, to see $\langle s, r^2 \rangle$ is normal, $\langle s, r^2 \rangle \in N_{D_8}\langle s, r^2 \rangle$ so we just need to check that $sr \in N_{D_8}\langle s, r^2 \rangle$ and that $r \in N_{D_8}\langle s, r^2 \rangle$. (if $r \in N_{D_8}\langle s, r^2 \rangle$, then r^{-1} is too! same for sr!)

I'll leave this to you!

2. DF 3.1 # 16.

Let $G = \langle S \rangle$. Consider the natural projection homomorphism $\phi : G \to G/N$. We showed in a previous homework that $\phi(S)$ generates G/N, since ϕ is surjective!

(you can also prove this without using previous homework – take any coset gN. Since S generates G we can write $g = s_1 s_2 \cdots s_k$ where each s_i is an element of S or its inverse is. Then $gN = s_1N\, s_2N \cdots s_kN$. In the notation from the book, $\bar{g} = \bar{s_1}\, \bar{s_2} \cdots \bar{s_k}$.)

3. DF 3.2 # 11.

Suppose $|G:K| = m$ and $|K:H| = n$. We want to show $|G:H| = mn$.

Let $g_1K, \dots g_mK$ be the left cosets of K in G, and $k_1H, \dots k_nH$ the left cosets of H in K.

We claim that the left cosets of H in G are g_ik_jH, for $i=1,\dots m$, $j=1,\dots n$.

and that, if $i,j \neq i',j'$, then $g_ik_jH \neq g_{i'}k_{j'}H$.

To see this, first note that any element of K can be written as k_jh for some $h \in H$, and any element of G can be written as g_ik for some $k \in K$. Thus, every element of G is of the form g_ik_jh for some i and j and some $h \in H$.

If $i \neq i'$ then $g_iK \cap g_{i'}K = \emptyset$, so $g_ik_jH \cap g_{i'}k_{j'}H = \emptyset$ for any j, j'
(because $k_jH \subset K$)

If $j \neq j'$, then $k_jH \cap k_{j'}H = \emptyset$, so $g_ik_{j'}H \cap g_ik_jH = \emptyset$.

4. a) $H \cap K$ is a subgroup of H and of K.
by Lagrange's theorem, $|H \cap K|$ divides $|H|$ and $|K|$.
Since $|H|$ and $|K|$ are relatively prime, $|H \cap K| = 1$.

b) As above, $|H \cap K|$ divides p. Since $H \neq K$, $H \cap K$ has fewer than p elements, so since p is prime $|H \cap K| = 1$.

c) by part b) any two subgroups of order 5 only share the identity element. This means that each subgroup of order 5 contains 4 elements that are not in any other subgroup of order 5. Since $|G| = 35$, and $\lfloor 35/4 \rfloor = 8$, there are at most 8 subgroups of order 5.
The argument for order 7 subgroups is similar.

d) If G is cyclic, then $G = \mathbb{Z}_{35} = \langle x \rangle$, and x^7 has order 5.

If not, every element of G has order 1, 5, or 7 (by Lagrange's theorem). Suppose for contradiction that G has no elements of order 5. Then every element belongs to a subgroup of order 7. (every element is either e, or generates a cyclic subgroup of order 7)

But we saw in part c) that there are at most 5 subgroups of order 7, and they all contain e. Thus, there are a total of at most $5 \cdot 6 + 1 = 31$ elements of G contained in a subgroup of order 7 — contradiction, since $|G| = 35$

The argument for elmts of order 7 is similar.

6. By Fermat's little theorem, $n_i^{31} \equiv n_i \pmod{31}$, if n_i is not a multiple of 31

so $n_i^{30} \equiv 1 \pmod{31}$

If n_i is a multiple of 31, then $n_i^{30} \equiv 1 \pmod{31}$.

Thus, $(n_1)^{30} + \dots + (n_{30})^{30}$ is the sum of 30 numbers, each of which is 0 or 1 mod 31, and at least one is 1.

It follows that $(n_1)^{30} + \dots + (n_{30})^{30} \equiv k \pmod{31}$ where k is some number between 1 and 30 (inclusive).

So $(n_1)^{30} + \dots + (n_{30})^{30} \not\equiv 0 \pmod{31}$

7a). $A = \ker(\Phi)$, so the first isomorphism theorem says that $G/A \cong \Phi(G) = \mathbb{C}^\times$.

b). Let $g \in GL_2\mathbb{C}$. Let $M = \frac{1}{\sqrt{\det(g)}} g$. Then $\det(M) = 1$.

and $g = M \cdot \frac{1}{\sqrt{\det(g)}} I$, so $G = AB$.

c) $A \cap B = \{ \lambda I \mid \det(\lambda I) = 1 \}$. Since $\det(\lambda I) = \lambda^2$,

$A \cap B = \{ \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \}$.

d) The second isomorphism theorem says that

$$AB/B \cong A/A\cap B$$

In our case,

$$GL_2\mathbb{C}/Z(G) \cong SL_2\mathbb{C}/\{+I, -I\}.$$

8a. Let $H = \mathrm{stab}(a)$.

Let $\Psi : \{\text{left cosets of } H\} \longrightarrow \text{orbit of } a$

be defined by $\Psi(xH) = x \cdot a$.

This is well defined, since if $xH = yH$, then $y^{-1}x \in H$

so $(y^{-1}x) \cdot a = a$

but this implies that $y^{-1} \cdot (x \cdot a) = a$

or $x \cdot a = y \cdot a$.

Ψ is injective, since if $x_1 \cdot a = x_2 \cdot a$, then $x_2^{-1} x_1 \cdot a = a$ (same argument as above)

so $x_2^{-1} x_1 \in H$, which implies that $x_2 H = x_1 H$.

Finally, Ψ is surjective since any point in the orbit of a is $x \cdot a$ for some $x \in G$, and $x \cdot a = \Psi(xH)$.