Hints and solutions to Problems 2

1) One direction is clear. For the other assume that $H \cup K$ is a subgroup, but $H \not\subseteq K$. Then there exists $h \in H$ with $h \notin K$.

   For $k \in K$ we have then $h \cdot k \in H \cup K$ since $H \cup K$ is a subgroup and both h, k are in the union $H \cup K$. If $h \cdot k = z \in K$ then $h = z \cdot k^{-1} \in K$ contrary to our assumption. Hence $z = h \cdot k$ is in H and so $k = h^{-1} \cdot z$ is also in H. Since k was arbitrary this implies $K \subseteq H$.

2) Let H be a normal subgroup of the group G and $C_G(H)$ it centralizer. Let $g \in G$ and x be in the centralizer. We have to show that then $g \cdot x \cdot g^{-1}$ is also in the centralizer, *i.e.* commutes with all elements of H. This can be seen as follows. Let $h \in H$. Then we have

$$(g \cdot x \cdot g^{-1}) \cdot h \,=\, g \cdot \big((x \cdot (g^{-1} \cdot h \cdot g)\big) \cdot g^{-1}\,.$$

   Since $x \in C_G(H)$ and since $g^{-1}hg \in H$ as H is normal x commutes with $g^{-1}hg$ and so

$$(g \cdot x \cdot g^{-1}) \cdot h \,=\, g \cdot (g^{-1} \cdot h \cdot g) \cdot x \cdot g^{-1} \,=\, h \cdot (g \cdot x \cdot g^{-1})\,.$$

   It follows that gxg^{-1} is also in the centralizer of H.

3) Clearly $\mathrm{U}_3(\mathbb{R})$ contains the identity matrix and is closed under matrix multiplication. One way (there are many others) to see that $\mathrm{U}_3(\mathbb{R})$ contains the inverse of every matrix in it is as follows: We have

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \,=\, \mathrm{I}_3 - A\,,$$

   where I_3 denotes the 3×3-identity matrix and we have set

$$A \,:=\, \begin{pmatrix} 0 & -a & -b \\ 0 & 0 & -c \\ 0 & 0 & 0 \end{pmatrix}\,.$$

   Now $A^3 = 0$ and so we have $(\mathrm{I}_3 - A) \cdot (\mathrm{I}_3 + A + A^2) = \mathrm{I}_3$, that is the inverse of $\mathrm{I}_3 - A$ is $\mathrm{I}_3 + A + A^2$, which is also in $\mathrm{U}_3(\mathbb{R})$.

   However $\mathrm{U}_3(\mathbb{R})$ is not normal in $\mathrm{SL}_3(R)$. To this end consider the matrix

$$B \,:=\, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}\,,$$

   which has determinant 1 and therefore is in $\mathrm{SL}_3(\mathbb{R})$. Its inverse is

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

Let a be a non zero real number. Then $A := \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ is in $\mathrm{U}_3(\mathbb{R})$ but

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

not.

To compute the center of $\mathrm{U}_3(\mathbb{R})$ we consider the matrices

$$L := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad R := \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} ,$$

which are both in $\mathrm{U}_3(\mathbb{R})$. We have

$$L^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad R^{-1} = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} ,$$

and compute

$$L^{-1} \cdot \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \cdot L = \begin{pmatrix} 1 & a & a+b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} .$$

Hence if

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

is in the center we have $a = 0$. On the other hand

$$R^{-1} \cdot \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \cdot R = \begin{pmatrix} 1 & 0 & b-c \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} ,$$

and so for

$$\begin{pmatrix} 1 & 0 & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

to be in the center we must have $c = 0$. A straightforward computation shows then that the matrices of the shape

$$\begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

are in the center of $\mathrm{U}_3(\mathbb{R})$ for all real numbers b. Therefore we have

$$Z(\mathrm{U}_3(\mathbb{R})) = \left\{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; b \in \mathbb{R} \right\}.$$

4) We show first that such a group is commutative. Since every element has order 2 we have $x^2 = e$ for all $x \in G$, and so $x^{-1} = x$. Let now $g, h \in G$. Then on the one hand we have $(g \cdot h)^{-1} = g \cdot h$, and on the other $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1} = h \cdot g$. Putting these two equations together we get $g \cdot h = h \cdot g$, and so G is commutative.

We define the $\mathbb{Z}/2$-scalar multiplication on G by

$$[n].g := g^n .$$

This is well defined since if $[n] = [m]$ then $n - m = 2l$ for some l and so $g^{n-m} = (g^2)^l = e^l = e$, or equivalently $g^n = g^m$. The addition in the vector space G is the multiplication in G. We have seen that G is abelian, and so to show that it is a vector space over $\mathbb{Z}/2$ one has only to check the distributive laws, the associative law for the scalar multiplication, and that $[1]$ acts as identity. This is straightforward (except for the unusual notation).

5) (i) Let $g \in G$ but not in H. Then $gH \neq H \neq Hg$ and G is the disjoint union $H \cup gH$ as well as the disjoint union $H \cup Hg$. It follows $gH = Hg$, or equivalently $gHg^{-1} = H$. Hence H is normal in G.

(ii) For instance the subgroup generated by the 2-cycle $(1, 2)$ in S_3 is an example of a subgroup of index 3, which is not normal.

6) Direct verification by computations shows that the center contains only the neutral element, but there are many other ways to prove this. (This computation can be simplified by observing that every element of S_4 is either a $2, 3$, or 4 cycle or a product of two 2-cycles, which commute with each other.)

7) Let $H \subset G$ be the normal subroup of order p. Since p is a prime we have $H =< x >$ for some $x \in G$ by Example 2.15 of the Lecture Notes. By the theorem of Lagrange (2.12 of the Lecture Notes) the quotient group G/H has order q and is therefore also cyclic, say $G/H =< yH >$ for some $y \in G$, which is not in H. These two elements do the job.

In fact, by the very definition x has order p. To see that y has order q observe first that (again by the very definition of y) the coset yH has order q in G/H. Hence $y^j \notin H$ for all $0 \leq j \leq q-1$, and so in particular $y^j \neq e$ for all $0 \leq j \leq q-1$, but $y^q \in H$. If $y^q \neq e$, then we have since H has order the prime number p that $(y^q)^i \neq e$ for all $0 \leq i \leq p-1$, and so y would have order pq and therefore be a generator of G, contradicting that G is not cyclic. Hence $q^q = e$.

We show now that every g in G can be written as claimed. We have since yH generates G/H that $gH = (yH)^j = y^j H$ for some $0 \leq j \leq q-1$, *i.e.* $y^{-j} \cdot g = h$ for some $h \in H$. Now $H =< x >$ and therefore $h = x^i$ for some $0 \leq i \leq p-1$. It follows $g = y^j \cdot x^i$.

To show uniqueness, assume that we have

$$y^l \cdot x^k \;=\; y^j \cdot x^i$$

with $0 \leq i, k \leq p-1$ and $0 \leq j, l \leq q-1$. This is equivalent to $y^{l-j} = x^{i-k}$. Set $a := y^{l-j} = x^{i-k}$. Then $a \in < x > \cap < y >$ and so by the corollary after 2.13 in the Lecture Notes we have $a^p = a^q = e$ because $| < x > | = p$ and $| < y > | = q$. Since p and q are different primes their greatest common divisor is 1 and so there exists $m, n \in \mathbb{Z}$, such that $mp + nq = 1$. We compute

$$a \;=\; a^1 \;=\; a^{mp+nq} \;=\; (a^p)^m \cdot (a^q)^n \;=\; e^m \cdot e^n \;=\; e\,.$$

Therefore $x^{i-k} = e = y^{l-j}$, and so p divides $i-k$ and q divides $l-j$ (again by the corollary after 2.13 in the Lecture Notes). Since $0 \leq i, k \leq p-1$ we have $-p < i-k < p$ and so this implies $i-k = 0$, or equivalently $i = k$. Analogous we get $j = l$.