P45 #12

Let $\sigma : H \to G$ be a homomorphism and let $a \in H$ with $o(a) < \infty$. One can restrict σ to $< a >= K$ and call $\overline{\sigma}$ this restriction. Then it is well known that

$$Im(\overline{\sigma}) \cong K/ker(\overline{\sigma}) \tag{0.1}$$

The result follows by taking cardinals.

If now σ is an isomorphism from H to G, then $\overline{\sigma}$ is an isomorphism from K to $Im(\overline{\sigma})$. In particular in 0.1 one has $\ker(\overline{\sigma}) = 1$; that allows to conclude.

P46 #23

Let G be a group of order $2n$. Write G as the disjoint union

$$\bigcup_{x \in G} \{x, x^{-1}\} = \left(\bigcup_{x \in G : x \neq x^{-1}} \{x, x^{-1}\} \right) \cup \left(\bigcup_{x \in G : x = x^{-1}} \{x, x^{-1}\} \right)$$

It is clear that the first union on the right hand side of the equality above has an even number of elements; hence, so does the second union (since $|G|$ is even). So, there is an even number of elements of G such that $x = x^{-1}$. These elements are those of order 2 and the identity.

P46 #24

(1) We have $A = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$; $A^2 = -Id$; $A^3 = -A$ and $A^4 = Id$. We also have $B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $B^2 = -Id$; $B^3 = -B$ and $B^4 = Id$. From this it is clear that $A^2 = B^2$. Also a short computation gives the last identity.
(2) Some computations show that $Q = \{Id, A, A^2, A^3, B, AB, A^2B, A^3B\}$.
(3) In order to find $Z(Q)$ one should write a table and check what are the elements commuting with everything. Doing these computations one finds $Z(Q) = \{Id, A^2\}$. Since $Q/Z(Q)$ has order 4 it is either a cyclic group or the klein group and therefore is abelian. Note that $Q/Z(Q)$ is in fact the klein group.
(4) It is clear that $Z(Q)$ is normal in Q and that $Z(Q)$ is the only subgroup of order 2 in Q. Also it is clear that Q and $\{Id\}$ are both normal in Q. Finally for the subgroup of order 4 (i.e. of index 2) corollary (4.6) of the book allows to conclude.

EXERCISE 1

(1) It is clear that G is non empty. Let $g = \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix}$ and $g' = \begin{pmatrix} x' & y' \\ 0 & 1 \end{pmatrix}$ be in G, then

$$gg'^{-1} = \begin{pmatrix} \frac{x}{x'} & y - \frac{xy'}{x'} \\ 0 & 1 \end{pmatrix}$$

To conclude, one needs to notice that $\frac{x}{x'} > 0$ as long as $x > 0, x' > 0$.

Similarly H is not empty. For $h = \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}$ and $h' = \begin{pmatrix} x' & 0 \\ 0 & 1 \end{pmatrix}$ be in G, we have

$$hh'^{-1} = \begin{pmatrix} \frac{x}{x'} & \\ 0 & 1 \end{pmatrix}$$

Again, $\frac{x}{x'} > 0$ as long as $x > 0, x' > 0$.

(2) H is not a normal subgroup of G. Indeed

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 2 & -1 \\ 0 & 1 \end{pmatrix} \notin H$$

(3) sorry I don't know how to insert pics in Tex :)

EXERCISE 2

(1) One can define $\varphi : \mathbb{Z} \to G$ by $\phi(n) = a^n$.
(2) In order to be able to factor φ through $n\mathbb{Z}$, it is necessary and sufficient to have $n\mathbb{Z} \subset \ker(\varphi)$. In other words , one wants $a^n = 1$ (i.e. the order of a must divide n).
(3) Here we use the additive notation. The morphism from $\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ are the one sending
  (a) $n \longmapsto 0$
  (b) $n \longmapsto 1 \cdot n$
  (c) $n \longmapsto 2 \cdot n$
  (d) $n \longmapsto 3 \cdot n$
  (e) $n \longmapsto 4 \cdot n$
  (f) $n \longmapsto 5 \cdot n$

  And amongst the morphism above, the only one factoring through $2\mathbb{Z}$ are (a) and (d).
(4) The morphism from $\mathbb{Z} \to \mathbb{Z}/8\mathbb{Z}$ are the one defined by
  (a) $n \longmapsto 0$
  (b) $n \longmapsto 1 \cdot n$
  (c) $n \longmapsto 2 \cdot n$
  (d) $n \longmapsto 3 \cdot n$
  (e) $n \longmapsto 4 \cdot n$
  (f) $n \longmapsto 5 \cdot n$
  (g) $n \longmapsto 6 \cdot n$
  (h) $n \longmapsto 7 \cdot n$

  And amongst the morphism above, the only one factoring through $2\mathbb{Z}$ are (a), (c), (e) and (g).

EXERCISE 3

(1) A morphism exists if $o(g)|7$.
(2) A morphism exists if $o(g)|15$.
(3) We use the notation of the previous exercise. The morphism is injective as long as $\ker(\varphi) = 15\mathbb{Z}$ (i.e. $o(g) = 15$).
(4) The morphism is surjective as long as $Im(\varphi) = G$ (i.e. $G =< g >$; hence G is cyclic).

EXERCISE 4

Let G be a group and $Z(G)$ be its center.

(1) Let $a, b \in Z(G)$, then by the very definition of $Z(G)$ we have $ab = ba$; hence $Z(G)$ is abelian.

(2) Let $H \leq Z(G)$. Let $a \in G$ and let $h \in H$. Then $ah = ha$ (since $h \in Z(G)$), which rewrites as $aha^{-1} = h$. Thus $aHa^{-1} = H$.

(3) Let $G = GL_2(\mathbb{R})$. It is clear that $\{aI_2 : a \in \mathbb{R}^*\} \subset Z(G)$. Let

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Z(G)$$

We see that M must commute with $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Thus

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

That gives $c = 0$ and $a = d$. Also M must commute with $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. Thus

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

that gives $b = 0$.