SOLUTIONS OF HOMEWORK PROBLEMS

2.31 If $a_1, a_2, \dots, a_{t-1}, a_t$ are elements in a group G, prove that

$$(a_1 a_2 \dots a_{t-1} a_t)^{-1} = a_t^{-1} a_{t-1}^{-1} \dots a_2^{-1} a_1^{-1}.$$

Solution:
By (v) of Theorem 3 we have

$$(a_1 a_2 \dots a_{t-1} a_t)^{-1} = a_t^{-1}(a_1 a_2 \dots a_{t-1})^{-1} = a_t^{-1} a_{t-1}^{-1}(a_1 a_2 \dots a_{t-2})^{-1} = \dots = a_t^{-1} a_{t-1}^{-1} \dots a_2^{-1} a_1^{-1}.$$

2.34 (i) How many elements of order 2 are there in S_5 and in S_6?

(ii) How many elements of order 2 are there in S_n?

Answer:
Case A: Let $n = 2k$. Then there are

$$\binom{n}{2} + \frac{\binom{n}{2}\binom{n-2}{2}}{2!} + \frac{\binom{n}{2}\binom{n-2}{2}\binom{n-4}{2}}{3!} + \dots + \frac{\binom{n}{2}\binom{n-2}{2}\cdots\binom{2}{2}}{k!}$$

elements of order 2 in S_n.
Case B: Let $n = 2k + 1$. Then there are

$$\binom{n}{2} + \frac{\binom{n}{2}\binom{n-2}{2}}{2!} + \frac{\binom{n}{2}\binom{n-2}{2}\binom{n-4}{2}}{3!} + \dots + \frac{\binom{n}{2}\binom{n-2}{2}\cdots\binom{3}{2}}{k!}$$

elements of order 2 in S_n.

In particularly, it follows that S_4 has

$$\binom{4}{2} + \frac{\binom{4}{2}\binom{2}{2}}{2!} = 9$$

elements of order 2 and S_5 has

$$\binom{5}{2} + \frac{\binom{5}{2}\binom{3}{2}}{2!} = 25$$

elements of order 2.

2.35 If G is a group, prove that the only element $g \in G$ with $g^2 = g$ is 1.

Solution: We rewrite $g^2 = g$ as $g \cdot g = g$. Multiplying both sides by g^{-1}, we get

$$(g \cdot g)g^{-1} = g \cdot g^{-1} \quad \Longrightarrow \quad g(g \cdot g^{-1}) = g \cdot g^{-1} \quad \Longrightarrow \quad g \cdot 1 = 1 \quad \Longrightarrow \quad g = 1.$$

2.36 Let H be a set containing an element e, and assume that there is an associative operation $*$ on H satisfying:

1. $e * x = x$ for all $x \in H$;
2. for every $x \in H$, there is $x' \in H$ with $x' * x = e$.

(i) Prove that if $h \in H$ satisfies $h * h = h$, then $h = e$.

(ii) For all $x \in H$, prove that $x * x' = e$.

(iii) For all $x \in H$, prove that $x * e = x$.

(iv) Prove that if $e' \in H$ satisfies $e' * x = x$ for all $x \in H$, then $e' = e$.

(v) Let $x \in H$. Prove that if $x'' \in H$ satisfies $x'' * x = e$, then $x'' = x'$.

(vi) Prove that H is a group.

Solution:
(i) Multiplying both sides of $h * h = h$ by h^{-1}, we get

$$h^{-1} * (h * h) = h^{-1} * h \quad \Longrightarrow \quad (h^{-1} * h) * h = h^{-1} * h \quad \Longrightarrow \quad e * h = e \quad \Longrightarrow \quad h = e.$$

(ii) Consider $(x * x') * (x * x')$. We have

$$(x * x') * (x * x') = x * [x' * (x * x')] = x * [(x' * x) * x'] = x * (e * x') = x * x'.$$

So, $(x * x') * (x * x') = x * x'$, and the result follows by (i).
(iii) We have

$$x * (x' * x) = x * e.$$

On the other hand, by (ii) we get

$$(x * x') * x = e * x = x.$$

Since $x * (x' * x) = (x * x') * x$ by the associative law, the result follows.
(iv) Since $e' * x = x$ for all $x \in H$, putting $x = e$, we have

$$e' * e = e.$$

On the other hand, by (iii) we get

$$e' * e = e',$$

and the result follows.
(v) We have

$$(x' * x) * x'' = e * x'' = x''.$$

On the other hand, by (ii) and (iii) we get

$$x' * (x * x'') = x' * e = x'.$$

Since $x' * (x * x'') = (x' * x) * x''$ by the associative law, the result follows.
(vi) Since there is an associative operation $*$, $e * x = x * e$ and $x' * x = x * x'$ for any $x \in H$, it follows that H is a group.

2.37 Let y be a group element of order m; if $m = tp$ for some prime p, prove that y^t has order p.

Solution:
Let g be the order of y^t. It follows that $(y^t)^g = 1$, so $y^{tg} = 1$. Note that $g \geq p$, because otherwise

$$g < p \quad \overset{\times t}{\Longrightarrow} \quad tg < tp \quad \overset{m=tp}{\Longrightarrow} \quad tg < m.$$

So, $y^{tg} = 1$ and $tg < m$, which is impossible, since m is the smallest positive number with $y^m = 1$. Finally, we note that

$$(y^t)^p = y^{tp} = y^m = 1.$$

So, p is the smallest power of y^t which gives 1, i.e. $g = p$.

Remark:
Note that the solution above does not use the fact that p is a prime. In other words, problem 2.37 is true for any positive integer p.

2.38 Let G be a group and let $a \in G$ have order pk for some prime p, where $k \geq 1$. Prove that if there is $x \in G$ with $x^p = a$, then the order of x is p^2k.

Solution:
Let g be the order of x. We first note that

$$x^{p^2k} = (x^p)^{pk} = a^{pk} = 1,$$

therefore

$$g \leq p^2k. \tag{$*$}$$

We now show that p^2k is the smallest power which gives 1. In fact, since $x^g = 1$, we get

$$(x^g)^p = 1 \quad \Longrightarrow \quad (x^p)^g = 1 \quad \Longrightarrow \quad a^g = 1,$$

therefore by Theorem 7 we obtain $pk \mid g$, hence

$$g = pkd \tag{$**$}$$

for some integer d. So,

$$1 = x^g = x^{pkd} = (x^p)^{kd} = a^{kd}.$$

But pk is the order of a, therefore $kd \geq pk$, so $d \geq p$. This and $(**)$ give

$$g = pkd \geq p^2k. \tag{$***$}$$

From $(*)$ and $(***)$ follows $g = p^2k$.

2.39 Let $G = GL(2, \mathbb{Q})$, and let

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}.$$

Show that $A^4 = E = B^6$, but that $(AB)^n \neq E$ for all $n > 0$.

Solution:
We have

$$A^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \quad A^4 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

and

$$B^2 = \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix}, \quad B^4 = \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix}^2 = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix},$$

$$B^6 = B^4 B^2 = \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Finally, we show by induction that

$$(AB)^n = \begin{bmatrix} 1 & -n \\ 0 & 1 \end{bmatrix}.$$

In fact, for $n = 1$ this is true, since

$$AB = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}.$$

Suppose this is true for some $n = k \geq 1$, that is

$$(AB)^k = \begin{bmatrix} 1 & -k \\ 0 & 1 \end{bmatrix}.$$

We prove that

$$(AB)^{k+1} = \begin{bmatrix} 1 & -k-1 \\ 0 & 1 \end{bmatrix}.$$

We have

$$(AB)^{k+1} = (AB)^k (AB) = \begin{bmatrix} 1 & -k \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -k-1 \\ 0 & 1 \end{bmatrix}.$$

2.40(i) Prove, by induction on $n \geq 1$, that

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}^n = \begin{bmatrix} \cos n\theta & -\sin n\theta \\ \sin n\theta & \cos n\theta \end{bmatrix}$$

Solution:
By $n = 1$ this is obviously true. Suppose this is true for some $n = k \geq 1$, that is

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}^k = \begin{bmatrix} \cos k\theta & -\sin k\theta \\ \sin k\theta & \cos k\theta \end{bmatrix}.$$

We prove that

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}^{k+1} = \begin{bmatrix} \cos(k+1)\theta & -\sin(k+1)\theta \\ \sin(k+1)\theta & \cos(k+1)\theta \end{bmatrix}.$$

We have

$$\begin{aligned}
\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}^{k+1} &= \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}^{k} \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \\
&= \begin{bmatrix} \cos k\theta & -\sin k\theta \\ \sin k\theta & \cos k\theta \end{bmatrix} \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \\
&= \begin{bmatrix} \cos k\theta\cos\theta - \sin k\theta\sin\theta & -\cos k\theta\sin\theta - \sin k\theta\cos\theta \\ \sin k\theta\cos\theta + \cos k\theta\sin\theta & -\sin k\theta\sin\theta + \cos k\theta\cos\theta \end{bmatrix}.
\end{aligned}$$

It is known that

$$\sin(\alpha+\beta) = \sin\alpha\cos\beta + \sin\beta\cos\alpha$$

and

$$\cos(\alpha+\beta) = \cos\alpha\cos\beta - \sin\alpha\sin\alpha,$$

therefore

$$\cos k\theta\cos\theta - \sin k\theta\sin\theta = \cos(k\theta+\theta) = \cos(k+1)\theta,$$

$$\sin k\theta\cos\theta + \cos k\theta\sin\theta = \sin(k\theta+\theta) = \sin(k+1)\theta,$$

and the result follows.

2.41 If G is a group in which $x^2 = 1$ for every $x \in G$, prove that G must be abelian.

Solution:
We have $x \cdot x = 1$ for every $x \in G$. This, in particularly, gives

$$(ab)(ab) = 1$$

for every $a,\ b \in G$. Multiplying both sides by ba, we get

$$ababba = ba \quad\Longrightarrow\quad aba1a = ba \quad\Longrightarrow\quad abaa = ba \quad\Longrightarrow\quad ab1 = ba \quad\Longrightarrow\quad ab = ba,$$

and the result follows.

2.42 If G is a group with an even number of elements, prove that the number of elements in G of order 2 is odd. In particular, G must contain an element of order 2.

Solution:
Let us split G into three subsets:

$$G = \{e\} \cup \underbrace{\{\text{elements of order } 2\}}_{S_1} \cup \underbrace{\{\text{elements of order} > 2\}}_{S_2}$$

Note that

$$x^2 = 1 \quad\Longleftrightarrow\quad x = x^{-1}.$$

This means that an element x coincides with its inverse if and only if $x^2 = 1$. In other words, an element x coincides with its inverse if and only if x has order 2 or $x = 1$. From this it follows that for any element $x \in S_2$ we have $x \neq x^{-1}$. Moreover, it is easy to see that

$$x_1 \neq x_2 \iff x_1^{-1} \neq x_2^{-1}$$

and

$$\text{order of } x = \text{order of } x^{-1}.$$

The information above immediately implies that S_2 has even number of elements. Since $|G|$ is even and $|\{e\}|$ is odd, it follows that S_1 has odd number of elements.

2.44 The **stochastic group** $\Sigma(2,\mathbb{R})$ consists of all those matrices in $\mathrm{GL}(2,\mathbb{R})$ whose column sums are 1; that is, $\Sigma(2,\mathbb{R})$ consists of all the nonsingular matrices

$$\begin{bmatrix} a & c \\ b & d \end{bmatrix}$$

with $a+b = 1 = c+d$. Prove that the product of two stochastic matrices is again stochastic, and that the inverse of a stochastic matrix is stochastic.

Solution:
We have

$$\begin{bmatrix} a_1 & c_1 \\ b_1 & d_1 \end{bmatrix}\begin{bmatrix} a_2 & c_2 \\ b_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 + c_1b_2 & a_1c_2 + c_1d_2 \\ b_1a_2 + d_1b_2 & b_1c_2 + d_1d_2 \end{bmatrix},$$

which is stochastic, since

$$a_1a_2 + c_1b_2 + b_1a_2 + d_1b_2 = a_2(a_1+b_1) + b_2(c_1+d_1) = a_2 + b_2 = 1$$

and

$$a_1c_2 + c_1d_2 + b_1c_2 + d_1d_2 = c_2(a_1+b_1) + d_2(c_1+d_1) = c_2 + d_2 = 1.$$

Also,

$$\begin{bmatrix} a & c \\ b & d \end{bmatrix}^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -c \\ -b & a \end{bmatrix} = \begin{bmatrix} \frac{d}{ad-bc} & -\frac{c}{ad-bc} \\ -\frac{b}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}$$

which is stochastic, since

$$\frac{d}{ad-bc} - \frac{b}{ad-bc} = \frac{d-b}{ad-bc} = \frac{d-b}{ad+bd-bd-bc} = \frac{d-b}{d(a+b)-b(d+c)} = \frac{d-b}{d-b} = 1$$

and

$$-\frac{c}{ad-bc} + \frac{a}{ad-bc} = \frac{a-c}{ad-bc} = \frac{a-c}{ad+ac-ac-bc} = \frac{a-c}{a(d+c)-c(a+b)} = \frac{a-c}{a-c} = 1.$$

2.45 (i) Define a **special linear group** by

$$\mathrm{SL}(2,\mathbb{R}) = \{A \in GL(2,\mathbb{R}) : \det(A) = 1\}.$$

Prove that SL $(2,\mathbb{R})$ is a subgroup of GL $(2,\mathbb{R})$.
(ii) Prove that GL $(2,\mathbb{Q})$ is a subgroup of GL $(2,\mathbb{R})$.

Solution:
(i) We will use Theorem 4. In order to apply this Theorem we should check that SL $(2,\mathbb{R})$ is nonempty and that $M_1M_2^{-1} \in$ SL $(2,\mathbb{R})$ whenever $M_1 \in$ SL $(2,\mathbb{R})$ and $M_2 \in$ SL $(2,\mathbb{R})$.

First of all note that SL $(2,\mathbb{R})$ is nonempty, since $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in$ SL $(2,\mathbb{R})$. Let

$$M_1 = \begin{bmatrix} a_1 & c_1 \\ b_1 & d_1 \end{bmatrix} \quad \text{and} \quad M_2 = \begin{bmatrix} a_2 & c_2 \\ b_2 & d_2 \end{bmatrix}$$

be from SL $(2,\mathbb{R})$. Then $\det(M_1M_2^{-1}) = 1$, since

$$\det(M_1M_2^{-1}) = \det(M_1)\det(M_2^{-1}) = \det(M_1)[\det(M_2)]^{-1} = 1 \cdot 1^{-1} = 1.$$

Finally,

$$M_1M_2^{-1} = \begin{bmatrix} a_1 & c_1 \\ b_1 & d_1 \end{bmatrix} \begin{bmatrix} a_2 & c_2 \\ b_2 & d_2 \end{bmatrix}^{-1} = \begin{bmatrix} a_1 & c_1 \\ b_1 & d_1 \end{bmatrix} \begin{bmatrix} \dfrac{d_2}{a_2d_2 - b_2c_2} & -\dfrac{c_2}{a_2d_2 - b_2c_2} \\ -\dfrac{b_2}{a_2d_2 - b_2c_2} & \dfrac{a_2}{a_2d_2 - b_2c_2} \end{bmatrix},$$

which is equal to

$$\begin{bmatrix} a_1 & c_1 \\ b_1 & d_1 \end{bmatrix} \begin{bmatrix} d_2 & -c_2 \\ -b_2 & a_2 \end{bmatrix},$$

since $a_2d_2 - b_2c_2 = \det M_1 = 1$. So,

$$M_1M_2^{-1} = \begin{bmatrix} a_1 & c_1 \\ b_1 & d_1 \end{bmatrix} \begin{bmatrix} d_2 & -c_2 \\ -b_2 & a_2 \end{bmatrix} = \begin{bmatrix} a_1d_2 - c_1b_2 & -a_1c_2 + c_1a_2 \\ b_1d_2 - d_1b_2 & b_1c_2 - d_1a_2 \end{bmatrix}.$$

From this, obviously, follows that if M_1 and M_2 have real entries, then $M_1M_2^{-1}$ has also real entries. So, $M_1M_2^{-1} \in$ SL $(2,\mathbb{R})$ whenever $M_1 \in$ SL $(2,\mathbb{R})$ and $M_2 \in$ SL $(2,\mathbb{R})$.

(ii) To prove that GL $(2,\mathbb{Q})$ is a subgroup of GL $(2,\mathbb{R})$, we use Theorem 4 again. First of all note that GL $(2,\mathbb{Q})$ is nonempty, since $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in$ GL $(2,\mathbb{Q})$. Let

$$M_1 = \begin{bmatrix} a_1 & c_1 \\ b_1 & d_1 \end{bmatrix} \quad \text{and} \quad M_2 = \begin{bmatrix} a_2 & c_2 \\ b_2 & d_2 \end{bmatrix}$$

be from GL $(2,\mathbb{Q})$. Then $\det(M_1M_2^{-1}) \neq 0$, since

$$\det(M_1M_2^{-1}) = \det(M_1)\det(M_2^{-1}) = \det(M_1)[\det(M_2)]^{-1},$$

which is nonzero, since $\det M_1 \neq 0$ and $\det M_2 \neq 0$. Finally,

$$M_1M_2^{-1} = \begin{bmatrix} a_1 & c_1 \\ b_1 & d_1 \end{bmatrix} \begin{bmatrix} a_2 & c_2 \\ b_2 & d_2 \end{bmatrix}^{-1} = \begin{bmatrix} a_1 & c_1 \\ b_1 & d_1 \end{bmatrix} \begin{bmatrix} \dfrac{d_2}{a_2d_2 - b_2c_2} & -\dfrac{c_2}{a_2d_2 - b_2c_2} \\ -\dfrac{b_2}{a_2d_2 - b_2c_2} & \dfrac{a_2}{a_2d_2 - b_2c_2} \end{bmatrix}$$

$$= \begin{bmatrix} \dfrac{a_1d_2 - c_1b_2}{a_2d_2 - b_2c_2} & \dfrac{a_1c_2 - c_1a_2}{a_2d_2 - b_2c_2} \\ -\dfrac{b_1d_2 - d_1b_2}{a_2d_2 - b_2c_2} & \dfrac{b_1c_2 - d_1a_2}{a_2d_2 - b_2c_2} \end{bmatrix}.$$

From this, obviously, follows that if M_1 and M_2 have rational entries, then $M_1M_2^{-1}$ has also rational entries. So, $M_1M_2^{-1} \in \mathrm{GL}\ (2, \mathbb{Q})$ whenever $M_1 \in \mathrm{GL}\ (2, \mathbb{Q})$ and $M_2 \in \mathrm{GL}\ (2, \mathbb{Q})$.

2.46 Give an example of two subgroups H and K of a group G whose union $H \cup K$ is not a subgroup of G.

Solution:
Let $G = \mathbf{V}$, $H = \{(1), (12)(34)\}$, and $K = \{(1), (13)(24)\}$. Then $H \cup K = \{(1), (12)(34), (13)(24)\}$, which is not a subgroup, since it is not closed. In fact, $(12)(34)(13)(24) = (14)(23) \notin H \cup K$.

2.48 If H and K are subgroups of a group G and if $|H|$ and $|K|$ are relatively prime, prove that $H \cap K = \{1\}$.

Solution:
Let x be any element from $H \cap K$. First of all note that by Corollary 2 we have

$$a^{|H|} = 1 = a^{|K|}. \tag{$*$}$$

Let g be the order of x. Then $(*)$ and Theorem 7 yield $g \mid |H|$ and $g \mid |K|$. Since $|H|$ and $|K|$ are relatively prime, it follows that $g = 1$, which implies $x = 1$.

2.49 Let $G = \langle a \rangle$ be a cyclic group of order n. Show that a^k is a generator of G if and only if $(k, n) = 1$.

Solution:
$\Longrightarrow$) Let $G = \langle a \rangle$ be a cyclic group of order n and let a^k be a generator of G. We prove that $(k, n) = 1$. First of all note that by Corollary 2 we have

$$a^{|G|} = 1 \quad \Longrightarrow \quad a^n = 1.$$

We now suppose to the contrary that $(k, n) = \ell > 1$. Then $k = \ell d_1$ and $n = \ell d_2$ for some $d_1, d_2 \in \mathbb{Z}$. Then

$$(a^k)^{d_2} = (a^{\ell d_1})^{d_2} = (a^{\ell d_2})^{d_1} = (a^n)^{d_1} = 1^{d_1} = 1.$$

Note that since $\ell > 1$, we have $d_2 < n$. This means that the order of a^k is $< n$. This is impossible, because by Theorem 6 the order of a generator should be equal to the order of G, which is n.

$\Longleftarrow$) Let $G = \langle a \rangle$ be a cyclic group of order n and let $(k, n) = 1$. We prove that a^k is a generator of G. In fact, let g be the order of a^k. Then

$$(a^k)^g = 1. \tag{$*$}$$

On the one hand, since $|\langle a\rangle| = n$, by Theorem 6 the order of a is n. From this and $(*)$ by Theorem 7 we get $n \mid kg$. This by Euclid's Lemma gives $n \mid g$, since $(k, n) = 1$. So, $n \leq g$. On the other hand,

$$(a^k)^n = (a^n)^k = 1^k = 1,$$

so $g \leq n$. Therefore $n = g$.

2.50 Prove that every subgroup S of a cyclic group $G = \langle a\rangle$ is itself cyclic.

Solution:
If $S = \{1\}$, we are done, since $\{1\}$ is cyclic. Suppose $S \neq \{1\}$, that is $S = \{1,\ a^{k_1},\ a^{k_2}, \ldots\}$. Let k be the smallest positive integer such that $a^k \in S$. If $S = \langle a^k\rangle$, we are done. Suppose $S \neq \langle a^k\rangle$. This means, that there exists $a^{k_i} \in S$ such that $k_i \neq dk$. Therefore by the Division Algorithm we get

$$k_i = dk + r, \quad 1 \leq r < k,$$

so $a^{k_i} = a^{dk+r} = a^{dk}a^r$, hence $a^r = a^{k_i}a^{-dk}$. Clearly, $a^{k_i}, a^{-dk} \in S$, therefore $a^r \in S$, which is impossible, since $1 \leq r < k$ and k is the smallest positive integer such that $a^k \in S$.

2.51 Prove that if G is a cyclic group of order n and if $d \mid n$, then G has a subgroup of order d.

Solution:
Let $G = \langle a\rangle$. By Theorem 6, the order of a is n. Then

$$a^n = 1.$$

Since $d \mid n$, we have $n = kd$. Consider $H = \langle a^k\rangle$ and let g be the order of a^k. By Theorem 6 we have $|H| = g$. We prove that the order of H is d, i.e. $g = d$.

In fact, since g is the order of a^k, it follows that $(a^k)^g = 1$, so $a^{kg} = 1$. Note that $g \geq d$, because otherwise

$$g < d \quad \overset{\times k}{\Longrightarrow} \quad kg < kd \quad \overset{n=kd}{\Longrightarrow} \quad kg < n.$$

So, $a^{kg} = 1$ and $kg < n$, which is impossible, since n is the smallest positive number with $a^n = 1$. Finally, we note that

$$(a^k)^d = a^{kd} = a^n = 1.$$

So, d is the smallest power of a^k which gives 1, i.e. $g = d$.

2.52 Let G be a group of order 4. Prove that either G is cyclic or $x^2 = 1$ for every $x \in G$. Conclude, using Exercise 2.41, that G must be abelian.

Solution:
Pick some $x \in G$ and consider $H = \langle a\rangle$. If $|H| = 4$, then $H = G$, therefore G is cyclic and we are done. Suppose $|H| < 4$. Since H is a subgroup of G, by Lagrange's Theorem we have $|H| = 2$ or $|H| = 1$, therefore by Theorem 6 the order of x is 2 (which means, that $x^2 = 1$) or 1 (which means, that $x = 1$, so $x^2 = 1$ again). So, in both cases $x^2 = 1$.

Finally, to show that G is abelian, we note that if G is cyclic, then it is abelian, since all cyclic groups are abelian. If $x^2 = 1$ for every $x \in G$, then G is abelian by Exercise 2.41.