Exercises from *Abstract Algebra* by I. N. Herstein

Exercise 2.1.18 If G is a finite group of even order, show that there must be an element $a \neq e$ such that $a = a^{-1}$.

Proof. First note that $a = a^{-1}$ is the same as saying $a^2 = e$, where e is the identity. I.e. the statement is that there exists at least one element of order 2 in G. Every element a of G of order at least 3 has an inverse a^{-1} that is not itself – that is, $a \neq a^{-1}$. So the subset of all such elements has an even cardinality (/size). There's exactly one element with order 1 : the identity $e^1 = e$. So G contains an even number of elements -call it $2k$– of which an even number are elements of order 3 or above – call that $2n$ where $n < k$– and exactly one element of order 1 . Hence the number of elements of order 2 is

$$2k - 2n - 1 = 2(k - n) - 1$$

This cannot equal 0 as $2(k - n)$ is even and 1 is odd. Hence there's at least one element of order 2 in G, which concludes the proof. □

Exercise 2.1.21 Show that a group of order 5 must be abelian.

Proof. Suppose G is a group of order 5 which is not abelian. Then there exist two non-identity elements $a, b \in G$ such that $a * b \neq b * a$. Further we see that G must equal $\{e, a, b, a * b, b * a\}$. To see why $a * b$ must be distinct from all the others, not that if $a *\, b = e$, then a and b are inverses and hence $a * b = b * a$. Contradiction. If $a * b = a$ (or $= b$), then $b = e$ (or $a = e$) and e commutes with everything. Contradiction. We know by supposition that $a * b \neq b * a$. Hence all the elements $\{e, a, b, a * b, b * a\}$ are distinct.

Now consider a^2. It can't equal a as then $a = e$ and it can't equal $a * b$ or $b * a$ as then $b = a$. Hence either $a^2 = e$ or $a^2 = b$. Now consider $a * b * a$. It can't equal a as then $b * a = e$ and hence $a * b = b * a$. Similarly it can't equal b. It also can't equal $a * b$ or $b * a$ as then $a = e$. Hence $a * b * a = e$.

So then we additionally see that $a^2 \neq e$ because then $a^2 = e = a * b * a$ and consequently $a = b * a$ (and hence $b = e$). So $a^2 = b$. But then $a * b = a * a^2 = a^2 * a = b * a$. Contradiction. Hence starting with the assumption that there exists an order 5 abelian group G leads to a contradiction. Thus there is no such group. □

Exercise 2.1.26 If G is a finite group, prove that, given $a \in G$, there is a positive integer n, depending on a, such that $a^n = e$.

Proof. Because there are only a finite number of elements of G, it's clear that the set $\{a, a^2, a^3, \ldots\}$ must be a finite set and in particular, there should exist some i and j such that $i \neq j$ and $a^i = a^j$. WLOG suppose further that $i > j$ (just reverse the roles of i and j otherwise). Then multiply both sides by $\left(a^j\right)^{-1} = a^{-j}$ to get

$$a^i * a^{-j} = a^{i-j} = e$$

Thus the $n = i - j$ is a positive integer such that $a^n = e$. $\square$

Exercise 2.1.27 If G is a finite group, prove that there is an integer $m > 0$ such that $a^m = e$ for all $a \in G$.

Proof. Let $n_1, n_2, \ldots, n_k$ be the orders of all k elements of $G = \{a_1, a_2, \ldots, a_k\}$. Let $m = \operatorname{lcm}(n_1, n_2, \ldots, n_k)$. Then, for any $i = 1, \ldots, k$, there exists an integer c such that $m = n_i c$. Thus

$$a_i^m = a_i^{n_i c} = (a_i^{n_i})^c = e^c = e$$

Hence m is a positive integer such that $a^m = e$ for all $a \in G$. $\square$

Exercise 2.2.3 If G is a group in which $(ab)^i = a^i b^i$ for three consecutive integers i, prove that G is abelian.

Proof. Let G be a group, $a, b \in G$ and i be any integer. Then from given condition,

$$\begin{aligned}(ab)^i &= a^i b^i \\ (ab)^{i+1} &= a^{i+1} b^{i+1} \\ (ab)^{i+2} &= a^{i+2} b^{i+2}\end{aligned}$$

From first and second, we get

$$a^{i+1} b^{i+1} = (ab)^i (ab) = a^i b^i ab \Longrightarrow b^i a = ab^i$$

From first and third, we get

$$a^{i+2} b^{i+2} = (ab)^i (ab)^2 = a^i b^i abab \Longrightarrow a^2 b^{i+1} = b^i aba$$

This gives

$$a^2 b^{i+1} = a\left(ab^i\right) b = ab^i ab = b^i a^2 b$$

Finally, we get

$$b^i aba = b^i a^2 b \Longrightarrow ba = ab$$

This shows that G is Abelian. $\square$

Exercise 2.2.5 Let G be a group in which $(ab)^3 = a^3b^3$ and $(ab)^5 = a^5b^5$ for all $a, b \in G$. Show that G is abelian.

Proof. We have

$$\begin{aligned}
&(ab)^3 = a^3b^3, \text{ for all } a, b \in G \\
\Longrightarrow &(ab)(ab)(ab) = a\left(a^2b^2\right)b \\
\Longrightarrow &a(ba)(ba)b = a\left(a^2b^2\right)b \\
\Longrightarrow &(ba)^2 = a^2b^2, \text{ by cancellation law.}
\end{aligned}$$

Again,

$$\begin{aligned}
&(ab)^5 = a^5b^5, \text{ for all } a, b \in G \\
\Longrightarrow &(ab)(ab)(ab)(ab)(ab) = a\left(a^4b^4\right)b \\
\Longrightarrow &a(ba)(ba)(ba)(ba)b = a\left(a^4b^4\right)b \\
\Longrightarrow &(ba)^4 = a^4b^4, \text{ by cancellation law.}
\end{aligned}$$

Now by combining two cases we have

$$\begin{aligned}
&(ba)^4 = a^4b^4 \\
\Longrightarrow &\left((ba)^2\right)^2 = a^2\left(a^2b^2\right)b^2 \\
\Longrightarrow &\left(a^2b^2\right)^2 = a^2\left(a^2b^2\right)b^2 \\
\Longrightarrow &\left(a^2b^2\right)\left(a^2b^2\right) = a^2\left(a^2b^2\right)b^2 \\
\Longrightarrow &a^2\left(b^2a^2\right)b^2 = a^2\left(a^2b^2\right)b^2 \\
\Longrightarrow &b^2a^2 = a^2b^2, \text{ by cancellation law.} \\
\Longrightarrow &b^2a^2 = (ba)^2, \text{ since } (ba)^2 = a^2b^2 \\
\Longrightarrow &b(ba)a = (ba)(ba) \\
\Longrightarrow &b(ba)a = b(ab)a \\
\Longrightarrow &ba = ab, \text{ by cancellation law.}
\end{aligned}$$

It follows that, $ab = ba$ for all $a, b \in G$. Hence G is abelian □

Exercise 2.2.6c Let G be a group in which $(ab)^n = a^nb^n$ for some fixed integer $n > 1$ for all $a, b \in G$. For all $a, b \in G$, prove that $\left(aba^{-1}b^{-1}\right)^{n(n-1)} = e$.

Proof. We start with the following two intermediate results. (1) $(ab)^{n-1} = b^{n-1}a^{n-1}$. (2) $a^nb^{n-1} = b^{n-1}a^n$. To prove (1), notice by the given condition for all $a, b \in G$ $(ba)^n = b^na^n$, for some fixed integers $n > 1$. Then, $(ba)^n = b^na^n \Longrightarrow b.(ab)(ab)\ldots.(ab).a = b\left(b^{n-1}a^{n-1}\right)a$, where (ab) occurs $n-1$ times $\Longrightarrow (ab)^{n-1} = b^{n-1}a^{n-1}$, by cancellation law. Hence, for all $a, b \in G$

$$(ab)^{n-1} = b^{n-1}a^{n-1}.$$

To prove (2), notice by the given condition for all $a, b \in G$ $(ba)^n = b^n a^n$, for some fixed integers $n > 1$. Then we have

$$
\begin{aligned}
&(ba)^n = b^n a^n \\
\Longrightarrow & b \cdot (ab)(ab) \ldots (ab) \cdot a = b\left(b^{n-1} a^{n-1}\right) a, \text{ where } (ab) \text{ occurs } n-1 \text{ times} \\
\Longrightarrow & (ab)^{n-1} = b^{n-1} a^{n-1}, \text{ by cancellation law} \\
\Longrightarrow & (ab)^{n-1}(ab) = \left(b^{n-1} a^{n-1}\right)(ab) \\
\Longrightarrow & (ab)^n = b^{n-1} a^n b \\
\Longrightarrow & a^n b^n = b^{n-1} a^n b, \text{ given condition} \\
\Longrightarrow & a^n b^{n-1} = b^{n-1} a^n, \text{ by cancellation law.}
\end{aligned}
$$

Therefore for all $a, b \in G$ we have

$$a^n b^{n-1} = b^{n-1} a^n$$

In order to show that

$$\left(aba^{-1}b^{-1}\right)^{n(n-1)} = e, \text{ for all } a, b \in G$$

it is enough to show that

$$(ab)^{n(n-1)} = (ba)^{n(n-1)}, \quad \forall x, y \in G.$$

Step 3 This is because of

$$
\begin{aligned}
(ab)^{n(n-1)} = (ba)^{n(n-1)} &\Longrightarrow \left(ba)^{-1}\right)^{n(n-1)} (ab)^{n(n-1)} = e \\
&\Longrightarrow \left(a^{-1}b^{-1}\right)^{n(n-1)} (ab)^{n(n-1)} = e \\
&\Longrightarrow \left(\left(a^{-1}b^{-1}\right)^n\right)^{n-1} \left((ab)^n\right)(n-1) = e \\
&\Longrightarrow \left((ab)^n \left(a^{-1}b^{-1}\right)^n\right)^{n-1} = e, \text{ by (1)} \\
&\Longrightarrow \left(aba^{-1}b^{-1}\right)^{n(n-1)} = e, \text{ (given condition)}
\end{aligned}
$$

Now, it suffices to show that

$$(ab)^{n(n-1)} = (ba)^{n(n-1)}, \quad \forall x, y \in G.$$

Now, we have

$$\begin{aligned}
(ab)^{n(n-1)} &= (a^n b^n)^{n-1}, \text{ by the given condition} \\
&= \left(a^n b^{n-1} b\right)^{n-1} \\
&= \left(b^{n-1} a^n b\right)^{n-1}, \text{ by (2)} \\
&= (a^n b)^{n-1} \left(b^{n-1}\right)^{n-1}, \text{ by (1)} \\
&= b^{n-1} (a^n)^{n-1} \left(b^{n-1}\right)^{n-1}, \text{ by (1)} \\
&= \left(b^{n-1} \left(a^{n-1}\right)^n\right) \left(b^{n-1}\right)^{n-1} \\
&= \left(a^{n-1}\right)^n b^{n-1} \left(b^{n-1}\right)^{n-1}, \text{ by (2)} \\
&= \left(a^{n-1}\right)^n \left(b^{n-1}\right)^n \\
&= \left(a^{n-1} b^{n-1}\right)^n, \text{ by (1)} \\
&= (ba)^{n(n-1)}, \text{ by (1)}.
\end{aligned}$$

This completes our proof. □

Exercise 2.3.17 If G is a group and $a, x \in G$, prove that $C\left(x^{-1}ax\right) = x^{-1}C(a)x$

Proof. Note that

$$C(a) := \{x \in G \mid xa = ax\}.$$

Let us assume $p \in C\left(x^{-1}ax\right)$. Then,

$$\begin{aligned}
& p\left(x^{-1}ax\right) = \left(x^{-1}ax\right)p \\
\Longrightarrow & \left(px^{-1}a\right)x = x^{-1}(axp) \\
\Longrightarrow & x\left(px^{-1}a\right) = (axp)x^{-1} \\
\Longrightarrow & \left(xpx^{-1}\right)a = a\left(xpx^{-1}\right) \\
\Longrightarrow & xpx^{-1} \in C(a).
\end{aligned}$$

Therefore,

$$p \in C\left(x^{-1}ax\right) \Longrightarrow xpx^{-1} \in C(a).$$

Thus,

$$C\left(x^{-1}ax\right) \subset x^{-1}C(a)x.$$

Let us assume

$$q \in x^{-1}C(a)x.$$

Then there exists an element y in $C(a)$ such that

$$q = x^{-1}yx$$

Now,

$$y \in C(a) \Longrightarrow ya = ay.$$

Also,

$$q\left(x^{-1}ax\right)=\left(x^{-1}yx\right)\left(x^{-1}ax\right)=x^{-1}(ya)x=x^{-1}(ya)x=\left(x^{-1}yx\right)\left(x^{-1}ax\right)=\left(x^{-1}yx\right)q.$$

Therefore,

$$q\left(x^{-1}ax\right)=\left(x^{-1}yx\right)q$$

So,

$$q\in C\left(x^{-1}ax\right).$$

Consequently we have

$$x^{-1}C(a)x\subset C\left(x^{-1}ax\right).$$

It follows from the aforesaid argument

$$C\left(x^{-1}ax\right)=x^{-1}C(a)x.$$

This completes the proof. □

Exercise 2.3.16 If a group G has no proper subgroups, prove that G is cyclic of order p, where p is a prime number.

Proof. Case-1: $G=(e), e$ being the identity element in G. Then trivially G is cyclic. Case-2: $G\neq(e)$. Then there exists an non-identity element in G. Let us consider an non-identity element in G, say $a\neq(e)$. Now look at the cyclic subgroup generated by a, that is, $\langle a\rangle$. Since $a\neq(e)\in G, \langle a\rangle$ is a subgroup of G. If $G\neq\langle a\rangle$ then $\langle a\rangle$ is a proper non-trivial subgroup of G, which is an impossibility. Therfore we must have

$$G=\langle a\rangle.$$

This implies, G is a cyclic group generated by a. Then it follows that every non-identity element of G is a generator of G. Now we claim that G is finite. □

Exercise 2.4.36 If $a>1$ is an integer, show that $n\mid\varphi(a^n-1)$, where ϕ is the Euler φ-function.

Proof. Proof: We have $a>1$. First we propose to prove that

$$\operatorname{Gcd}\left(a, a^n-1\right)=1.$$

If possible, let us assume that $\operatorname{Gcd}\left(a, a^n-1\right)=d$, where $d>1$. Then d divides a as well as a^n-1. Now, d divides $a\Longrightarrow d$ divides a^n. This is an impossibility, since d divides a^n-1 by our assumption. Consequently, d divides 1 , which implies $d=1$. Hence we are contradict to the fact that $d>1$. Therefore

$$\operatorname{Gcd}\left(a, a^n-1\right)=1.$$

Then $a\in U_{a^n-1}$, where U_n is a group defined by

$$U_n:=\left\{\bar{a}\in\mathbb{Z}_n\mid\operatorname{Gcd}(a, n)=1\right\}.$$

We know that order of an element divides the order of the group. Here order of the group U_{a^n-1} is $\phi\left(a^n-1\right)$ and $a\in U_{a^n-1}$. This follows that $\mathrm{o}(a)$ divides $\phi\left(a^n-1\right)$. □

Exercise 2.5.23 Let G be a group such that all subgroups of G are normal in G. If $a, b \in G$, prove that $ba = a^j b$ for some j.

Proof. Let G be a group where each subgroup is normal in G. let $a, b \in G$.

$$\begin{aligned} \langle a \rangle \triangleright G \Rightarrow b \cdot \langle a \rangle = \langle a \rangle \cdot b. \\ \Rightarrow \quad b \cdot a = a^j \cdot b \text{ for some } j \in \mathbb{Z}. \end{aligned}$$

(hence for $a_1 b \in G \quad a^j b = b \cdot a$). □

Exercise 2.5.30 Suppose that $|G| = pm$, where $p \nmid m$ and p is a prime. If H is a normal subgroup of order p in G, prove that H is characteristic.

Proof. Let G be a group of order pm, such that $p \nmid m$. Now, Given that H is a normal subgroup of order p. Now we want to prove that H is a characterestic subgroup, that is $\phi(H) = H$ for any automorphism ϕ of G. Now consider $\phi(H)$. Clearly $|\phi(H)| = p$. Suppose $\phi(H) \neq H$, then $H \cap \phi(H) = \{e\}$. Consider $H\phi(H)$, this is a subgroup of G as H is normal. Also $|H\phi(H)| = p^2$. By lagrange's theorem then $p^2 \mid pm \Longrightarrow p \mid m$ - contradiction. So $\phi(H) = H$, and H is characterestic subgroup of G □

Exercise 2.5.31 Suppose that G is an abelian group of order $p^n m$ where $p \nmid m$ is a prime. If H is a subgroup of G of order p^n, prove that H is a characteristic subgroup of G.

Proof. Let G be an abelian group of order $p^n m$, such that $p \nmid m$. Now, Given that H is a subgroup of order p^n. Since G is abelian H is normal. Now we want to prove that H is a characterestic subgroup, that is $\phi(H) = H$ for any automorphism ϕ of G. Now consider $\phi(H)$. Clearly $|\phi(H)| = p^n$. Suppose $\phi(H) \neq H$, then $|H \cap \phi(H)| = p^s$, where $s < n$. Consider $H\phi(H)$, this is a subgroup of G as H is normal. Also $|H\phi(H)| = \frac{|H||\phi(H)|}{|H \cap \phi(H)|} = \frac{p^{2n}}{p^s} = p^{2n-s}$, where $2n - s > n$. By lagrange's theorem then $p^{2n-s} | p^n m \Longrightarrow p^{n-s} | m \Longrightarrow p \mid m$-contradiction. So $\phi(H) = H$, and H is characterestic subgroup of G. □

Exercise 2.5.37 If G is a nonabelian group of order 6, prove that $G \simeq S_3$.

Proof. Suppose G is a non-abelian group of order 6 . We need to prove that $G \cong S_3$. Since G is non-abelian, we conclude that there is no element of order 6. Now all the nonidentity element has order either 2 or 3 . All elements cannot be order 3 .This is because except the identity elements there are 5 elements, but order 3 elements occur in pair, that is a, a^2, both have order 3 , and $a \neq a^2$. So, this is a contradiction, as there are only 5 elements. So, there must be an element of order 2 . All elements of order 2 will imply that G is abelian, hence there is also element of order 3 . Let a be an element of order 2 , and b be an element of order 3 . So we have e, a, b, b^2, already 4 elements. Now $ab \neq e, b, b^2$. So ab is another element distinct from the ones already constructed.

$ab^2 \neq e, b, ab, b^2, a$. So, we have got another element distinct from the other. So, now $G = \left\{e, a, b, b^2, ab, ab^2\right\}$. Also, ba must be equal to one of these elements. But $ba \neq e, a, b, b^2$. Also if $ba = ab$, the group will become abelian. so $ba = ab^2$. So what we finally get is $G = \left\langle a, b \mid a^2 = e = b^3, ba = ab^2 \right\rangle$. Hence $G \cong S_3$. $\square$

Exercise 2.5.43 Prove that a group of order 9 must be abelian.

Proof. We use the result from problem 40 which is as follows: Suppose G is a group, H is a subgroup and $|G| = n$ and $n \nmid (i_G(H))!$. Then there exists a normal subgroup $K\ neq { e }$ and $K \subseteq H$. So, we have now a group G of order 9. Suppose that G is cyclic, then G is abelian and there is nothing more to prove. Suppose that G s not cyclic,then there exists an element a of order 3 , and $A = \langle a \rangle$. Now $i_G(A) = 3$, now $9 \nmid 3\ !$, hence by the above result there is a normal subgroup K, non-trivial and $K \subseteq A$. But $|A| = 3$, a prime order subgroup, hence has no non-trivial subgroup, so $K = A$. So A is normal subgroup. Now since G is not cyclic any non-identity element is of order 3.So Let $a(\neq e) \in G$.Consider $A = \langle a \rangle$. As shown before A is normal. a commutes with any if its powers. Now Let $b \in G$ such that $b \notin A$. Then $bab^{-1} \in A$ and hence $bab^{-1} = a^i$.This implies $a = b^3ab^{-3} = a^{i^3} \implies a^{i^3-1} = e$. So, 3 divides $i^3 - 1$. Also by fermat's little theorem 3 divides $i^2 - 1$.So 3 divides $i - 1$. But $0 \leq i \leq 2$. So $i = 1$, is the only possibility and hence $ab = ba$. So $a \in Z(G)$ as b was arbitrary. Since a was arbitrary $G = Z(G)$. Hence G is abelian. $\square$

Exercise 2.5.44 Prove that a group of order p^2, p a prime, has a normal subgroup of order p.

Proof. We use the result from problem 40 which is as follows: Suppose G is a group, H is a subgroup and $|G| = n$ and $n \nmid (i_G(H))!$. Then there exists a normal subgroup $K \neq \{e\}$ and $K \subseteq H$.

So, we have now a group G of order p^2. Suppose that the group is cyclic, then it is abelian and any subgroup of order p is normal. Now let us suppose that G is not cyclic, then there exists an element a of order p, and $A = \langle a \rangle$. Now $i_G(A) = p$, so $p^2 \nmid p\ !$, hence by the above result there is a normal subgroup K, non-trivial and $K \subseteq A$. But $|A| = p$, a prime order subgroup, hence has no non-trivial subgroup, so $K = A$. so A is normal subgroup. $\square$

Exercise 2.5.52 Let G be a finite group and φ an automorphism of G such that $\varphi(x) = x^{-1}$ for more than three-fourths of the elements of G. Prove that $\varphi(y) = y^{-1}$ for all $y \in G$, and so G is abelian.

Proof. Let us start with considering b to be an arbitrary element in A.

1. Show that $\left|A \cap \left(b^{-1}A\right)\right| > \frac{|G|}{2}$, where

$$b^{-1}A = \left\{b^{-1}a \mid a \in A\right\}$$

First notice that if we consider a map $f : A \to b^{-1}A$ defined by $f(a) = b^{-1}a$, for all $a \in A$, then f is a 1-1 map and so $\left|b^{-1}A\right| \geq |A| > \frac{3}{4}|G|$. Now using inclusion-exclusion principle we have

$$\left|A \cap \left(b^{-1}A\right)\right| = |A| + \left|b^{-1}A\right| - \left|A \cup \left(b^{-1}A\right)\right| > \frac{3}{4}|G| + \frac{3}{4}|G| - |G| = \frac{1}{2}|G|$$

2. Argue that $A \cap \left(b^{-1}A\right) \subseteq C(b)$, where $C(b)$ is the centralizer of b in G.

Suppose $x \in A \cap \left(b^{-1}A\right)$, that means, $x \in A$ and $x \in b^{-1}A$. Thus there exist an element $a \in A$ such that $x = b^{-1}a$, which gives us $xb = a \in A$. Now notice that $x, b \in A$ and $xb \in A$, therefore we get

$$\phi(xb) = (xb)^{-1} \Longrightarrow \phi(x)\phi(b) = (xb)^{-1} \Longrightarrow x^{-1}b^{-1} = b^{-1}x^{-1} \Longrightarrow xb = bx$$

Therefore, we get $xb = bx$, for any $x \in A \cap \left(b^{-1}A\right)$, that means, $x \in C(b)$.

3. Argue that $C(b) = G$. We know that centralizer of an element in a group G is a subgroup (See Page 53). Therefore $C(b)$ is a subgroup of G. From statements **1** and **2**, we have

$$|C(b)| \geq \left|A \cap \left(b^{-1}A\right)\right| > \frac{|G|}{2}$$

We need to use the following remark to argue $C(b) = G$ from the above step. Remark. Let G be a finite group and H be a subgroup with more then $|G|/2$ elements then $H = G$.

Proof of Remark. Suppose $|H| = p$ Then by Lagrange Theorem, there exist an $n \in \mathbb{N}$, such that $|G| = np$, as $|H|$ divide $|G|$. Now by hypothesis $p > \frac{G|}{2}$ gives us,

$$p > \frac{|G|}{2} \Longrightarrow np > \frac{n|G|}{2} \Longrightarrow n < 2 \Longrightarrow n = 1$$

Therefore we get $H = G$.

Now notice that $C(b)$ is a subgroup of G with $C(b)$ having more than $|G|/2$ elements. Therefore, $C(b) = G$.

4. Show that $A \in Z(G)$.

We know that $x \in Z(G)$ if and only if $C(a) = G$. Now notice that, for any $b \in A$ we have $C(b) = G$. Therefore, every element of A is in the center of G, that means, $A \subseteq Z(G)$.

5. 5how that $Z(G) = G$.

As it is given that $|A| > \frac{3|G|}{4}$ and $A \leq |Z(G)|$, therefore we get

$$|Z(G)| > \frac{3}{4}|G| > \frac{1}{2}|G|.$$

As $Z(G)$ is a subgroup of G, so by the above Remark we have $Z(G) = G$. Hence G is abelian.

6. Finally show that $A = G$.

First notice that A is a subgroup of G. To show this let $p, q \in A$. Then we have

$$\phi(pq) = \phi(p)\phi(q) = p^{-1}q^{-1} = (qp)^{-1} = (pq)^{-1}, \quad \text{As } G \text{ is abelian.}$$

Therefore, $pq \in A$ and so we have A is a subgroup of G. Again by applying the above remark. we get $A = G$. Therefore we have

$$\phi(y) = y^{-1}, \quad \text{for all } y \in G$$

$\square$

Exercise 2.6.15 If G is an abelian group and if G has an element of order m and one of order n, where m and n are relatively prime, prove that G has an element of order mn.

Proof. Let G be an abelian group, and let a and b be elements in G of order m and n, respectively, where m and n are relatively prime. We will show that the product ab has order mn in G, which will prove that G has an element of order mn.

To show that ab has order mn, let k be the order of ab in G. We have $a^m = e$, $b^n = e$, and $(ab)^k = e$, where e denotes the identity element of G. Since G is abelian, we have

$$(ab)^{mn} = a^{mn}b^{mn} = e \cdot e = e.$$

Thus, k is a divisor of mn.

Now, observe that $a^k = b^{-k}$. Since m and n are relatively prime, there exist integers x and y such that $mx + ny = 1$. Taking kx on both sides of the equation, we get $a^{kx} = b^{-kx}$, or equivalently, $(a^k)^x = (b^k)^{-x}$. It follows that $a^{kx} = (a^m)^{xny} = e$, and similarly, $b^{ky} = (b^n)^{mxk} = e$. Therefore, m divides ky and n divides kx. Since m and n are relatively prime, it follows that mn divides k. Hence, $k = mn$, and ab has order mn in G. This completes the proof. $\square$

Exercise 2.7.7 If φ is a homomorphism of G onto G' and $N \triangleleft G$, show that $\varphi(N) \triangleleft G'$.

Proof. We first claim that $\varphi(N)$ is a subgroup of G'. To see this, note that since N is a subgroup of G, the identity element e_G of G belongs to N. Therefore, the element $\varphi(e_G) \in \varphi(N)$, so $\varphi(N)$ is a non-empty subset of G'.

Now, let $a', b' \in \varphi(N)$. Then there exist elements $a, b \in N$ such that $\varphi(a) = a'$ and $\varphi(b) = b'$. Since N is a subgroup of G, we have $a, b \in N$, so $ab^{-1} \in N$. Thus, we have

$$\varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1}) = a'b'^{-1} \in \varphi(N),$$

which shows that $a', b' \in \varphi(N)$ implies $a'b'^{-1} \in \varphi(N)$. Therefore, $\varphi(N)$ is a subgroup of G'.

Next, we will show that $\varphi(N)$ is a normal subgroup of G'. Let $\varphi(N) = N'$, a subgroup of G'. Let $x' \in G'$ and $h' \in N'$. Since φ is onto, there exist elements $x \in G$ and $h \in N$ such that $\varphi(x) = x'$ and $\varphi(h) = h'$.

Since N is a normal subgroup of G, we have $xhx^{-1} \in N$. Thus,

$$\varphi(xhx^{-1}) = \varphi(x)\varphi(h)\varphi(x^{-1}) = x'h'x'^{-1} \in \varphi(N),$$

which shows that $x' \in G'$ and $h' \in N'$ implies $x'h'x'^{-1} \in \varphi(N)$. Therefore, $\varphi(N)$ is a normal subgroup of G'. This completes the proof. $\square$

Exercise 2.8.12 Prove that any two nonabelian groups of order 21 are isomorphic.

Proof. By Cauchy's theorem we have that if G is a group of order 21 then it has an element a of order 3 and an element b of order 7. By exercise 2.5.41 we have that the subgroup generated by b is normal, so there is some $i = 0, 1, 2, 3, 4, 5, 6$ such that $aba^{-1} = b^i$. We know $i \neq 0$ since that implies $ab = a$ and so that $b = e$, a contradiction, and we know $i \neq 1$ since then $ab = ba$ and this would imply G is abelian, which we are assuming is not the case. Now, a has order 3 so we must have $b = a^3ba^{-3} = b^{i^3} \bmod 7$, and so i is restricted by the modular equation $i^3 \equiv 1 \bmod 7$

x	$x^3 \bmod 7$
2	1
3	6
4	1
5	6
6	6

Therefore the only options are $i = 2$ and $i = 4$. Now suppose G is such that $aba^{-1} = b^2$ and let G' be another group of order 21 with an element c of order 3 and an element d of order 7 such that $cdc^{-1} = d^4$. We now prove that G and G' are isomorphic. Define

$$\begin{aligned} \phi : G &\to G' \\ a &\mapsto c^{-1} \\ b &\mapsto d \end{aligned}$$

since a and c^{-1} have the same order and b and d have the same order this is a well defined function. Since

$$\begin{aligned} \phi(a)\phi(b)\phi(a)^{-1} &= c^{-1}dc \\ &= \left(cd^{-1}c^{-1}\right)^{-1} \\ &= \left(d^{-4}\right)^{-1} \\ &= d^4 \\ &= \left(d^2\right)^2 \\ &= \phi(b)^2 \end{aligned}$$

ϕ is actually a homomorphism. For any $c^id^j \in G'$ we have $\phi\left(a^{-i}b^j\right) = c^id^j$ so ϕ is onto and $\phi\left(a^ib^j\right) = c^{-i}d^j = e$ only if $i = j = 0$, so ϕ is 1-to-l. Therefore G and G' are isomorphic and so up to isomorphism there is only one nonabelian group of order 21 . $\square$

Exercise 2.8.15 Prove that if $p > q$ are two primes such that $q \mid p-1$, then any two nonabelian groups of order pq are isomorphic.

Proof. For a nonabelian group of order pq, the structure of the group G is set by determining the relation $aba^{-1} = b^{k^{\frac{p-1}{q}}}$ for some generator k of the cyclic group. Here we are using the fact that $k^{\frac{p-1}{q}}$ is a generator for the unique subgroup of order q in U_p (a cyclic group of order m has a unique subgroup of order d for each divisor d of m). The other possible generators of this subgroup are $k^{\frac{l(p-1)}{q}}$ for each $1 \leq l \leq q-1$, so these give potentially new group structures. Let G' be a group with an element c of order q, an element d of order p with structure defined by the relation $cdc^{-1} = d^{k^{\frac{l(p-1)}{q}}}$. We may then define

$$\begin{aligned} \phi : G' &\to G \\ c &\mapsto a^l \\ d &\mapsto b \end{aligned}$$

since c and a^l have the same order and b and d have the same order this is a well defined function. Since

$$\begin{aligned} \phi(c)\phi(d)\phi(c)^{-1} &= a^l b a^{-l} \\ &= b^{\left(k^{\frac{p-1}{q}}\right)^l} \\ &= b^{k^{\frac{l(p-1)}{q}}} \\ &= \phi(d)^{k^{\frac{l(p-1)}{q}}} \end{aligned}$$

$\phi\left(c^i d^j\right) = a^{li} b^j = e$ only if $i = j = 0$, so ϕ is 1-to-l. Therefore G and G' are isomorphic and so up to isomorphism there is only one nonabelian group of order pq. $\square$

Exercise 2.9.2 If G_1 and G_2 are cyclic groups of orders m and n, respectively, prove that $G_1 \times G_2$ is cyclic if and only if m and n are relatively prime.

Proof. The order of $G \times H$ is $n.\ m$. Thus, $G \times H$ is cyclic iff it has an element with order n. m. Suppose $\gcd(n.m) = 1$. This implies that g^m has order n, and analogously h^n has order m. That is, $g \times h$ has order $n.\ m$, and therefore $G \times H$ is cyclic.

Suppose now that $\gcd(n.m) > 1$. Let g^k be an element of G and h^j be an element of H. Since the lowest common multiple of n and m is lower than the product $n.m$, that is, $\operatorname{lcm}(n, m) < n.\ m$, and since $\left(g^k\right)^{lcm(n,m)} = e_G$, $\left(h^j\right)^{lcm(n,m)} = e_H$, we have $\left(g^k \times h^j\right)^{lcm(n,m)} = e_{G \times H}$. It follows that every element of $G \times H$ has order lower than $n.m$, and therefore $G \times H$ is not cyclic. $\square$

Exercise 2.10.1 Let A be a normal subgroup of a group G, and suppose that $b \in G$ is an element of prime order p, and that $b \notin A$. Show that $A \cap (b) = (e)$.

Proof. If $b \in G$ has order p, then (b) is a cyclic group of order p. Since A is a subgroup of G, we have $A \cap (b)$ is a subgroup of G. Also, $A \cap (b) \subseteq (b)$. So $A \cap (b)$ is a subgroup of (b). Since (b) is a cyclic group of order p, the only subgroups of (b) are (e) and (b) itself.

Therefore, either $A \cap (b) = (e)$ or $A \cap (b) = (b)$. If $A \cap (b) = (e)$, then we are done. Otherwise, if $A \cap (b) = (b)$, then $A \subseteq (b)$. Since A is a subgroup of G and $A \subseteq (b)$, it follows that A is a subgroup of (b).

Since the only subgroups of (b) are (e) and (b) itself, we have either $A = (e)$ or $A = (b)$. If $A = (e)$, then $A \cap (b) = (e)$ and we are done. But if $A = (b)$, then $b \in A$ as $b \in (b)$, which contradicts our hypothesis that $b \notin A$. So $A \neq (b)$.

Hence $A \cap (b) \neq (b)$. Therefore, $A \cap (b) = (e)$. This completes our proof. $\square$

Exercise 2.11.6 If P is a p-Sylow subgroup of G and $P \triangleleft G$, prove that P is the only p-Sylow subgroup of G.

Proof. let G be a group and P a sylow-p subgroup. Given P is normal. By sylow second theorem the sylow-p subgroups are conjugate. Let K be any other sylow-p subgroup. Then there exists $g \in G$ such that $K = gPg^{-1}$. But since P is normal $K = gPg^{-1} = P$. Hence the sylow-p subgroup is unique. $\square$

Exercise 2.11.7 If $P \triangleleft G$, P a p-Sylow subgroup of G, prove that $\varphi(P) = P$ for every automorphism φ of G.

Proof. Let ϕ be an automorphism of G. Let P be a normal sylow p-subgroup. $\phi(P)$ is also a sylow-p subgroup. But since P is normal, it is unique. Hence $\phi(P) = P$. $\square$

Exercise 2.11.22 Show that any subgroup of order p^{n-1} in a group G of order p^n is normal in G.

Proof. Proof: First we prove the following lemma.

Lemma: If G is a finite p-group with $|G| > 1$, then $Z(G)$, the center of G, has more than one element; that is, if $|G| = p^k$ with $k \geq 1$, then $|Z(G)| > 1$.

Proof of the lemma: Consider the class equation

$$|G| = |Z(G)| + \sum_{a \notin Z(G)} [G : C(a)],$$

where $C(a)$ denotes the centralizer of a in G. If $G = Z(G)$, then the lemma is immediate. Suppose $Z(G)$ is a proper subset of G and consider an element $a \in G$ such that $a \notin Z(G)$. Then $C(a)$ is a proper subgroup of G. Since $C(a)$ is a subgroup of a p-group, $[G : C(a)]$ is divisible by p for all $a \notin Z(G)$. This implies that p divides $|G| = |Z(G)| + \sum_{a \notin Z(G)} [G : C(a)]$.

Since p also divides $|G|$, it follows that p divides $|Z(G)|$. Hence, $|Z(G)| > 1$. □

This proves our **lemma**.

We will prove the result by induction on n. If $n = 1$, the G is a cyclic group of prime order and hence every subgroup of G is normal in G. Thus, the result is true for $n = 1$. Suppose the result is true for all groups of order p^m, where $1 \leq m < n$. Let H be a subgroup of order p^{n-1}. Consider $N(H) = \{g \in H : gH = Hg\}$. If $H \neq N(H)$, then $|N(H)| > p^{n-1}$. Thus, $|N(H)| = p^n$ and $N(H) = G$. In this case H is normal in G. Let $H = N(H)$. Then $Z(G)$, the center of G, is a subset of H and $Z(G) \neq \{e\}$. By Cauchy's theorem and the above Claim, there exists $a \in Z(G)$ such that $o(a) = p$. Let $K = \langle a \rangle$, a cyclic group generated by a. Then K is a normal subgroup of G of order p. Now, $|H/K| = p^{n-2}$ and $|G/K| = p^{n-1}$. Thus, by induction hypothesis, H/K is a normal subgroup of G/K. □

Exercise 3.2.21 If σ, τ are two permutations that disturb no common element and $\sigma\tau = e$, prove that $\sigma = \tau = e$.

Proof. Note that $\sigma\tau = e$ can equivalentnly be phrased as τ being the inverse of σ. Our statement is then equivalent to the statement that an inverse of a nonidentity permutation disturbs at least one same element as that permutation. To prove this, let σ be a nonidentity permutation, then let $(i_1 \cdots i_n)$ be a cycle in σ. Then we have that

$$\sigma(i_1) = i_2, \sigma(i_2) = i_2, \ldots, \sigma(i_{n-1}) = i_n, \sigma(i_n) = i_1,$$

but then also

$$i_1 = \tau(i_2), i_2 = \tau(i_3), \ldots, i_{n-1} = \tau(i_n), i_n = \tau(i_1),$$

i.e. its inverse disturbs $i_1, \ldots, i_n$. □

Exercise 4.1.19 Show that there is an infinite number of solutions to $x^2 = -1$ in the quaternions.

Proof. Let $x = ai + bj + ck$ then

$$x^2 = (ai + bj + ck)(ai + bj + ck) = -a^2 - b^2 - c^2 = -1$$

This gives $a^2 + b^2 + c^2 = 1$ which has infinitely many solutions for $-1 < a, b, c < 1$. □

Exercise 4.1.34 Let T be the group of 2×2 matrices A with entries in the field $\mathbb{Z}_2$ such that $\det A$ is not equal to 0. Prove that T is isomorphic to S_3, the symmetric group of degree 3.

Proof. The order of T is $2^4 - 2^3 - 2^2 + 2 = 6$; we now find those six matrices:

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
$$A_3 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad A_4 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$
$$A_5 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad A_6 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

with orders $1, 2, 2, 2, 3, 3$ respectively. Note that S_3 is composed of elements

$$\text{id}, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)$$

with orders 1, 2, 2, 2, 3, 3 respectively. Also note that, by Problem 17 of generate S_3. We also have that $\begin{pmatrix} 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$, that $\begin{pmatrix} 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 3 \end{pmatrix}$ and $\begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 \end{pmatrix} =$ id

Now we can check that $\tau(A_2) = \begin{pmatrix} 1 & 2 \end{pmatrix}, \tau(A_5) = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$ induces an isomorphism. We compute

$$\begin{aligned}
&\tau(A_1) = \tau(A_2A_2) = \tau(A_2)\tau(A_2) = \text{id} \\
&\tau(A_3) = \tau(A_5A_2) = \tau(A_5)\tau(A_2) = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 3 \end{pmatrix} \\
&\tau(A_4) = \tau(A_2A_5) = \tau(A_2)\tau(A_5) = \begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 3 \end{pmatrix} \\
&\tau(A_6) = \tau(A_5A_5) = \tau(A_5)\tau(A_5) = \begin{pmatrix} 1 & 3 & 2 \end{pmatrix}
\end{aligned}$$

Thus we see that τ extendeds to an isomorphism, since A_2 and A_5 generate T, so that $\tau(A_iA_j) = \tau(A_i)\tau(A_j)$ follows from writing A_i and A_j in terms of A_2 and A_5 and using the equlities and relations shown above. □

Exercise 4.2.5 Let R be a ring in which $x^3 = x$ for every $x \in R$. Prove that R is commutative.

Proof. To begin with
$$2x = (2x)^3 = 8x^3 = 8x.$$

Therefore $6x = 0 \quad \forall x$. Also

$$(x+y) = (x+y)^3 = x^3 + x^2y + xyx + yx^2 + xy^2 + yxy + y^2x + y^3$$

and

$$(x-y) = (x-y)^3 = x^3 - x^2y - xyx - yx^2 + xy^2 + yxy + y^2x - y^3$$

Subtracting we get
$$2\left(x^2y + xyx + yx^2\right) = 0$$

Multiply the last relation by x on the left and right to get

$$2\left(xy + x^2yx + xyx^2\right) = 0 \quad 2\left(x^2yx + xyx^2 + yx\right) = 0.$$

Subtracting the last two relations we have

$$2(xy - yx) = 0.$$

We then show that $3\left(x + x^2\right) = 0 \forall x$. You get this from

$$x + x^2 = \left(x + x^2\right)^3 = x^3 + 3x^4 + 3x^5 + x^6 = 4\left(x + x^2\right).$$

In particular

$$3\left(x + y + (x + y)^2\right) = 3\left(x + x^2 + y + y^2 + xy + yx\right) = 0$$

we end-up with $3(xy + yx) = 0$. But since $6xy = 0$, we have $3(xy - yx) = 0$. Then subtract $2(xy - yx) = 0$ to get $xy - yx = 0$. □

Exercise 4.2.6 If $a^2 = 0$ in R, show that $ax + xa$ commutes with a.

Proof. We need to show that

$$a(ax + xa) = (ax + xa)a \text{ for } a, x \in R.$$

Now,

$$\begin{aligned} a(ax + xa) &= a(ax) + a(xa) \\ &= a^2x + axa \\ &= 0 + axa = axa. \end{aligned}$$

Again,

$$\begin{aligned} (ax + xa)a &= (ax)a + (xa)a \\ &= axa + xa^2 \\ &= axa + 0 = axa. \end{aligned}$$

It follows that,

$$a(ax + xa) = (ax + xa)a, \text{ for } x, a \in R.$$

This shows that $ax + xa$ commutes with a. This completes the proof. □

Exercise 4.2.9 Let p be an odd prime and let $1 + \frac{1}{2} + ... + \frac{1}{p-1} = \frac{a}{b}$, where a, b are integers. Show that $p \mid a$.

Proof. First we prove for prime $p = 3$ and then for all prime $p > 3$. Let us take $p = 3$. Then the sum

$$\frac{1}{1} + \frac{1}{2} + \ldots + \frac{1}{(p-1)}$$

becomes

$$1 + \frac{1}{3-1} = 1 + \frac{1}{2} = \frac{3}{2}.$$

Therefore in this case $\frac{a}{b} = \frac{3}{2}$ implies $3 \mid a$, i.e. $p \mid a$. Now for odd prime $p > 3$. Let us consider $f(x) = (x-1)(x-2)\ldots(x-(p-1))$. Now, by Fermat, we know that the coefficients of $f(x)$ other than the x^{p-1} and x^0 are divisible by p. So if,

$$f(x) = x^{p-1} + \sum_{i=0}^{p-2} a_i x^i$$

and $p > 3$.

Then $p \mid a_2$, and

$$f(p) \equiv a_1 p + a_0 \pmod{p^3}$$

But we see that

$$f(x) = (-1)^{p-1} f(p-x) \text{ for any } x,$$

so if p is odd,

$$f(p) = f(0) = a_0,$$

So it follows that:

$$0 = f(p) - a_0 \equiv a_1 p \pmod{p^3}$$

Therefore,

$$0 \equiv a_1 \pmod{p^2}.$$

Hence,

$$0 \equiv a_1 \pmod{p}.$$

Now our sum is just $\frac{a_1}{(p-1)!} = \frac{a}{b}$. It follows that p divides a. This completes the proof. $\square$

Exercise 4.3.1 If R is a commutative ring and $a \in R$, let $L(a) = \{x \in R \mid xa = 0\}$. Prove that $L(a)$ is an ideal of R.

Proof. First, note that if $x \in L(a)$ and $y \in L(a)$ then $xa = 0$ and $ya = 0$, so that

$$xa - ya = 0$$
$$(x-y)a = 0,$$

i.e. $L(a)$ is an additive subgroup of R. (We have used the criterion that H is a subgroup of G if for any $h_1, h_2 \in H$ we have that $h_1 h_2^{-1} \in H$.

Now we prove the conclusion. Let $r \in R$ and $b \in L(a)$, then $ba = 0$, and so $xba = 0$ which by associativity of multiplication in R is equivalent to

$$(xb)a = 0,$$

so that $xb \in L(a)$. Since R is commutative, (1) implies that $(bx)a = 0$, so that $bx \in L(a)$, which concludes the proof that $L(a)$ is an ideal. $\square$

Exercise 4.3.25 Let R be the ring of 2×2 matrices over the real numbers; suppose that I is an ideal of R. Show that $I = (0)$ or $I = R$.

Proof. Suppose that I is a nontrivial ideal of R, and let

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

where not all of a, b, cd are zero. Suppose, without loss of generality – our steps would be completely analogous, modulo some different placement of 1 s in our matrices, if we assumed some other element to be nonzero – that $a \neq 0$. Then we have that

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in I$$

and so

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in I$$

so that

$$\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} \in I$$

for any real x. Now, also for any real x,

$$\begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix} \in I.$$

Likewise

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & x \end{pmatrix} \in I$$

and

$$\begin{pmatrix} 0 & 0 \\ 0 & x \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ x & 0 \end{pmatrix}$$

Thus, as

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

and since all the terms on the right side are in I and I is an additive group, it follows that

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

for arbitrary a, b, c, d is in I, i.e. $I = R$ Note that the intuition for picking these matrices is that, if we denote by E_{ij} the matrix with 1 at position (i, j) and 0 elsewhere, then

$$E_{ij}\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}E_{nm} = a_{j,n}E_{im}$$

$\square$

Exercise 4.4.9 Show that $(p-1)/2$ of the numbers $1, 2, \ldots, p-1$ are quadratic residues and $(p-1)/2$ are quadratic nonresidues $\mod p$.

Proof. To find all the quadratic residues $\bmod p$ among the integers $1, 2, \ldots, p-1$, we compute the least positive residues modulo p of the squares of the integers $1, 2, \ldots, p-1\}$.

Since there are $p-1$ squares to consider, and since each congruence $x^2 \equiv a(\bmod p)$ has either zero or two solutions, there must be exactly $\frac{(p-1)}{2}$ quadratic residues mod p among the integers $1, 2, \ldots, p-1$. The remaining

$$(p-1) - \frac{(p-1)}{2} = \frac{(p-1)}{2}$$

positive integers less than $p-1$ are quadratic non-residues of $\bmod p$. □

Exercise 4.5.16 Let $F = \mathbb{Z}_p$ be the field of integers $\mod p$, where p is a prime, and let $q(x) \in F[x]$ be irreducible of degree n. Show that $F[x]/(q(x))$ is a field having at exactly p^n elements.

Proof. In the previous problem we have shown that any for any $p(x) \in F[x]$, we have that

$$p(x) + (q(x)) = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 + (q(x))$$

for some $a_{n-1}, \ldots, a_0 \in F$, and that there are p^n choices for these numbers, so that $F[x]/(q(x)) \leq p^n$. In order to show that equality holds, we have to show that each of these choices induces a different element of $F[x]/(q(x))$; in other words, that each different polynomial of degree $n-1$ or lower belongs to a different coset of $(q(x))$ in $F[x]$.

Suppose now, then, that

$$a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 + (q(x)) = b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 + (q(x))$$

which is equivalent with $(a_{n-1} - b_{n-1})^{n-1} + \cdots (a_1 - b_1)\, x + (a_0 - b_0) \in (q(x))$, which is in turn equivalent with there being a $w(x) \in F[x]$ such that

$$q(x)w(x) = (a_{n-1} - b_{n-1})^{n-1} + \cdots (a_1 - b_1)\, x + (a_0 - b_0)\,.$$

Degree of the right hand side is strictly smaller than n, while the degree of the left hand side is greater or equal to n except if $w(x) = 0$, so that if equality is hold we must have that $w(x) = 0$, but then since polynomials are equal iff all of their coefficient are equal we get that $a_{n-1} - b_{n-1} = 0, \ldots, a_1 - b_1 = 0, a_0 - b_0 = 0$, i.e.

$$a_{n-1} = b_{n-1}, \ldots, a_1 = b_1, a_0 = b_0$$

which is what we needed to prove. □

Exercise 4.5.23 Let $F = \mathbb{Z}_7$ and let $p(x) = x^3 - 2$ and $q(x) = x^3 + 2$ be in $F[x]$. Show that $p(x)$ and $q(x)$ are irreducible in $F[x]$ and that the fields $F[x]/(p(x))$ and $F[x]/(q(x))$ are isomorphic.

Proof. We have that $p(x)$ and $q(x)$ are irreducible if they have no roots in $\mathbb{Z}_7$, which can easily be checked. E.g. for $p(x)$ we have that $p(0) = 5, p(1) = 6, p(2) = 6, p(3) = 4, p(4) = 6,\ p(5) = 4, p(6) = 4$, and similarly for $q(x)$.

We have that every element of $F[x]/(p(x))$ is equal to $ax^2 + bx + c + (p(x))$, and likewise for $F[x]/(q(x))$. We consider a map $\tau : F[x]/(p(x)) \to F[x]/(q(x))$ given by

$$\tau\left(ax^2 + bx + c + (p(x))\right) = ax^2 - bx + c + (q(x)).$$

This map is obviously onto, and since $|F[x]/(p(x))| = |F[x]/(q(x))| = 7^3$ by Problem 16, it is also one-to-one. We claim that it is a homomorphism. Additivity of τ is immediate by the linearity of addition of polynomial coefficient, so we just have to check the multiplicativity; if $n = ax^2 + bx + c + (p(x))$ and $m = dx^2 + ex + f + (p(x))$ then

$$\begin{aligned}
\tau(nm) &= \tau\left(adx^4 + (ae + bd)x^3 + (af + be + cd)x^2 + (bf + ce)x + cf + (p(x))\right) \\
&= \tau\left(2adx + 2(ae + bd) + (af + be + cd)x^2 + (bf + ce)x + cf + (p(x))\right) \\
&= \tau\left((af + be + cd)x^2 + (bf + ce + 2ad)x + (cf + 2ae + 2bd) + (p(x))\right) \\
&= (af + be + cd)x^2 - (bf + ce + 2ad)x + cf + 2ae + 2bd + (q(x)) \\
&= adx^4 - (ae + bd)x^3 + (af + be + cd)x^2 - (bf + ce)x + cf + (q(x)) \\
&= \left(ax^2 - bx + c + (q(x))\right)\left(dx^2 - ex + f + (q(x))\right) \\
&= \tau(n)\tau(m).
\end{aligned}$$

where in the second equality we used that $x^3 + p(x) = 2 + p(x)$ and in the fifth we used that $x^3 + q(x) = -2 + q(x)$ □

Exercise 4.5.25 If p is a prime, show that $q(x) = 1 + x + x^2 + \cdots x^{p-1}$ is irreducible in $Q[x]$.

Proof. Lemma: Let F be a field and $f(x) \in F[x]$. If $c \in F$ and $f(x + c)$ is irreducible in $F[x]$, then $f(x)$ is irreducible in $F[x]$. Proof of the Lemma: Suppose that $f(x)$ is reducible, i.e., there exist non-constant $g(x), h(x) \in F[x]$ so that

$$f(x) = g(x)h(x).$$

In particular, then we have

$$f(x + c) = g(x + c)h(x + c).$$

Note that $g(x + c)$ and $h(x + c)$ have the same degree at $g(x)$ and $h(x)$ respectively; in particular, they are non-constant polynomials. So our assumption is wrong. Hence, $f(x)$ is irreducible in $F[x]$. This proves our Lemma.

Now recall the identity

$$\frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots\ldots + x^2 + x + 1.$$

We prove that $f(x+1)$ is \$ —textbffirreducible in $\mathbb{Q}[x]$ and then apply the Lemma to conclude that $f(x)$ is irreducible in $\mathbb{Q}[x]$.3\$ Note that

$$\begin{aligned} f(x+1) &= \frac{(x+1)^p - 1}{x} \\ &= \frac{x^p + px^{p-1} + \ldots + px}{x} \\ &= x^{p-1} + px^{p-2} + \ldots. + p. \end{aligned}$$

Using that the binomial coefficients occurring above are all divisible by p, we have that $f(x+1)$ is irreducible $\mathbb{Q}[x]$ by Eisenstein's criterion applied with prime p.

Then by the lemma $f(x)$ is irreducible $\mathbb{Q}[x]$. This completes the proof. □

Exercise 4.6.2 Prove that $f(x) = x^3 + 3x + 2$ is irreducible in $Q[x]$.

Proof. Let us assume that $f(x)$ is reducible over $\mathbb{Q}[x]$. Then there exists a rational root of $f(x)$. Let p/q be a rational root of $f(x)$, where $\gcd(p,q) = 1$. Then $f(p/q) = 0$. Now,

$$\begin{aligned} & f(p/q) = (p/q)^3 + 3(p/q) + 2 \\ \Longrightarrow & (p/q)^3 + 3(p/q) + 2 = 0 \\ \Longrightarrow & p^3 + 3pq^2 = -2q^3 \\ \Longrightarrow & p\left(p^2 + 3q^2\right) = -q^3 \end{aligned}$$

It follows that, p divides q which is a contradiction to the fact that $\gcd(p,q) = 1$. This implies that $f(x)$ has no rational root. Now we know that, a polynomial of degree two or three over a field F is reducible if and only if it has a root in F. Now $f(x)$ is a 3 degree polynomial having no root in $\mathbb{Q}$. So, $f(x)$ is irreducible in $\mathbb{Q}[x]$. This completes the proof. □

Exercise 4.6.3 Show that there is an infinite number of integers a such that $f(x) = x^7 + 15x^2 - 30x + a$ is irreducible in $Q[x]$.

Proof. Via Eisenstein's criterion and observation that 5 divides 15 and -30, it is sufficient to find infinitely many a such that 5 divides a, but $5^2 = 25$ doesn't divide a. For example $5 \cdot 2^k$ for $k = 0, 1, \ldots$ is one such infinite sequence. □

Exercise 5.1.8 If F is a field of characteristic $p \neq 0$, show that $(a+b)^m = a^m + b^m$, where $m = p^n$, for all $a, b \in F$ and any positive integer n.

Proof. Since F is of characteristic p and we have considered arbitrary two elements a, b in F we have

$$\begin{aligned} & pa = pb = 0 \\ \Longrightarrow\ & p^n a = p^n b = 0 \\ \Longrightarrow\ & ma = mb = 0. \end{aligned}$$

Now we know from Binomial Theorem that

$$(a+b)^m = \sum_{i=0}^{m} \left(\begin{array}{c} m \\ i \end{array} \right) a^i b^{m-i}$$

Here

$$\left(\begin{array}{c} m \\ i \end{array} \right) = \frac{m!}{i!(m-i)!}.$$

Now we know that for any integer n and any integer k satisfying $1 \leq k < n, n$ always divides $\left(\begin{array}{c} n \\ k \end{array} \right)$. So in our case for i in the range $1 \leq i < m, m$ divides $\left(\begin{array}{c} m \\ i \end{array} \right)$. It follows that p divides $\left(\begin{array}{c} m \\ i \end{array} \right)$, for i satisfying $1 \leq i < m$, since $m = p^n$ for any integer n. Therefore other than the terms a^m and b^m in the expansion $\sum_{i=0}^{m} \left(\begin{array}{c} m \\ i \end{array} \right) a^i b^{m-i}$ will vanish due to char p nature of F. Hence we have

$$\sum_{i=0}^{m} \left(\begin{array}{c} m \\ i \end{array} \right) a^i b^{m-i} = a^m + b^m$$

This follows that, for all $a, b \in F$

$$(a+b)^m = a^m + b^m.$$

This completes the proof. □

Exercise 5.2.20 Let V be a vector space over an infinite field F. Show that V cannot be the set-theoretic union of a finite number of proper subspaces of V.

Proof. Assume that V can be written as the set-theoretic union of n proper subspaces $U_1, U_2, \ldots, U_n$. Without loss of generality, we may assume that no U_i is contained in the union of other subspaces.

Let $u \in U_i$ but $u \notin \bigcup_{j \neq i} U_j$ and $v \notin U_i$. Then, we have $(v + Fu) \cap U_i = \varnothing$, and $(v + Fu) \cap U_j$ for $j \neq i$ contains at most one vector, since otherwise U_j would contain u.

Therefore, we have $|v + Fu| \leq |F| \leq n - 1$. However, since n is a finite natural number, this contradicts the fact that the field F is finite.

Thus, our assumption that V can be written as the set-theoretic union of proper subspaces is wrong, and the claim is proven. □

Exercise 5.3.7 If $a \in K$ is such that a^2 is algebraic over the subfield F of K, show that a is algebraic over F.

Proof. Since a^2 is algebraic over F, there exist a non-zero polynomial $f(x)$ in $F[x]$ such that $f\left(a^2\right) = 0$. Consider a new polynomial $g(x)$ defined as $g(x) = f\left(x^2\right)$. Clearly $g(x) \in F[x]$ and $g(a) = f\left(a^2\right) = 0$. □

Exercise 5.3.10 Prove that $\cos 1°$ is algebraic over $\mathbb{Q}$.

Proof. Since $(\cos(1°) + i\sin(1°))^{360} = 1$, the number $\cos(1°) + i\sin(1°)$ is algebraic. And the real part and the imaginary part of an algebraic number are always algebraic numbers. □

Exercise 5.4.3 If $a \in C$ is such that $p(a) = 0$, where $p(x) = x^5 + \sqrt{2}x^3 + \sqrt{5}x^2 + \sqrt{7}x + \sqrt{11}$, show that a is algebraic over $\mathbb{Q}$ of degree at most 80.

Proof. Given $a \in \mathbb{C}$ such that $p(a) = 0$, where

$$p(x) = x^5 + \sqrt{2}x^3 + \sqrt{5}x^2 + \sqrt{7}x + \sqrt{11}$$

Here, we note that $p(x) \in \mathbb{Q}(\sqrt{2}, \sqrt{5}, \sqrt{7}, \sqrt{11})$ and

$$\begin{aligned}[Q(\sqrt{2}, \sqrt{5}, \sqrt{7}, \sqrt{11}) : \mathbb{Q}] &= [Q(\sqrt{2}, \sqrt{5}, \sqrt{7}, \sqrt{11}) : Q(\sqrt{2}, \sqrt{5}, \sqrt{7})] \cdot [\mathbb{Q}(\sqrt{2}, \sqrt{5}, \sqrt{7}) : \mathbb{Q}(\sqrt{2}, \sqrt{5})] \\ &\quad \cdot [\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \\ &= 2 \cdot 2 \cdot 2 \cdot 2 \\ &= 16\end{aligned}$$

Here, we note that $p(x)$ is of degree 5 over $\mathbb{Q}(\sqrt{2}, \sqrt{5}, \sqrt{7}, \sqrt{11})$. If a is root of $p(x)$, then

$$[Q(\sqrt{2}, \sqrt{5}, \sqrt{7}, \sqrt{11}, a) : \mathbb{Q}] = [Q(\sqrt{2}, \sqrt{5}, \sqrt{7}, \sqrt{11}) : Q(\sqrt{2}, \sqrt{5}, \sqrt{7}, \sqrt{11})] \cdot 15$$

and $[Q(\sqrt{2}, \sqrt{5}, \sqrt{7}, \sqrt{11}) : Q(\sqrt{2}, \sqrt{5}, \sqrt{7}, \sqrt{11})] \leq 5$. We get equality if $p(x)$ is irreducible over $Q(\sqrt{2}, \sqrt{5}, \sqrt{7}, \sqrt{11})$. This gives

$$[Q(\sqrt{2}, \sqrt{5}, \sqrt{7}, \sqrt{11}, a) : \mathbb{Q}] \leq 16 \cdot 5 = 80$$

□

Exercise 5.5.2 Prove that $x^3 - 3x - 1$ is irreducible over $\mathbb{Q}$.

Proof. Let $p(x) = x^3 - 3x - 1$. Then

$$p(x+1) = (x+1)^3 - 3(x+1) - 1 = x^3 + 3x^2 - 3$$

We have $3|3, 3|0$ but $3 \nmid 1$ and $3^2 \nmid 3$. Thus the polynomial is irreducible over $\mathbb{Q}$ by 3 -Eisenstein criterion. $\square$

Exercise 5.6.14 If F is of characteristic $p \neq 0$, show that all the roots of $x^m - x$, where $m = p^n$, are distinct.

Proof. Let us consider $f(x) = x^m - x$. Then $f \in F[x]$. Claim: $f(x)$ has a multiple root in some extension of F if and only if $f(x)$ is not relatively prime to its formal derivative, $f'(x)$.

Proof of the Claim: Let us assume that $f(x)$ has a multiple root in some extension of F. Let y be a multiple root of $f(x)$. Then over a splitting field, we have

$$f(x) = (x-y)^n g(x), \text{ for some integer } n \geq 2.$$

Here $g(x)$ is a polynomial such that $g(y) \neq 0$. Now taking derivative of f we get

$$f'(x) = n \cdot (x-y)^{n-1} g(x) + (x-y)^n g'(x)$$

here $g'(x)$ implies derivative of g with respect to x. Since we have $n \geq 2$, this implies $(n-1) \geq 1$. Hence, (1) shows that $f'(x)$ has y as a root. Therefore, $f(x)$ is not relatively prime to $f'(x)$. We now prove the other direction. Conversely, let us assume that $f(x)$ is not relatively prime to $f'(x)$. Let y is a root of both $f(x)$ and $f'(x)$. Since y is a root of $f(x)$, we can write

$$f(x) = (x-y) \cdot g(x)$$

for some polynomial $g(x)$. then taking derivative of $f(x)$ we have

$$f'(x) = g(x) + (x-y) \cdot g'(x)$$

where $g'(x)$ is the derivative of $g(x)$ with respect to x. Since y is a root of $f'(x)$ also we have

$$f'(y) = 0$$

Then we have

$$\begin{aligned} &f'(y) = g(y) + (y-y) \cdot g'(y) \\ \Longrightarrow &f'(y) = g(y) \\ \Longrightarrow &g(y) = 0. \end{aligned}$$

This implies y is a root of $g(x)$ also. Therefore we have

$$g(x) = (x-y) \cdot h(x)$$

for some polynomial $h(x)$. Now form (2) we have

$$f(x) = (x - y)^2 \cdot h(x).$$

This follows that y is a multiple root of $f(x)$. Therefore, $f(x)$ has a multiple root in some extension of the field F. This completes the proof of the Claim.

In our case, $f(x) = x^m - x$, where $m = p^n$. Now we calculate the derivative of f. That is

$$f'(x) = mx^{m-1} - 1 = -1(\text{mod} p).$$

By the above condition it follows that, f' has no root same as f, that is, $f(x)$ and $f'(x)$ are relatively prime. Hence, $f(x)$ has no multiple root in F. Since $f(x) = x^m - x$ is a polynomial of degree m, it follows that $f(x)$ has m distinct roots in F, where $m = p^n$. This completes the proof. □