```tex
\end{itemize}

Suppose that we have two series from $H$ to $G$, the first given by \eqref{e: cs}, the second by:
\begin{equation}\label{second series}
H=H_0 \unlhd H_1 \unlhd H_2 \unlhd \cdots \unlhd H_l=G.
\end{equation}

Series \eqref{e: cs} and \eqref{second series} are called \emph{equivalent} if $k=l$ and there exists
a permutation $\pi\in S_k$ such that, for $i=1,\dots, k$,  $$G_i/ G_{i-1} \cong H_{i\pi}/ H_{i\pi-1}.
$$

The series \eqref{second series} is said to be a \emph{refinement} of series \eqref{e: cs} if $k\leq
l$ and there are non-negative integers $j_0 < j_1 < \dots < j_k \leq l$ such that $G_i = H_{j_i}$ for
$i=0,\dots, k$.

Now the key result concerning series is due to Schreier \cite[7.7]{rose}:

\begin{lem}\label{l: composition series}
Any two series have equivalent refinements.
\end{lem}
 \begin{exercise}
  Prove this.
 \end{exercise}

One important consequence of Lemma~\ref{l: composition series} is that if $G$ is a group admitting a
composition series, then the multiset of composition factors associated with any composition series
of $G$ is an invariant of the group $G$. In \S\ref{s: sdp} we will briefly examine how, given $M$ a
finite multiset of simple groups, one might construct a group $G$ for which $M$ is the multiset of
composition factors.
\subsection{Derived series}

For $g,h\in G$, define the {\it commutator} of $g$ and $h$,
$$[g,h]:=g^{-1}h^{-1}gh.$$
The {\it commutator subgroup}, or {\it derived subgroup} of $G$, written $G'$ or $[G,G]$ or $G^{(1)}
$, is the group
$$\langle [g,h] \mid g,h \in G\rangle.$$

\begin{warning}
$G'$ is the group {\it generated} by all commutators of the group $G$, i.e. the smallest subgroup of
$G$ that contains all commutators. The set of all commutators in $G$ is not necessarily a group.
\end{warning}

\begin{iexercise}\label{e: commutator}
 Prove that, for $N$ a normal subgroup of $G$, the quotient $G/N$ is abelian if and only if $G'\leq
 N$.
\end{iexercise}

\begin{exercise}
 Find an example of a group $G$ such that $G'$ is not equal to the set of all commutators.
\end{exercise}

We can generalize this construction as follows:
\begin{equation*}
 \begin{aligned}
  G^{(0)} &:= G; \\
  G^{(n)} &:= [G^{(n-1)}, G^{(n-1)}] \textrm{ for } n\in \mathbb{N}.
   \end{aligned}
\end{equation*}
We obtain a descending sequence of groups
$$\cdots \unlhd G^{(2)} \unlhd G^{(1)} \unlhd G$$
which is called the {\it derived series} of $G$. If, for some $k$, $G^{(k)}=G^{(k+1)}$ then, clearly,
$G^{(k)} = G^{(l)}$ for every $l\geq k$ and we say that the derived series \emph{terminates} at
$G^{(k)}$. Note that if the derived series does not terminate for any $k$ then it is not strictly
```

```latex
speaking a series. (Of course the derived series of a finite group always terminates.)

\begin{exercise}
 Prove that (provided it terminates) the derived series is a normal series.
\end{exercise}

We call $G$ {\it perfect} if $G=[G,G]$. If $G$ is finite, then the derived series terminates after
$k$ steps at a perfect group.

\subsection{Solvable groups}

We say that $G$ is {\it soluble} or {\it solvable} if $G$ has an abelian series.
\begin{exercise}
Prove that, if $G$ is finite, then $G$ is solvable if and only if all composition factors of $G$ are
cyclic of prime order. Give an example of a solvable group that does not have a composition series.
\end{exercise}

\begin{iexercise}
 Prove that a finite group $G$ is solvable if and only if the derived series of $G$ terminates at $\{1\}$.
\end{iexercise}

\newpage

\section{Permutation groups}\label{s: permutation groups}

Throughout this section, assume that $G$ is a group that acts (on the right) on some set $\Omega$.
Equivalently, there exists a group homomorphism $\phi: G \to \symme(\Omega)$, the set of permutations
on the set $\Omega$. Recall that
\begin{itemize}
 \item for $\omega \in \Omega$, $G_\omega:=\{ g\in g \mid \omega^g=\omega\}$, is the \emph{stabilizer} of $\omega$;
 \item $G_{(\Omega)}:= \bigcap\limits_{\omega\in \Omega} G_\omega$ is the \emph{kernel} of the action;
 \item for $\omega \in \Omega$, $\omega^G:= \{\omega^g \mid g\in G\}$ is the \emph{orbit} of $\omega$.
\end{itemize}

Note that $G_{(\Omega)}$ is precisely the kernel of $\phi$.

We say that the action of $G$ on $\Omega$ is
\begin{itemize}
 \item \emph{faithful}, if $G_{\Omega)}=\{1\}$; equivalently, $\phi$ is a monomorphism and we think of $G$ as a subgroup of $\symme(\Omega)$;
 \item \emph{transitive}, if $\omega^G = \Omega$ for some (and hence all) $\omega\in\Omega$.
 \end{itemize}

\begin{remark}
When a group theorist speaks of a `permutation group', they mean an abstract group $G$ accompanied by
some fixed embedding of $G$ in $\symme(\Omega)$, for some set $\Omega$. Equivalently, they mean an
abstract group $G$ accompanied by some faithful action. Indeed for a long time this was the only
context in which groups were studied, in the immediate aftermath of the work of Galois.
\end{remark}

\begin{example}
 Let $H$ be any subgroup of $G$. The group $G$ acts transitively on $H\backslash G$, the set of right cosets of $H$ via right multiplication.
\end{example}
\begin{iexercise}\label{e: sub action}
 Prove that any transitive action is isomorphic to an action of this kind, i.e. given a transitive action of $G$ on $\Omega$, there exists a subgroup $H\leq G$ such that the action of $G$ on $\Omega$ is isomorphic to the action of $G$ on $H\backslash G$. You may need to recall what it means for two group actions to be isomorphic.
```

```latex
\end{iexercise}
Recall that when $G$ is finite the Orbit-Stabilizer Theorem asserts that, for all $\omega\in\Omega$,
$$|G| = |G_\omega| \cdot |\omega^G|.$$
\begin{exercise}
Use (E\ref{e: sub action}) to prove the orbit-stabilizer theorem.
\end{exercise}

\begin{exercise}\label{e: stab conj}
Prove that if $G$ acts transitively on $\Omega$ and $G_\omega$ is a stabilizer, then the set of all
stabilizers equals the set of all conjugates of $G_\omega$. Under what conditions is the action of
$G$ by conjugation on this set of conjugates is isomorphic to the action of $G$ on $\Omega$?
\end{exercise}
\begin{exercise}
What conditions on $H$ result in the action of $G$ on $H\backslash G$ being faithful?
\end{exercise}
\begin{iexercise}
 Let $G$ be a finite group acting transitively on a set $\Omega$. Show that the average number of
 fixed points of the elements of $G$ is $1$, i.e.
 $$\frac1{|G|}\sum\limits_{g\in G} |\{\omega\in \Omega \mid \omega^g=\omega\}|=1.$$
\end{iexercise}



\begin{example}
Let $3\leq n\in \mathbb{Z}^+$ and let $G:=D_{2n}$, the dihedral group of order $2n$. In other words
$$G:= \langle g, h \mid g^n = h^2 = 1, h^{-1}gh=g^{-1}\rangle.$$
Define $\Omega$ to be the corners of an $n$-gon which we might as well label $1,\dots, n$. We can
define $g$ to act like the permutation $(1,2,\dots, n)$ and $h$ to reflect the polygon through a line
passing through $1$; see Figure~\ref{d10} for an example when $n=5$. Thus
$$h:=(2, n-1)(3, n-2)\dots\left(\lfloor \frac{n+2}{2}\rfloor, \lceil\frac{n+2}{2}\rceil\right).$$
\end{example}
\begin{exercise}
Check that this gives a well-defined action of $G$ on $\Omega$ that is both faithful and transitive.
What are the stabilizers in this action?
\end{exercise}

\begin{center}
\begin{figure}
\begin{tikzpicture}[scale=0.4]%[transform shape]
  \node[fill=black, text=white, circle, inner sep=0.05cm] (N-0) at (0:5.4cm) {1};
 \node[fill=black, text=white,circle, inner sep=0.05cm] (N-1) at (72:5.4cm) {2};
 \node[fill=black, text=white,circle, inner sep=0.05cm] (N-2) at (144:5.4cm) {3};
 \node[fill=black, text=white,circle, inner sep=0.05cm] (N-3) at (216:5.4cm) {4};
 \node[fill=black, text=white,circle, inner sep=0.05cm] (N-4) at (288:5.4cm) {5};
  \path (N-1) edge (N-2);
  \path (N-2) edge (N-3);
  \path (N-3) edge (N-4);
  \path (N-4) edge (N-0);
  \path (N-0) edge (N-1);
  \end{tikzpicture} \\
\caption{$D_{10}$ acts on the pentagon with $g=(1,2,3,4,5)$ and $h=(2,5)(3,4)$.}\label{d10}
\end{figure}
\end{center}

\subsection{Multiple transitivity}

As soon as we have an action of a group $G$ on a set $\Omega$, we can define others. For instance,
define an action of $G$ on $\Omega^2=\Omega\times \Omega$ via
$$(\omega_1, \omega_2)^g := (\omega_1^g, \omega_2^g),$$
for all $g\in G$.

In fact this defines a natural action on the set of distinct pairs,
$$\Omega^{(2)}:= \{(\omega_1, \omega_2) \mid \omega_1 \neq \omega_2\}.$$
We say that the \emph{original} action of $G$ on $\Omega$ is \emph{$2$-transitive} if the induced
```

```latex
action of $G$ on $\Omega^{(2)}$ is transitive. One defines \emph{$k$-transitivity} for $2\geq k\in
\mathbb{Z}^+$ similarly. It is convenient to define an action to be \emph{$1$-transitive} if and only
if it is transitive.

\begin{iexercise}
 For which values of $n$ is the action of $D_{2n}$ on an $n$-gon, $2$-transitive?
\end{iexercise}
\begin{exercise}
 Show that, for $k\geq 2$, if an action is $k$-transitive, then it is $k-1$-transitive.
\end{exercise}
\begin{exercise}
 Let $G=S_n$, the symmetric group on $n$ letters. What is the largest value of $k$ for which $G$ is
 $k$-transitive? What about $G=A_n$, the alternating group on $n$ letters?
\end{exercise}

\subsection{Blocks and primitivity}

A \emph{$G$-congruence} on $\Omega$ is an equivalence relation $\sim$ on $\Omega$ such that
$$\alpha\sim \beta \implies \alpha^g\sim \beta^g$$
for all $g\in G$. Any action always admits two $G$-congruences which we call {\it trivial}, as
follows:
\begin{itemize}
 \item Define $\alpha \sim_1 \beta$ if and only if $\alpha=\beta$;
 \item Define $\alpha \sim_2 \beta$ always.
\end{itemize}

The equivalence classes of a $G$-congruence are called \emph{blocks}. Note that, for $\sim_1$, there
are $|\Omega|$ blocks all of cardinality $1$ while, for $\sim_2$, there is one block of cardinality
$|\Omega|$.

The action of $G$ on $\Omega$ is called {\it primitive} if the only $G$-congruences on $\Omega$ are
the trivial ones. We call the action {\it imprimitive} if it is not primitive. (I may also write
things like ``$G$ acts primitively on the set $\Omega$'', and will trust you to figure out what I
mean.)

\begin{lem}\label{l: prim normal trans}
 Suppose that $G$ acts primitively on $\Omega$ and let $N\unlhd G$ with $N\not\leq G_{(\Omega)}$.
 Then $N$ acts transitively on $\Omega$.
\end{lem}
\begin{proof}
Let $\Lambda_1,\dots, \Lambda_k$ be the orbits of $N$ on $\Omega$. Define an equivalence relation $
\sim$ on $\Omega$ such that $\alpha \sim\beta$ if and only if there exists $i$ such that $\alpha,
\beta\in \Lambda_i$. Now suppose that $\alpha\sim\beta$. By definition $\beta=\alpha^n$ for some
$n\in N$. Let $g\in G$ and observe that
$$\beta^g = (\alpha^n)^g = (\alpha^g)^{g^{-1}ng}.$$
Since $N$ is normal, $g^{-1}ng\in N$ and we conclude that $\alpha^g\sim \beta^g$ and hence $\sim$ is
a $G$-congruence on $\Omega$.

Since $G$ is primitive, $\sim$ must be one of the two trivial $G$-congruences, $\sim_1$ or $\sim_2$.
Since $N\not\leq G_{(\Omega)}$ we conclude that $|\Lambda_i|\geq 2$ for some $i=1,\dots, k$ and so $
\sim\neq \sim_1$. We conclude that $\sim=\sim_2$ which implies, in particular that $k=1$ and $N$ acts
transitively on $\Omega$.

\end{proof}

Taking $N$ to equal $G$ in this lemma we observe, in particular, that if $|\Omega|>2$ and an action
is primitive, then it is transitive.

\begin{exercise}
 Prove that if an action is transitive and $\sim$ is a $G$-congruence, then all of the blocks
 associated with $\sim$ have the same cardinality.
\end{exercise}
\begin{exercise}
```

```
 Prove that if an action is 2-transitive, then it is primitive.
\end{exercise}
\begin{iexercise}
 Prove that $G$ acts primitively on $\Omega$ if and only if $G$ acts transitively and any stabilizer,
 $G_\omega$, is a maximal subgroup of $G$.
\end{iexercise}

\subsection{Iwasawa's Criterion}

The point of the material covered so far has been to allow us to state a famous lemma of Iwasawa
which gives a criterion for a finite permutation group to be simple.

\begin{lem}\label{l: iwasawa}{\rm (Iwasawa's criterion)}
 Let $G$ be a finite group acting primitively on a set $\Omega$. Let $\omega\in\Omega$ and assume
 that $G_\omega$ has a normal subgroup $A$ which is abelian such that
 $$\langle A^g \mid g\in G \rangle = G$$
 If $K\lhd G$, either $K\leq G_{(\Omega)}$ or $G'\leq K$. In particular if $G$ is perfect and
 faithful on $\Omega$, then $G$ is simple.
\end{lem}

\begin{exercise}
 Use Iwasawa's criterion to show that $A_5$ is simple.
\end{exercise}
\begin{iexercise}
 Now use Iwasawa's criterion to show that $A_n$ is simple for $n\geq 5$. Hint: consider the action on
 unordered triples from $\{1,\dots, n\}$.
\end{iexercise}

\begin{proof}
 Let $K$ be a normal subgroup of $G$ that is not contained in $G_{(\Omega)}$. Lemma~\ref{l: prim
 normal trans} implies, therefore, that $K$ acts transitively on $\Omega$ and hence $G=G_\omega K$
 (use the Orbit-Stabilizer Theorem to see this). Thus, for all $g\in G$, there exists $g_1\in
 G_\omega, k\in K$ such that $g=g_1k$ and this implies, in particular, that
 $$\{A^g \mid g\in G\} = \{A^k \mid k\in K\}.$$
 Now, since $\langle A^k \mid k\in K\rangle \leq AK \leq G$ we conclude that $G=AK$. Then
$$G/K = AK/K \cong A/A\cap K.$$
Since the right hand side is a quotient of an abelian group it must itself be abelian, and we
conclude that $G/K$ is abelian. Hence, by (E\ref{e: commutator}), $K\geq G'$.
\end{proof}

\begin{iexercise}
Prove the following variant on Iwasawa's criterion: Suppose that $G$ is a finite perfect group acting
faithfully and primitively on a set $\Omega$, and suppose that the stabilizer of a point has a normal
soluble subgroup $S$, whose
conjugates generate $G$. Then $G$ is simple.
\end{iexercise}

\subsection{Groups acting on groups}\label{s: sdp}

Given a group $G$ with a composition series, one can (in theory) calculate its composition factors.
What about the reverse process?
Suppose we are given a multiset of composition factors, how does one construct a group $G$ to which
they correspond? In general there are many ways to do this, and we briefly outline one such here.
\footnote{This section is a little terse; more detail can be found in \cite{rose}.}

Let $H$ and $K$ be groups. Recall that an \emph{automorphism} of $K$ is simply a group isomorphism
$K\to K$. The set of all automorphisms of $K$ forms a group, which we label $\Aut(K)$. Now let $\phi:
H \to \Aut(K)$ be a group homomorphism. We define $G:= K\rtimes_\phi H$ to be the group whose
elements are the elements of $H\times K$, with group multiplication given by
$$(h_1, k_1)(h_2, k_2) = (h_1\cdot h_2, k_1^{\phi(h_2)}\cdot k_2).$$
\begin{iexercise}
 Check that this gives a well-defined group. If $\phi$ is the trivial homomorphism, what is
 $K\rtimes_\phi H$?
```

```latex
\end{iexercise}

The next lemma lists some basic properties of this construction.

\begin{lem}
Let $G=K\rtimes_\phi H$.
 \begin{enumerate}
  \item The subset $K_0:=\{(1,k) \mid k\in K\}$ is a normal subgroup of $K\rtimes_\phi H$ that is
  isomorphic to $K$;
  \item The subset $H_0:=\{(h,1) \mid h\in H\}$ is a subgroup of $K\rtimes_\phi H$ that is isomorphic
  to $K$;
  \item $G/K_0 \cong H$;
  \item The natural conjugation action of $H_0$ on $K_0$ is isomorphic to the action of $H$ on $K$
  given by $\phi$.
 \end{enumerate}
\end{lem}
\begin{proof}
 \begin{iexercise}
  Prove this.
 \end{iexercise}
\end{proof}

In what follows I will tend to identify the groups $K_0$ and $K$, and the groups $H_0$ and $H$. This
allows me to abuse notation and think of $K\rtimes_\phi H$ as a semi-direct product of two of its
\emph{subgroups}, a point of view that is helpful. Usually, too, the homomorphism $\phi$ is obvious
from the context, so I will tend to write the semidirect product as $K\rtimes H$.

Suppose that $G$ is a group with normal subgroup $K$ such that $G/K\cong H$. In this case we write
$G=K.H$ and call $G$ \emph{ an extension of $K$ by $H$}.\footnote{{\bf Warning}: Some authors call
this \emph{ an extension of $H$ by $K$}.} A semi-direct product $G:=K\rtimes H$ is an example of a
group $K.H$, but it is important to note that not all groups $K.H$ can be expressed as a semi-direct
product. In the literature groups $K.H$ that can be expressed as a semi-direct product are called
\emph{split extensions} and are sometimes denoted $K:H$; those that can't be expressed as a semi-
direct product are called \emph{non-split extensions}.\footnote{If you know about short exact
sequences, then this terminology will make sense to you. If you don't, I recommend you look 'em up.}

\begin{remark}
 In the particular case where groups $K$ and $H$ are simple, any group $K.H$, in particular any semi-
 direct product $K\rtimes H$, is an example of a group with composition factors $\{H,K\}$. Thus semi-
 direct products allow us to `construct a group from its composition factors', as we set out to do at
 the start of this section.
\end{remark}
\begin{exercise}
 Find an example of a group $G=K.H$ (where $K$ and $H$ are both non-trivial finite groups) which is
 non-split. Hint: there is precisely one example with $|G|\leq 7$, and it is abelian. The smallest
 non-abelian examples have $|G|=8$.
\end{exercise}
\begin{exercise}
 Write down as many groups as you can which have composition factors $\{C_2, A_6\}$. Identify those
 that can be written as split extensions.
\end{exercise}

Understanding the automorphism group of a group is sometimes important. For any group $G$ there is a
homomorphism
$$\phi: G \to \Aut(G), g \mapsto \phi_g$$
where $\phi_g: G\to G, h \mapsto g^{-1}hg.$ In other words, the natural action of a group on itself
by conjugation induces a set of group automorphisms. We define $\Inn(G):= \Ima(\phi)$ and call $
\Inn(g)$ \emph{the set of inner automorphisms of $G$}.

\begin{lem}\label{l: aut group}
 \begin{enumerate}
  \item $\Inn(G) \unlhd \Aut(G)$;
  \item $\ker(\phi) = Z(G)$.
```

```latex
 \end{enumerate}
\end{lem}
\begin{proof}
 \begin{exercise}
  Prove this.
 \end{exercise}
\end{proof}

Note, in particular, that if $Z(G)$ is trivial, then $G$ embeds into its own automorphism group. In
particular this allows us to define the notion of an \emph{almost simple group}: it is a group $G$
with a simple normal subgroup $S$ such that
$$S\leq G \leq Aut(S).$$

\section{Fields and Vector Spaces}

We will need some background knowledge concerning linear algebra over an arbitrary field. I will
assume that you are familiar with the definition of a field, a vector space, and with some basic
facts about polynomials over fields; in particular I will also assume the following basic result,
which is {\it Vandermonde's Theorem}.

\begin{prop}\label{p: bound on number of roots}
Let $f\in k[X]$ be a polynomial of degree $n\geq 0$ with coefficients in a field $k$. Then $f$ has at
most $n$ roots.
\end{prop}

\subsection{A diversion into division rings}

There is a natural definition of the notion of a field, namely a {\it division ring}, in which one
does not require that multiplication is commutative. Much of what will be discussed below applies in
this setting but not all. We give an example of a division ring next and briefly mention some things
to beware of in this more general setting.

\begin{example}
 The real octonions, $\mathbf{H}$, are defined to be a 4-dimensional vector space over the real
 numbers, $\mathbb{R}$. Addition is defined to be the usual addition of vectors.

To define multiplication we introduce some notation: we write a vector $(a,b,c,d)$ as $a+bi+cj+dk$,
we define multiplication by a vector $a+0i+0j+0k$ as the usual scalar multiplication, we define the
multiplication of basis vectors as
 $$i^2=j^2=k^2=-1, \, ij=k, \, ji=-k, \, jk=i, \, kj=-i, \, ki=j, \, ik=-j,$$
 and we use distributivity to extend this definition so that multiplication is defined for all pairs
 of octonions.
\end{example}
\begin{exercise}
 Check that $\mathbb{H}$ is a division ring.
\end{exercise}
\begin{iexercise}
 Show that Proposition~\ref{p: bound on number of roots} does not hold in $\mathbb{H}$.
\end{iexercise}

One cannot immediately talk of a vector space over a division ring - one distinguishes between {\it
left} and {\it right} vector spaces. For instance, for a division ring $k$, a left vector space is a
left unital $k$-module.

Our choice to eschew the generality offered by division rings is justified by our desire to focus on
finite fields, and by the following classical result.

\begin{thm}
 {\rm (Wedderburn's theorem)} A finite division ring is a field.
\end{thm}

\subsection{Back to fields}
```

```latex
Throughout this section $k$ is a field; we write $k^*:=k\backslash\{0\}$.

\begin{lem}\label{l: mult cyclic}
Any finite subgroup of the multiplicative group $(k^*, \cdot)$ is cyclic.
\end{lem}
\begin{proof}
Let $H$ be a minimal non-cyclic subgroup of $(k^*, \cdot)$. Our knowledge of abelian groups implies
that $H\cong C_p\times C_p$ for some prime $p$. Now every element of $H$ satisfies the polynomial
$X^p=1$ which is a contradiction of Proposition~\ref{p: bound on number of roots}.
\end{proof}

Of course, if $k$ is finite, then this result implies that $(k^*,\cdot)$ is cyclic. In this case we
call those elements of $k^*$ that generate $(k^*,\cdot)$ the \emph{primitive elements}.

\begin{example}
Let $p$ be a prime and define $\Fp:=\mathbb{Z}/p\mathbb{Z}$, the integers modulo $p$, with the usual
addition and multiplication. Then $\Fp$ is a field.
\end{example}

\begin{lem}\label{l: existence of prime power fields}
 Let $q=p^a$ where $p$ is a prime and $a$ is a positive integer. Then there exists a finite field of
 order $q$.
\end{lem}
\begin{proof}
{\rm (Sketch)} The previous example gives the result for $a=1$. Now let $f(X) \in \Fp[X]$ be an
irreducible monic polynomial of degree at least 2. Since $\Fp[X]$ is a Principal Ideal Domain we
conclude that $I:=\langle f(X)\rangle$ is a maximal ideal of $\Fp[X]$ and we conclude that $\Fp[X]/I$
is a field. Since every element of $\Fp[X]/I$ contains a unique (and distinct) polynomial of degree
less than $a$, we conclude that $\Fp[X]/I$ is a field of order $p^a$.

It remains to show that, for every $p$ and every $a>1$, there exists a monic irreducible polynomial
of degree $a$ over $\Fp$. We omit this part.
\end{proof}

A variant of the preceding result, using the theory of splitting fields can be found at \url{https://
kconrad.math.uconn.edu/blurbs/galoistheory/finitefields.pdf}

Given a monic irreducible $f(X)\in\Fp[X]$, one can do computations in $F:=k[X]/\langle f(X)\rangle$
by observing that
$$F:=\{c_{a-1}X^{a-1}+c_{a-2}X^{a-2}+\cdots +c_1X+c_0 +\langle f(x)\rangle \mid c_0,\dots, c_{a-1}\in
\Fp\}.$$
(We are using the fact, mentioned in the proof, that every element of $\Fp[X]/I$ contains a unique
(and distinct) polynomial of degree less than $a$.)

Now one represents the element $c_{a-1}X^{a-1}+c_{a-2}X^{a-2}+\cdots +c_1X+c_0 +\langle f(x)
\rangle\in F$ by the string
$$c_{a-1}\alpha^{a-1}+c_{a-2}\alpha^{a-2}+\cdots +c_1\alpha+c_0$$
where $\alpha$ is just a convenient symbol. Addition and multiplication on the resulting set of
polynomials in $\alpha$ are just the usual addition and multiplication of polynomials, with the extra
rule that $f(\alpha)=0$.

\begin{iexercise}
 Show that $X^2+1\in\mathbb{F}_3[X]$ is irreducible, and compute the addition and multiplication
 tables for $\mathbb{F}_9:=\mathbb{F}_3[x]/\langle X^2+1\rangle$.
\end{iexercise}
\begin{iexercise}
Show that $X^3+X+1\in \mathbb{F}_2[X]$ is irreducible, and compute the addition and multiplication
tables for $\mathbb{F}_8 = \mathbb{F}_2[x]/\langle X^3+X+1\rangle$.
\end{iexercise}


\begin{lem}\label{l: fields have prime power order}
 Any finite field $k$ has order $p^a$ where $p$ is a prime and $a$ is a positive integer.
```