Recall that $f \in E[x]$ has a root at $a \in E$ iff $x - a$ divides $f$ in $E[x]$. We say that $f$ has a repeated root at $a$ iff $(x - a)^2$ divides $f$.

The formal derivative $f'$ of $f$ is defined in the obvious way (where $mb$ is the sum of $m$ copies of $b$). It is easy to show that $c' = 0$, $(f + g)' = f' + g'$, $(cf)' = cf'$, and $(fg)' = f'g + fg'$ where $c \in E$ and $f, g \in E[x]$.

Lemma: $f$ has a repeated root at $a$ iff $f(a) = f'(a) = 0$.

Proof: divide $f$ by $(x - a)^2$ and write the remainder as $C(x - a) + D$.

Proof: The L-R direction is obvious, so suppose that $f$ has no repeated root in a splitting field $F/E$ but (for contradiction) that it does have a repeated root $b$ in some extension $G/E$. Let $H/G$ be a splitting field for $f/G$ and let $F' = E(R)$ where $R$ are the roots of $f$ in $H$. Then by uniqueness of splitting field there is an IM $\sigma$ from $F'$ to $F$ extending $id_E$, but the easily $\sigma(b)$ is a repeated root for $f$ in $F$.

Theorem: Let $f \in E[x]$ be irreducible with $f' \neq 0$, then $f$ is separable.

Proof: as $E[x]$ is a PID the ideal $(f, f') = (d)$ for some $d$. $d$ divides the irreducible $f$ so $d$ is a unit or an associate of $f$. But $deg(f') < deg(f)$ and $d$ divides $f'$, so $d$ is a unit and $(f, f') = E[x]$. Choose $A, B$ such that $Af + Bf' = 1$. Then the same equation holds in any extension field $F/E$ and shows that there is no $b \in F$ such that $f(b) = f'(b) = 0$.

Remark: if $f' = 0$ then all roots are repeated. Also if $E$ has characteristic zero then only constants have derivative zero, hence all irreducibles are separable.

Definition: a nonzero polynomial is separable iff all its irreducible factors are separable. If $F/E$ as an extension then $a \in F$ is separable over $E$ iff $a$ is algebraic/$E$ and the minimal polynomial $m_a^E$ is separable over $E$. An extension $F/E$ is separable iff it is algebraic and every $a \in F$ is separable over $E$.

We work towards the following theorem (proof next time): a finite extension $F/E$ is Galois iff $F$ is a normal and separable extension of $E$ iff $F$ is a splitting field for a separable $f \in E[x]$.

Lemma (slightly stronger than form I stated in class): Let $F/E$ be finite and let $a \in F$. Let $k$ be the number of elements of form $\sigma(a)$ for some $\sigma \in \Gamma(F/E)$, and let $l$ be the number of roots of $m_a^E$ in $F$. Then $k \leq l \leq \left[ E(a) : E \right]$ and $|\Gamma(F/E)| \leq k|\Gamma(F/E(a))|$. 

Proof: $\deg(m_a^E) = [E(a) : E]$, so $l \leq [E(a) : E]$. Also $m_a(a) = 0$ and $m_a \in E[x]$, so easily for every $\sigma \in \Gamma(F/E)$ we have $m_a(\sigma(a)) = 0$. Hence the elements of form $\sigma(a)$ are among the roots of $m_a$, and $k \leq l$.

Easily $\Gamma(F/E(a)) \leq \Gamma(F/E)$, so as usual $\Gamma(F/E)$ is the union of left cosets of $\Gamma(F/E(a))$ each with size $|\Gamma(F/E(a))|$. Now for $\sigma, \tau \in \Gamma(F/E)$, we see that $\sigma(a) = \tau(a)$ iff $\tau^{-1} \sigma(a) = a$ iff $\tau^{-1} \sigma \in \Gamma(F/E(a))$. So there are $k$ cosets (in fact this is just an orbit-stabiliser argument!)