1. Exercise 10.1.20. Let $\mathbb{F}$ be a field.

   (a) Show that the following are equivalent for a polynomial $f(x) \in F[x]$.

      i. $f(x)$ has no repeated root in any extension field of $\mathbb{F}$.
      ii. $f(x)$ has no repeated root in some splitting field over $\mathbb{F}$.
      iii. $f(x)$ and $f'(x)$ are relatively prime in $\mathbb{F}[x]$

      i. $\implies$ ii. Suppose f has no repeated root in any extension of $\mathbb{F}$. f has a splitting field, and by assumption it must have no repeated roots in this field.

      ii. $\implies$ iii. Suppose f has no repeated roots in an extension $\mathbb{E}$ in which it splits. Then suppose for the sake of contradiction that there exists some $g \in \mathbb{F}[x]$ so that $g|f$ and $g|f'$, and that g is nonconstant. By Kronecker's Theorem, take a root $\alpha \in \mathbb{E}$ of g. Then $x - a|g$ and so $x - \alpha|f$, $x - \alpha|f'$. But if $x - \alpha|f'$, then $(x - \alpha)^2|f$, a contradiction since we assumed that f had no repeated root.

      iii. $\implies$ i. Suppose that f, f' are relatively prime in $\mathbb{F}[x]$. Then suppose for the sake of contradiction that there is some extension $\mathbb{E}$ of $\mathbb{F}$ so that f has a repeated root in $\mathbb{E}$. Then $(x - \alpha)^2|f$. But then $(x - \alpha)$ would divide f', contradicting f, f' being coprime.

   (b) If $f(x)$ is as in (a), show that $f(x)$ is separable, but not conversely.

   Solution: Let f have no repeated roots in its splitting field. Then clearly none of its factors can have repeated roots, so it must be separable.

   Counterexample: Take $f(x) = x^2 + 2x + 1$ which has a repeated root in the trivial extension $\mathbb{F}$ of $\mathbb{F}$, but its irreducible factor $(x + 1)$ has no repeated root in any extension $\mathbb{E}$ of $\mathbb{F}$.

2. Exercise 10.1.26 (a) (b)

   (a) Show that the following conditions are equivalent for a field $\mathbb{F}$ (then called a perfect field):

      i. Every algebraic extension of $\mathbb{F}$ is separable.
      ii. Every finite extension of $\mathbb{F}$ is separable.
      iii. Every irreducible polynomial in $\mathbb{F}[x]$ is separable.

   i. $\implies$ ii. Suppose that every algebraic extension of $\mathbb{F}$ is separable. Then, if $\mathbb{E}$ were a finite extension, it would have to be algebraic and as such it would be separable.

   ii. $\implies$ iii. Suppose that every finite extension of $\mathbb{F}$ is separable, and that f is irreducible in $\mathbb{F}[x]$. Let $\mathbb{E}$ be the splitting field of f over $\mathbb{E}$. Then $\mathbb{E}$ is a finite extension, and by hypothesis $\mathbb{E}$ must be separable. Since the minimal monic polynomial for any root u_i of f is $x - u_i \in E[x]$, and these are all seperable since $\mathbb{E}$ is seperable. we can say f is seperable since it is the product of all these and a constant in $\mathbb{F}$.

   iii. $\implies$ i. Suppose all irreducible polynomials in $\mathbb{F}[x]$ are seperable, and $\mathbb{E}$ be an algebraic extension of $\mathbb{F}$. Let $u \in \mathbb{E}$, and $m(x)$ be the minimal monic polynomial for u. Then since m is irreducible, it is separable by hypothesis. Therefore the algebraic extension $\mathbb{E}$ is seperable.

   (b) Show that every field of characteristic 0 is perfect.

   Solution: Let f be of characteristic 0. Then an irreducible p is separable (Nicholson Chapter 10, Theorem 4), satisfying iii. Therefore $\mathbb{F}$ is perfect.

3. Exercise 10.2.12 If $\mathbb{E}$ is a finite extension of $\mathbb{F}$ and $G = gal(\mathbb{E} : \mathbb{F})$, show that the extension E of F is Galois if and only if $|G| = [\mathbb{E} : \mathbb{F}]$.

   $\Longrightarrow$ **:** Since the Galois group is a group of automorphisms fixing $\mathbb{F}$, this follows from Dedekind-Artin since $\mathbb{F} = \mathbb{E}_G$.

   $\Longleftarrow$: Let $\mathbb{E}$ be a finite extension of $\mathbb{F}$ and $|G| = [\mathbb{E} : \mathbb{F}]$. We want to show that the fixed set of $\mathbb{E}$ under G is precisely $\mathbb{F}$ in order to show that the extension is Galois. If the extension is degree 1, the result is clear, since the fixed set of $G = \{e\}$ is $\mathbb{F}$. So suppose the degree of the extension is ≥ 2.

   Then let $u \in \mathbb{E} \setminus \mathbb{F}$, and suppose for the sake of contradiction that $u \in \mathbb{E}_G$. Then for any $\sigma \in G$, $\sigma(u) = u$. But since σ is uniquely defined by where it sends u, this must mean that $\sigma = e$ and therefore $G = \{e\}$. But then $|G| = [\mathbb{E} : \mathbb{F}] = 1 < 2$, a contradiction. Therefore $\mathbb{E}_G = \mathbb{F}$, and the extension is Galois.