# MAT 347
# Separability and perfectness
# March 4, 2016

## The Frobenius

This worksheet will involve fields of prime characteristic. Recall that a field $L$ has *characteristic* $p$ if $p \cdot 1 = 0$ in $L$.

1. Let $p$ be a prime. Let $L$ be a field with characteristic $p$. Consider the *Frobenius* map $\sigma_p : L \to L$ defined by $\sigma(a) = a^p$ for all $a \in L$. Show that $\sigma_p$ is a field homomorphism.

2. Show that $\sigma_p$ is always injective.

3. Show that if $L$ is finite, then $\sigma_p$ is surjective and hence is an automorphism.

4. Find a field for which $\sigma_p$ is not surjective.

## Separable polynomials

**Definition 1.** *Let $L$ be a field. A polynomial $f(X) \in L[X]$ is* separable *if it has no multiple roots in its splitting field; in other words, $f(X)$ is separable if $f(X)$ splits into* distinct *linear factors in its splitting field. (*Note: *Some authors give a different definition of separability for non-irreducible polynomials.)*

5. Give a few examples of irreducible separable polynomials. Do you think that every irreducible polynomial is separable?

6. Let $p$ be a prime. Let $F = \mathbb{F}_p(T)$, where $T$ is formal variable. Consider the polynomial $f(X) := X^p - T \in F[X]$. Prove that it is irreducible.

7. Let $K$ be a splitting field of $f(X)$ over $F$ and let $\alpha \in K$ be a root of $f(X)$. Show that $f(X)$ splits in $K[X]$ in an unorthodox way. In particular, $f(X)$ is an irreducible, unseparable polynomial in $F[X]$.

8. What is $\mathrm{Gal}(K/F)$?

**Definition 2.** *Let $K/F$ be an algebraic field extension. An element $\alpha \in K$ is called* separable over $F$ *if $m_{\alpha,F}(X) \in F[X]$ is separable. The extension $K/F$ is called* separable *if $\alpha$ is separable over $F$ for every $\alpha \in K$. $F$ is called* perfect *if every irreducible polynomial in $F[X]$ is separable (equivalently every algebraic extension of $F$ is separable).*

## Formal derivatives

**Definition 3.** *Let $R$ be a ring. Suppose $f(X) = a_n X^n + \cdots + a_0 \in R[X]$. The* formal derivative *of $f(X)$ is the polynomial $Df(X) = na_n X^{n-1} + \cdots + 2a_2 X + a_1 \in R[X]$. Note that each coefficient is being "multiplied" by an integer using the action $\mathbb{Z} \times R \to R$.*

**Remark 0.1.** *$Df(x)$ is like the usual derivative $f'(x)$ from calculus, but in the context of algebra, you shouldn't think of the derivative as a "rate of change". $Df$ is just a purely formal way of obtaining one polynomial from another. Having said that, $Df$ obeys all the same rules as $f'(x)$: for all $f, g \in R[x]$, $n \in \mathbb{Z}$, and $a \in R$,*

$$\begin{array}{rcl} D(a) & = & 0 \\ D(f+g) & = & Df + Dg \\ D(fg) & = & f \cdot Dg + g \cdot Df \\ D(af) & = & aDf \\ D(f^n) & = & nf^{n-1} \cdot Df \\ deg(Df) < deg(f) & or & Df = 0 \end{array}$$

*These are the rules on which we base all our calculations with $Df$.*

9. Let $R \subseteq S$ be PIDs with the same identity. Let $a, b \in R$ and let $d$ be a greatest common divisor of $a$ and $b$ in $R$. Show that $d$ is also a greatest common divisor of $a$ and $b$ in $S$. In particular, we can talk about $a$ and $b$ being relatively prime without specifying where.

10. Let $F$ be a field. Let $f(X) \in F[X]$. Let $\alpha$ be a root of $f(X)$ in its splitting field. Prove that $\alpha$ is a multiple root of $f(X)$ iff $\alpha$ is also a root of $Df$.

11. Show that $f(X)$ is separable if and only if $f(X)$ and $Df(X)$ are relatively prime.

12. Conclude that if $f(X)$ is irreducible and unseparable, then $Df(X) = 0$.

13. Show that the only polynomials with zero derivative over a field with characteristic zero are the constants. Therefore every field with characteristic zero is perfect.

Thus we see that inseparable irreducible polynomials only live in fields of prime characteristic. That is why they were hard to find at the beginning! Let us study the prime characteristic case further.

14. Let $p$ be a prime and let $F$ be a field with characteristic $p$. Let $f(X) \in F[X]$. Prove that $Df(X) = 0$ iff $f(X) = g(X^p)$ for some $g(X) \in F[X]$.

15. Let $p$ be a prime and let $F$ be a field with characteristic $p$. Show that $F$ is perfect iff $F^p = F$.

16. Show that every finite field is perfect.