Debra Griffin
Field Extensions, Part II, Handout
Worksheet #1 - 3

---

**1.** *Let $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in F[x]$ where $F$ is a field. The derivative of the polynomial is $f'(x) = na_nx^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1$.*

**(a)** *Prove that for all $f(x), g(x) \in F[x]$, we have $(f(x) + g(x))' = f'(x) + g'(x)$.*

**Proof:**

Let $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{i=0}^{m} b_i x^i$ for some $a_i, b_i \in F$, $m, n \in \mathbb{Z}^+$.

Without loss of generality, assume $n \geq m$. Note that $b_i = 0 \ \forall \ i > m$.

Then $(f(x) + g(x))' = (\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{m} b_i x^i)' = (\sum_{i=0}^{n} (a_i + b_i)x^i)' = \sum_{i=1}^{n} i(a_i + b_i)x^{i-1} =$

$\sum_{i=1}^{n} ia_i x^{i-1} + \sum_{i=1}^{m} ib_i x^{i-1} = f'(x) + g'(x)$.

---

**(b)** *Prove that for all $f(x), g(x) \in F[x]$, we have $(f(x)g(x))' = f(x)g'(x) + f'(x)g(x)$.*

**Proof**:

Define $f(x)$, $g(x)$ as in part (a).

We first note that $\forall \ a \in F$, $\forall \ n \in \mathbb{Z}^+$,

$(ax^n g(x))' = (\sum_{i=0}^{m} ab_i x^{n+i})' = \sum_{i=1}^{m} (n+i)ab_i x^{n+i-1} = a\sum_{i=1}^{m} (ib_i x^{n+i-1} + nb_i x^{n+i-1}) =$

$ax^n \sum_{i=1}^{m} ib_i x^{i-1} + ax^{n-1} \sum_{i=1}^{m} nb_i x^i = ax^n \sum_{i=1}^{m} ib_i x^{i-1} + nax^{n-1} \sum_{i=0}^{m} b_i x^i = ax^n g'(x) + nax^{n-1} g(x)$.

So then we can apply part (a) to get

$(f(x)g(x))' = (a_0 g(x) + a_1 x g(x) + a_2 x^2 g(x) + \cdots + a_n x^n g(x))'$

$= [a_0 g(x)]' + [a_1 x g(x)]' + [a_2 x^2 g(x)]' + \cdots + [a_n x^n g(x)'$

$= [a_0 g'(x)] + [a_1 x g'(x) + a_1 g(x)] + [a_2 x^2 g'(x) + 2a_2 x g(x)] + \cdots + [a_n x^n g'(x) + na_n x^{n-1} g(x)]$

$= a_0 g'(x) + a_1 x g'(x) + a_2 x^2 g'(x) + \cdots + a_n x^n g'(x) + [a_1 g(x) + 2a_2 x g(x) + \cdots + na_n x^{n-1} g(x)]$

$= f(x)g'(x) + f'(x)g(x)$.

---

**(c)** *Prove that for all $f(x), g(x) \in F[x]$, we have $[(f(x))^n]' = n(f(x))^{n-1} f'(x)$.*

**Proof**:

We will show the result by induction.

Let $n = 1$. Then $(f(x))' = 1 \bullet (f(x))^{1-1} f'(x)$.

Let $n > 1$ and assume the result is true for power of $f(x)$ less than $n$.

Then, by part (b), $[(f(x))^n]' = [(f(x))^{n-1} f(x)]' = (f(x))^{n-1} f'(x) + [(f(x))^{n-1}]' f(x)$.

And our induction hypothesis gives us that

$= (f(x))^{n-1} f'(x) + (n-1)(f(x))^{n-2} f'(x) \bullet f(x)$

$= (f(x))^{n-1} f'(x) + (n-1)(f(x))^{n-1} f'(x)$

$= n(f(x))^{n-1} f'(x)$.

---

**1. (d)** *Let K be a splitting field for f (x). Prove that f (x) has no repeated roots in K if and only if f (x) and f '(x) are relatively prime.*

**Proof**:

We will show the forward implication by contradiction.

Assume $f(x)$ has no repeated roots and suppose gcd $(f, f') \neq 1$.

Then $\exists\, g(x) \in K[x]$ such that $g(x)$ is monic, $g(x) \mid f(x)$ and $g(x) \mid f'(x)$.

Since $K$ is a splitting field of $f(x)$, we have the unique factorization of

$f(x) = (x - a_1)\cdots(x - a_n)$, and without loss of generality,

$g(x) = (x - a_1)\cdots(x - a_t)$ for some $t < n$. So $x - a_i \mid f(x)$ and $x - a_i \mid f'(x)$ for some $i$.

Thus $f(x) = g(x)(x - a_i)$ and $f'(x) = h(x)(x - a_i)$ for some $g(x), h(x) \in R[x]$.

And $f'(x) = g'(x)(x - a_i) - g(x)$. Since $(x - a_i) | f'(x)$, then $(x - a_i) | g(x)$.

$\therefore\ (x - a)^2 \mid f(x)$. Hence $f$ has a repeated root, a contradiction to our assumption.

$\therefore$ gcd $(f, f') = 1$.

To prove the converse, we will again show a contradiction.

Assume gcd $(f, f') = 1$ and suppose $f(x)$ has a repeated root, $x - a$.

Then $f(x) = g(x)(x - a)^2$, for some $g(x) \in R[x]$.

By part (b), $f'(x) = g'(x)(x - a)^2 + g(x)((x - a)^2)' = g'(x)(x - a)^2 + 2g(x)(x - a)$.

$\therefore\ x - a \mid f'(x)$, a contradiction to gcd $(f, f') = 1$.

$\therefore\ f(x)$ has no repeated roots.

---

**2.** *Let R be a UFD and let f (x) ∈ R[x] such that deg f (x) = n. Prove that f (x) has at most n roots.*

**Proof**:

Since $R$ is a UFD then $R[x]$ is a UFD (Theorem 6.25).

Thus any factorization of $f(x)$ is unique up to units.

And $n = \deg f \in R[x] = \deg f \in \mathrm{Frac}(R)[x]$.

So there is a splitting field $E$, of $\mathrm{Frac}(R)$, also a UFD, such that

$f(x) = (x - a_1)(x - a_2)\cdots(x - a_n) \in E[x]$.

And since any factorization of f is unique, then $f$ has at most $n$ roots in $E$.

---

**3.** *Let F be a field. We have proven that F* is an Abelian group with respect to multiplication. Prove that F* is cyclic.*

**Proof**:

If $F^*$ is infinite then the theorem is false.

Assume $F^*$ is a finite subgroup of $F$.

Let $c \in F^*$ be an element of largest order (there must be one since $F^*$ is finite), say $\circ(c) = m$.

Claim: $\forall\, a \in F, \circ(a) \mid m$.

Suppose $\exists\, a \in F$ of order $n$ such that $n \nmid m$.

Then $\exists\, p$, a prime, such that $m = p^u b$ and $n = p^v d$

for some $b, d \in \mathbb{Z}$, $u, v \in \mathbb{N} \cup \{0\}$, $u < v$, and $(p, b) = 1 = (p, d)$.

(Note that u could be 0, hence $p^u$ could be 1). So

(1) $\circ(a) = n = p^v d$ and $(p^v, d) = 1 \Rightarrow \circ(a^d) = p^v$.

(2) $\circ(c) = m = p^u b$ and $(p^u, b) = 1 \Rightarrow \circ(c^{p^u}) = b$.

(1) is true as $(a^d)^{p^v} = a^{p^v d} = a^m = 1$ and if $\exists\, h < p^v$ such that $\circ(a^d) = h$, then $a^{hd} = 1$, contradicting that $\circ(a) = m = p^v sd > dh$, where $m$ is the smallest positive integer such that $a^m = 1$. Similarly (2) is true.

So then, since $(p^v, b) = 1$, we have $\circ(a^d \bullet c^{p^u}) = p^v \bullet b > p^u \bullet b = m$, contradicting that $c$ is the element of $F^*$ of largest order.

$\therefore\ \forall\, a \in F^*, \circ(a) \mid m$.

So then $\forall\, a \in F^*$, $a^m = 1_{F^*}$. Thus every element of $F^*$ is a root of $x^m - 1_{F^*}$.

Since this polynomial has at most $m$ roots, then $|F^*| \leq m$.

But $\langle c \rangle$ is a subgroup of $F^*$ of order $m$.

$\therefore\ \langle c \rangle$ must be all of $F^*$.

---