10. Lemmas about Polynomials

My methods are really methods of working and thinking; this is why they have crept in everywhere.
Emmy Noether

Many of today's problems will start "let k be a field". As a reminder, good examples of fields are $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Z}_p$ for p a prime. The axioms of a field are included on the next page.

For k a field, we write $k[x]$ for the ring of polynomials with coefficients in x. As a reminder, two polynomials are equal if they have exactly the same coefficients. For example, x and x^2 are **different** polynomials of $\mathbb{Z}_2[x]$, even though we have $a = a^2$ for every a in $\mathbb{Z}_2$.

The ***degree*** of a polynomial is the largest n for which the coefficient of x^n is nonzero. We leave the degree of the 0 polynomial undefined.[1]

Problem 10.1. Let k be a field and let $f(x)$ and $g(x)$ be nonzero polynomials in $k[x]$. Show that $\deg(fg) = \deg(f) + \deg(g)$.

Problem 10.2. Let k be a field, let $f(x)$ be a polynomial in $k[x]$, and let r be an element of k.

(1) Show that there is a polynomial $g(x)$ in $k[x]$ such that
$$f(x) = (x - r)g(x) + f(r).$$
(2) Suppose that $f(r) = 0$. Show that $f(x)$ is divisible by $x - r$.

Now, let r_1, r_2, ..., r_m be distinct elements of k.

(3) Suppose that $f(r_1) = f(r_2) = \cdots = f(r_m)$. Show that $f(x)$ is divisible by $\prod_{i=1}^{m}(x - r_i)$.
(4) Assume that $f(x)$ is not the 0 polynomial. Show that the number of roots of $f(x)$ in k is $\leq \deg(f)$.

Problem 10.3. Let k be a field and let $a(x)$ and $b(x)$ be polynomials in $k[x]$, with $b(x) \neq 0$. Show that there are polynomials $q(x)$ and $r(x)$ with $a(x) = b(x)q(x)+r(x)$ and either $\deg r(x) < \deg b(x)$ or $r(x) = 0$.

We write $k[x]_{f(x)}$ for the ring of polynomials modulo $f(x)$.[2]

Problem 10.4. Let k be a field and let $f(x)$ be a nonzero polynomial in $k[x]$ with degree d. Show that each element of $k[x]_{f(x)}$ can be written uniquely in the form $\sum_{j=0}^{d-1} a_j x^j$, with a_0, a_1, ..., a_{d-1} in k.

Problem 10.5. Let k be a field and let $a(x)$ and $b(x)$ be polynomials in $k[x]$.

(1) Let $\langle a(x),\ b(x)\rangle$ be the set of all polynomials which can be written in the form $a(x)u(x)+b(x)v(x)$. Show that there is a polynomial in $\langle a(x),\ b(x)\rangle$ which divides $a(x)$ and $b(x)$. We'll call this polynomial the ***GCD of*** $a(x)$ ***and*** $b(x)$ and write it $\mathrm{GCD}(a(x),\ b(x))$.
(2) Show that the GCD of $a(x)$ and $b(x)$ divides every polynomial in $\langle a(x),\ b(x)\rangle$.
(3) Show that, if $c(x)$ divides $a(x)$ and divides $b(x)$, then $c(x)$ divides the GCD of $a(x)$ and $b(x)$.

Problem 10.6. Let k be a field and let $a(x)$ and $b(x)$ be polynomials in $k[x]$. We say that $a(x)$ and $b(x)$ are ***relatively prime*** if there is no polynomial $d(x)$ with $\deg d > 0$ dividing both $a(x)$ and $b(x)$. Show that, if $a(x)$ and $b(x)$ are relatively prime, then there are polynomials $u(x)$ and $v(x)$ such that $a(x)u(x) + b(x)v(x) = 1$.

We say that a polynomial $p(x)$ is ***irreducible*** if $\deg p(x) > 0$ (so $p \neq 0$) and it is impossible to factor $p(x)$ as $q(x)r(x)$ with $\deg q$ and $\deg r$ both > 0.

Problem 10.7. Let k be a field and let $p(x)$ in $k[x]$ be irreducible. Show that $k[x]_{p(x)}$ is a field.

---

[1] In David's opinion, there are good reasons to define the degree of the 0-polynomial to be ∞, 0 or $-\infty$. Some people define it to be -1, but David does not think there is any good reason to do this.

[2] I'm trying to copy PROMYS notation here. We'll see if I am willing to keep it up all summer: The standard notation would be $k[x]/f(x)$ or $k[x]/f(x)k[x]$. Similarly, most mathematicians would write $\mathbb{Z}/17$ or $\mathbb{Z}/17\mathbb{Z}$, not $\mathbb{Z}_{17}$, for the integers modulo 17.

The axioms of a field

Let F be some set with binary operations $+$ and $\cdot$.Then F is called a ***field*** if it obeys the following axioms.

Identity Axioms: There are elements 0 and 1 of F such that

$$x + 0 = x \qquad x \cdot 1 = x$$

for all $x \in F$.

Inverse Axioms: For all $x \in F$, there is an element $-x$ such that

$$x + (-x) = 0.$$

If x is a nonzero element of F, there is an element x^{-1} such that

$$x \cdot x^{-1} = 1.$$

Commutativity Axioms: For all x and y in F, we have

$$x + y = y + x \qquad x \cdot y = y \cdot x.$$

Associativity Axioms: For all x, y and z in F, we have

$$x + (y + z) = (x + y) + z \qquad x \cdot (y \cdot z) = (x \cdot y) \cdot z.$$

Distributivity Axiom: For all x, y and z in F, we have

$$x \cdot (y + z) = x \cdot y + x \cdot z \qquad (x + y) \cdot z = x \cdot z + y \cdot z.$$

Nontriviality Axiom: We have

$$0 \neq 1.$$