Summary of results: Polynomials over commutative rings

Alan Haynes, haynes@math.uh.edu

Last update: January 26, 2022

We assume familiarity with the definitions of the terms commutative ring, ideal, prime ideal, irreducible element, greatest common divisor, Euclidean Domain (ED), Principal Ideal Domain (PID), Unique Factorization Domain (UFD), Integral Domain (ID), field, and field of fractions. Recall that for commutative rings we have the following heirarchy:

$$\text{(ED)} \Rightarrow \text{(PID)} \Rightarrow \text{(UFD)} \Rightarrow \text{(ID)}.$$

Theorem (Division Algorithm)**.** *Suppose that F is a field, that $f, g \in F[x]$ and that $g \neq 0$. Then there are unique polynomials $q, r \in F[x]$ satisfying*

$$f = qg + r \quad \textit{and} \quad r = 0 \textit{ or } \deg(r) < \deg(g).$$

Corollary. *If F is a field then $F[x]$ is a UFD. In particular, for any $f \in F[x] \setminus \{0\}$, there exist $\lambda \in F$ and monic irreducible polynomials $f_1, \ldots, f_n \in F[x]$ such that*

$$f = \lambda f_1 \cdots f_n,$$

and this factorization into monic irreducible polynomials is unique up replacement of the factors by associates, and reordering.

Theorem (Gauss's Lemma)**.** *Suppose that R is a UFD and F is its field of fractions. If f is irreducible in $R[x]$ then it is irreducible in $F[x]$.*

Theorem. *A ring R is a UFD if and only if $R[x]$ is a UFD.*

Useful results for factoring polynomials:

(1) **Bezout's Theorem**: If F is a field and if $f \in F[x]$, then an element $\alpha \in F$ is a root of f if and only if $(x - \alpha)|f$.

Corollary: If F is a field then any non-zero polynomial $f \in F[x]$ has at most $\deg(f)$ roots.

(2) **Abel's Theorem**: Suppose that F is a field, that $f, g \in F[x]$, and that f is irreducible. Then either $f|g$ or $\gcd(f, g) = 1$.

Corollary: If F is a field and if $f, g \in F[x]$ are both monic and irreducible then either $f = g$ or $\gcd(f, g) = 1$.

(3) **Lemma**: If f is a polynomial with coefficients in a field F, and if $\deg(f) = 2$ or 3, then f is irreducible over F if and only if f has no roots in F.

Lemma: Suppose that $f \in \mathbb{Z}[x]$ is given by

$$f(x) = \sum_{i=0}^{n} a_i x^i, \quad \text{with } a_i \in \mathbb{Z},\ a_n \neq 0.$$

If $f(p/q) = 0$ for some $p/q \in \mathbb{Q}$ with $\gcd(p, q) = 1$, then $p|a_0$ and $q|a_n$.

Lemma: Let F be a field and suppose that $f, g \in F[x]$ satisfy $\deg(f) \geq 1$ and $f(x) = g(x + \lambda)$ for some $\lambda \in F$. Then f is irreducible over F if and only if g is irreducible over F.

(4) **Reduction Test**: Suppose that R is an ID and that $I \subseteq R$ is a proper ideal, and let $f \in R[x]$ be a non-constant monic polynomial. If the image of f in $(R/I)[x]$ is irreducible, then f is irreducible over R.

Eisenstein's Criterion: Suppose that R is an ID and that P is a prime ideal in R, and suppose that $f \in R[x]$ is given by

$$f(x) = \sum_{i=0}^{n} a_i x^i,$$

with $a_i \in P$ for $0 \leq i < n$, with the gcd of the coefficients of f equal to 1, and with $a_n \notin P$ and $a_0 \notin P^2$. Then f is irreducible over R.

Eisenstein's Criterion Over $\mathbb{Z}$: Suppose that $f \in \mathbb{Z}[x]$ is given by

$$f(x) = \sum_{i=0}^{n} a_i x^i,$$

with $\gcd(a_0, \ldots, a_n) = 1$, and suppose that p is a prime such that $p|a_i$ for $0 \leq i < n$, and such that $p \nmid a_n$ and $p^2 \nmid a_0$. Then f is irreducible over $\mathbb{Z}$ (and therefore over $\mathbb{Q}$ by Gauss's Lemma).